CA ControlMinder

Implementation Guide

12.8

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 ControlMinder product are provided "as is", for informational purposes only. Adjust them to your specific environment and do not use them in production without running tests and validations.

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 ControlMinder
- CA ControlMinder
- CA Single Sign-On (eTrust 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 SDM (formerly Unicenter Service Desk)
- CA User Activity Reporting Module (formerly CA Enterprise Log Manager)
- CA IdentityMinder

Documentation Conventions

The CA ControlMinder 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
Underline	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 ControlMinder documentation uses the following file location conventions:

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

- *ACSharedDir*—A default directory used by CA ControlMinder for UNIX.
  - UNIX—/opt/CA/AccessControlShared
- *ACServerInstallDir*—The default CA ControlMinder 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:

- Email Notifications for Events
- Configure the Connection to CA Business Intelligence
- Installing and Customizing a UNIX Endpoint - Updated the chapter to include the following updates:
  - UNIX Installation Parameters File-Customize UNIX Installation
  - Customize the CA ControlMinder RPM Package
  - How to Install CA ControlMinder on Debian or Ubuntu Linux
  - customize_eac_pkg Command—Customize Solaris Native Package
  - Customize the bff Native Package Files
  - Install AIX Native Packages
  - customize_eac_bff Command—Customize a bff Native Package File
  - How to Install CA ControlMinder on Solaris Zones
- Customize the CA ControlMinder RPM Package
- Implementing CA ControlMinder High Availability on Linux Using Veritas Cluster Server
- Adding the Users Directory Certificate to the Keystore
- Enterprise Management Server SSL Communication
- Change the ac_entm_pers Password

Contents

Appendix B: Changing Communication Encryption Methods 453

Appendix C: Changing CA ControlMinder Service Account Settings 483

Chapter 1: About this Guide

This guide provides information about how to plan, install, and customize the various components of CA ControlMinder. These include CA ControlMinder servers and endpoints for Windows and UNIX, and the CA ControlMinder Endpoint Management component. Enterprise management and reporting installation chapters only apply to CA ControlMinder.

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

Chapter 2: Planning Your Enterprise Implementation

This section contains the following topics:

Planning for a Security System

The primary goal of any security system is to protect organization information assets. To implement security effectively, you must be aware of threats that exist and then determine the best ways to protect your site from these threats.

You have two basic ways to protect against unauthorized use of computer resources:

- Prevent unauthorized users from accessing the system
- Control what authorized users have access to

CA ControlMinder provides tools to protect your system in both ways. CA ControlMinder also provides auditing tools that let you monitor user activity to track attempts to misuse the computer system.

Once you have determined your security goals, you can write a security policy statement and put together an implementation team. The implementation team sets priorities that help determine what data, applications, and users must be secured.

Preparing an Implementation Plan

To ensure that your security goals come from the security policy, repeatedly check the implementation plan. Gradually phase in the new security controls to provide an adjustment period for users.

- Define specific goals based on the security plan.

  Define the goals to help you implement the security plan.

- Define a pilot group of users as a prototype to implement CA ControlMinder.

  Test all CA ControlMinder features on the pilot group before protecting entities outside of the group. Testing with the pilot group can help you learn how to protect the rest of the organization.

- Decide what to protect

  CA ControlMinder protects business data, jobs, and users in the pilot group.

- Define a method to roll out the security control

Consider how to phase in the new security controls with minimum disruption to current work patterns. Consider a period of only auditing and not restricting access for various resources and classes. The resulting audit records show which users tend to require resource access.

Note: For more information about Warning mode (audit-only mode), see the *Endpoint Administration Guide for UNIX* and the *Endpoint Administration Guide for Windows*.

Getting Management Commitment

A management decision to install CA ControlMinder is not enough to guarantee adequate security at your site. A successful security project requires active management involvement. Management must decide on security policy procedures, allocated security function resources, and user accountability. Without such management support, security procedures fall into misuse and become more of an administrative chore than a viable protection scheme. This situation can result in a false sense of security and can lead to serious security exposures.

The security administrator works with management to prepare a clear, inclusive security policy statement. This statement includes the following items:

- A policy for full-time employees, part-time employees, contract employees, and consultants.
- A policy for external users
- A policy outlining expected user behavior
- Physical protection considerations

- User departmental security requirements
- Auditing requirements

The resulting security policy helps to ensure a CA ControlMinder implementation plan that is both realistic and consistent with the installation security policy.

Deciding How to Protect

Before you install CA ControlMinder, decide what features of the software you want to use.

CA ControlMinder provides the following protection methods:

- Native security using CA ControlMinder Endpoint Management lets you implement the security features that are already familiar to you.
- Advanced native security lets you guard against more sophisticated attacks. CA ControlMinder lets you:
  - Limit the rights of privileged accounts
  - Assign special privileges to ordinary users, such as the ability to change user passwords for special users
  - Support multiple file systems including NTFS, FAT, and CDFS
  - Centralize security policies and auditing across heterogeneous environment containing Windows and UNIX systems
- Advanced policy management lets you deploy multiple-rule policies (script files) you create for your enterprise. This policy-based method lets you create version-controlled policies and assign and unassign policies to host groups in your enterprise. You can also directly deploy and remove deployed policies (undeploy) and view deployment status and deployment deviation.
- A Policy Model database (PMDB) lets you propagate a security database with users, groups, and access rules to a set of subscribers. The PMDB regularly propagates all the updates that it receives to subscribers. This mechanism eases the administrative burden on system administrators.
- Privileged User Password Management (PUPM) provides role-based access management for privileged accounts on target endpoints from a central location. PUPM also provides secure storage of privileged accounts and application ID passwords, and controls access to privileged accounts and passwords based on policies.
- UNIX Authentication Broker (UNAB) lets you validate local UNIX user and group credentials against Active Directory. Users use a single repository to log in to all platforms with the same user name and password.

Educating and Training Staff

Part of the role of the security administrator is to tell the system users what they need to know to work without disruption when CA ControlMinder is installed.

The amount of detailed information each user needs to know about CA ControlMinder depends on the functions you authorize the person to use. Examples of information required by various types of system users include the following:

- SAM users

  How to check out and check in privileged account passwords and understand when to request access to privileged accounts and when to break glass.

- All users defined in the CA ControlMinder endpoint databases
  - How to identify themselves to the system by a user name and a password and how to change a password. They should also be aware of the significance of their password to system security.
  - Be familiar with the Password Manager, If you implement password policy validation.
  - How to use the *secons -d-* and *secons -d+* commands that disable and enable concurrent logins. *Concurrent logins* are multiple sessions initiated by the same user onto a system from more than one terminal at the same time.
  - Be familiar with the sesudo command, which enables user substitution based on predefined access rules with or without password checking.

- Technical support personnel

  Be familiar with migration considerations and with the steps required to install or reinstall CA ControlMinder. Users who maintain the database must be familiar with the database utilities.

- Auditors

  Users with the AUDITOR attribute should be familiar with the auditing tools (CA ControlMinder Endpoint Management and the seaudit utility).

  Note: For more information about the seaudit utility, see the *Reference Guide*.

- Programmers writing unauthorized applications

  Programmers can use the CA ControlMinder* function library in their applications to request security-related services, including controlling access to protected resources (by using the SEOSROUTE_RequestAuth function). Your installation can create installation-defined resource classes. If your installation creates records in those classes, an application can issue a SEOSROUTE_RequestAuth command to check whether a user has sufficient authority to complete an action. The level of authority required for a particular user action is determined by the way the application invokes the SEOSROUTE_RequestAuth function.

  Note: For more information about the CA ControlMinder API, see the *SDK Guide*.

- Programmers writing authorized applications

  Programmers writing authorized applications (programs that run with the SERVER attribute) can use the CA ControlMinder* function library to request security-related services, including:

  - User identification and verification
  - User logout service
  - User authorization request

How to Implement CA ControlMinder Enterprise Management

Before you implement CA ControlMinder Enterprise Management in your enterprise, you should understand which components to install, in what order, and where to install them. Observe the following guidelines when you implement an enterprise deployment of CA ControlMinder Enterprise Management:

- Use a 'top-to-bottom' approach in the implementation process. Begin by installing the Enterprise Management Server, install additional Distribution Servers, implement Enterprise Reporting and then install the CA ControlMinder endpoints.
- Before you begin the implementation, verify that the computers that you use meet the required specifications and that all prerequisite software is installed.

  Note: For more information about the required hardware and software specifications, see the CA ControlMinder Compatibility Matrix that is available from the CA ControlMinder product page on CA Support.

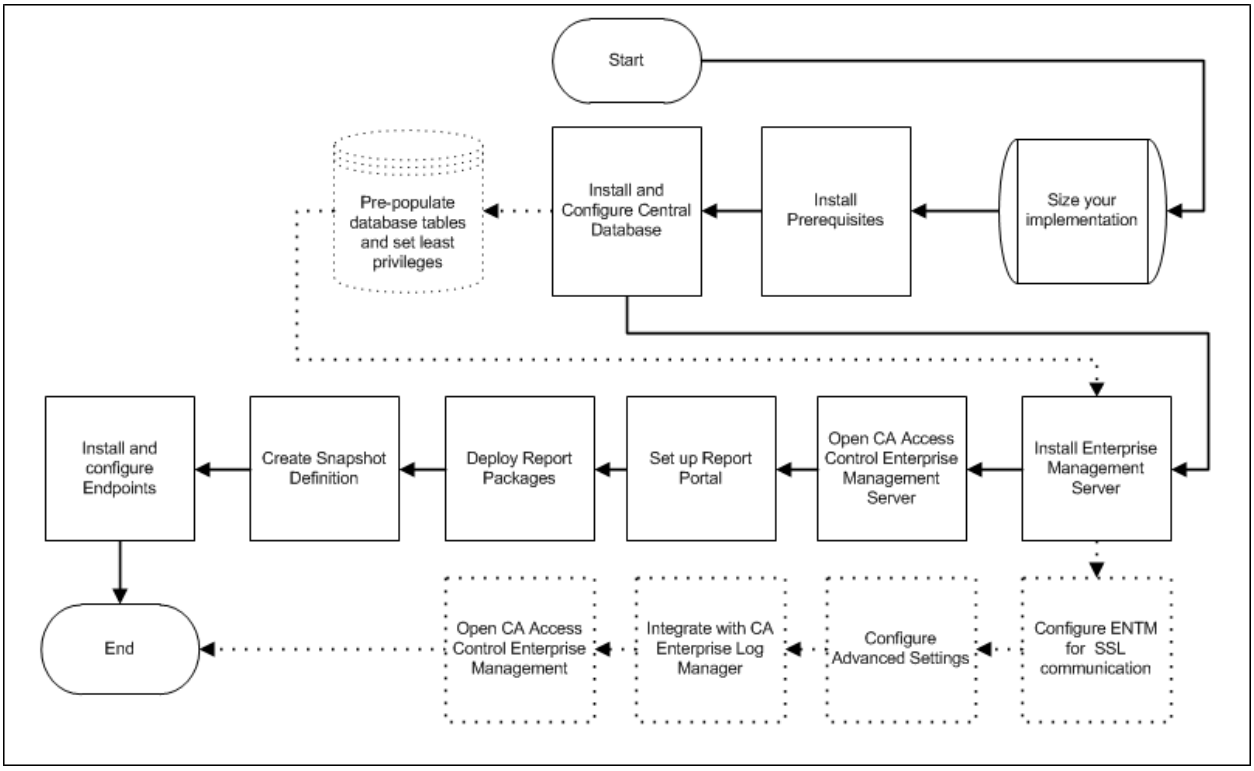
Use the following process to implement CA ControlMinder Enterprise Management:

1. Decide which deployment architecture to use
2. Install a supported RDBMS as the central database
3. (Optional) Install a supported user store
4. Install the Enterprise Management Server
5. Implement Enterprise Reporting
6. (Optional) Integrate with CA User Activity Reporting Module
7. Install the endpoints

The following diagram illustrates the implementation process for CA ControlMinder Enterprise Management:

Implementing the Enterprise Management Server

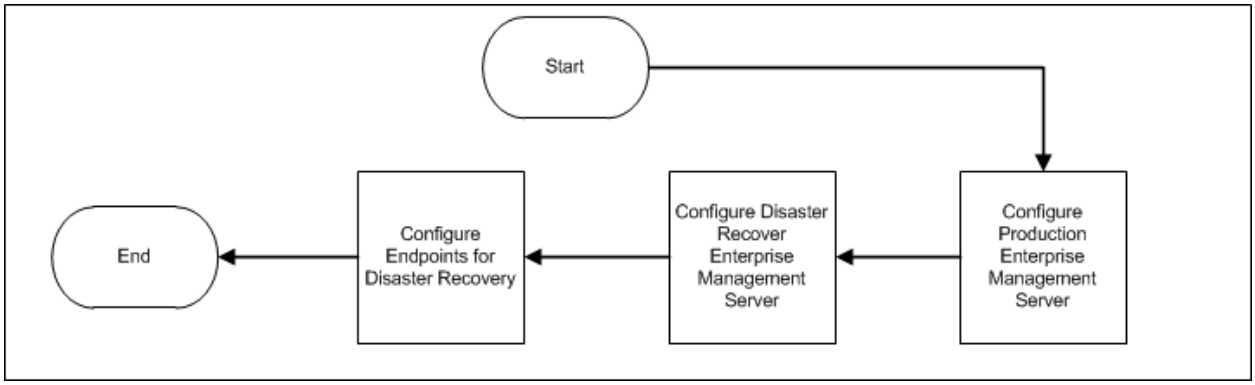
Use this diagram to help you implement the Enterprise Management Server:



Note: The dashed lines represent optional steps.

Implementing CA ControlMinder for Disaster Recovery

Use the following diagram to help you implement CA ControlMinder for disaster recovery:



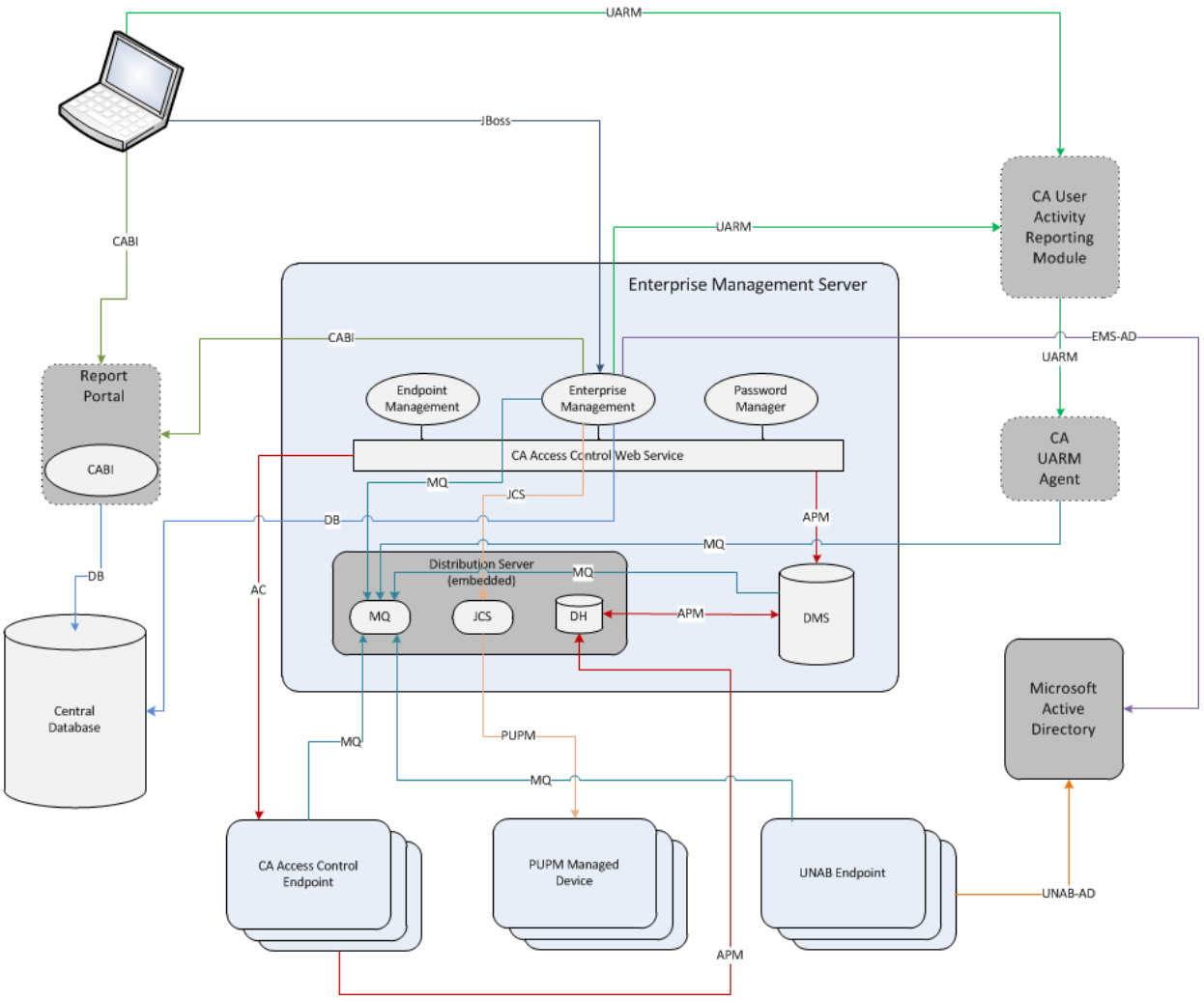
CA ControlMinder Enterprise Management Deployment Architectures

Before you begin to implement CA ControlMinder Enterprise Management, you should decide with of the following implementation architectures to use:

- Default—In a default deployment, you install all the components of CA ControlMinder Enterprise Management on a single server. Implementing the default architecture is the fastest way to implement CA ControlMinder Enterprise Management. The default implementation architecture does not support high availability and disaster recovery capabilities.
- Load Balancing—the load balancing deployment architecture enables you to use a common user and data stores to distribute workload among the Enterprise Management Servers. In a load balancing deployment you deploy a primary and multiple load balancing Enterprise Management Servers.
- High Availability—the high availability deployment architecture enables you to implement CA ControlMinder Enterprise Management for failover and redundancy. In a high availability implementation you deploy CA ControlMinder Enterprise Management on multiple servers to help ensure continued access to data from endpoints in case of a server failure.
- Disaster Recovery—the disaster recovery deployment architecture enables you to implement CA ControlMinder Enterprise Management for disaster recovery. In a disaster recovery deployment you deploy CA ControlMinder Enterprise Management on multiple servers to help ensure disaster recovery capabilities.

Default Enterprise Deployment Architecture

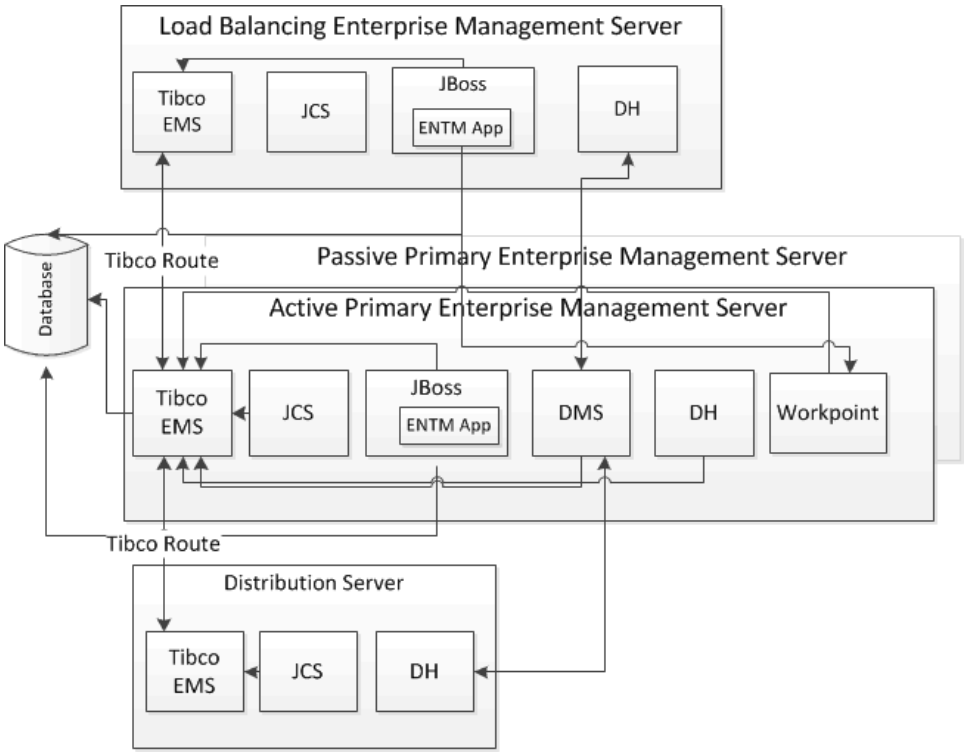
The following diagram shows how you can deploy CA ControlMinder in your enterprise:



Note: Dashed lines indicate optional components.

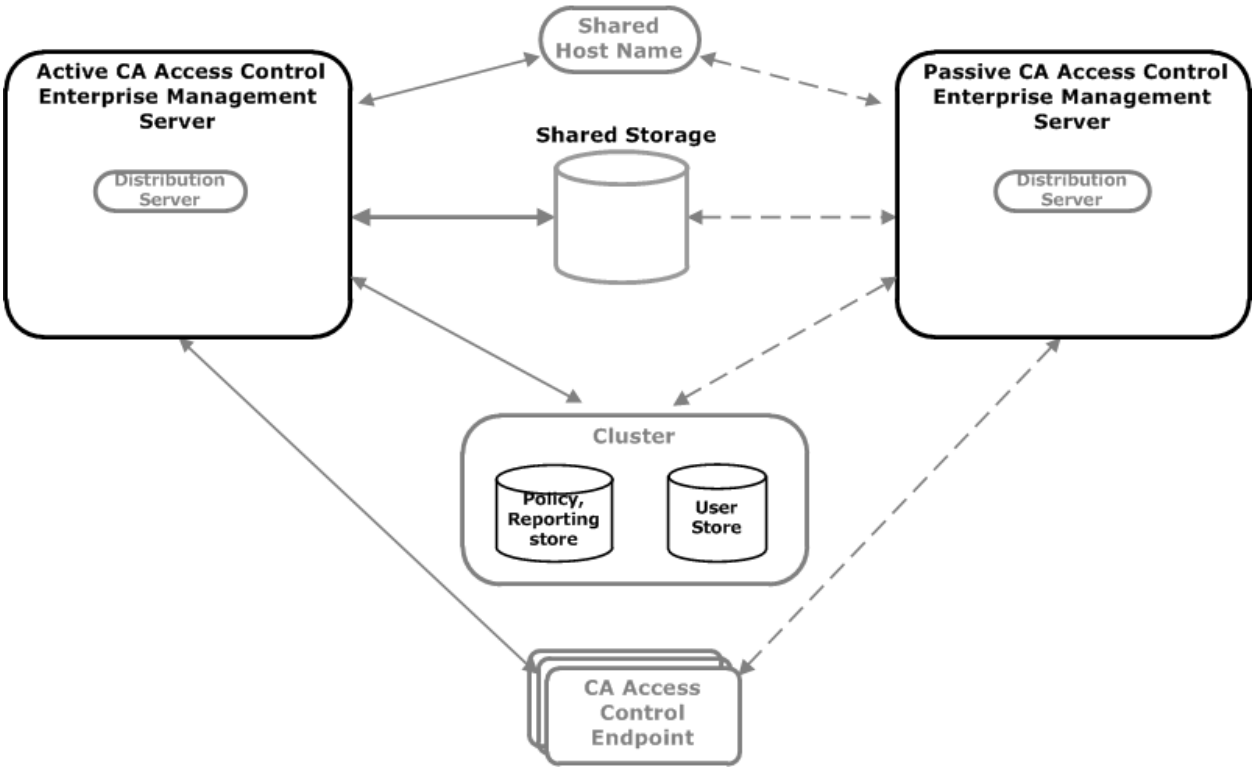
Load Balancing Deployment Architecture

The following diagram shows how you can deploy the load balancing Enterprise Management Servers in your enterprise:



High Availability Deployment Architecture

The following diagram shows CA ControlMinder Enterprise Management in a high availability environment:

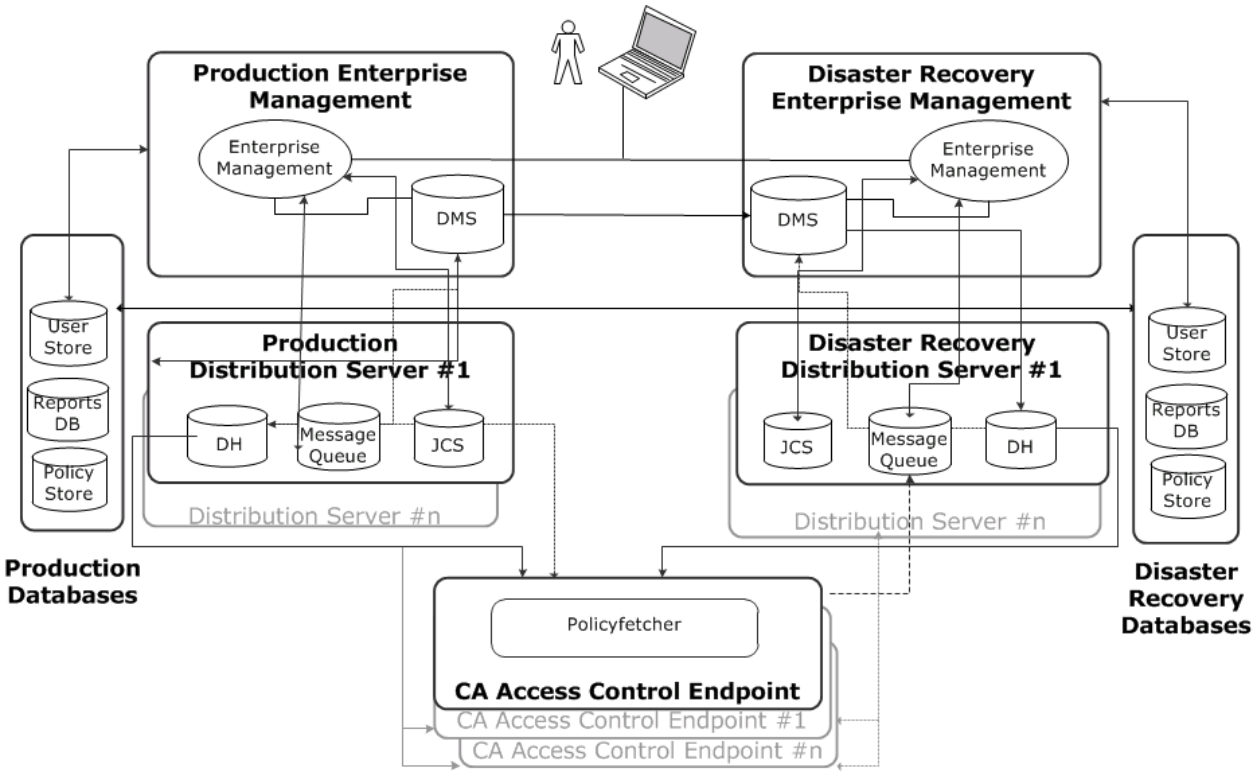


As illustrated in the preceding diagram, a high availability deployment has the following components:

- A primary Enterprise Management Server and at least one secondary Enterprise Management Server
- A clustered installation of a policy and reporting store and a user store
- Shared storage that is accessible by both the primary and secondary CA ControlMinder Enterprise Management servers
- A shared host name
- CA ControlMinder endpoints able to work with both the primary and secondary Enterprise Management Servers

Disaster Recovery Architecture

The following diagram shows how you deploy CA ControlMinder in a disaster recovery configuration.



Components of CA ControlMinder Enterprise Management

CA ControlMinder Enterprise Management consists of or makes use of the following components:

Enterprise Management Server

The Enterprise Management Server is the central management server and contains components and tools that let you deploy policies to endpoints, manage privileged accounts, and define resources, accessors, and access levels. The Enterprise Management Server also contains components that manage communication between the Enterprise Management Server, the endpoints, and other components.

CA ControlMinder is silently installed when you install the Enterprise Management Server. CA ControlMinder protects the Enterprise Management Server and provides core functionality that supports the applications in the Enterprise Management Server.

Distribution Server

The Distribution Server handles communication between the Application Server and the endpoints. The Distribution Server contains the following components:

- Distribution Host (DH)
- Message Queue (MQ)
- Java Connector Server (JCS)

Note: For failover purposes, you can install more than one Distribution Server in your enterprise, or install the Distribution Server components on separate computers. The Distribution Server is installed by default on the Enterprise Management Server.

Distribution Host (DH)

The DH is responsible for distributing policy deployments, made on the DMS, to endpoints, and for receiving deployment status from endpoints to send to the DMS. To accomplish this task, the DH uses two Policy Model databases:

- **DH Writer**—responsible for writing data it receives from endpoints to the DMS.

  The name of this PMDB is *DHName*WRITER where *DHName* is the name of the DH, **DH__** by default.

- **DH Reader**—responsible for reading data from the DMS so that endpoints can retrieve it.

  The name of this PMDB is *DHName* where *DHName* is the name of the DH, **DH__** by default.

By default, the DH is installed on the same computer as the Distribution Server. However, you can also install multiple DH nodes so that each manages a section of your enterprise for load balancing.

Message Queue

The Message Queue manages inbound and outbound messages between the Enterprise Management Server and other components. The Message Queue has a dedicated queue for each client component that communicates with the Enterprise Management Server, as follows:

- Report queue—Receives scheduled snapshots of the endpoint databases.

  The reporting service uses the snapshots to generate CA ControlMinder reports.

- Audit queue—Receives audit events that occur on the endpoints.

  You can configure CA User Activity Reporting Module to collect and report on the audit events.

- Server to endpoint queue—Receives data from the DMS that is collected by endpoints.

  For example, when you deploy a UNAB config policy the DMS sends the config policy to this queue. The UNAB agent then collects the policy from the queue and deploys the policy on the UNAB endpoint.

- Endpoint to server queue—Receives information from endpoints that is collected by the DMS.

  For example, a UNAB endpoint sends a heartbeat notification to this queue. The DMS then collects the heartbeat notification from the queue and updates the endpoint status in its database.

Java Connector Server (JCS)

The Java Connector Server (JCS) communicates with Java supported managed devices, such as Windows operating systems and SQL servers, and manages privileged accounts on SAM endpoints.

Web-based Applications

You use web-based applications to manage an enterprise installation of CA ControlMinder. The web-based applications are installed on the Application Server. The Application Server is installed by default on the Enterprise Management Server.

The Application Server contains the following web-based applications:

- CA ControlMinder Enterprise Management—Lets you manage policies across your enterprise and configure endpoints.CA ControlMinder Enterprise Management also contains Privileged User Password Management (SAM), which lets you manage privileged accounts across the enterprise and acts as a password vault for the privileged accounts.
- CA ControlMinder Endpoint Management—Lets you administer and configure individual CA ControlMinder endpoints through a central administration server.
- CA ControlMinder Password Manager—Lets you manage CA ControlMinder user passwords. You can modify the password of a CA ControlMinder user or force the user to change their own password when they next log in.

CA ControlMinder Enterprise Management

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

To help you navigate CA ControlMinder Enterprise Management, subject specific tasks are grouped under tabs. Using these tasks you can:

- View your implementation of CA ControlMinder throughout the enterprise
- Configure hosts and host groups and assign policies to CA ControlMinder and UNAB endpoints
- Check out and check in privileged account passwords
- Configure privileged accounts, endpoints, password policies and password consumers
- Display reports, manage snapshot definitions and capture snapshot data
- Manage users, groups, roles and tasks
- Manage system wide connection settings
- View audit records

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

Deployment Map Server (DMS)

The DMS sits at the core of advanced policy management. The purpose of the DMS is to keep up-to-date information on policies (policy versions, scripts) and policy deployment status on each computer. The DMS stores versions of your policies that you can later assign, unassign, deploy, and undeploy as required.

A DMS is a Policy Model node and it uses a PMDB as its data repository. It collects the data it receives from notifications from each endpoint it is configured for and stores deployment information for each of these endpoints.

Report Portal

The report portal lets you view CA ControlMinder reports.

CA ControlMinder reports provide information about the data in the CA ControlMinder database on each endpoint, that is, the rules and policies that you deploy on the endpoint and deviations from the rules and policies. You view CA ControlMinder reports in CA Business Intelligence or in CA ControlMinder Enterprise Management.

The central RDBMS stores the endpoint data that is used in CA ControlMinder reports.

Central RDBMS

The central RDBMS stores the following:

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

Note: The web-based applications are CA ControlMinder Enterprise Management, CA ControlMinder Endpoint Management, and CA ControlMinder Password Manager.

Endpoints

An enterprise deployment of CA ControlMinder has three types of endpoints:

- CA ControlMinder endpoint—An endpoint on which you have installed CA ControlMinder.

  CA ControlMinder endpoints can also optionally serve as SAM endpoints.
- UNAB endpoint—A UNIX endpoint on which you have installed the UNIX Authentication Broker (UNAB).
- SAM endpoint—An endpoint that you manage with Privileged User Password Management (PUPM).

CA User Activity Reporting Module Components

You can send CA ControlMinder audit events from each of the endpoints and from the Enterprise Management Server to CA User Activity Reporting Module for collection and reporting. The following components support CA User Activity Reporting Module integration with CA ControlMinder:

- CA User Activity Reporting Module Agent—Collects audit events from the audit queue on the Distribution Server and sends the audit events to the CA User Activity Reporting Module Server for processing.
- CA User Activity Reporting Module Server—Receives the audit events and may apply suppression and summarization rules before the events are stored.

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

User Store

You can configure CA ControlMinder and the CA ControlMinder web-based applications to use the groups and users that are defined in Active Directory or Sun One. This means you can use a single data store for all your users.

Note: The web-based applications are CA ControlMinder Enterprise Management, CA ControlMinder Endpoint Management, and CA ControlMinder Password Manager.

Sizing the Implementation

Before you can begin to implement CA ControlMinder, you should scope the size of your implementation and allocate resources accordingly. Use the following information to help you assess the scope of your implementation.

We recommend that you install one Distribution Server for every 3000 CA ControlMinder endpoints.

The following table describes the amount of database size that you should allocate for the various components on the Enterprise Management Server and the Report Portal computer:

Component	Criteria	Gauge	Allocation
Enterprise Management Server	Active Directory as the user store	For each 1000 Active Directory accounts	20 MB
CA ControlMinder	Reports snapshot	For each 1000 CA ControlMinder endpoints	5 GB for each snapshot
SAM	Endpoint type definitions	For each 1000 PUPM endpoints	2 MB
SAM	Privileged accounts	For each 1000 privileged accounts	75 MB
SAM	Privileged Account password operations	For each 1000 PUPM privileged account passwords operation	250 MB
CA Business Intelligence	CMS and auditing databases	For a basic installation	300 MB

Note: For more information about system requirements, see the *Release Notes.*

CA ControlMinder Database Size Limitation

The CA ControlMinder database is limited to one million (1,000,000) objects. This size limitation is only likely to affect your deployment if you use advanced policy management in a large environment.

If the CA ControlMinder database in your enterprise is expected to hold 1,000,000 objects, you need to remove old DEPLOYMENT objects that are no longer in use.

Example: Calculating the Number of Objects in the CA ControlMinder Database

The following example shows you how to calculate the number of objects that you can expect to have in the DMS-the central CA ControlMinder management database.

In this example, we have an enterprise deployment of CA ControlMinder on 5000 endpoints, each holding 50 assigned policies. As a result, the DMS contains at least 250,000 objects, as follows:

```
5,000 endpoints X 50 policies = 250,000 DEPLOYMENT objects
```

If over time you create four versions of each policy, and assign these policies to each of your 5000 endpoints, the number of objects in the DMS will reach the 1,000,000 objects limit, as follows:

```
5,000 endpoints X 50 policies X 4 version = 1,000,000 DEPLOYMENT objects
```

Sizing and Performance Data

Before you begin implementing CA ControlMinder in your environment, we recommend that you review the sizing and performance data. Use the information to plan and allocate resources accordingly.

Note: The data is gathered after testing performance in small, medium, and large CA ControlMinder environments.

Tested Capabilities

The following performance capabilities of CA ControlMinder were tested on small (100 accounts), medium (1000 accounts), and large (100,000 accounts) CA ControlMinder environments:

- Account Password Check-out and Check-in
- Password reset via Password Policy
- Capture Snapshot

Data Configurations

Components and features were tested with the following data configurations:

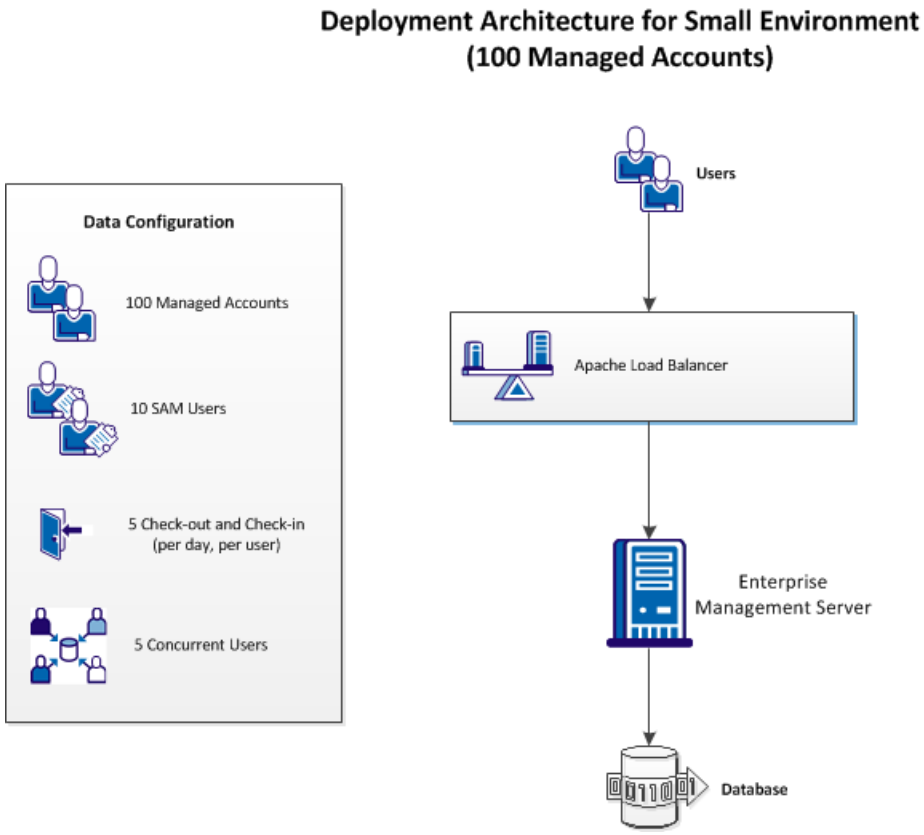
Features Tested	Small Environment	Medium Environment	Large Environment
Managed Accounts	100	1000	100,000
SAM users	10	100	1000
Check-out and Check-in (per day, per user)	5	5	5
Frequency of Bulk Password Change	90 days	90 days	90 days
Number of Enterprise Management Servers	1	2 (1 Primary, 1 Load balancing)	2 (1 Primary, 1 Load balancing)

Deployment Architecture

This section details the Deployment Architecture for small, medium, and large environments.

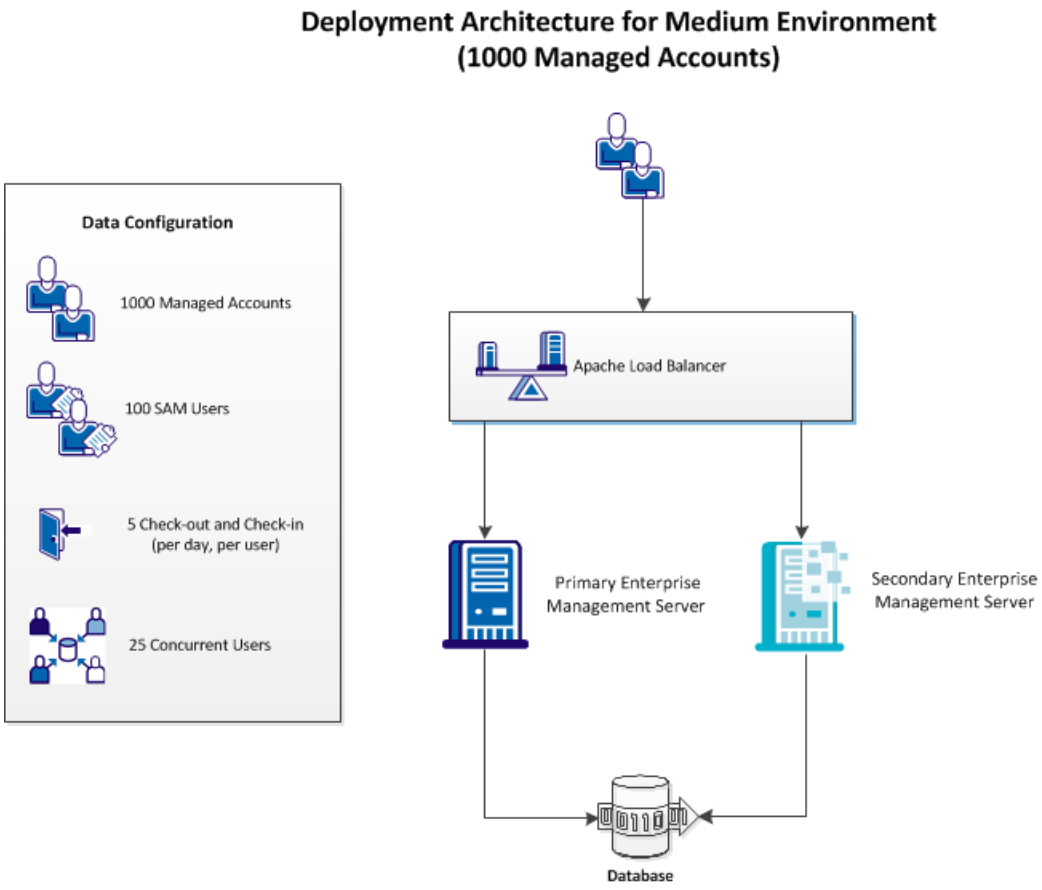
Deployment Architecture for Small Environment (100 Managed Accounts)

The following diagram shows the tested deployment architecture for a small environment:



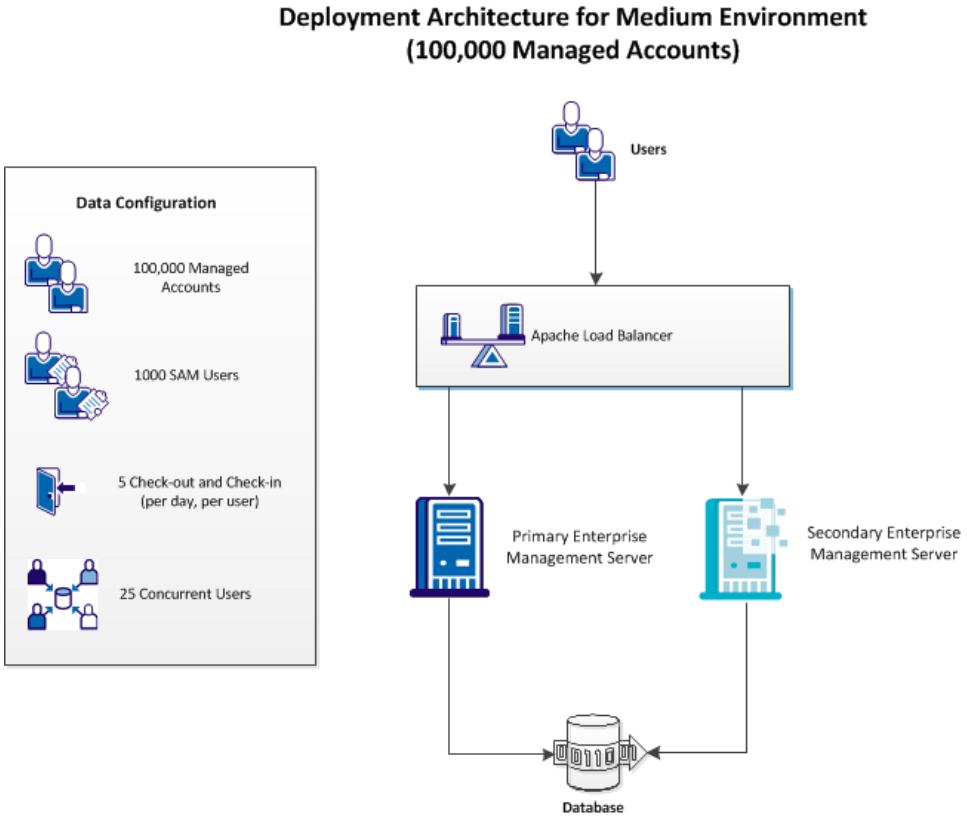
Deployment Architecture for Medium Environment (1000 Managed Accounts)

The following diagram shows the tested deployment architecture on a medium environment:



Deployment Architecture for Large Environment (100,000 Managed Accounts)

The following diagram shows the tested deployment architecture on a large environment:



Hardware and Software Configurations

This section details the configurations that were tested and profiled during product performance testing.

Hardware and Software Configuration for Small Environments

The following testing environment was used to collect the performance data:

Component	Details	Specifications
Enterprise Management Server	Operating System	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1
	System Type	x64-based Computer

Component	Details	Specifications
	Number of Processors	2
	Physical Memory (RAM)	8,192 MB
	Object/User Store	SQL 2008/Active Directory
	3rd Party Details	Jboss-4.2.3.GA Java version 1.6.0_30 Java(TM) SE Runtime Environment (build 1.6.0_30-b12) Java HotSpot(TM) 64-Bit Server VM (build 20.5-b03, mixed mode)
Database	Operating System	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1
	System Type	x64-based Computer
	Number of Processors	2
	Physical Memory (RAM)	8,192 MB
	Database	Microsoft SQL Server 2008
Active Directory	Operating System	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1
	System Type	x64-based Computer
	Number of Processors	2
	Physical Memory (RAM)	4,096 MB
	Number of AD users/groups	1000 users and 100 groups (each group contains 10 users)
Load Balancer (Apache Server)	Operating System	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1
	System Type	x64-based Computer
	Number of Processors	2
	Physical Memory (RAM)	2,048 MB

Component	Details	Specifications
	Apache Version	Apache HTTP Server Version 2.2

Hardware and Software Configuration for Medium Environments

The following testing environment was used to collect the performance data:

Component	Details	Specifications
Enterprise Management Server	Operating System	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1
	System Type	x64-based Computer
	Number of Processors	2
	Physical Memory (RAM)	8,192 MB
	Object/User Store	SQL 2008/Active Directory
	3rd Party Details	Jboss-4.2.3.GA Java version 1.6.0_30 Java(TM) SE Runtime Environment (build 1.6.0_30-b12) Java HotSpot(TM) 64-Bit Server VM (build 20.5-b03, mixed mode)
Database	Operating System	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1
	System Type	x64-based Computer
	Number of Processors	4
	Physical Memory (RAM)	8,192 MB
	Database	Microsoft SQL Server 2008
Active Directory	Operating System	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1
	System Type	x64-based Computer
	Number of Processors	2

Component	Details	Specifications
	Physical Memory (RAM)	4,096 MB
	Number of AD users/groups	10,000 users and 500 groups (each group contains 100 users)
Load Balancer (Apache Server)	Operating System	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1
	System Type	x64-based Computer
	Number of Processors	2
	Physical Memory (RAM)	2,048 MB
	Apache Version	Apache HTTP Server Version 2.2

Hardware and Software Configuration for Large Environments

The following testing environment was used to collect the performance data:

Component	Details	Specifications
Enterprise Management Server	Operating System	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1
	System Type	x64-based Computer
	Number of Processors	2
	Physical Memory (RAM)	8,192 MB
	Object/User Store	SQL 2008/Active Directory
	3rd Party Details	Jboss-4.2.3.GA Java version 1.6.0_30 Java(TM) SE Runtime Environment (build 1.6.0_30-b12) Java HotSpot(TM) 64-Bit Server VM (build 20.5-b03, mixed mode)
Database	Operating System	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1
	System Type	x64-based Computer

Component	Details	Specifications
	Number of Processors	4
	Physical Memory (RAM)	8,192 MB
	Database	Microsoft SQL Server 2008
Active Directory	Operating System	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1
	System Type	x64-based Computer
	Number of Processors	2
	Physical Memory (RAM)	4,096 MB
	Number of AD users/groups	100,000 users and 10,000 groups (each group contains 1000 users)
Load Balancer (Apache Server)	Operating System	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1
	System Type	x64-based Computer
	Number of Processors	2
	Physical Memory (RAM)	2,048 MB
	Apache Version	Apache HTTP Server Version 2.2

Performance Results

This section details the performance results that were tested and profiled during product performance testing.

Database Activity Summary (Small Environment)

The following table details the database activity during the performance testing for a small environment:

Activity	Database Growth
Database size on a fresh installation of the Enterprise Management Server	15.06 MB
Database size after creating 100 accounts on a fresh installation of the Enterprise Management Server	21.06 MB
Database growth during privileged accounts check-out and check-in	3 MB
Database growth during Password Reset via Password Policy	0.039 MB
Database growth during Capture Snapshot	3 MB
Database growth per day when no activity is reported	3 MB

Database Activity Summary (Medium Environment)

The following table details the database activity during the performance testing for a medium environment:

Activity	Database Growth
Database size on a fresh installation of the Enterprise Management Server	15.06 MB
Database size after creating 1000 accounts on a fresh installation of the Enterprise Management Server	69.56 MB
Database growth during privileged accounts check-out and check-in	56 MB
Database growth during Password Reset via Password Policy	1 MB
Database growth during Capture Snapshot	31.63 MB
Database growth per day when no activity is reported	3 MB

Database Activity Summary (Large Environment)

The following table details the database activity during the performance testing for a large environment:

Activity	Database Growth
Database size on a fresh installation of the Enterprise Management Server	15.06 MB
Database size after creating 100,000 accounts on a fresh installation of the Enterprise Management Server	1045.19 MB
Database growth during privileged accounts check-out and check-in	556 MB
Database growth during Password Reset via Password Policy	138 MB
Database growth during Capture Snapshot	705 MB
Database growth per day when no activity is reported	3 MB

Consolidated Database Metrics

The following table details the consolidated database activity for the small, medium, and large environments:

Event	Small Environment	Medium Environment	Large Environment
Database size on a fresh installation of the Enterprise Management Server	15.06 MB	15.06 MB	15.06 MB
Database growth after creating managed accounts on a fresh installation of the Enterprise Management Server	6 MB	54.5 MB	1030.13 MB
Database growth during privileged accounts check-out and check-in	3 MB	56 MB	556 MB
Database growth during Password Reset via Password Policy	0.039 MB	1 MB	138 MB
Database growth during Capture Snapshot	3 MB	31.63 MB	705 MB

Event	Small Environment	Medium Environment	Large Environment
Database growth during Database growth per day when no activity is reported	3 MB	3 MB	3 MB

Chapter 3: Installing the Enterprise Management Server

This section contains the following topics:

Environment Architecture

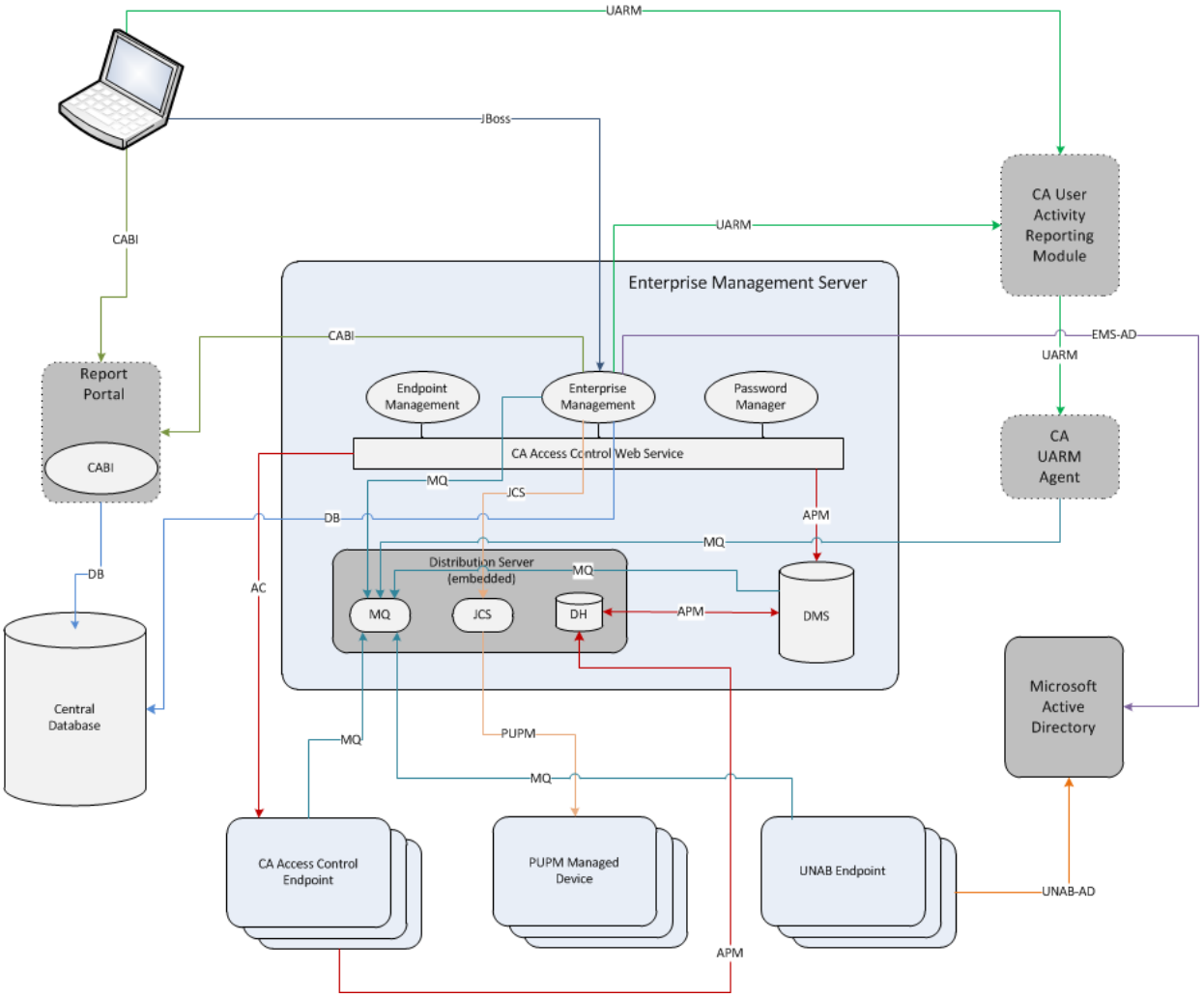
An enterprise installation of CA ControlMinder lets you centrally manage policies, privileged accounts, and CA ControlMinder endpoints; view information about the policies on each endpoint; and report on the security status of endpoints. You can manage these features through web-based interfaces or through utilities.

To manage your enterprise installation of CA ControlMinder, install the Enterprise Management Server on a central computer and configure it for your enterprise.

CA ControlMinder is installed silently when you install the Enterprise Management Server. CA ControlMinder protects the Enterprise Management Server and provides core functionality that supports the applications in the Enterprise Management Server.

Once you installed the Enterprise Management Server, you install and configure the CA ControlMinder and UNAB endpoints. If you have existing CA ControlMinder endpoints, configure each endpoint for advanced policy management and reporting.

The following diagram shows the Enterprise Management Server architecture:



The previous diagram illustrates the following:

- The Enterprise Management Server uses the following ports:
  - Port 8891 for symmetric encryption and port 5249 for SSL communication with the CA ControlMinder endpoints.
  - Ports 1433 (MS SQL) or 1521 (Oracle) to communicate with the RDBMS.
  - Ports 389 or 686 for encrypted communication with Active Directory.
  - Port 20411 for encrypted communication with the Java Connector Server (JCS)
  - Port 7243 for encrypted communication with the Message Queue

- SAM communicates with the endpoints according to the endpoint type (Windows Agentless, SSH Device and more).
- Enterprise Management Server communciates with CA Business Intelligence using port 8080.
- Enterprise Management Server communicates with CA User Activity Reporting Module using port 5250 for encrypted communication.
- UNAB communicates with Active Directory using the following ports: 53, 88, 123, 289, 445, 464, 3268.

How to Prepare the Enterprise Management Server

Prepare the Enterprise Management Server on Windows

Valid on Windows

Before you install the Enterprise Management Server, you prepare the server. If you are upgrading an r12.5 or later installation, you have already prepared the Enterprise Management Server and you do not need to complete these steps again.

Note: When you install the Enterprise Management Server, the installation program also installs CA ControlMinder Endpoint Management, if it is not already installed. If you have installed CA ControlMinder Endpoint Management, do not repeat those steps.

Follow these steps:

1. Prepare the central database for Enterprise Management.

   You can also choose to prepare the database by manually creating and configuring the central database using the RDBMS native management tools.

2. Install the prerequisite software using *one* of the following methods:

   - Run the prerequisite installation utility (see page 61).

     CA ControlMinder provides a utility that installs the Java Development Kit (JDK) and the JBoss application server. If you already have installed the software, you can skip this step.

   - Use existing software or install the prerequisite software manually, as follows:

     Note: You can find prerequisite third-party software on the CA ControlMinder Third Party Components DVDs. For information about supported versions, see the *Release Notes*.

a. Install a supported version of Java Development Kit (JDK).

b. Install a supported JBoss version. We recommend that you run JBoss as a service.

Note: If you already have JBoss installed, we recommend that you run JBoss once before installing CA ControlMinder Enterprise Management to resolve any open ports issues. The CA ControlMinder Enterprise Management installation program does not use the default JBoss ports. For example, the installation program uses port number 18080 rather than port number 8080 for HTTP connections. Verify that you specify the ports that JBoss uses during the Enterprise Management Server installation.

You can now install CA ControlMinder Enterprise Management on the Enterprise Management Server.

Prepare the Enterprise Management Server on Linux

Valid on Linux

Before you install the Enterprise Management Server, you prepare the server. If you are upgrading an r12.5 or later installation, you have already prepared the Enterprise Management Server and you do not need to complete these steps again.

When you install the Enterprise Management Server, the installation program also installs CA ControlMinder Endpoint Management, if it is not already installed. If you have installed CA ControlMinder Endpoint Management, do not repeat those steps.

Follow these steps:

1. Prepare the central database for Enterprise Management.

   Note: If the database administrator wants to review and control the changes that CA ControlMinder makes to the database, you can prepare the database manually by creating and configuring the central database using the RDBMS native management tools.

2. Install a supported version of Java Development Kit (JDK) or use existing software:

   Note: You can find prerequisite third-party software on the CA ControlMinder Third Party Components DVDs. For information about supported versions, see the *Release Notes*.

   a. Print your system information to determine whether the server architecture is 32-bit or 64-bit:

      ```
      uname –m
      ```

      If the command returns"i386" or "i686", it is a 32-bit architecture. If it returns "x86_64", it is a 64-bit architecture.

   b. Change to the "x86" directory (for 32-bit) or to the "x64" directory (for 64-bit, respectively) on the installation media, and run the installer. For example:

      ```
      chmod 750 jdk-7u21-linux-x64.rpm.bin
      ```

      ```
      ./jdk-7u21-linux-x64.rpm.bin
      ```

   c. Append the JDK/bin path to the system PATH.

      For example, to set the path "/usr/java/jdk1.7.0_21/" using the bash shell, enter the following command:

      ```
      export PATH=/usr/java/jdk1.7.0_21/bin:$PATH
      ```

      Note: To set the path permanently, add this command to your shell startup file.

3. Install a supported JBoss version or use existing software. We recommend that you run JBoss as a daemon.

   Note: If you already have JBoss installed, we recommend that you run JBoss once before installing CA ControlMinder Enterprise Management to resolve any open ports issues. The CA ControlMinder Enterprise Management installation program does not use the default JBoss ports. For example, it uses port number 18080 rather than the default port number 8080 for HTTP connections.

   a. Extract the JBoss archive to install it.

      ```
      cp jboss-4.2.3.GA.zip /opt/
      unzip jboss-4.2.3.GA.zip
      ```

   b. Change the port number from 8080 to 18080, and change the redirect port from 8443 to 18443 in server.xml.

      ```
      vi
      /opt/jboss-4.2.3.GA/server/default/deploy/jboss-web.deploye
      r/server.xml
      <Connector URIEncoding="UTF-8" acceptCount="150"
      address="${jboss.bind.address}" connectionTimeout="20000"
      disableUploadTimeout="true" emptySessionPath="true"
      enableLookups="false" maxHttpHeaderSize="8192"
      maxThreads="250" port="18080" protocol="HTTP/1.1"
      redirectPort="18443"/>
      <Connector SSLEnabled="true" URIEncoding="UTF-8"
      clientAuth="false" keyAlias="entm"
      keystoreFile="/opt/jboss-4.2.3.GA/server/default/deploy/Ide
      ntityMinder.ear/custom/ppm/truststore/ssl.keystore"
      keystorePass="secret" maxThreads="150" port="18443"
      protocol="HTTP/1.1" scheme="https" secure="true"
      sslProtocol="TLS"/>
      <Connector address="${jboss.bind.address}"
      emptySessionPath="true" enableLookups="false" port="8009"
      protocol="AJP/1.3" redirectPort="18443"/>
      ```

c. Change the naming port from 1099 to 11099 in jboss-minimal.xml.

```
vi /opt/jboss-4.2.3.GA/server/default/conf/jboss-minimal.xml
<mbean code="org.jboss.naming.NamingService"
      name="jboss:service=Naming"
      xmbean-dd="resource:xmdesc/NamingService-xmbean.xml">
      <attribute name="CallByValue">false</attribute>
      <attribute name="Port">11099</attribute>
```

d. Change the naming port from 1099 to 11099 in jboss-service.xml.

```
vi /opt/jboss-4.2.3.GA/server/default/conf/jboss-service.xml
<mbean code="org.jboss.naming.NamingService"
      name="jboss:service=Naming"
      xmbean-dd="resource:xmdesc/NamingService-xmbean.xml">
      <attribute name="CallByValue">false</attribute>
      <attribute name="Port">11099</attribute>
```

e. Configure JBoss to start as a daemon. For more information see https://community.jboss.org/wiki/startjbossonbootwithlinux.

4. Change the maximum number of open files to avoid failures during the installation:

```
ulimit –n 10000
```

5. Verify that the rpmbuild package from your Linux distribution is installed.

   The Enterprise Management Server requires the rpmbuild package to install the Advanced Policy Management option on the server.

You can now install CA ControlMinder Enterprise Management on the Enterprise Management Server.

Prepare the Central Database for Enterprise Management

CA ControlMinder Enterprise Management requires a relational database management system (RDBMS). Set this up before you install CA ControlMinder Enterprise Management.

You have two options for setting up your database to work with CA ControlMinder Enterprise Management:

- Prepopulate the central database using deployment scripts CA ControlMinder provides.

  Using this option, you separate between the database preparation and CA ControlMinder Enterprise Management installation. The database administrator can review and control the changes CA ControlMinder makes to the database.

- Let CA ControlMinder Enterprise Management prepare the central database during the installation automatically.

  Using this option, the CA ControlMinder Enterprise Management installation populates the database as part of the installation process.

Follow these steps:

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

   Note: For a list of supported RDBMS software, see the *Release Notes*.

2. Configure the RDBMS for CA ControlMinder Enterprise Management:

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

   - For Oracle, perform the following steps:

   a. Create a user for the central database. This user must have the following permissions and settings:

      – System Privileges: ADMINISTER DATABASE TRIGGER, ALTER SESSION, CREATE CLUSTER, CREATE DATABASE LINK, CREATE SEQUENCE, CREATE SESSION, CREATE SYNONYM, CREATE TABLE, CREATE VIEW, CREATE ANY INDEXTYPE, CREATE OPERATOR, CREATE PROCEDURE, CREATE TRIGGER, CREATE TYPE, EXECUTE ON SYS.DBMS_CRYPTO, SELECT ANY DICTIONARY, UNLIMITED TABLESPACE

   b. Enter the following commands to increase the number of connections to the database:

      ```
      ALTER SYSTEM SET transactions=275 SCOPE=SPFILE

      ALTER SYSTEM SET sessions=250 SCOPE=SPFILE

      ALTER SYSTEM SET processes=200 SCOPE=SPFILE
      ```

   - For SQL Server:

      a. Create a new case-*insensitive* database.

         The database must have the sort order SQL_Latin1_General_CP1_CI_AS.

      b. Create a new login, make the new database the default database of the login.

      c. Set the login as the database owner.

      Note: The SQLServer requires the same collation between the master the UserDB.

3. (Optional) Prepopulate the central database using the deployment scripts CA ControlMinder provides.

   a. Insert the appropriate CA ControlMinder Server Components DVD for your operating system into your optical disc drive.

   b. Copy the deployment script for your RDBMS to a temporary local folder.

      By default, the database deployment scripts are on the optical media at the following location:

      - Oracle: /Schema/oracle_database_deployment_script.sql
      - SQL Server: /Schema/mssql_database_deployment_script.sql

   c. Deploy the deployment scripts (see page 60).

   d. Configure the database user that you use for the CA ControlMinder Enterprise Management installation.

      - For Oracle, keep the ALTER SESSION, CREATE SESSION, EXECUTE ON SYS.DBMS_CRYPTO, and SELECT ANY DICTIONARY system privileges for the user you created.
      - For SQL Server, create a user, select the database that you created earlier as the default, map the user to the database, and set the following permissions: CONNECT.SELECT, INSERT, DELETE, UPDATE, EXECUTE.

   e. Reset the predefined user account passwords. Follow these steps:

      a. Login to CA ControlMinder Enterprise Management as a user with administrative privileges.

      b. Select Users and Groups, Users, Reset User Password.

         The Reset User Password screen opens.

      c. Type in a search query to display all available users and select Search.

         CA ControlMinder Enterprise Management displays the following user accounts: [default user], superadmin, neteautoadmin, selfreguser

      d. Do the following for each account:

         Select a user account and click Select.

         The reset password window opens.

         Type in the account password in the Confirm Password field.

         (Optional) Select the Password Must Change option and click Submit.

         CA ControlMinder Enterprise Management resets the account password.

Central Database Script Deployment Examples

Deploying the script populates the central database and prepares it for the CA ControlMinder Enterprise Management installation. You deploy the script using the native database tools.

Example: Deploy the CA ControlMinder Oracle Deployment Script on Oracle Database 10g

This example shows you how to deploy the CA ControlMinder Oracle deployment on an Oracle Database 10g.

1. Click Start, All Programs, Oracle - *ORACLE_HOME*, Application Development, SQL Plus.

   The Oracle SQL*PLUS window opens.

2. Connect to the Oracle database using the user you created earlier.

3. Enter the full pathname to the script file preceded by the @ sign. For example:

   ```
   @C:\ temp_directory\oracle_database_deployment_script.sql
   ```

   Oracle deploys the script to the database.

Example: Deploy the CA ControlMinder Microsoft SQL Server Deployment Script on SQL Server 2005

This example shows you how to deploy the CA ControlMinder Microsoft SQL Server deployment on a SQL Server 2005.

1. Click Start, All Programs, Microsoft SQL Server 2005, SQL Server Management Studio.

   A login window appears.

2. Log in as a system administrator.

   The Microsoft SQL Server Management Studio opens.

3. Click File, Open, File.

   The Open File dialog appears.

4. Browse for and select the CA ControlMinder Microsoft SQL Server deployment script, and click Open.

5. From the Available Databases drop-down list, select the database that you created earlier to deploy the script on.

6. Click Execute to deploy the script.

   Microsoft SQL Server deploys the script to the database.

Run the Prerequisite Software Installation Utility

Valid on Windows

CA ControlMinder Enterprise Management requires the Java Development Kit (JDK) and the JBoss application server to run. The correct versions of this prerequisite third-party software are supplied on the CA ControlMinder Third-Party Components DVDs. Also on these DVDs is a utility that installs the prerequisite software as follows:

- Sets JDK and JBoss to install with settings appropriate for CA ControlMinder Enterprise Management.
- Installs JBoss as a service.
- Lets you launch the CA ControlMinder Enterprise Management installation with prerequisite software settings preconfigured.

If you already have the software installed, you can skip this procedure. If not, we recommend that you use the supplied utility to install it as described in this procedure.

If you already have JBoss installed, we recommend that you run JBoss once before installing CA ControlMinder Enterprise Management to resolve any open ports issues.

Follow these steps:

1. Insert the CA ControlMinder Third-Party Components DVD for Windows into your optical disc drive.
2. Navigate to the PrereqInstaller directory on the optical disc drive and run **install_PRK.exe**.

   The InstallAnywhere wizard opens.
3. Complete the wizard as required.

   Note: To configure additional JBoss port numbers, select Advanced Configuration on the JBoss Ports Settings page. If you specify a JBoss port that is busy, the installer prompts you to specify a different port number.

4. Review the details in the summary report and click Install.

   The prerequisite software installs. This can take some time.

5. Do *one* of the following:

   - If you want to start the CA ControlMinder Enterprise Management installation process after the prerequisite software installs, when prompted, insert the CA ControlMinder Server Components DVD for your operating system into your optical disc drive and select Done. Close the Product Explorer window if it appears.
   - If you want to install additional Enterprise Management Servers, for high availability or disaster recovery, specify a custom FIPS key to install CA ControlMinder Enterprise Management with. When prompted, click Done and click Finish to close the dialog that appears.
   - If you do not want to start the CA ControlMinder Enterprise Management installation process after the prerequisite software installs, when prompted, click Done and click Finish to close the dialog that appears.

     The prerequisite software installation process is complete.

How to Install the Enterprise Management Server Components

The Enterprise Management Server components let you centrally manage your enterprise deployment of CA ControlMinder. After you install the Enterprise Management Server components, you install the reporting service and the CA ControlMinder and UNAB endpoints.

Before you begin the implementation, verify that the computers you are using meet the required hardware and software specifications.

Note: For more information about the required hardware and software specifications, see the CA ControlMinder Compatibility Matrix that is available from the CA ControlMinder product page on CA Support.

To install the Enterprise Management Server components, do the following:

1. Prepare the Enterprise Management Server.

   Before you install the Enterprise Management Server, prepare the computer by installing and configuring the prerequisites.

   Note: We recommend that you install the latest software updates and patches for your system before you install the Enterprise Management Server.

2. Install the master CA ControlMinder Enterprise Management.

   All the web-based applications, the Distribution Server, the DMS, and CA ControlMinder are installed.

3. (Optional) Install the Load Balancing Enterprise Management Servers.
4. (Optional) Configure the Enterprise Management Server to use Sun ONE directory or CA Directory user stores.

   You can define CA ControlMinder Enterprise Management to use the Sun ONE or CA Directory user stores in place of Active Directory or the relational database user store.
5. (Optional) Configure the Enterprise Management Server for SSL communication, as follows:

   a. Configure JBoss for SSL communications.

   b. (Active Directory) Configure the Enterprise Management Server for SSL communication.
6. (Optional) Set up advanced configuration.

   Use the CA IdentityMinder Management Console to perform advanced configuration tasks, such as to modify the properties of the central database to generate custom reports and configure CA ControlMinder Enterprise Management to send email notifications when a specific event occurs.
7. (Optional) Implement enterprise reporting.

   The Enterprise Management Server provides reporting capabilities through a CA Business Intelligence Common Reporting server (CA ControlMinder Report Portal).
8. (Optional) Integrate with CA User Activity Reporting Module.

   You have installed the Enterprise Management Server. You can now install and configure your endpoints.

More information:

How to Set Up Reporting Service Server Components (see page 105)

Install CA ControlMinder Enterprise Management on Windows

Installing CA ControlMinder Enterprise Management installs all the Enterprise Management Server components. You must prepare the Enterprise Management Server before you install CA ControlMinder Enterprise Management.

We recommend that you use the Prerequisite Kit installer to initiate the CA ControlMinder Enterprise Management installation. Install_PRK.exe installs required third-party software and then starts the CA ControlMinder Enterprise Management installation.

Note: You cannot install CA ControlMinder Enterprise Management by network install. Copy the entire contents of the Disk 1 directory of the CA ControlMinder Server Components DVD to your installation directory or map a drive to the DVD instead.

Important! If you install CA ControlMinder Enterprise Management for High Availability, specify the same FIPS key on the primary and secondary Enterprise Management Servers. Specify a custom FIPS key if you install CA ControlMinder Enterprise Management for High Availability with FIPS support.

Follow these steps:

1. Stop JBoss Application Server if it is running.
2. Stop CA ControlMinder services if you are installing CA ControlMinder Enterprise Management on a computer that already has CA ControlMinder installed.
3. Insert the CA ControlMinder Server Components DVD for Windows into your optical disk drive.
4. Expand the Components folder in the Product Explorer, select CA ControlMinder Enterprise Management, then click Install.
5. Complete the wizard as required. The following installation inputs are not self-explanatory:

   Select Installation Mode

   Defines the Enterprise Management Server installation mode:

   - Primary Enterprise Management Server—Select to install the primary Enterprise Management Server.
   - Load Balancing Enterprise Management Server—Select to install a Load Balancing Enterprise Management Server.

   Important! Installation mode applies to new installations only.

Choose Install Folder

Defines the full path of the installation folder.

Default: \ProgramFiles\CA\AccessControlServer\

Note: On 64 bit operating systems the default installation folder is:

`\Program Files(x86)\CA\AccessControlServer\`

Important: The product does not support special characters in the installation directory path.

Java Development Kit (JDK)

Defines the location of an existing JDK.

Note: If you launch the CA ControlMinder Enterprise Management installation immediately after you use the CA ControlMinder Third Party Component DVDs to install the prerequisite software, this wizard page does not appear. The installation utility configures the installation settings on this page based on the values you provided in the prerequisite software installation process.

JBoss Application Server Information

Defines the JBoss instance that you want to install the application on.

To do this, define the:

- JBoss folder, which is the top directory where you have JBoss installed.

  For example, C:\jboss-4.2.3.GA on Windows or /opt/jboss-4.2.3.GA on Solaris.

- URL, which is the IP address or host name of the computer you are installing on.
- Port JBoss uses.
- Port JBoss uses for secure communications (HTTPS).
- Naming port number.

Note: If you launch the CA ControlMinder Enterprise Management installation immediately after you use the CA ControlMinder Third Party Component DVDs to install the prerequisite software, this wizard page does not appear. The installation utility configures the installation settings on this page based on the values you provided in the prerequisite software installation process.

Communication Password

(Primary Enterprise Management Server Only) Defines the password used for CA ControlMinder Enterprise Management Server inter-component communication.

Note: CA ControlMinder Enterprise Management uses the communication password to manage the Message Queue keystore and administrator account, handle communication between CA ControlMinder Enterprise Management and the endpoints and manage the Java Connection Server.

Primary Enterprise Management Server Information

(Load Balancing Enterprise Management Server Only) Defines the Primary Enterprise Management Server host name or IP address and the full pathname to the FIPS key.

Note: By default, the FIPS key is located in the following path, where *JBoss_HOME* is the directory where you installed JBoss:

JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/config/keys

Database Information

Defines the connection details to the RDBMS:

- **Database Type**—Specifies a supported RDBMS.
- **Host Name**—Defines the name of the host where you have the RDBMS installed.
- **Port Number**—Defines the port used by the RDBMS you specified. The installation program provides the default port for your RDBMS.
- **Service Name**—(Oracle) Defines the name that identifies your RDBMS on the system. For example, for Oracle Database 10g this is *orcl* by default.
- **Database Name**—(MS SQL) Defines the name of the database you created.
- **Username**—Defines the name of the user that you created when you prepared the database.

  Note: You granted this user the appropriate database permissions when you prepared the database.
- **Password**—Defines the RDBMS password of the user that you created when you prepared the database.

The installation program checks the connection to the database before it continues.

Active Directory Settings

Defines the Active Directory user store settings:

- **Host**—Defines the Domain Controller host name of Active Directory.
- **Port**—Defines the port used by default for LDAP queries against Active Directory, for example, 389.
- **Search Root**—Defines the search root, for example, ou=DomainName, DC=com.

  Note: Set the Search Root at least one node higher in the directory tree than the Distinguished Names (DNs) for the users specified for User DN and System User. Otherwise, Enterprise Management might launch without displaying any tabs.

- **User DN**—Defines the Active Directory user account name that is used to manage CA ControlMinder Enterprise Management. For example: CN=Administrator, cn=Users, DC=DomainName, DC=Com.

  Note: This user issues LDAP queries against Active Directory. You can choose to define a user with read-only privileges for this parameter. However, if you define a user with read-only privileges, you cannot assign admin roles or privileged access roles to users in CA ControlMinder Enterprise Management. Instead, you modify the member policy for each role to point to an Active Directory group.

- **Password**—Defines the password of the Active Directory user account that is used to manage CA ControlMinder Enterprise Management.

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

Note: You can use the DSQUERY directory querying utility to discover the user Distinguished Name (User DN). You must run this query on the Active Directory server. For example:

```
dsquery user -name administrator
"CN=Administrator,CN=Users,DC=lab.DC=demo"
```

System User

(Active Directory only) Defines the DN of the Active Directory user who is assigned the System Manager admin role in CA ControlMinder Enterprise Management.

Example: CN=SystemUser, ou=OrganizationalUnit, DC=DomainName, DC=Com

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

Administrator Password

(Embedded user store only) Defines the password of *superadmin*, the CA ControlMinder Enterprise Management administrator. Make a note of the password so you can log in to CA ControlMinder Enterprise Management when the installation is complete.

Note: In this step you create the superadmin user in the embedded user store. The superadmin user is assigned the System Manager admin role in CA ControlMinder Enterprise Management. You log in as superadmin the first time you log in to CA ControlMinder Enterprise Management. For more information about the System Manager admin role, see the *Enterprise Administration Guide*.

FIPS Key Location

Defines the path to a copy of the original FIPSkey.dat. The FIPS key file ensures that the encrypted database is readable after migration.

The Enterprise Management Server is installed after you complete the wizard. Reboot the computer to complete the installation.

6. Select Yes, restart my system and click Done.

   The computer reboots. You can now configure CA ControlMinder Enterprise Management for your enterprise.

More information:

Change the Message Queue Administrator Password (see page 499)

Install CA ControlMinder Enterprise Management on Linux

Installing CA ControlMinder Enterprise Management installs all the Enterprise Management Server components. Prepare the Enterprise Management Server before you install CA ControlMinder Enterprise Management.

Use the console installation to install CA ControlMinder Enterprise Management on a Linux computer.

Follow these steps:

1. Shut down the JBoss Application Server if it is running.
2. Stop CA ControlMinder services if you are installing CA ControlMinder Enterprise Management on a computer that already has CA ControlMinder installed. Perform the following steps:

   a. Enter the following command to stop CA ControlMinder services:

      ```
      /opt/CA/AccessControl/bin/secons -sk
      ```

      CA ControlMinder is stopped.

   b. Enter the following command to unload CA ControlMinder:

      ```
      /opt/CA/AccessControl/bin/SEOS_load -u
      ```

   CA ControlMinder is stopped and the computer is ready for installation.

3. Complete the following steps:

   a. Insert the appropriate CA ControlMinder Server Components DVD for your operating system into your optical disc drive.

   b. Mount the optical disc drive. Do *not* specify the noexec option. If you specify the noexec option, the installation fails.

      Note: In some releases of Linux, the operating system automounts the optical disc drive with the noexec option.

c. Open a terminal window and set a writeable temporary directory as the working directory.

Note: The installer unpacks the installation files to the working directory. If you specify a working directory on the optical media, the installation fails because the installer cannot unpack the files.

d. Execute the installer, specifying the full path to the installer in the command. For example, if you mount the optical disc drive in the /media directory, enter the following command:

```
/media/EnterpriseMgmt/Disk1/InstData/NoVM/install_EntM.bin -i console
```

Important! If you install CA ControlMinder Enterprise Management for High Availability, specify the same FIPS key on the primary and secondary Enterprise Management Servers. Specify a custom FIPS key if you install CA ControlMinder Enterprise Management for High Availability with FIPS support.

Important! The product does not support special characters in the installation directory path.

The InstallAnywhere console appears after a few moments.

4. Complete the prompts as required. The following installation inputs are not self-explanatory:

Select Installation Mode

Defines the Enterprise Management Server installation mode:

- Primary Enterprise Management Server—Select to install the primary Enterprise Management Server.
- Load Balancing Enterprise Management Server—Select to install a Load Balancing Enterprise Management Server.

Important! **Installation mode applies to new installations only.**

Java Development Kit (JDK)

Defines the location of an existing JDK.

JBoss Application Server Information

Defines the JBoss instance that you want to install the application on.

You need to:

- Define the JBoss folder, which is the top directory where you have JBoss installed.

  For example, /opt/jboss-4.2.3.GA

- Define the port JBoss uses.
- Define the port JBoss uses for secure communications (HTTPS).
- Define the naming port number.

Note: The CA ControlMinder Enterprise Management installation program does not use the default JBoss ports but instead adds 10000 to the default JBoss port numbers. For example, the installation program uses port number 18080 rather than port number 8080 for HTTP connections. Ensure that you specify the ports that JBoss uses.

Communication Password

(Primary Enterprise Management Server Only) Defines the password used for CA ControlMinder Enterprise Management Server inter-component communication.

Note: CA ControlMinder Enterprise Management uses the communication password to manage the Message Queue keystore and administrator account, handle communication between CA ControlMinder Enterprise Management and the endpoints and manage the Java Connection Server.

Primary Enterprise Management Server Information

(Load Balancing Enterprise Management Server Only) Defines the Primary Enterprise Management Server host name or IP address and the full pathname to the FIPS key.

Note: By default, the FIPS key is located in the following path, where *JBoss_HOME* is the directory where you installed JBoss:

JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/config/keys

Database Information

Defines the connection details to the RDBMS:

- **Database Type**—Specifies a supported RDBMS.
- **Host Name**—Defines the name of the host where you have the RDBMS installed.
- **Port Number**—Defines the port used by the RDBMS you specified. The installation program provides the default port for your RDBMS.

- **Service Name**—(Oracle) Defines the name that identifies your RDBMS on the system. For example, for Oracle Database 10g this is *orcl* by default.
- **Database Name**—(MS SQL) Defines the name of the database you created.
- **Username**—Defines the name of the user that you created when you prepared the database.

  Note: You granted this user the appropriate database permissions when you prepared the database.
- **Password**—Defines the RDBMS password of the user that you created when you prepared the database.

The installation program checks the connection to the database before it continues.

User Store Type

Defines the user store type CA ControlMinder Enterprise Management uses. Select *one* of the following:

- **Embedded User Store**—CA ControlMinder Enterprise Management stores user information in the RDBMS.
- **Active Directory—**you specify the connection information details in the next screen.
- **Other User Store**—you specify the user store configuration information after the CA ControlMinder Enterprise Management installation completes.

Note: To deploy login authorization policies to UNAB, you must select either Active Directory or Other User Store as the user store. If you select Active Directory or Other User Store as the user store, you cannot create or delete users and groups in CA ControlMinder Enterprise Management. For more information about UNAB and Active Directory restrictions, see the *Enterprise Administration Guide*.

Active Directory Settings

Defines the Active Directory user store settings:

- **Host**—Defines the Domain Controller host name of Active Directory.
- **Port**—Defines the port used by default for LDAP queries against Active Directory, for example, 389.
- **Search Root**—Defines the search root, for example, ou=DomainName, DC=com.

  Note: Set the Search Root at least one node higher in the directory tree than the Distinguished Names (DNs) for the users specified for User DN and System User. Otherwise, Enterprise Management might launch without displaying any tabs.

- **User DN**—Defines the Active Directory user account name that is used to manage CA ControlMinder Enterprise Management. For example: CN=Administrator, cn=Users, DC=DomainName, DC=Com.

  Note: This user issues LDAP queries against Active Directory. You can choose to define a user with read-only privileges for this parameter. However, if you define a user with read-only privileges, you cannot assign admin roles or privileged access roles to users in CA ControlMinder Enterprise Management. Instead, you modify the member policy for each role to point to an Active Directory group.

- **Password**—Defines the password of the Active Directory user account that is used to manage CA ControlMinder Enterprise Management.

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

Note: You can use the DSQUERY directory querying utility to discover the user Distinguished Name (User DN). You must run this query on the Active Directory server. For example:

```
dsquery user -name administrator
"CN=Administrator,CN=Users,DC=lab.DC=demo"
```

System User

(Active Directory only) Defines the DN of the Active Directory user who is assigned the System Manager admin role in CA ControlMinder Enterprise Management.

Example: CN=SystemUser, ou=OrganizationalUnit, DC=DomainName, DC=Com

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

Administrator Password

(Embedded user store only) Defines the password of *superadmin*, the CA ControlMinder Enterprise Management administrator. Make a note of the password so you can log in to CA ControlMinder Enterprise Management when the installation is complete.

Note: In this step you create the superadmin user in the embedded user store. The superadmin user is assigned the System Manager admin role in CA ControlMinder Enterprise Management. You log in as superadmin the first time you log in to CA ControlMinder Enterprise Management. For more information about the System Manager admin role, see the *Enterprise Administration Guide*.

5. Review the pre-installation summary information. If the information is correct, press Enter.

   CA ControlMinder Enterprise Management is installed.

6. Press Enter.

   The installer closes.

7. Reboot the computer, if necessary.

   Proceed to configure CA ControlMinder Enterprise Management for your enterprise.

Block HTTP Access on the Enterprise Management Server

Symptom:

After installation, HTTP and HTTPS ports are open by default. You need to disable the HTTP port.

Solution:

To disable the HTTP port, comment out the HTTP connector in the JBoss configuration.

Follow these steps:

1. Browse to *JBOSS_HOME*/server/default/deploy/jboss-web.deployer and edit the server.xml file.
2. Search for the following string that defines the default port of the HTTP connector: `port="18080"`

   Note: If you have configured a different port in the installation wizard, the port number may be different.

   This port attribute is part of a <Connector> element.

3. Comment out this <Connector> element by surrounding the element with comment tags (<!-- and -->).

   The HTTP connector is disabled.

4. Restart the JBoss service.

Example

```
<!-- <Connector port="18080" address="${jboss.bind.address}"
         connectionTimeout="20000" /> -->
```

Create a Subscriber after Installing Load Balancing Enterprise Management Server and Distribution Server

If you install multiple Enterprise Management Servers, you must create a subscriber before starting CA ControlMinder Enterprise Management. Complete the following procedure in the Primary Enterprise Management Server.

Important! Complete this step if you install the Load Balancing Enterprise Management Servers and the Distribution Servers.

Follow these steps:

1. Open a command prompt window.
2. Enter the following command to create a subscriber.

   sepmd -n DMS__DH__@<LB_entm>

Note: For more information about the sepmd utility, see the *Reference Guide*.

Chapter 4: Configuring the Enterprise Management Server for SUN ONE and CA Directory

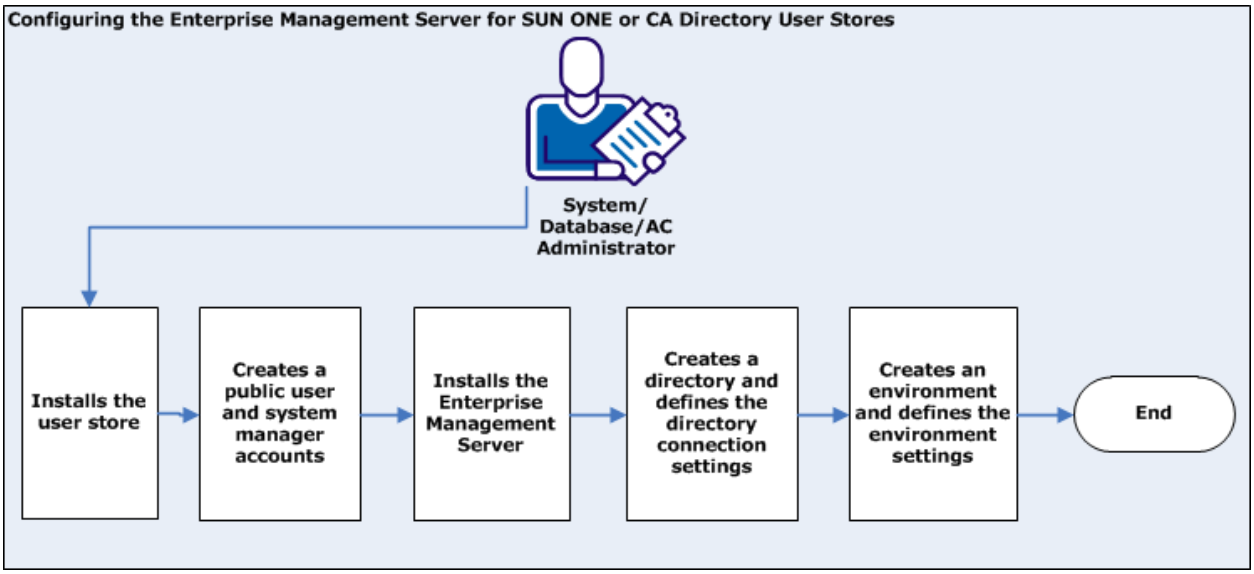
This scenario describes how you configure the Enterprise Management Server for SUN ONE or CA Directory. If you are using SUN ONE or CA Directory as the user store, you configure the user store settings after you install CA ControlMinder Enterprise Management. You use the CA IdentityMinder Management Console to configure the directory and environment settings.

Important! To use SUN ONE directory or CA Directory as the user store, select the Other User Store option in the Select User Store screen at the CA ControlMinder Enterprise Management installation wizard.

The target audience for this scenario is:

- System Administrators
- Database Administrators
- CA ControlMinder Administrators

The following diagram illustrates the steps you complete to configure the Enterprise Management Server for SUN ONE or CA Directory user stores:



Follow these steps:

1. Install the user store directory.

   Note: For SUN ONE, verify that you install the SUN ONE Directory Suite and Administration Services. For more information about CA Directory, refer to the *CA Directory Installation Guide*.

2. Create a public user and a system manager account.

   You specify the user credentials when you create the environment.

3. Install the Enterprise Management Server.

   Note: Do not specify a user store during the installation. For more information about the Enterprise Management Server installation, refer to the *Implementation Guide.*

4. Create a directory and define the connection settings:

   - SUN ONE (see page 76)
   - CA Directory (see page 80)

5. Create an environment and define the environment settings:

   - SUN ONE (see page 77)
   - CA Directory (see page 81)

   Note: You use the CA IdentityMinder Management Console to configure and define the settings for the directory and the environment.

6. Stop the CA ControlMinder services using the secons -s command.

7. Start the CA ControlMinder services using the seosd -start command.

Create a Directory for the SUN ONE User Store

A directory provides information about a user directory that the Enterprise Management Server manages. You configure the SUN ONE directory settings after you install the Enterprise Management Server.

Follow these steps:

1. Navigate to the following directory, where *JBOSS_HOME* indicates the directory where you installed JBoss:

   `JBOSS_HOME/server/default/deploy/IdentityMinder.ear/user_console.war/META-INF/`

2. Locate the SAM_iPlanet_directory.xml file and copy the file to a temporary directory.

3. Open the CA IdentityMinder Management Console as follows:

   `http://enterprise_host:port/idmmanage`

4. Select Directories, New.

   The new directory window opens.

5. Select Browse and locate the SAM_iPlanet_directory.xml file. Click Next.

6. Enter the following information:

   - **Name**—defines the directory logical name
   - **Description**—(optional) specifies a description for the directory
   - **Object Connection Name**—specifies the name of the user store
   - **Host**—defines the directory host name or IP address
   - **Port**—defines the directory port number

     Example:389
   - **Search root**—defines the organization search root. Directory search will start from the root level
   - **User DN**—defines a user account with privileges to log in to the directory

     Example: cn=Username, ou=Administration, ou=Corporate, o=Democorp, c=AU
   - **Password**—defines the user account password
   - **Confirm password**—enter the user account password to confirm the password
   - **Secure connection**—indicates that the connection to the directory is secured

7. Click Next and Finish.

   The new directory is created. You now need to create an environment.

Create an Environment for the SUN ONE User Store

Valid for Windows

After you create and configure the directory settings for the SUN ONE directory, you create an environment. An environment is a view of the user store. In an environment you manage users, groups, organizations, tasks and roles.

Note: The JBoss application server service automatically starts during Windows startup and if an environment does not exist, one is created. We recommend that you disable the automatic service startup. If the environment exists, delete it before you create the environment for the SUN ONE user store.

Before you create the environment, you must define the system manager account in the Sun ONE user directory.

Important! Verify that you do not define the system manager account directly under the search root Organization Unit (OU) rather, under an Organization Unit that is located under the search root. For example, if the search root you defined is dc=company, dc-com, create the system manager account under the Users OU as follows: uid=Sysmanager,ou=Users,dc=company,dc=com

Follow these steps:

1. Navigate to the following directory, where *JBOSS_HOME* indicates the directory where you installed JBoss:

   JBOSS_HOME/server/default/deploy/IdentityMinder.ear/user_console.war/META-INF/

   a. Locate the following files and copy them to a temporary directory:

      ac-RoleDefinitions_Iplanet_EN.xml

      ac-environmentSettings.xml

   b. Delete the ac-environment.properties files, if exists.

2. Open the CA IdentityMinder Management Console, select Environments, then select New.

   The new environment screen appears.

3. Enter **ac-env** as the name of the environment, provide a description and enter **ac** as the public URL alias, then click Next..

   A screen appears displaying a list of available directories.

4. Select the SUN ONE directory you have defined to associate with this environment, then click Next.

   a. (Optional) Select the directory to use as the provisioning directory for this environment, then click Next.

   b. (Optional) Specify the user account to authenticate anonymous connections with, then select Validate.

      CA IdentityMinder Management Console validates the user account.

5. Click Next to continue.

6. Select Import Roles from File and use Browse to locate the file ac-RoleDefinitions_iPlanet_EN.xml, click Next.

7. Specify the user manager account, select Add and then select Next.

   A summary screen opens.

   Important! Verify that the user manager account exists in the directory.

8. Review the summary and click Finish.

   CA IdentityMinder Management Console creates the environment.

9. Select Environments, ac-env, Advanced Settings, then click Import.

   The Import Settings window opens.

   a. Browse to the directory where you saved the ac-environmentSettings.xml file, select it, then click Finish.

      CA IdentityMinder Management Console creates the environment.

10. Select Continue then select Start.

    The environment starts up.

11. Select Environments, ac-env, Advanced Settings, Workflow.

    The workflow properties windows opens

    a. Check the box next to the Enabled property to enable workflow and then click save.

       CA IdentityMinder Management Console applies the changes to the environment.

12. Select Environments, ac-env, System Manager.

    The System Manager windows opens.

    a. Specify the system manager user account, then select Validate.

       CA IdentityMinder Management Console displays the system manager account properties.

    b. Select Next, Finish.

       CA IdentityMinder Management Console displays the system manager configuration output and specifies errors, if identified.

    c. Select Continue.

13. In the Status field, select Restart.

    CA IdentityMinder Management Console restarts the environment.

14. Restart the JBoss application server.

15. Open a Command Prompt window and navigate to the bin directory.
16. Run the following command to execute ComponentRegistration:

    ```
    ComponentRegistration -comp jcs -register -userDN cn=root,dc=etasa -serverDN dc=im,dc=etasa -pwd <communication_password> -port 20411 -ssl yes -file C:\temp\output.txt -verbose
    ```

    For example: ComponentRegistration -comp jcs -register -userDN cn=root,dc=etasa -serverDN dc=im,dc=etasa -pwd *password* -port 20411 -ssl yes -file C:\temp\output.txt -verbose

You have defined the SUN ONE directory as the user store for CA ControlMinder Enterprise Management. You can now log in to CA ControlMinder Enterprise Management.

Create a Directory for CA Directory

A directory provides information about a user directory that CA ControlMinder Enterprise Management manages. You configure the CA Directory settings after you install CA ControlMinder Enterprise Management.

Important! If the UID attribute in the directory does not contain a value, you must edit the SAM_CA_Directory.xml file before you create the directory. For example:

```
<ImsManagedObjectAttr physicalname="uid" displayname="User ID" description="User ID" valuetype="String" required="true" multivalued="false" wellknown="%USER_ID%" maxlength="0" permission="WRITEONCE"/>
```

Note: The UID attribute must have unique user-defined data. Each of the CA Directory attributes is mapped once to the CA ControlMinder Enterprise Management attributes in the CA Directory XML file.

Follow these steps:

1. Navigate to the following directory, where JBoss_HOME indicates the directory where you installed JBoss:

   ```
   JBoss_HOME/server/default/deploy/IdentityMinder.ear/user_console.war/META-INF/
   ```

2. Copy the following files file to a temporary directory.
   a. SAM_CA_Directory.xml
   b. ac-RoleDefinitions_CADir_EN.xml
   c. ac-environmentSettings.xml
3. Delete the ac-environment.properties file, if it exists.

4. Start the JBoss application server.
5. Open the CA IdentityMinder Management Console as follows:

   `http://enterprise_host:port/idmmanage`

   The CA IdentityMinder Management Console opens.
6. Select Directories, New.

   The new directory window opens.
7. Select Browse and locate the SAM_CA_Directory.xml file. Click Next.
8. Enter the following details:
   - **Name**—defines the directory logical name
   - **Description**—(optional) specifies a description for the directory
   - **Object Connection Name**—specifies the name of the user store
   - **Host**—defines the directory host name or IP address
   - **Port**—defines the directory port number

     Example:389
   - **Search root**—defines the organization search root. Directory search will start from the root level

     Note: Leave this field blank if you work with multiple domains
   - **User DN**—defines a user account with privileges to log in to the directory

     Example: cn=Username, ou=Administration, ou=Corporate, o=Democorp, c=AU
   - **Password**—defines the user account password
   - **Confirm password**—enter the user account password to confirm the password
   - **Secure connection**—indicates that the connection to the directory is secured
9. Click Next and Finish.

   The new directory is created. You now need to create an environment.

Create an Environment for CA Directory

Valid on Windows

After you create and configure the directory settings for CA Directory, you create an environment. An environment is a view of the user store. In an environment you manage users, groups, organizations, tasks and roles.

Note: The JBoss application server service automatically starts during Windows startup and if an environment does not exist, one is created. We recommend that you disable the automatic service startup. If the environment exists, delete it before you create the environment for CA Directory.

Before you create the environment, define the system manager account in CA Directory.

Important! Verify that you do not define the system manager account directly under the search root Organization Unit (OU) rather, under an Organization Unit that is located under the search root. For example, if the search root you defined is dc=company, dc-com, create the system manager account under the Users OU as follows: uid=Sysmanager,ou=Users,dc=company,dc=com

Note: For multiple domDN.ins support, define the user full DN.

Follow these steps:

1. Open the CA IdentityMinder Management Console, select Environments, then select New.

   The new environment screen appears.

2. Enter **ac-env** as the name of the environment, provide a description and enter **ac** as the public URL alias, then click Next.

   A screen appears displaying a list of available directories.

3. Select CA Directory to associate with this environment, then click Next.

   a. (Optional) Select the directory to use as the provisioning directory for this environment, then click Next.

   b. (Optional) Specify the user account to authenticate anonymous connections with, then select Validate.

      CA IdentityMinder Management Console validates the user account.

4. Click Next to continue.

5. Select Import Roles from File and use Browse to locate the file ac-RoleDefinitions_CADir_EN.xml, click Next.

6. Specify the user manager account, select Add and then select Next.

   Note: For multiple domains support, specify the user full DN.

   A summary screen opens.

   Important! Verify that the user manager account exists in the directory.

7. Review the summary and click Finish.

   CA IdentityMinder Management Console creates the environment.

8. Select Environments, ac-env, Advanced Settings, then click Import.

   The Import Settings window opens.

   a. Browse to the directory where you saved the ac-environmentSettings.xml file, select it, then click Finish.

      CA IdentityMinder Management Console creates the environment.

9. Select Continue then select Start.

The environment starts up.

10. Select Environments, ac-env, Advanced Settings, Workflow.

    The workflow properties windows opens

    a. Check the box next to the Enabled property to enable workflow and then click save.

       CA IdentityMinder Management Console applies the changes to the environment.

11. Select Environments, ac-env, System Manager.

    The System Manager windows opens.

    a. Specify the system manager user account, then select Validate.

       CA IdentityMinder Management Console displays the system manager account properties.

    b. Select Next, Finish.

       CA IdentityMinder Management Console displays the system manager configuration output and specifies errors, if identified.

    c. Select Continue.

12. In the Status field, select Restart.

    CA IdentityMinder Management Console restarts the environment.

13. Restart the JBoss application server.

14. Restart the CA ControlMinder services.

You have defined CA ControlMinder Enterprise Management to use CA Directory. You can now log in to CA ControlMinder Enterprise Management.

Configure the Connection to the Connector Server

CA ControlMinder Enterprise Management communicates with the Connector Server to search for and manage privileged accounts on the managed devices. By default, CA ControlMinder Enterprise Management is installed with a connector server with configuration settings that apply to the CA ControlMinder Enterprise Management computer. You can add more connector servers according to your needs.

Follow these steps:

1. In CA ControlMinder Enterprise Management, click System, Connection Management, Connector Server, Create Connector Server.

   The Create Connector Server: Select Connector Server task page appears.

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

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

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

   Name

   Defines the connection name.

   Description

   (Optional) Defines the connection description.

   Host

   Defines the Connector Server name that you want CA ControlMinder Enterprise Management to work against.

   Example: host1.comp.com

   Port

   Defines the port that the Connector Server uses to communicate.

   Example: 20411

   Secured

   Specifies whether the connection between CA ControlMinder Enterprise Management and the Connector Server is secured.

   Username

   Defines the user name of a user with management privileges.

   Example: cn=root, dc=etasa

   Password

   Defines the password of the user account with management privileges.

   Primary

   Specifies whether this is the connection that CA ControlMinder Enterprise Management uses by default when you log in.

   Note: If you specify a primary connection, log out and log back in before the connection is established.

Provisioning Domain Name

Defines the name of the provisioning domain that CA IdentityMinder manages.

Note: The domain name is case-sensitive.

Type

Specifies the type of Connector Server.

5. Click Submit.

   CA ControlMinder Enterprise Management uses the information that you specified to try to log in to the Connector Server. If the information is correct, the connection is set and you can now use CA ControlMinder Enterprise Management to manage privileged accounts. If the information is incorrect and CA ControlMinder Enterprise Management cannot log in to the Connector Server, an error message appears with the reason the connection could not be established.

Start CA ControlMinder Enterprise Management

After you install CA ControlMinder Enterprise Management you need to start CA ControlMinder and the web application server.

Follow these steps:

1. Verify that CA ControlMinder services are started.

   CA ControlMinder Enterprise Management requires that CA ControlMinder is running.

2. Verify that JBoss Application Server service is started. If JBoss Application Server services are not started, do one of the following:

   - (Windows) Click Start, Programs, CA, ControlMinder, Start Task Engine.

     Note: The Task Engine may take some time to load the first time you start it.

   - (Windows) Start the JBoss Application Server service from the Services panel.
   - (Linux) Enter ./JBOSS_HOME/bin/run.sh -b 0.0.0.0

   When the JBoss Application Server completes loading, you can log in to the CA ControlMinder Enterprise Management web-based interface.

Open CA ControlMinder Enterprise Management

Once you install and start CA ControlMinder Enterprise Management you can start the web-based interface from a remote computer using the URL for CA ControlMinder Enterprise Management.

To open CA ControlMinder Enterprise Management

1. Open a web browser and enter *one* of the following URLs, for your host:
   - To use a non-SSL connection, enter the following URL:

     http://*enterprise_host*:*port*/iam/ac
   - To use an SSL connection, enter the following URL:

     https://*enterprise_host*:*HTTPSport*/iam/ac
2. Use your credentials to log in.

   The CA ControlMinder Enterprise Management home page appears.

Note: You can also open CA ControlMinder Enterprise Management from a Windows computer where you installed it by clicking Start, Programs, CA, Access Control, Enterprise Management.

Example: Open CA ControlMinder Enterprise Management

Enter the following URL into your web browser to open CA ControlMinder Enterprise Management from any computer on the network:

```
http://appserver123:18080/iam/ac
```

The URL suggests that CA ControlMinder Enterprise Management is installed on a host named appserver123 and uses the default CA ControlMinder Enterprise Management port 18080.

Example: Open CA ControlMinder Enterprise Management Using SSL

Enter the following URL into your web browser to open CA ControlMinder Enterprise Management using SSL from any computer on the network:

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

The URL suggests that CA ControlMinder Enterprise Management is installed on a host named appserver123 and uses the default CA ControlMinder Enterprise Management SSL port 18443.

Advanced Configuration

You use the CA IdentityMinder Management Console to perform advanced configuration tasks. These tasks include modifying the reporting database properties to generate custom reports and configuring CA ControlMinder Enterprise Management to send email notifications when a specific event occurs.

The CA IdentityMinder Management Console lets you create and manage environments that control the management and graphical presentation of a directory.

Note: For more information, see the *CA IdentityMinder Management Console Online Help*, which you can access from the application.

More information:

Enable the CA IdentityMinder Management Console (see page 87)
Open the CA IdentityMinder Management Console (see page 88)
Setting Up Email Notifications for Events (see page 88)

Enable the CA IdentityMinder Management Console

When you install the Enterprise Management Server for the first time, the CA IdentityMinder Management Console option is disabled. To enable the CA IdentityMinder Management Console, change the default settings.

Important!: Complete the following procedure only if you selected to use Active Directory or the embedded user store during installation.

To enable the CA IdentityMinder Management Console

1. Stop JBoss if it is running. Do *one* of the following:
   - From the JBoss job windows, interrupt (Ctrl+C) the process.
   - Stop the JBoss Application Server service from the Services Panel.
2. Navigate to the following directory, where *JBoss_HOME* is the directory where you installed JBoss:

   ```
   JBoss_HOME/server/default/deploy/
   IdentityMinder.ear/management_console.war/WEB-INF
   ```
3. Open the *web.xml* file in an editable form.
4. Search for the following section:

   ```
   AccessFilter
   ```

5. In the <param-value> field, change the value to True.
6. Save and close the file.
7. Start JBoss.

   The CA IdentityMinder Management Console is enabled.

Open the CA IdentityMinder Management Console

The CA IdentityMinder Management Console has a web-based interface. Once you enable the CA IdentityMinder Management Console and start CA ControlMinder Enterprise Management, you can open the CA IdentityMinder Management Console from any computer on your network.

To open the CA IdentityMinder Management Console, open a web browser and enter the following URL, for your host:

`http://enterprise_host:port/idmmanage`

The CA IdentityMinder Management Console opens.

Example: Open the CA IdentityMinder Management Console

Enter the following URL into your web browser to open the CA IdentityMinder Management Console from any computer on the network:

`http://appserver123:18080/idmmanage`

In this example, the CA IdentityMinder Management Console is installed on a host named appserver123 and uses the default CA ControlMinder Enterprise Management port 18080.

Setting Up Email Notifications for Events

This scenario describes how a system administrator configures email notifications for events, such as when users request shared account passwords or check out account passwords.

Email Notifications

Email notifications are generated from email templates and inform CA ControlMinder Enterprise Management users of events in the system. It is a best practice to enable email notifications for events related to approval workflows.

When you enable email notifications, the Enterprise Management Server generates 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 ControlMinder Enterprise Management user is created or modified.

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

How Email Notifications Work

Email notifications inform users of events in the system.

1. When an event occurs, CA ControlMinder Enterprise Management checks if an email notification is enabled for the event.
2. If an email notification is enabled, CA ControlMinder 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 ControlMinder Enterprise Management looks in the Approved subdirectory.
3. CA ControlMinder 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 ControlMinder Enterprise Management sends that email template to the recipients.
   - If an email template with the same name as the event does not exist, CA ControlMinder Enterprise Management sends the defaultEvent.tmpl email template to the recipients.

Example

The following use case is an example of events and of notifications that are sent for them.

1. A user requests to use an account next Tuesday. An email is sent to the approver to let her know she has a request in her worklist.

   A CreatePrivilegedAccountExceptionNotStartedEvent notification is sent to the 'pending' folder.

2. The approver approves the request. The user receives an email to inform him that the request was approved.

   A CreatePrivilegedAccountExceptionNotStartedEvent notification is sent to the 'approved' folder.

3. On Tuesday the account becomes available to the user. The user receives an email to inform him that he can start working with the account.

   A CreatePrivilegedAccountExceptionEvent notification is sent to the 'completed' folder.

4. Tuesday is over and the account is no longer available to the user. The user receives an email to inform him that he no longer has access to the account.

   A DeletePrivilegedAccountExceptionEvent is sent to the 'completed' folder.

The most commonly used events are:

BreakGlassCheckOutAccountEvent

Sends a notification to the approver when a privileged account performs a Break Glass action.

CheckOutAccountPasswordEvent

Sends a notification to the approver every time a password is checked out.

CreatePrivilegedAccountExceptionEvent

Sends a notification to the requestor if an account is available. If you want to enable notification for this event, edit the template in the “completed” folder.

CreatePrivilegedAccountExceptionNotStartedEvent

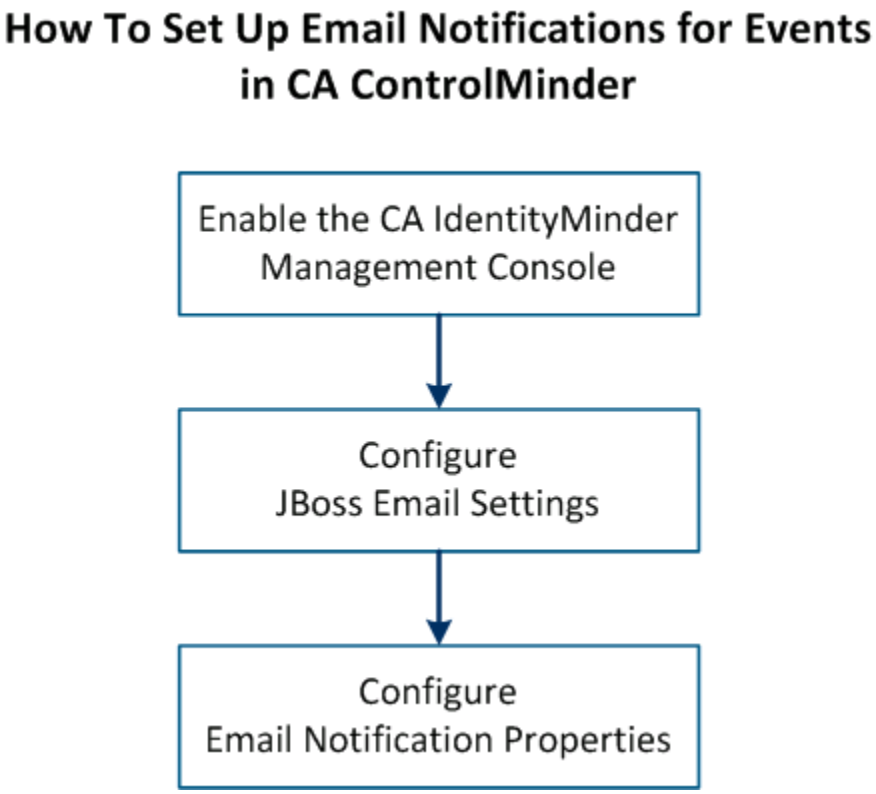
Sends a notification to the approver that a request for access to a privileged account is pending in his worklist. Sends notifications to the requestor when the request is approved, rejected, or completed.

How To Set Up Email Notifications for Events

You use the CA IdentityMinder Management Console to set email notification options and define the reporting database settings in an environment.

When you open the CA IdentityMinder Management Console, you work in an *environment*. An environment controls the management and graphical presentation of a directory. For example, you can set email notification options and define the reporting database settings in an environment. We recommend that you only enable email notifications for SAM events.

Important! Changes you make to the environment may affect the stability of CA ControlMinder Enterprise Management. For assistance, contact CA Support at http://ca.com/support.



Follow these steps:

1. Enable the CA IdentityMinder Management Console (see page 87)
2. Configure JBoss Email Settings (see page 92)
3. Configure Email Notification Properties (see page 94)

Configure JBoss Email Settings

To send email notifications, you configure the mail-service.xml and email.properties files in your JBoss installation, and modify existing CA ControlMinder email templates accordingly.

Follow these steps:

1. Connect to the Enterprise Management machine and stop JBoss if it is running. Do *one* of the following:
   - If JBoss is not installed as a service, interrupt the JBoss application server window (Ctrl+C).
   - If JBoss is installed as a service, stop the JBoss service from the Services panel.
2. Open the mail-service.xml file for editing. By default, the file is located in a subdirectory of your JBoss installation directory:

   JBOSS_HOME/server/default/deploy/mail-service.xml
3. Locate the "mail.smtp.host" entry in mail-service.xml. Change the SMTP host default value to the full DNS domain name of your outgoing email server (the SMTP server).

   ```
   <property name="mail.smtp.host" value="mail.ca.com" />
   ```

   Note: The hosts file on the Enterprise Management Server must be able to resolve the full DNS domain name that you specify for this property to the IP address of the SMTP server.
4. Specify the email address of the notification sender.

   ```
   <property name="mail.from" value="sendername@ca.com" />
   ```
5. (Optional) Enable SMTP authentication and TLS security by providing the SMTP user name and password, and by adding SMTP configuration properties.

   ```
   <attribute name="User">MySMTPUser</attribute>
   <attribute name="Password">MySMTPPassword</attribute>
   <attribute name="Configuration">
     <configuration>
       <property name="mail.smtp.auth" value="true"/>
       <property name="mail.smtp.starttls.enable" value="true"/>
     </configuration>
   </attribute>
   ```

   Note: If you are using an SMTP service that does not require authentication, you can skip this step.

Do the following for each event for which you want to configure email notifications.

Follow these steps:

1. Open the email template that corresponds to the event.

   Examples:

   a. To configure email notifications that informs recipients that a privileged account password request was approved, open the CreatePrivilegedAccountExceptionEvent.tmpl file in the following directory:

   JBoss_HOME/server/default/deploy/IdentityMinder.ear/custom/emailTemplates/default/approved

   b. To configure an email notification that informs recipients about a pending endpoint status, open the EndpointStatusEvent.tmpl file in the following directory:

   JBoss_HOME/server/default/deploy/IdentityMinder.ear/custom/emailtemplates/default/pending

2. Modify the template host name and port from 'http://localhost:8080/iam/ac" to the Enterprise Management Server host name and port, for example, "https://computer.com:18443/iam/ac".

3. Save and close the file.

Configure the email.properties file.

Follow these steps:

1. Browse to the following directory and open the email.properties file.

   JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/config/

2. Specify the same sender email address as in the mail-service.xml file, using the following format.

   admin.email.address=*sendername@ca.com*

3. Save and close the email.properties file.

4. Restart JBoss.

Configure Email Notification Properties

Open the CA IdentityMinder Management Console to configure email notification properties in your environments.

Note: For more information about environments, see the *CA IdentityMinder Management Console Online Help*, which is available from the console.

Important! Changes you make to the environment may affect the stability of CA ControlMinder Enterprise Management. For assistance, contact CA Support at http://ca.com/support.

Follow these steps:

1. Click Environments. Click the environment that you want to configure, then click Advanced Settings, E-mail.

   The E-mail Properties window appears.

2. Configure the applicable options for your enterprise, as follows:

   Events e-mail Enabled

   Enables email notifications for CA ControlMinder Enterprise Management events, including SAM events.

   Tasks e-mail Enabled

   Enables email notifications for CA ControlMinder Enterprise Management tasks. We recommend that you do not enable email notifications for tasks, because CA ControlMinder Enterprise Management does not provide email templates for tasks.

   Template Directory

   Specifies the location of the email templates that CA ControlMinder Enterprise Management uses to create the email messages. Set this value to "default".

   Note: The email templates are located in the following directory:

   JBoss_HOME`/server/default/deploy/IdentityMinder.ear/custom/emailTemplates/default/`

3. Specify the events for which you want email notifications to be sent.

   We recommend that you specify only SAM events for which email templates are provided. Do the following:

   a. Select the check box next to every event, *except for* the following SAM events:

      - CreatePrivilegedAccountExceptionNotStartedEvent
      - CreatePrivilegedAccountExceptionEvent
      - BreakGlassCheckOutAccountEvent
      - CheckOutAccountPasswordEvent

   b. Click Delete.

      All but the SAM events are deleted. You have configured CA ControlMinder Enterprise Management to send email notifications for these SAM events.

4. Click Save.

   The email notification properties are saved, and you return to the Environment Properties window.

5. Click Restart.

   The CA IdentityMinder Management Console restarts the environment and applies your changes.

Note: For more information about email notifications, see the *Enterprise Administration Guide*.

Email Templates

CA ControlMinder 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 ControlMinder 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. ■ CreatePrivilegedAccountExceptionEvent—Informs recipient that a requested account is available. ■ CreatePrivilegedAccountExceptionNotStartedEvent.tmpl—Informs recipient that a request for access to a privileged account is pending in the worklist. ■ defaultEvent.tmpl—Informs recipients that CA ControlMinder Enterprise Management completed an event. ■ defaultTask.tmpl—Informs recipients that CA ControlMinder 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. ■ CheckOutAccountPasssswordEvent.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.

Uninstall CA ControlMinder Enterprise Management on Windows

Valid on Windows

To uninstall CA ControlMinder Enterprise Management on Windows, you must be logged in to the Windows system as a user with Windows administrative privileges (that is, the Windows administrator or a member of the Windows Administrators group).

Note: This procedure does not uninstall the prerequisite software. If you want to uninstall the prerequisite software, you must uninstall JBoss before you uninstall the JDK. For more information about uninstalling prerequisite software, refer to the product documentation.

To uninstall CA ControlMinder Enterprise Management on Windows

1. Stop JBoss if it is running.
2. Click Start, Control Panel, Add or Remove Programs.

   The Add or Remove Program dialog appears.
3. Scroll through the program list and select CA ControlMinder Enterprise Management.
4. Click Change/Remove.

   The Uninstall CA ControlMinder Enterprise Management wizard appears.
5. Follow the wizard instructions to uninstall CA ControlMinder Enterprise Management.

   The uninstall completes and removes CA ControlMinder Enterprise Management from your computer.
6. Click Done to close the wizard.

Uninstall CA ControlMinder Enterprise Management on Linux

If you want to remove CA ControlMinder Enterprise Management from your computer you need to use the uninstall program that CA ControlMinder Enterprise Management provides.

Follow these steps:

1. Stop JBoss by doing *one* of the following:
   - From the JBoss job windows, interrupt (Ctrl+C) the process.
   - From a separate window, type:

     `./JBoss_path/bin/shutdown -S`
2. Enter the following command:

   `"/ACPMInstallDir/Uninstall_EnterpriseManagement/Uninstall_CA_Access_Control_Enterprise_Management"`

   ACPMInstallDir

   Defines the installation directory of CA ControlMinder Enterprise Management. By default this path is:

   `/opt/CA/AccessControlServer/`

   InstallAnywhere loads the uninstall wizard or console.
3. Follow the prompts to uninstall CA ControlMinder Enterprise Management.

   The uninstall completes and removes CA ControlMinder Enterprise Management from your computer.

Remove Additional Components from the Enterprise Management Server

To completely uninstall CA ControlMinder Enterprise Management, you remove additional components from the computer after you run the uninstallation program.

To prevent the loss of business data, the uninstall program does not remove the following resources:

- CA ControlMinder Endpoint Management filters, located at *JBoss_Dir*/server/default/conf/accesscontrol
- Message Queue data files, located at *ACServerDir*/MessageQueue/tibco/ems/data

To remove additional components from the Enterprise Management Server

1. Delete the following directories:
   - *JBoss_Dir*/server/default/deploy/IdentityMinder.ear
   - *JBoss_Dir*/server/default/deploy/SiteMinderAgent.ear

2. Uninstall CA ControlMinder.
3. (Windows) Delete the following registry key:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\uninstall\CA Access Control Advanced Policy Management Server
4. Delete the JCS, as follows:
   a. (Windows) Use the Add or Remove Programs dialog to uninstall CA IdentityMinder – Connector Server.
   b. Terminate the jcs.exe process.
   c. Delete the CA IdentityMinder – Connector Server (Java) service.
5. Delete the directory in which you installed the Enterprise Management Server.

   For example, delete C:\Program Files\CA\AccessControlServer

   All CA ControlMinder Enterprise Management components are now removed from the computer.

More information:

Uninstallation Methods (see page 173)

Implementing the Distribution Server

The Distribution Server handles communication between the Enterprise Management Server and the endpoints. The Distribution Server is installed by default on the Enterprise Management Server. For scalability purposes to manage endpoints that are located behind firewalls, you can add more than one Distribution Servers in your enterprise.

Install the Distribution Server

The following procedure takes you through the steps of installing the Distribution Servers.

Follow these steps:

1. Insert the appropriate CA ControlMinder Server Components DVD for your operating system into your optical disc drive.
2. Complete the following steps:
   - On Windows:

     If you have autorun enabled, the Product Explorer automatically appears. Perform the following steps:

     a. If the Product Explorer does not appear, navigate to the optical disc drive directory and double-click the ProductExplorerx86.EXE file.

     b. Expand the Components folder in the Product Explorer, select CA ControlMinder Distribution Server, then click Install
   - On Linux:

     a. Mount the optical disc drive.

     b. Open a terminal window and navigate to the following directory on the optical disc drive:

     /DistServer/Disk1/InstData/NoVM

     c. Run the following command:

     ```
     ./install_DistServer.bin -i console
     ```
3. Complete the wizard as required. The following installation inputs are not self-explanatory:

   Message Queue Settings

   Defines the Message Queue server administrator password (Communication Password).

   Limits: Minimum of six (6) characters

   Java Connector Server - Provisioning Directory Information

   Defines the password for the Java Connector Server.

   The CA ControlMinder Distribution Server installation is complete.

   Important! Verify that you specify the same Communication Password you defined while installing the Enterprise Management Server. The Enterprise Management Server uses the communication password to manage the Message Queue keystore, administrator account, handle communication between CA Access Control Enterprise Management and the endpoints, and manage the Java Connection Server.

More information:

Set Up the Production Distribution Server (see page 437)
Set Up the Disaster Recovery Distribution Server (see page 439)

Chapter 5: Implementing Enterprise Reporting

This section contains the following topics:

Enterprise Reporting Capabilities

CA ControlMinder Enterprise Management provides reporting capabilities through a CA Business Intelligence Common Reporting server (CA ControlMinder Reports Portal). Enterprise reporting lets you view the security status of each endpoint (users, groups, and resources) from a central location. CA ControlMinder reports describe the rules and policies on each endpoint that determine who can do what, and any policy deviations.

Once configured, CA ControlMinder enterprise reporting works independently to collect data from each endpoint and to store the information in the central server on a continues basis without the need for manual intervention. 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. Each endpoint reports on its status whether the collection server is up or down.

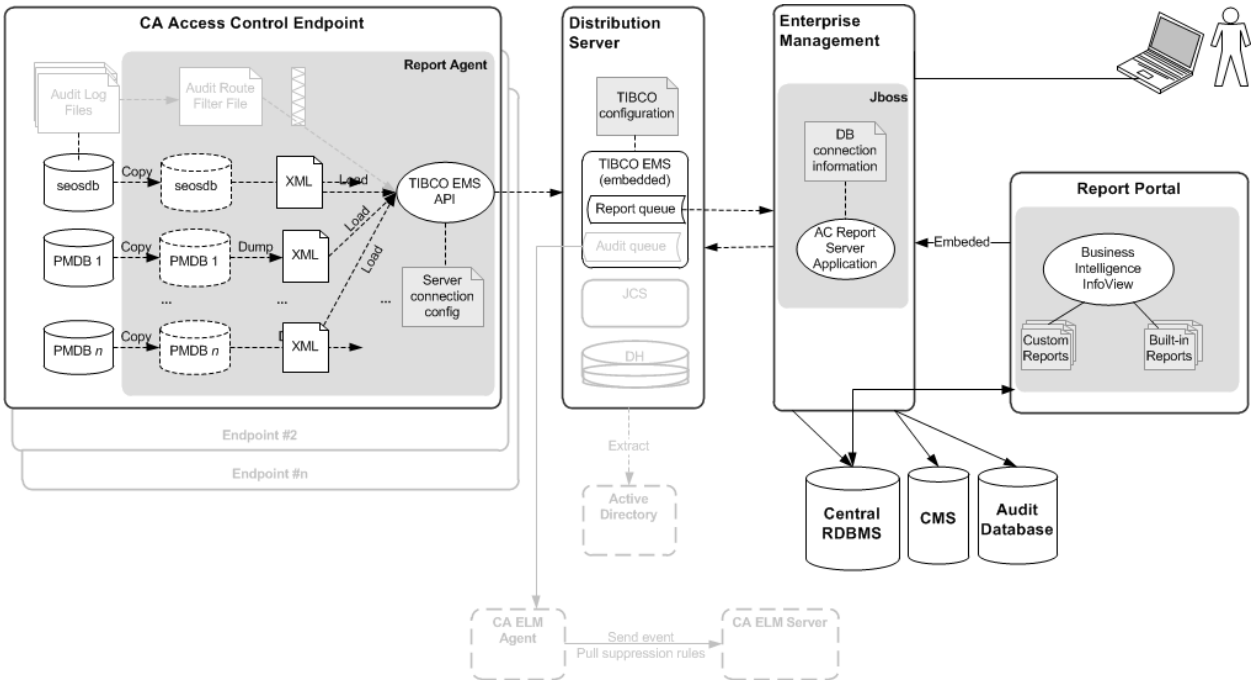
Reporting Service Architecture

The CA ControlMinder reporting service provides a server-based platform for CA ControlMinder enterprise reporting. You can use this platform to create reports that contain data from all your CA ControlMinder endpoints. The reports that you create can be viewed and managed over a web-enabled application.

The reporting service lets you build a reporting environment on top of an existing CA ControlMinder infrastructure.

Note: For more information about enterprise reporting, see the *Enterprise Administration Guide*.

The following diagram shows the architecture of reporting services components. The diagram also shows the flow of data among the components.



The preceding diagram illustrates the following:

- Each endpoint, which contains a CA ControlMinder database (seosdb) and any number of Policy Models (PMDB), has the Report Agent component installed.
- The Report Agent collects data from the endpoint and sends it to the Distribution Server for processing.
- In a simple enterprise model, one Distribution Server processes all endpoint data and sends it to the central database for storage. You can also replicate Distribution Server components to design for fault tolerance and faster processing in large enterprise environments.
- The central database (an RDBMS) stores endpoint data.
- The Report Portal lets you access the data in the central database to produce built-in reports, or to interrogate the data and produce custom reports.

How to Set Up Reporting Service Server Components

To use enterprise reporting, install and configure the CA ControlMinder reporting service server components. After you install and configure the server components, configure the Report Agent on each endpoint.

Note: Report Agent installation and configuration are part of the CA ControlMinder and UNAB endpoint installation and are not covered in this procedure.

To set up reporting service server components, follow these steps:

1. If you have not already done so, install and configure the Enterprise Management Server.
2. Set up the Report Portal computer (CA Business Intelligence).

   You can find the CA Business Intelligence installation files on the CA Support website.
3. Deploy the CA ControlMinder report package on the Report Portal.
4. Configure the connection to CA Business Intelligence.
5. Create a snapshot definition.

   You can now generate and view reports in CA Business Intelligence and CA ControlMinder Enterprise Management.

Note: For more information about generating and viewing reports, see the *Enterprise Administration Guide*.

More information:

Configure a Windows Endpoint for Reporting (see page 171)
Configure a UNIX Endpoint for Reporting (see page 254)
Configure UNAB for Reporting (see page 345)

How to Set Up the Report Portal Computer

The Report Portal lets you access the endpoint data that CA ControlMinder Enterprise Management stores in the central database to produce built-in reports, or to interrogate the data and produce custom reports. The Report Portal uses CA Business Intelligence.

Note: If you already have an older version of the Report Portal or a standalone installation of CA Business Intelligence or BusinessObjects Enterprise XI, you do not need to upgrade and can use the existing installation instead.

To set up the Report Portal, do the following:

1. If you use an Oracle database, install a full Oracle client on the Report Portal computer.
2. If you use Microsoft SQL Server, install the Microsoft SQL Server Native Client on the Report Portal computer.
3. If you have not already done so, set up the central database and Distribution Server.

   Note: You set up the central database and Distribution Server when you install the Enterprise Management Server.
4. (UNIX) If the Report Portal computer is a Solaris or a Linux computer, prepare the UNIX computer for CA Business Intelligence installation.
5. Synchronize the system times of the Report Portal computer and the Enterprise Management Server.

   If you do not synchronize the system times, reports that CA ControlMinder Enterprise Management generates will remain in a pending or recurring status.
6. Install CA Business Intelligence for your operating system.

   You can find the CA Business Intelligence installation files on the CA Support website.

   Note: Report Portal for Windows authenticates connections using Microsoft SQL Server Authentication by default. You can configure the Report Portal to work in Windows Authentication (see page 477)if you want to use a domain user account settings for authentication.

   The Report Portal is set up and you can now deploy the CA ControlMinder report package.

Note: For more information about CA Business Intelligence, see the *CA Business Intelligence Installation Guide*, which is available from CA Technologies Support.

Example: Install CA Business Intelligence on Windows

The following procedure demonstrates how you can install CA Business Intelligence on Windows:

Note: The installation can take approximately an hour to complete.

1. Insert the CA Business Intelligence for Windows DVD into your optical disc drive.
2. Navigate to the \Disk1\InstData\VM folder and double-click install.exe.

   The CA Business Intelligence installation wizard begins.

3. Complete the installation wizard using the following table:

Information	Action
Installation language	Select a supported installation language you want to use, then click OK. **Note:** You need a localized operating system to install in any of the supported non-English languages.
License Agreement	Select I accept the terms of the License Agreement and click Next.
Installation Type	Select Typical and click Next
Non-Root Credentials	Enter a non-root user name and password.
BusinessObjects XI Administrator Password	Type P@ssw0rd twice to set and confirm the password and click Next. **Note:** For password rules, see the *CA Business Intelligence Installation Guide*, which is available from the CA ControlMinder bookshelf.
Web Server Configuration	Click Next to accept the defaults.
CMS Database Settings	Enter the following information, then click Next: ■ **MySQL Root Password:** P@ssw0rd ■ **User Name:** cadbusr ■ **Password:** C0nf1dent1al ■ **Database Name:** MySQL1 **Note:** The CA Business Intelligence Central Management Server (CMS) is used for internal management purposes only.
Enable Auditing	Click Next to accept the defaults.
Audit Database Settings	Enter the following information, then click Next: ■ **User Name:** cadbusr ■ **Password:** C0nf1dent1al ■ **Database Name:** MySQL1
Review Settings	Review the settings and click Install to complete the installation.

The installation starts and can take up to an hour to complete.

Important! The CA Business Intelligence Central Management Server (CMS) is used for internal management purposes only and does not contain the report data that is used to generate and display the reports. The reporting database that you defined when you installed CA ControlMinder Enterprise Management, contains data that the Report Agent uploads to the Distribution Server. For more information about the CMS, see to the *CA Business Intelligence Installation Guide*.

Prepare Linux for CA Business Intelligence Installation

Before you can install CA Business Intelligence on Linux, you prepare the computer for installation. You create a non-root user for the CA Business Intelligence installation, verify that the Oracle RDBMS is exposed to the installation of CA Business Intelligence and set the environment variables.

Follow these steps:

1. Log in as a root user.
2. Create a non-root user. The CA Business Intelligence installation requires a non-root user.

   For example, enter the following commands to create a user named bouser that belongs to the group other:

   ```
   groupadd other
   useradd -d /home/bouser -g other -m -s /bin/bash -c bouser bouser
   passwd bouser
   ```

   When prompted, enter and confirm a password for the user you defined.
3. Verify that the LANG environment variable is configured as follows:

   ```
   LANG=en US.utf8
   ```
4. Log in as the non-root user you created.

5. Enter the following commands to verify that the ORACLE_HOME and TNS_ADMIN environment variables are set correctly:

   ```
   echo $ORACLE_HOME
   echo $TNS_ADMIN
   ```

   A non-empty output verifies that these environment variables are valid. For example:

   ```
   /opt/oracle/app/oracle/product/10.2.0/client_1
   /opt/oracle/app/oracle/product/10.2.0/client_1/admin/network
   ```

   If you receive an empty output for the commands, verify that the variables are set for the non-root user you created. For example, edit /home/bouser/.profile as follows:

   ```
   ORACLE_HOME=/opt/oracle/app/oracle/product/10.2.0/client_1
   export ORACLE_HOME
   TNS_ADMIN=$ORACLE_HOME/network/admin
   export TNS_ADMIN
   ```

6. Verify that LD_LIBRARY_PATH for your non-root user contains the following paths:

   ```
   $ORACLE_HOME/lib:$ORACLE_HOME/lib32
   ```

   For example, type the following command and search the output for these paths:

   ```
   echo $LD_LIBRARY_PATH
   ```

   If these paths are missing, append them to LD_LIBRARY_PATH. For example, edit /home/bouser/.profile as follows:

   ```
   LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib:$ORACLE_HOME/lib32
   export LD_LIBRARY_PATH
   ```

7. Verify that the folders in LD_LIBRARY_PATH and TNS_ADMIN are accessible, as follows:

   ```
   ls -l $ORACLE_HOME
   ls -l $TNS_ADMIN/tnsnames.ora
   ```

   The commands should not return a **permission denied** error. If they do, you must grant proper permissions. For example, the root/oracle user should run the following command:

   ```
   chmod -R +xr $ORACLE_HOME
   ```

8. Verify that Oracle connectivity is valid, using the TNS Ping utility as follows:

   ```
   $ORACLE_HOME/bin/tnsping service_name
   ```

   The output from TNS Ping should look be similar to the following example:

   ```
   TNS Ping Utility for Solaris: Version 10.2.0.1.0 - Production on 07-MAY-2008
   09:17:02
   Copyright (c) 1997, 2005, Oracle.  All rights reserved.
   Used parameter files:
   /opt/oracle/app/oracle/oracle/product/10.2.0/client_1/network/admin/sqlnet.or
   a
   Used TNSNAMES adapter to resolve the alias
   Attempting to contact (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL =
   TCP)(HOST = 172.16.234.75)(PORT = 1521))) (CONNECT_DATA = (SERVICE_NAME =
   service_name)))
   OK (30 msec)
   ```

   You can now install CA Business Intelligence on Linux.

Report Package Deployment

The report package is a .BIAR file, which deploys the CA ControlMinder standard reports. It contains a collection of artifacts and descriptors for deployment on the Report Portal. To make use of these standard reports, you need to import the report package file into BusinessObjects InfoView.

Note: The package is backwards compatible with previous versions of the Report Portal. You do not need to upgrade the Report Portal to make use of the latest report package. You can also deploy localized report packages, which are provided as separate .biar files, alongside each other.

Deploy the Report Package on the Report Portal

To use the standard CA ControlMinder reports, import the report package file into BusinessObjects InfoView.

Note: This procedure describes how you deploy a report package on the Report Portal when no previous version of the same package is already deployed.

Follow these steps:

1. Verify that the central database, Distribution Server, and Report Portal are set up.

   Note: Verify that the JAVA_HOME variable is set up on the Report Portal computer.

2. Insert the CA Business Intelligence for Windows DVD into your optical disc drive and navigate to the \Disk1\cabi\biconfig folder.

3. Copy the contents of the biconfig directory into a temporary directory.

4. Insert the appropriate CA ControlMinder Server Components DVD for your operating system into your optical disc drive and navigate to the \ReportPackages folder.

5. Copy the following files from the optical disc into the same temporary directory:

   - \ReportPackages*RDBMS**import_biar_config*.xml
   - \ReportPackages*RDBMS**AC_BIAR_File*.biar

   RDBMS

   Defines the type of RDBMS used for CA ControlMinder reporting.

   Values: Oracle, MSSQL2005

   ***import_biar_config*.xml**

   Defines the name of the import configuration file (.xml) for your RDBMS.

   Values: import_biar_config_oracle10g.xml, import_biar_config_oracle11g.xml, import_biar_config_mssql_2005.xml

   Note: If you use MS SQL Server 2008 as your central database, configure the import_biar_config_mssql_2005.xml file.

   ***AC_BIAR_File*.biar**

   Defines the name of the CA ControlMinder reports file (.biar) for your language and RDBMS.

   Note: The <biar-file name> property of the import configuration file for your RDBMS points to this file. The property is set by default to the name of the English version for your RDBMS.

6. Edit your copy of the *import_biar_config*.xml file. Define the following XML properties:

   <biar-file name>

   Defines the full pathname to the CA ControlMinder reports file (.biar). You copied the file in the previous step.

   <networklayer>

   Defines the network layer supported by your RDBMS.

   Values (Windows):

   - OLE DB—for MS SQL Server authentication mode.
   - Oracle OCI
   - ODBC—for Windows Authentication mode.

   <rdms>

   Defines the type of RDBMS used for CA ControlMinder reporting.

   Values (Oracle OCI): Oracle 10 or Oracle 11

   Values (ODBC): Generic ODBC datasource

   Values (OLE DB): MS SQL Server 2005, MS SQL Server 2008 or any value *except* Oracle 10 or Oracle 11

   Note: For more information about the values that you can specify for this property, see the CA Business Intelligence documentation.

   <username>

   Defines the user name of the RDBMS administrative user you created when you prepared the central database for Enterprise Management.

   <password>

   Defines the password of the RDBMS administrative user you created when you prepared the central database for Enterprise Management.

   <datasource>

   Defines *one* of the following:

   - (Oracle) The name of the database
   - (SQL Server 2005 or 2008) The database you created
   - (ODBC) The DSN you created

   Important! Specify the name of the database used by CA ControlMinder for reporting and not the CA Business Intelligence CMS.

   <server>

   Defines the name of the SQL Server 2005 or 2008 computer. Leave this value empty for Oracle Database 10g, 11g, and ODBC.

7. Perform the following:

   - Open a command prompt and enter the following command:

     System_Drive:\BO\biconfig.bat -h *host_name* -u *user_name* -p *password* -f *ac_biar_config*.xml

     host_name

     Defines the Report Portal host name.

     user_name

     Defines the Report Portal administrator you configured when you installed the Report Portal.

     password

     Defines the password for the Report Portal administrator.

     For example:

     ```
     biconfig.bat -h reportportal.comp.com -u Administrator -p P@ssw0rd -f
     C:\BO\import_biar_config_oracle11g.xml
     ```

   - (UNIX) Set the execute permission for the script file biconfig.sh and execute it as follows:

     temp_dir/biconfig.sh -h *host_name* -u *user_name* -p *password* -f *ac_biar_config*.xml

     For example:

     ```
     biconfig.sh -h reportportal.comp.com -u Administrator -p P@ssw0rd -f
     /tmp/rp/import_biar_config_orcl.xml
     ```

   The batch file imports the CA ControlMinder reports into InfoView. The import can take a few minutes to complete. A log file (biconfig.log) is created in the same folder as the batch file and indicates whether the import was successful.

Example: Sample Oracle Database 11g Import Configuration File

The following code snippet is an example of an edited import configuration file (import_biar_config_oracle11g.xml) for Oracle Database 11g:

```
<?xml version="1.0"?>
<biconfig version="1.0">
  <step priority="1">
    <add>
      <biar-file name="c:\temp\AccessControl_R12.5_EN_ORCL_22_JUN_2009.biar">
        <networklayer>Oracle OCI</networklayer>
        <rdms>Oracle 11</rdms>
        <username>root</username>
        <password>P@ssw0rd</password>
        <datasource>orcl</datasource>
        <server></server>
      </biar-file>
    </add>
  </step>
</biconfig>
```

Example: Sample Microsoft SQL Server 2005 Import Configuration File

The following code snippet is an example of an edited import configuration file (import_biar_config_mssql2005.xml) for MS SQL Server 2005:

```
<?xml version="1.0"?>
<biconfig version="1.0">
  <step priority="1">
    <add>
      <biar-file name="c:\temp\AccessControl_R12.5_EN_SQL_11_JUN_2009.biar">
        <networklayer>OLE DB</networklayer>
        <rdms>MS SQL Server 2005</rdms>
        <username>dbAdmin</username>
        <password>P@ssw0rd</password>
        <datasource>r125db</datasource>
        <server>rdbms.org</server>
      </biar-file>
    </add>
  </step>
</biconfig>
```

More information:

Configure a Windows Endpoint for Reporting (see page 171)
Configure a UNIX Endpoint for Reporting (see page 254)

Configure BusinessObjects for Large Deployments

To run CA ControlMinder reports on large deployments, you need to change the BusinessObjects default configuration. You change the maximum number of concurrent connections that the BusinessObjects page server can create (the default is 20,000). You also change the maximum number of values that are shown in input parameters selection lists.

To configure BusinessObjects for large deployments

1. Change the number of concurrent connections that the BusinessObjects page server can create:
   a. On the Report Portal computer, click Start, Programs, Crystal Enterprise, Central Configuration Manager (CCM).

      The BusinessObjects Configuration Manager opens.

   b. Right-click Crystal Page Server and select stop.

   c. Right-click Crystal Page Server and select Properties.

   d. Verify that the following text appears after *-restart* in the Path to Executable field:

      ```
      -maxDBResultRecords 0
      ```

   e. Restart the BusinessObjects page server.

2. Change the maximum number of values that are shown in the input parameters selection lists for reports:
   a. Open the Windows Registry Editor.

   b. Navigate to the following registry key:

      ```
      HKEY_CURRENT_USER\Software\Business Objects\Suite
      12.0\CrystalReports\DatabaseOptions
      ```

   c. Click Edit, New, DWORD Value.

      A new registry entry of type REG_DWORD appears.

   d. Rename the entry to *QPMaxLOVSize*.

   e. Double-click the entry and edit its Value data to 1000.

      The new registry entry is set.

   f. Open BusinessObjects Central Management Console (CMC).

   g. Navigate to the Servers management area.

h. Click the Web Intelligence Report Server whose settings you want to change.

The Web Intelligence Report Server page opens in the Properties tab.

i. Modify the following values to more than 1000 or as required:

- List of Values Batch Size
- Maximum Size of List of Values for Custom Sorting

Click Apply to submit changes and restart the server so that the changes take effect immediately.

Configure the Connection to CA Business Intelligence

CA ControlMinder Enterprise Management provides reporting capabilities through a CA Business Intelligence Common Reporting server (CA ControlMinder Report Portal). After installing the Report Portal and deploying the reports, you need to configure the connection from CA ControlMinder Enterprise Management to CA Business Intelligence. You use the CA IdentityMinder Management Console to configure this connection.

To configure the connection to CA Business Intelligence

1. Enable the CA IdentityMinder Management Console (see page 87).
2. Open the CA IdentityMinder Management Console (see page 88).
3. Click Environments, ac-env, Advanced Settings, Reports.

   The Reports Properties window appears.
4. Enter the database and Business Objects properties.

   Important! The CA Business Intelligence Central Management Server (CMS) is used for internal management purposes only and does not contain the report data that is used to generate and display the reports. For more information about the CMS, see the *CA Business Intelligence Installation Guide*.

   Note: For more information, see the *CA IdentityMinder Management Console Online Help*, which you can access from the application.

   Important! In the Business Objects Port field, enter the port number that the Report Portal uses. The default port is 8080. In the Business Objects Report folder field, enter ControlMinder.
5. Click Save.

   The CA Business Intelligence settings are saved.

Note: For more information about CA Business Intelligence, see the *CA Business Intelligence Installation Guide*, which is available from CA Technologies Support.

Create a Snapshot Definition

Reports are based on data snapshots that are collected from CA ControlMinder and UNAB endpoints and stored in the central database, on SAM data from CA ControlMinder Enterprise Management, and on data from the user store.

You create a snapshot definition and capture snapshot data before you can run and view CA ControlMinder reports. A snapshot definition specifies the report data that CA ControlMinder collects and the schedule for data collection.

The snapshot parameter XML file specifies the report data that CA ControlMinder collects. By default, this file specifies to include all CA ControlMinder and UNAB endpoints, SAM data, and data from the user store in the report snapshot. You can customize the snapshot parameter XML file to limit the scope of the report snapshot.

To help ensure that the reports contain the most up-to-date data, do not schedule the snapshot to run more often than the endpoint snapshots. For example, if you configure your endpoints to send a snapshot each week and configure CA ControlMinder Enterprise Management to capture a snapshot each day, report data is collected weekly from the endpoints but daily from SAM and the user store, and out-of-date endpoint data appears in the reports.

Important! Do not enable more than one snapshot definition. CA ControlMinder Enterprise Management cannot successfully run all reports if more than one snapshot definition is enabled.

Note: By default, you must have the System Manager role to create a snapshot definition.

Follow these steps:

1. In CA ControlMinder Enterprise Management, do as follows:
   a. Click Reports.
   b. Click the Tasks subtab.
   c. Expand the Manage Snapshot Definition tree in the task menu on the left.

      The Create Snapshot Definition task appears in the list of available tasks.
2. Click Create Snapshot Definition.

   The Create Snapshot Definition: Select Snapshot Definition page appears.
3. Click OK.

   The Create Snapshot Definition page appears.

4. Complete the following fields in the Profile tab:

Snapshot Definition Name

Defines the name of the snapshot definition.

Snapshot Definition Description

Specifies any additional information to describe the snapshot definition.

Enabled

Specifies that CA ControlMinder Enterprise Management enables the snapshot definition.

Note: If you do not select this checkbox, CA ControlMinder Enterprise Management does not capture snapshots and you cannot view reports. You can enable only one snapshot at a time.

Identifier

Specifies the snapshot parameter XML file that defines the scope of the report snapshot.

Options:

- HOST_PROTECTION.XML—Collect reporting data from CA ControlMinder endpoints.
- HOST_PROTECTION_SAM_LDAP.XML—Collect reporting data from CA ControlMinder and SAM endpoints that use an LDAP user store.
- HOST_PROTECTION_SAM_RDB.XML—Collect reporting data from CA ControlMinder and SAM endpoints.
- HOST_PROTECTION_SAM_UNAB_LDAP.XML—Collect reporting data from CA ControlMinder, UNAB and SAM endpoints that use an LDAP user store.
- HOST_PROTECTION_UNAB_LDAP.XML—Collect reporting data from UNAB endpoints.
- SAM_LDAP.XML—Collect reporting data from SAM endpoints that use an LDAP user store.
- SAM_RDB.XML—Collect reporting data from SAM endpoints.

Keep Last

Specifies the number of successful snapshots stored in the central database. CA ControlMinder deletes old snapshots when the number of snapshots in the database reaches the number that you specify.

Note: The number of snapshots should be greater than zero. If you do not specify a value for this field, CA ControlMinder stores unlimited snapshots. We recommend that you store a maximum of three successful snapshots.

5. Click the Recurrence tab and select Schedule.

   The schedule options appear.

6. Specify the snapshot execution time and recurrence pattern, and click Submit.

   Note: We recommend that you schedule the snapshot to run less frequently than the snapshots from CA ControlMinder and UNAB endpoints.

   CA ControlMinder is configured to capture snapshots at the scheduled time and frequency.

Note: After you create a snapshot definition, you can choose to capture snapshots on demand and capture snapshots at the scheduled time and frequency. For more information about capturing snapshot data, see the *Enterprise Administration Guide*.

Limit the Scope of the Report Snapshot

When CA ControlMinder Enterprise Management captures a report snapshot, it collects data from snapshots of CA ControlMinder and UNAB endpoints, SAM data from CA ControlMinder Enterprise Management, and data from the user store. After CA ControlMinder Enterprise Management collects the report data, it stores the data in the central database.

The snapshot parameter XML file specifies the report data that CA ControlMinder Enterprise Management collects. You can limit the scope of the report snapshot by customizing the snapshot parameter XML file.

For example, if you use Active Directory as your user store, CA ControlMinder Enterprise Management collects data for every Active Directory user when it captures a report snapshot. This operation may take a long time to complete. To decrease the time it takes to capture a snapshot, you can limit the scope of the Active Directory snapshot by customizing the snapshot parameter XML file.

To limit the scope of the report snapshot

1. Navigate to the following directory, where *JBOSS_HOME* is the directory where you installed JBoss:

   JBOSS_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/config/imrexport/sample

2. Copy the sample xml file that is most suitable for your use case. Rename the new file, and save the file in the same directory.

   You have created a new snapshot parameter XML file.

3. Open the new snapshot parameter XML file in an editable form.

4. Edit the entries in the <!--IM COLLECTORS--> section to specify the scope of the data that CA ControlMinder Enterprise Management collects from the user store.

5. Comment out (!--) and (--) the entries in the <!--PUPM COLLECTORS--> section that correspond to the CA ControlMinder Enterprise Management components that you do not want to include in the report snapshot.
6. (Optional) Limit the scope of the Active Directory snapshot:
   a. Review the How the LDAP Queries Limit the Report Snapshot (see page 126) and the LDAP Syntax Considerations (see page 126) topics.

      The information in these topics helps you define the correct LDAP queries in the following steps.

   b. Locate the following element in the <!--PUPM COLLECTORS--> section:

      ```
      <export object="com.ca.ppm.export.ADUsersCollector">
      </export>
      ```

      This element specifies the Active Directory user data that is included in the snapshot.

   c. Edit the element so it appears as follows, where *ldap_query* specifies an LDAP query that defines the users for which data is collected:

      ```
      <export object="com.ca.ppm.export.ADUsersCollector">
              <where attr="%USER" satisfy="ANY">
                      <value op="EQUALS">(ldap_query)</value>
              </where>
      </export>
      ```

   d. Locate the following element in the <!--PUPM COLLECTORS--> section:

      ```
      <export object="com.ca.ppm.export.ADGroupsCollector">
      </export>
      ```

   e. Edit the element so it appears as follows, where *ldap_query* specifies an LDAP query that defines the groups for which data is collected:

      ```
      <export object="com.ca.ppm.export.ADGroupsCollector">
              <where attr="%USER" satisfy="ANY">
                      <value op="EQUALS">(ldap_query)</value>
              </where>
      </export>
      ```

      You have limited the scope of the Active Directory snapshot.
7. Save and close the new snapshot parameter XML file.
8. Modify the snapshot definition in CA ControlMinder Enterprise Management to use the new snapshot parameter XML file.

   When the capture snapshot task runs, it collects only the data that you specified in the snapshot parameter XML file.

Example: Limit the Scope of Report Snapshots to CA ControlMinder Endpoints

If you do not use SAM and UNAB, you can limit the scope of the report snapshot to collect data only from CA ControlMinder endpoints. To limit the scope of data collection to CA ControlMinder endpoints, you comment (!--) and (--) all the entries under the <-- PUPM COLLECTORS --> section *except* for the ReportIdMarkerCollector entry.

The following is a snippet from a sample XML file after it was modified to comment all entries under the <-- PUPM COLLECTORS --> section, excluding the ReportIdMarkerCollector entry:

```
<!--  PUPM COLLECTORS -->
        <!-- export object="com.ca.ppm.export.AccountPasswordCollector">
        </export -->

        <!-- export object="com.ca.ppm.export.PPMRolesCollector">
                <exportattr attr="|rolemembers|" />
        </export -->

        <!-- export object="com.ca.ppm.export.
                PrivilegedAccountExceptionCollector">
        </export -->

        <!-- export object="com.ca.ppm.export.PPMPasswordPolicyCollector">
        </export -->

        <!-- export object="com.ca.ppm.export.ADUsersCollector">
        </export -->

        <export object="com.ca.ppm.export.PPMAccountUserAccessCollector">
        </export --!>

        <!-- export object="com.ca.ppm.export.ADGroupsCollector">
                <exportattr attr="|groupmembers|" />
        </export -->

        <export object="com.ca.ppm.export.ReportIdMarkerCollector">
        </export>
```

Snapshot Parameter XML File Syntax—Limit Report Snapshot

The snapshot parameter XML file specifies that report data that CA ControlMinder Enterprise Management collects. You can limit the scope of the report snapshot by editing the snapshot parameter XML file.

CA ControlMinder Enterprise Management collects report data only for the objects that meet the criteria that you define in the snapshot parameter XML file. Each collector in the file defines a set of objects that CA ControlMinder Enterprise Management collects.

Each collector has the following structure:

```
<export object=" ">
        <where attr=" " satisfy=" ">
                <value> </value>
        </where>
        <exportattr attr=" " />
</export>
```

Note: The <where>, <value>, and <exportattr> elements are optional.

Each collector contains the following elements:

<export>

Indicates the object data that CA ControlMinder Enterprise Management collects. For example, the <export> element may specify that CA ControlMinder Enterprise Management collects user data.

The <export> element can include one or more <exportattr> and <where> elements, which let you collect only the data that meets certain criteria. If you do not specify any <exportattr> or <where> elements, CA ControlMinder Enterprise Management collects all of the data for the object.

The <export> element has only the object parameter.

<where>

Filters the collected data based on the criteria defined by the <value> element. A <where> element must include at least one <value> element. You can specify multiple <where> elements to refine your filter (they act as OR elements).

The following table describes the parameters for the <where> element:

Parameter	Description
attr	Indicates the attribute to use in the filter.

Parameter	Description
satisfy	Indicates whether some or all of the value evaluations must be satisfied for the object or attributes to be collected. ■ ALL—An attribute or object must satisfy all of the value evaluations. ■ ANY—An attribute or object must satisfy at least one value evaluation.

<value>

Defines, in a <where> element, the condition that an attribute or an object must meet to be collected. The <value> element requires the operator (op) parameter. The operator can be EQUALS or CONTAINS.

Note: In the <!--PUPM COLLECTORS--> section of the snapshot parameter XML file, you can use LDAP syntax in <value> elements. The LDAP syntax lets you specify the user and group data that CA ControlMinder Enterprise Management collects from Active Directory.

<exportattr>

Indicates a specific attribute to collect. Use the <exportattr> element to collect a subset of attributes for the object you are collecting. For example, you can use the <exportattr> element to collect only a user's ID.

The <exportattr> element has the attr parameter.

The following table shows attributes that can be used in a <where> element or an <exportattr> element, by object:

Object	Attributes you can use in a <where> element	Attributes you can use in an <exportattr> element
role	You can filter with the name attribute. name—the roles with names that satisfy the filter	You can collect any of the following attributes: ■ |tasks|—all tasks associated with the role ■ |rules|—all member, admin, owner, and scope rules that apply to the role ■ |users|—all members, administrators, and owners of the role ■ |rolemembers|—all role members ■ |roleadmins|—all role administrators ■ |roleowners|—all role owners
user	Any well-known or physical attribute and any of the following attributes: ■ |groups|—the members of a group ■ |roles|—the members of a role ■ |orgs|—users whose profiles exist in organizations that satisfy the filter	You can collect any of the following attributes: ■ |all_attributes|—all available user attributes ■ |groups|—all groups where the user is a member or admin ■ |roles|—all roles where the user is a member, admin, or an owner

Object	Attributes you can use in a <where> element	Attributes you can use in an <exportattr> element
group	Any well-known or physical attribute or the following attribute: |groups|—the list of nested groups within a group that satisfies the filter	You can collect any well-known or physical attribute or any of the following attributes: ■ |all_attributes|—all attributes defined for the Group object in the directory configuration file (directory.xml) ■ |groups|—all nested groups within the group ■ |users|—all members of the group ■ |groupadmins|—all users who are administrators of the specified group ■ |groupmembers|—all users who are members of the specified group ■ |users|—all group administrators and members
organization	Any well-known or physical attribute	You can collect any well-known or physical attribute or any of the following attributes: ■ |all_attributes|—all attributes defined for the Organization object in the directory configuration file (directory.xml) ■ |orgs|—all nested organizations within the organization ■ |groups|—all groups in the organization ■ |users|—all users in the organization

How LDAP Queries Limit the User and Group Data in the Report Snapshot

If you use Active Directory as your user store, you can specify the user and group data that is captured in the report snapshot.

You can use LDAP queries in the snapshot parameter XML file that filter the Active Directory data by user and by group. However, you cannot use LDAP queries that filter the Active Directory data by role membership. You can use LDAP queries only in the <!--PUPM COLLECTORS--> section of the snapshot parameter XML file

The following process describes how the LDAP queries in the snapshot parameter XML file limit the Active Directory data that CA ControlMinder Enterprise Management collects. This information helps you write the correct LDAP query to limit the report snapshot.

When CA ControlMinder Enterprise Management captures an Active Directory report snapshot, it does the following:

1. Collects data for only the Active Directory users that are specified in the LDAP query within the following element:

   ```
   <export object="com.ca.ppm.export.ADUsersCollector">
   ```

   If the element does not contain an LDAP query, CA ControlMinder Enterprise Management includes data for all Active Directory users in the snapshot.

2. Collects data for only the Active Directory groups that are specified in the LDAP query within the following element:

   ```
   <export object="com.ca.ppm.export.ADGroupsCollector">
   ```

   If the element does not contain an LDAP query, CA ControlMinder Enterprise Management includes data for all Active Directory groups in the snapshot.

   Note: CA ControlMinder Enterprise Management does not collect data for any user that is not returned by the query in Step 1. If a user is a member of a group that is returned by the query in Step 2, but the user is not returned by the query in Step 1, CA ControlMinder Enterprise Management does not include any data for the user in the Active Directory snapshot.

LDAP Syntax Considerations

Consider the following when you write LDAP queries to limit the scope of the Active Directory snapshot:

- You can use the following logical operators in the LDAP query:
  - EQUAL TO (=)
  - OR (|)

- AND (&)

  Note: Some restrictions apply to the use of the ampersand (&) character.

- NOT (!)
- wildcard (*)

- You can use the ampersand character (&) and left angle bracket character (<) only in the following contexts:
  - As a markup delimiter
  - Within a comment
  - Within a processing instruction
  - Within a CDATA section

Use the string **&** or the Unicode character reference to represent the ampersand character in any other context. Use the string **<** or the Unicode character reference to represent the left angle bracket character in any other context.

- You can use the right angle bracket character (>) only at the end of a string marking the end of a CDATA section ( ]]>).

  Use the string **>** or the Unicode character reference to represent the right angle bracket character in any other context.

Example: The Ampersand Character

The following snippet of a snapshot parameter XML file specifies to include all Active Directory user data in the report snapshot. The LDAP query in the snippet uses the & string to represent an ampersand:

```
<export object ="com.ca.ppm.export.ADUsersCollector">
        <where attr="%USER%" satisfy="ANY">
                <value op="EQUALS">(&amp;(objectClass=user))</value>
        </where>
</export>
```

Deploy the Report Package on a Report Portal That You Installed with CA ControlMinder r12.0

Valid on Windows

To make use of the standard CA ControlMinder reports, you need to import the report package file into BusinessObjects InfoView.

This procedure describes how you deploy a report package on an existing installation of CA Business Intelligence that you installed with CA ControlMinder r12.0.

Follow these steps:

1. Insert the appropriate CA ControlMinder Server Components DVD for your operating system into your optical disc drive and navigate to the /ReportPackages directory.
2. Create a temporary folder for the installation files:
   - On Windows, create a folder named BO under the root C:\ drive.

     Note: You need approximately 2 GB of memory in this folder.
   - On Linux, create the directory /work/bo
3. Copy the following files from the optical disc drive into the same temporary directory:
   - /ReportPackages/*RDBMS/import_biar_config*.xml
   - /ReportPackages/*RDBMS/AC_BIAR_File*.biar

   RDBMS

   Defines the type of RDBMS you are using.

   Values: Oracle, MSSQL2005

   ***import_biar_config*.xml**

   Defines the name of the import configuration file (.xml) for your RDBMS.

   Values: import_biar_config_oracle10g.xml, import_biar_config_oracle11g.xml, import_biar_config_mssql_2005.xml

   Note: If you use MS SQL Server 2008 as your central database, configure the import_biar_config_mssql_2005.xml file.

   ***AC_BIAR_File*.biar**

   Defines the name of the CA ControlMinder reports file (.biar) for your language and RDBMS.

   Note: The <biar-file name> property of the import configuration file for your RDBMS points to this file. It is set by default to the name of the English version for your RDBMS.

4. Insert the CA ControlMinder r12.0 Server Components DVD for your platform into the optical disc drive and navigate to the /ReportPortal directory.

   Note: This DVD is part of the media you received with r12.0.

5. Complete one of the following steps:

   - On Windows, copy the contents of the \ReportPortal\BO directory from the DVD to the C:\BO folder that you created.
   - On Linux, extract /ReportPortal/bo_install.tar.gz to the /work/bo folder you created.

6. Copy the contents of the \ReportPortal\BO directory from the DVD to the C:\BO folder that you created.

7. Open the target directory and browse to *BO_files*/biek-sdk.

8. Edit your copy of the biekInstall.properties file as follows:

   ```
   BIEK_CONNECT_LAYER=networklayer
   BIEK_CONNECT_DB=rdms
   BIEK_CONNECT_USER=rdbms_adminUserName
   BIEK_CONNECT_PASSWORD=rdbms_adminUserPass
   BIEK_CONNECT_SOURCE=rdbms_Datasource
   BIEK_CONNECT_SERVER=rdbms_hostName
   BIEK_BO_USER=InfoView_adminUserName
   BIEK_BO_PASSWORD=InfoView_adminUserPass
   BIEK_BIAR_FILE=AC_BIAR_File.biar
   ```

   networklayer

   Defines the network layer supported by your RDBMS.

   Limit: Case-sensitive.

   rdms

   Defines the type of RDBMS you are using.

   Limit: Case-sensitive.

   rdbms_adminUserName

   Defines the user name of the RDBMS administrative user you created.

   rdbms_adminUserPass

   Defines the password of the RDBMS administrative user you created.

   rdbms_Datasource

   Defines the name of the Transparent Network Substrate (TNS) of the Oracle database.

   rdbms_hostName

   Defines the host name of the RDBMS server.

InfoView_adminUserName

Defines the user name of the InfoView administrative user. By default, this user is *Administrator*.

InfoView_adminUserPass

Defines the password of the InfoView administrative user. By default, this user does not have a password (leave it empty).

***AC_BIAR_File*.biar**

Defines the full pathname to the CA ControlMinder reports file (.biar). This is the file you copied earlier.

9. Launch the *BO_Files*/biek-sdk/importBiarFile.bat batch file.

   The file imports the CA ControlMinder reports into InfoView. The import may take a few minutes to complete.

Chapter 6: Preparing Your Endpoint Implementation

This section contains the following topics:

Deciding on the Policy Objects to Protect

The following sections describe some of the important objects that can be used by your security policy to authorize access to your enterprise applications and data.

Users

In CA ControlMinder, there are different types of users. Each type of user has a certain level of authority and certain limitations. Part of developing a security policy for your organization is deciding which special privileges to grant to whom.

CA ControlMinder stores information about a user, such as the number of times the user is permitted to log on, and the type of auditing to be done on the user. Information about a user is stored in properties of database records.

Note: For more information about users, see the *Endpoint Administration Guide*.

Types of Users

CA ControlMinder supports the following types of users, that are used for managing resources in the CA ControlMinder database:

Regular users

Your organization's in-house end users—the people who carry out the business of your organization. You can limit regular users' access to the system with both the native OS and CA ControlMinder.

Users with special privileges (sub administrators)

Regular users who have been given the ability to perform one or more specific administrative tasks. When regular users are given the ability to carry out specific administrative functions, the workload of the administrator is lessened. In CA ControlMinder, this is called task delegation.

Administrators

Users who have the highest authority within the native OS and CA ControlMinder. Administrators can add, delete, and update users and can perform almost all administrative tasks. With CA ControlMinder, you are able to limit the abilities of the native superuser. You can allocate administration tasks to specific users whose accounts are not automatically known. This means that it is not immediately clear to an intruder which user performs administrative tasks.

Group administrators

Users who can perform most administrative functions, such as adding, deleting, and updating users, within one particular group. This type of user, with its particular, limited authority, is not found in native Windows.

Password managers

Users who have the authority to change the password of other users. A password manager cannot change other user attributes. This type of user is not found in the native OS.

Group password managers

Users who have the authority to change the password of other users in one particular group. A group password manager cannot change other user attributes for users within the group. This type of user is not found in the native OS.

Auditors

Users who have the authority to read audit logs. They also determine the kind of auditing done on each login and each attempt to access a resource. This type of user is not found in the native OS.

Group auditors

Users who can read audit logs relevant to their group. They also have the authority to determine the kind of auditing done within a particular group. This type of user is not found in the native OS.

Operators

Users who can display (read) all the information in the database, shut down CA ControlMinder, and use the secons utility to perform tasks such as manage CA ControlMinder tracing and display run-time statistics. This type of user is not found in the native OS.

Note: For more information about the secons utility, see the *Reference Guide*.

Group operators

Users who can display all the information in the database for the group in which they are defined. This type of user is not found in the native OS.

Server

A special type of user that is really a process, which can ask for authorization for other users.

Security Policies and Users

When preparing the implementation, you should decide:

- What special privileges, if any, to give to the defined users
- What global authorization and group authorization attributes to grant to defined users

  For example, you should decide whom to define as system administrators, password managers, group password managers, auditors, and operators.

Groups

A group is a set of users who usually share the same access authorizations. Administrators can add users to groups, remove users from groups, and assign or deny access to system resources by group. This type of group exists in both native OS and CA ControlMinder.

The group record contains information about the group. The most important information stored in the group record is the list of users who are members of the group.

Important! Authorization rules for a group record apply recursively for each user in the group's hierarchy.

For example, Group A has two members: User X and Group B. User Y is a member of Group B. When you change an authorization rule for Group A, CA Access Control applies the changed authorization rule to all the users and groups in the Group A hierarchy, that is, User X, Group B, and User Y.

Information in a group record is stored in *properties*.

In CA ControlMinder, a group administrator can manage group functions for the specific group in which the group administrator is defined. A group password manager can change the password of group members.

Security Policies and Groups

When developing a security policy for your organization, you should decide:

- What groups to create for security administration purposes
- Which users to join to each group
- Whether to define group administrators and group password managers, and if so, which users to give these administrative roles

Predefined Groups of Users

CA ControlMinder includes predefined groups to which a user can be joined. One such group is the _restricted group. For users in the _restricted group, all files and registry keys are protected by CA ControlMinder. If a file or a registry key do not have an access rule explicitly defined, access permissions are covered by the _default record for that class (FILE or REGKEY).

Use the _restricted group with caution. Users in the _restricted group may not have sufficient authorization to do their work. If you plan to add users to the _restricted group, consider using Warning mode initially. In Warning mode, the audit log shows which files and registry keys users need for their work. After examining the audit log, you can grant the appropriate authorizations and turn Warning mode off.

Predefined Groups for Resource Access

Other types of predefined groups in CA ControlMinder define the type of access that is allowed or prohibited to a particular resource. These groups include the following:

- _network

  (Windows only) The _network group defines access from the network to a particular resource. All users are treated as if they are members of the group; no user has to be explicitly added to the group.

  For example, you can specify that a particular resource can only be read from the network. Using selang, you define the new resource as follows:

  ```
  newres FILE c:\temp\readonly defaccess(none)
  ```

  Then specify the access allowed through the network:

  ```
  authorize FILE c:\temp\readonly gid(_network) access(read)
  ```

  You can also do this using CA ControlMinder Endpoint Management.

  Now when accessing c:\temp\readonly from the network, users can read the file only from the network.

- _interactive

  The _interactive group defines the access permitted to a particular resource from the computer on which the resource resides. For example, You can authorize READ access to a file from the computer on which it is defined, although no access is permitted to the resource from the network.

The following points are important:

- There is no connection in CA ControlMinder between the _network and _interactive groups. This means that there can be a rule in the _network group that defines access from the network to a specific resource. Another rule in the _interactive group can define access to the same resource.
- You do not have to add users to the _network and _interactive groups.
- These groups can protect all the Windows resources defined in the database.

Authorization Attributes

An authorization attribute is set in the user record in the database and permits the user to do things that an ordinary user cannot do. The two kinds of authorization attributes are *global* and *group*. Each global authorization attribute permits the user to perform certain types of functions on any record in the database. A group authorization attribute permits the user to perform certain types of functions within one specified group. The functions and the limits of each global and group authorization attribute are described in the following sections.

Global Authorization Attributes

Users who have a global authorization attribute set in their own user records can perform special functions on any relevant record in the database. The global authorization attributes are:

- ADMIN
- AUDITOR
- OPERATOR
- PWMANAGER
- SERVER
- IGN_HOL

Note: For more information about global authorization attributes, see the *Endpoint Administration Guides*.

Group Authorization Attributes

Users who have a *group authorization attribute* in their own user records can perform special functions within a specified group. The group authorization attributes are:

- GROUP-ADMIN
- GROUP-AUDITOR
- GROUP-OPERATOR
- GROUP-PWMANAGER

Note: For more information about group authorization attributes, see the *Endpoint Administration Guides*.

Using a Warning Period

In addition to deciding what to protect, the implementation team must consider how to phase in the new security controls. To minimize disruption to current work patterns, you should consider an initial period in which you only monitor access to resources, rather than enforcing access restrictions.

You can monitor access by putting the resources into Warning Mode. When Warning Mode is enabled for a resource or a class, and user access violates access restrictions, CA ControlMinder records a Warning message in the audit log, and gives the user access to the resource.

Note: If you use Warning Mode, consider increasing the maximum size of the audit logs. For more information about Warning Mode, see the *Endpoint Administration Guide*.

CA ControlMinder Backdoor

When you first install CA ControlMinder, for example in an evaluation deployment, you may incorrectly define rules in the CA ControlMinder database. Incorrectly defined rules can prevent users from logging in or executing commands. For example, you may mistakenly define a rule that denies access to the system directory or to vital parts of the Windows registry.

Because it is difficult to stop CA ControlMinder and fix these mistakes, CA ControlMinder comes with a backdoor that lets you fix these types of problems. Because backdoors can be maliciously exploited, CA ControlMinder also lets you disable this backdoor once your system is set up and stable.

To access this backdoor, when you start the computer, select the Windows Safe Mode or Safe Mode with Networking from the boot menu. When you select one of these options the system starts without automatically starting the CA ControlMinder services.

To disable this backdoor, define the registry value 'LockEE' of data type reg_dword under the registry key HKEY_LOCAL_MACHINE\Software\ComputerAssociates\ AccessControl\AccessControl\ and set it to 1.

Note: This registry value does not exist by default.

Now when you start the system with LockEE set to 1 in:

- Safe Mode, only CA ControlMinder Engine and CA ControlMinder Watchdog load.

  The CA ControlMinder Agent (and any Policy Models), which rely on network services, do not load.
- Safe Mode with Networking, CA ControlMinder starts normally.

On UNIX you can work with CA ControlMinder in single user mode. When you work in single user mode, the following limitations apply:

- selang is supported in local mode (selang -l) only
- network classes are not supported
- PMDB functionality (including using selang env pmd) does not work

Implementation Tips

This section provides some miscellaneous implementation information to consider once you have installed CA ControlMinder.

Types of Security

You can handle security at your site by using one of the following approaches:

- Whatever is not explicitly allowed is forbidden. This is the ideal approach, but it is impossible to use during implementation. Since no rules exist that allow anything to be done on the system, the system blocks all attempts to define access rules. It is like locking yourself out of your car with the keys still in the ignition.
- Whatever is not specifically forbidden is allowed. This approach may be less secure, but it is a practical way to implement a security system.

CA ControlMinder lets you start with the second approach and, once access rules have been defined, switch to the first approach. Default access (defaccess) and universal access (_default) rules let you define approach and switch protection policy at any time.

Important! You may need to add all users to the _restricted group when switching a protection policy. Performance may be significantly effected when switching between protection policies.

Accessors

An *accessor* is an entity that can access resources. The most common type of accessor is a user or group, for whom access authorities should be assigned and checked. When programs access resources, the owner (a user or group) of the program is the accessor. Accessors fall into three categories:

- A person who is associated with a specific user ID
- A person who is a member of a group that has access authority
- A production process that is associated with a certain user ID

The most common type of accessor is a user, a person who can perform a login and for whom access authorities should be assigned and checked. One of the most important features of CA ControlMinder is accountability. Each action or access attempt is performed on behalf of a user who is held responsible for the request.

CA ControlMinder lets you define groups of users. Users are usually grouped together by projects, departments, or divisions. By grouping users together, you can significantly reduce the amount of work needed to administer and manage security.

You can define new users and groups and modify existing users and groups through CA ControlMinder Endpoint Management or through selang commands.

Resources

An essential part of any security policy is deciding which system resources must be protected and defining the type of protection these resources are to receive.

Resource Classes and Access Rules

When installed, CA ControlMinder immediately begins intercepting system events and checking for users' authority to access resources. Until you tell CA ControlMinder how to restrict access to your system's resources and which resources to restrict, the result of all authorization checks is to permit access.

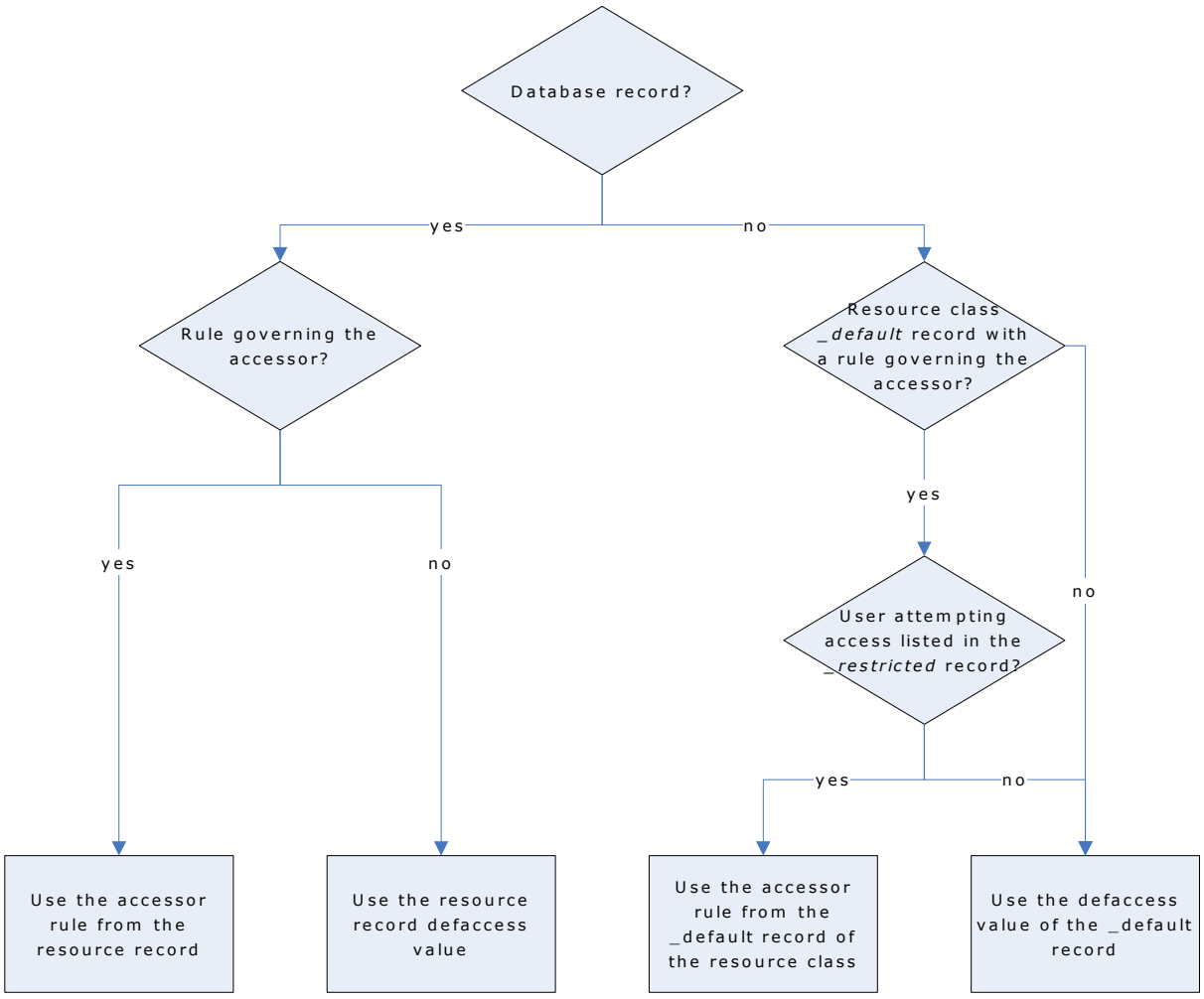
The properties of a protected resource are stored in a resource record, and resource records are grouped into classes. The most important information contained in a resource record is its access rules. An *access rule* governs the permission of one or more accessors to work with one or more resources. Several ways to define access rules are:

- An access control list (a specific list of the accessors authorized to access the resource and the exact access they can have), also called an ACL
- A negative access control list (a specific list of the accessors for which access should be denied), also called NACL
- A default access for the resource, which specifies access rules for accessors not specifically listed in an ACL
- A universal access (the _default record for a class), which specifies access for resources that do not yet have specific resource records in that class
- A program ACL, which defines access for a specific accessor through a specific program
- A conditional ACL, which makes access dependent on some condition. For example, in a TCP record, you can define access to a specific remote host through a specific accessor
- An Inet ACL, which defines access for inbound network activity through specific ports

Using defaccess and _default

When access to a resource is requested, the database is searched in the following order to determine how the request should be treated, and CA ControlMinder uses the first access rule that is found. Notice the distinction between *default access* (defaccess) and _default.

1. If the resource has a record in the database, and the record has a rule governing the accessor, then CA ControlMinder uses that rule.
2. If the record exists but does not have a rule governing the accessor, that *record's* default access rule—its *defaccess value*—is applied to the accessor.
3. If the record does not exist, but in the resource class the _default record has a rule governing the accessor, then CA ControlMinder uses that rule.
4. If the record does not exist, and in the resource class the _default record does not have a rule governing the accessor, then the _default record's default access rule-its defaccess value-is applied to the accessor. For files and registry keys, this applies only to _ restricted users (see page 134).



Note: For more information about resource classes and access rules see the *selang Reference Guide*.

Chapter 7: Installing and Customizing a Windows Endpoint

This section contains the following topics:

Before You Begin

Before you can install CA ControlMinder, you must make sure certain preliminary requirements are met and several items of necessary information are available.

Installation Methods

You can install CA ControlMinder for Windows from the CA ControlMinder Endpoint Components for Windows DVD using the following methods:

- **Product Explorer**—The easiest way to install CA ControlMinder is to use the Product Explorer. The Product Explorer is a graphical installation program that lets you select between different architecture installations of CA ControlMinder and install the Runtime SDK. The Product Explorer steps you through each stage of the installation process and prompts you for the information that you must provide at each stage.
- **Command line**—The command line interface to the installation program lets you:
  - Set custom defaults for running the graphical installation program

    You can pass defaults to the graphical installation program from the command line. Use this method to create a batch file that opens the installation program with the preset defaults you want to use, but lets you customize options for each installation.
  - Perform a silent installation

    You can silently install CA ControlMinder, rather than just pass defaults to the graphical installation program, using the command line. Use this method to push the installation to remote computers.
- **Unicenter Software Delivery**—You can create a package for distributing CA ControlMinder with Unicenter Software Delivery.

Firewall Settings

When you install CA ControlMinder on Windows Server 2003, or Windows Server 2008, CA ControlMinder opens port 8891 for non-SSL TCP connections and port 5249 for SSL TCP connections. This serves as the default port for CA ControlMinder agent-client connections.

Note: For more information on ports CA ControlMinder uses on Windows, see the *Reference Guide*.

New Installations

When installing a new instance of CA ControlMinder, note the following:

- Read the *Release Notes*.

  This document contains information about supported platforms, known issues, considerations, and other important information you should read before installing CA ControlMinder.

- The Windows Administrator or a member of the Administrators group must install CA ControlMinder.

- Install CA ControlMinder in a unique directory, different from any other product installation directory.

- You must have Microsoft Internet Explorer 6.x or 7.x installed.

- CA ControlMinder needs the Microsoft Visual C++ 2005 Redistributable Package to complete the product installation.

  If this package is missing, the installation program installs it first.

- Using CA Technologies Licensing

  All CA Technologies enterprise products and their options require a license file, CA.OLF, for each computer within a network where CA Technologies software runs. When you purchase CA ControlMinder, you receive a license certificate that contains necessary information to successfully install and license the product.

  In order to install an enterprise license file, copy the CA.OLF file (with the addition of the CA ControlMinder line) to the CA_license directory (for example, C:\Program Files\CA\SharedComponents\CA_LIC).

Upgrades and Reinstallations

When upgrading CA ControlMinder, note the following:

- Read the *Release Notes*.

  This document contains information about supported platforms, CA ControlMinder versions you can upgrade from, known issues, considerations, and other important information you should read before installing CA ControlMinder.

- We recommend that you perform a scaled-down internal testing of the new release before you upgrade your production environment.

- You may need to reboot the computer when you upgrade CA ControlMinder for the installation to complete. Future patches may not require a reboot.

  Note: For information about which releases of CA ControlMinder require a reboot when you upgrade, see the *Release Notes*.

- If your environment is set up with a PMDB hierarchy or you are setting such an environment, we recommend that you:
  - Install or upgrade each computer in your hierarchy bottom-up (subscribers first).

    Upgraded PMDBs having subscribers with an earlier version may result in erroneous commands being sent. This can happen as a result of new PMDBs containing classes and properties that do not exist in the earlier version PMDBs.

    Note: A PMDB hierarchy running on a single computer can be upgraded simultaneously.
  - Do *not* upgrade during PMDB or policy updates.
  - Back up subscriber and PMDB policies.

  Note: Earlier PMDB versions are permitted to have later versions of subscribers, but not vice versa. As commands in earlier versions are supported in later versions, earlier PMDBs can propagate to current CA ControlMinder subscribers.
- You must use the same encryption key that was used before the upgrade.
- The installation program automatically saves and upgrades registry settings of your previous installation. If an earlier version's registry key was relocated, the upgrade process copies your previous settings to the new location.

  CA ControlMinder registry settings are stored in the following location:

  `HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl`
- Full auditing is enabled by default when you upgrade CA ControlMinder.

  Important! Depending on the rules you have in the database, the number of audit events that CA ControlMinder records to the log file could significantly increase as a result of this feature. We recommend that you review your audit log file size and backup settings.

  Note: For more information about full auditing and how to configure and use the registry settings for audit log backup, see the *Endpoint Administration Guide for Windows*.

Coexistence with Other Products

When installing CA ControlMinder, consider the issue of CA ControlMinder coexistence with other programs on the computer.

CA ControlMinder runs in an environment alongside other programs, for example, CA Antivirus. This can lead to collisions between CA ControlMinder and the programs running on the local computer. To this end, the coexistence utility (eACoexist.exe) runs during CA ControlMinder installation to detect programs on the local computer that can cause a conflict. The utility uses a plug-in (binary module) for each coexisting program CA ControlMinder supports. If a program CA ControlMinder detects is trusted, CA ControlMinder registers the program by creating a SPECIALPGM rule. This SPECIALPGM rule determines the access to this program and makes sure that CA ControlMinder bypasses it when granting access.

Note: For more information about the eACoexist utility and the supported plug-ins, see the *Reference Guide*.

Example: Trusted Program Rules for Dr Watson

This example shows you the trusted program rules the coexistence utility can create for the Dr Watson application if it discovers it on the same computer as CA ControlMinder. These rules are as follows on a computer with a default Windows 2000 Server installation:

```
editres SPECIALPGM ('C:\WINNT\system32\DRWTSN32.EXE') pgmtype(DCM)
editres PROGRAM ('C:\WINNT\system32\DRWTSN32.EXE') owner(nobody) defacc(x) trust
```

Product Explorer Installations

The CA ControlMinder Product Explorer lets you select between different architecture installations of CA ControlMinder and install the Runtime SDK. You can also view system requirements for installation components.

Note: If you have autorun enabled, the Product Explorer automatically displays when you insert the CA ControlMinder Endpoint Components for Windows DVD into your optical disc drive.

Install Using Product Explorer

The CA ControlMinder Product Explorer lets you select between different architecture installations of CA ControlMinder and install the Runtime SDK. The Product Explorer uses a graphical interface to install CA Access Control and provides interactive feedback.

To install using Product Explorer

1. Log into the Windows system as a user with Windows administrative privileges (that is, as the Windows administrator or a member of the Windows Administrators group.)
2. Close any applications that are running on your Windows system.
3. Insert the CA ControlMinder Endpoint Components for Windows DVD into your optical disc drive.

   If you have autorun enabled, the Product Explorer automatically appears. Otherwise, navigate to the optical disc drive directory and double-click the PRODUCTEXPLORERX86.EXE file.
4. From the Product Explorer main menu, expand the Components folder, select CA ControlMinder for Windows (*my_architecture*), then click Install.

   You need to select the installation option that matches the architecture of the computer you are installing on (32-bit, 64-bit x64, or 64-bit Itanium).

   The Choose Setup Language window appears.
5. Select the language you want to install CA ControlMinder with and click OK.

   The CA ControlMinder installation program starts loading and, after a short while, the Introduction screen appears.

   Note: If the installation program detects an existing installation of CA ControlMinder, you are prompted to select whether you want to upgrade CA ControlMinder.
6. Follow the instructions on the installation screens.

   During the installation, the installation program prompts you to supply information. For the information that you need when installing CA ControlMinder, refer to the installation worksheets (see page 149).

   The installation program installs CA ControlMinder. When the installation is complete, you are given the choice of restarting Windows now or later.
7. Select Yes, I want to restart my computer now, and then click OK.

   After your system reboots, you can check that CA ControlMinder was installed properly (see page 170).

   Note: If you choose to restart your computer later, an additional warning cautions you that the installation is not complete until your computer is rebooted. Some CA ControlMinder functionality, such as logon interception, does not work until after you restart your computer.

Installation Worksheets

The installation program prompts you for the information it requires for the initial CA ControlMinder setup. The following sections explain what information you need to provide and give recommendations.

Feature Selection

The Select Features screen of the installation program lets you define the location where you want CA ControlMinder installed, and the features you want to install on this computer. The following features are available:

Feature	Description	Recommendation
Task Delegation	Lets you grant ordinary users the necessary privileges to perform administrative tasks. **Note:** Selected by default.	Select this feature if you want to provide users with sub-administration rights. You can also configure this post installation.
SDK	Creates a subdirectory called SDK. It contains the libraries and files required for using the CA ControlMinder SDK, and API samples.	Select this feature if you want to develop in-house CA ControlMinder-secured applications.
Stack Overflow Protection (STOP)	Enables the CA ControlMinder stack overflow protection feature.	Select this feature to protect your program from being exploited.
Mainframe Password Synchronization	Lets you synchronize user passwords with your mainframe computers.	Select this feature if you have mainframe computers you want to keep synchronized.
Unicenter Integration	Lets you integrate Unicenter NSM with CA ControlMinder and migrate Unicenter NSM data. CA ControlMinder sends audit data to the host specified by the configuration parameters of Unicenter NSM or a host you select. **Note:** This feature is only available if you have Unicenter NSM installed on this computer.	

Feature	Description	Recommendation
Advanced Policy Management Client	Configures the local computer for advanced policy management.	Select this feature for every endpoint you want to be able to deploy policies to (using advanced policy management). **Note:** For more information about advanced policy management, see the *Enterprise Administration Guide*.
Policy Model Subscriber	Configures the local computer to receive updates from a PMDB parent.	Select this feature for every endpoint you want to be able to update from a PMDB parent. **Note:** For more information on the Policy Model service, see the *Endpoint Administration Guide for Windows*.
SAM Integration	The SAM integration configures the local computer for Shared Accounts Management (SAM), so that you can discover and manage privileged accounts and applications on the computer.	Select this feature for every endpoint that has shared accounts that you want to use SAM to manage. **Note:** For more information about SAM, see the *Enterprise Administration Guide*.
Report Agent	Lets you configure the computer to send scheduled snapshots of the database to the Distribution Server. You can then select to also send audit records to the Distribution Server.	Select the Report Agent feature if you want to include this endpoint in your enterprise reports. Select the Audit Routing sub-feature if you want to use CA User Activity Reporting Module to manage your enterprise audit logs.

Administrator and Host Information

The following table explains what information you need to provide and gives recommendations:

Information	Description	Recommendation
Administrators	Lets you define users with administrative access to the CA ControlMinder database.	
Administration terminals	Lets you define computers from which administrators can administer the CA ControlMinder database.	If the administrators are using CA ControlMinder Endpoint Management to administer CA ControlMinder, you only need to define the computer where CA ControlMinder Endpoint Management is installed. You do not need to define the computer where the administrator opens the browser.
DNS domain names	Lets you enter the domain names of your networks for CA ControlMinder to add to host names.	You must enter at least one domain name that CA ControlMinder adds to host names.

Users and Groups

The following table explains what information you need to provide and gives recommendations:

Information	Description	Recommendation
Support users and groups from primary stores	Lets you use existing enterprise user stores (primary stores) so that you do not need to duplicate these users in the CA ControlMinder database.	We recommend that you set CA ControlMinder to support primary stores, that is, to support enterprise user stores. If you choose *not* to support enterprise stores, you will have to duplicate, in the CA ControlMinder database, the accessors you want to protect.

Information	Description	Recommendation
Import Windows users' and groups' data	If you choose to create the accessors you want to protect, it lets you automatically create existing Windows users and groups into the database.	If you select to import Windows users and groups, select one or more of the following options: ■ **Import users**—import your Windows users to the database. ■ **Import groups**—import your Windows groups to the database. ■ **Connect users to their default groups**—automatically add the imported users to the appropriate imported groups in the database. ■ **Change owner of imported data**—define someone other than you as an owner of the imported data. By default, the owner of these records is set to the administrator doing the installation (you). ■ **Import from domain**—import the accessor data from the specified domain.

Unicenter Integration

The following table explains what information you need to provide and gives recommendations:

Information	Description	Recommendation
Integrate CA ControlMinder with Unicenter TNG	Lets you set CA ControlMinder to send audit data to the host specified by the configuration parameters of Unicenter TNG or a host you select.	To integrate, you specify that audit data should be sent to Unicenter NSM and then select the host to which CA ControlMinder should send the audit data.
Integrate CA ControlMinder with Unicenter Calendars	Lets you set support of integration of Users and Access permissions with Unicenter NSM calendars.	Configure CA ControlMinder to retrieve updates from the Unicenter NSM calendar host server more or less frequently than the default of 10 minutes.
Migrate Unicenter Security Data	Lets you migrate Unicenter security data to CA ControlMinder.	If you do not select this option, the Unicenter Security to CA ControlMinder migration is not performed and user names in CA ControlMinder appear fully qualified (DOMAINNAME\USERNAME). With migration, user names are not qualified (USERNAME).

Inter-Component Communication Encryption

The following table explains what information you need to provide and gives recommendations.

Screen	Description	Recommendation
SSL Communication	Lets you specify whether you want to use Secure Socket Layer (SSL) for inter-component communications. You can use both SSL and symmetric key encryption.	We recommended that you use both SSL (which uses public keys), and symmetric key encryption.
Certificate Settings	If you chose to use SSL, lets you specify what certificates to use.	We recommend that you use a certificate from a well-known Certificate Authority (CA).
Generate Certificate	Lets you create a self-signed certificate and key pair to use as a root certificate.	Although it is not recommended, you can use self-signed certificates. If you use self-signed certificates you must allow their use on all hosts.
Change Certificate Settings	Lets you change certificate settings.	We strongly recommended that you change the settings from the default certificate and key pair. You can also specify a password to protect the private key for the server certificate.
Existing Certificate	Lets you supply the information for the certificate you have installed.	
Encryption Settings	Lets you set the encryption method and the key for symmetric encryption.	We strongly recommend that you change the encryption key from its default setting.

More information:

Symmetric Encryption (see page 453)
SSL, Authentication, and Certificates (see page 457)

Policy Model Subscriber Settings

The following table explains what information you need to provide and gives recommendations:

Information	Description	Recommendation
Specify Parent Policy Model Databases	Lets you define one or more parent PMDBs to which this database subscribes. The local database will not accept updates from any PMDB that you do not specify in this list. Define the parent PMDB in the format *pmdb@hostname.com*	After the installation is finished, you need to define this database as a subscriber on the parent PMDB. **Note:** Specify _NO_MASTER_ as a parent PMDB to indicate that the local database accepts updates from any PMDB.
Password Policy Model	Lets you define the parent password Policy Model from which password changes are propagated. Define the password PMDB in the format *pmdb@hostname.com*	After the installation is finished, you need to define this database as a subscriber on the password PMDB.

Advanced Policy Management Client

The following table explains what information you need to provide and gives recommendations:

Information	Description	Recommendation
Specify Advanced Policy Management Server host name	Lets you define the name of the server where the advanced policy management server components are installed.	Define the host name using the format *dhName@hostName.* **Note:** For more information on advanced policy management and reporting, see the *Enterprise Administration Guide*.

Report Agent Configuration

The following table explains what information you need to provide and gives recommendations:

Information	Description	Recommendation
Select Report Schedule	Lets you specify when the Report Agent sends snapshots of the database to the Distribution Server.	We recommend that you do not schedule the Report Agent to send snapshots at times when there is a heavy drain on system resources.

Information	Description	Recommendation
Audit Routing Configuration	Lets you specify to keep time-stamped backups of the audit log file. **Note:** This option displays only if you chose to install Audit Routing on the Select Features page.	Make sure you select to keep time-stamped backups of your audit log file. This is the default setting and is required to ensure that all audit records can be read by the Report Agent. CA ControlMinder overwrites the backup audit log files when they reach 50 files. If this is not suitable, you should edit the audit_max_files token in the logmgr registry subkey to a value suitable to your enterprise.

Distribution Server Configuration

The following table explains what information you provide and gives recommendations:

Information	Description	Recommendation
Server Name	Lets you define the name of the host where the Distribution Server is installed.	You must specify the fully-qualified host name of the host where the Distribution Server is installed.
Use Secure Communication	Lets you specify whether you want to use SSL for communication between the Distribution Server and the Report Agent, and the Distribution Server and the SAM Agent.	We recommend that you use SSL. If you do not use SSL, the Distribution Server uses TCP to communicate with the Report Agent and the SAM Agent.
Server Port	Lets you define the port number that is used for communication between the Distribution Server and the Report Agent, and the Distribution Server and the SAM Agent.	If you use SSL communication, the default server port is 7243. If you do not use SSL communication, the default server port is 7222.

Information	Description	Recommendation
Communication Key	Lets you define a new key to authenticate communication between the Distribution Server and the Report Agent, and the Distribution Server and the SAM Agent.	Make sure that you use the same key when you install the Distribution Server. **Note:** If you use SSL communication you must specify a communication key. If you do not use SSL communication, you can choose not to specify a communication key.

Command Line Installations

You can use the command line to:

- Pass defaults to the graphical installation program.
- Silently install CA ControlMinder.

Set Custom Defaults for the Installation Program

To set the CA ControlMinder installation program with the defaults you want to use for your company, you can use the command line. The graphical installation program accepts input from the command line that determines which options are preselected.

To set custom defaults for the installation program

1. Log in to the Windows system as a user with Windows administrative privileges (that is, as the Windows administrator or a member of the Windows Administrators group.)
2. Close any applications that are running on your Windows system.
3. Insert the CA ControlMinder Endpoint Components for Windows DVD into your optical disc drive.

   The CA ControlMinder Product Explorer appears if you have autorun enabled.
4. Close the Product Explorer if it appears.

5. Open a command line and navigate to the following directory on the optical disc drive:

   `\architecture`

   architecture

   Defines the architecture abbreviation for your operating system.

   Can be one of **X86**, **X64**, and **IA64**.

6. Enter the following command:

   `setup [/s] /v"<insert_params_here>"`

   The *<insert_params_here>* variable specifies the installation settings you want to pass to the installation program.

   The installation program appears. The installation program screens will show the default options you chose to pass, and lets you modify these to install CA ControlMinder.

Install Silently

To install CA ControlMinder without interactive feedback, you can install CA ControlMinder silently using the command line.

To install CA ControlMinder silently

1. Log in to the Windows system as a user with Windows administrative privileges (that is, as the Windows administrator or a member of the Windows Administrators group.)
2. Close any applications that are running on your Windows system.
3. Insert the CA ControlMinder Endpoint Components for Windows DVD into your optical disc drive.

   The CA ControlMinder Product Explorer appears if you have autorun enabled.
4. Close the Product Explorer if it appears.

5. Open a command line and navigate to the following directory on the optical disc drive:

   `\architecture`

   architecture

   Defines the architecture abbreviation for your operating system.

   Can be one of **X86**, **X64**, and **IA64**.

6. Enter the following command:

   `setup /s /v"/qn COMMAND=keyword <insert_params_here>"`

   The *<insert_params_here>* variable specifies the installation settings you want to pass to the installation program.

   Note: To execute a silent installation you have to accept the license agreement. The *keyword* required for accepting the license agreement and silently installing CA ControlMinder is found at the bottom of the license agreement available when running the installation program.

setup Command—Install CA ControlMinder for Windows

Use the setup command to install CA ControlMinder for Windows with preset custom defaults (see page 156) or when performing a silent installation (see page 157).

Note: For more information about the command line syntax, see the Windows Installer SDK documentation that is available at the Microsoft Developer Network Library.

This command has the following format:

`setup [/s] [/L] [/v"<insert_params_here>"]`

/s

Hides the setup initialization dialog.

/L

Defines the CA ControlMinder installation language.

Note: For more information about the CA ControlMinder installation languages that are supported in this release, see the *Release Notes*.

/v "*<insert_params_here>*"

Defines the parameters to pass to the installation program.

Note: All parameters must be placed within the quotes ("").

The following parameters are passed to the installation program through the /v parameter:

/l[*mask*] *log_file*

Defines the full path and name of the installation log file. Use the mask *v to log all available information.

/forcerestart

Specifies to force the computer to restart after the installation is complete if the installer requires a reboot.

/norestart

Specifies not to restart the computer after the installation is complete.

/qn

Specifies a silent installation, with the */s* option.

Important! Use the *COMMAND* parameter to execute a silent installation.

AC_API={1 | 0}

Specifies whether to install SDK libraries and samples (1).

Default: 0 (not installed).

ADMIN_USERS_LIST=\"*users*\"

Defines a space-separated list of users with administrative access to the CA ControlMinder database.

Default: User performing the installation.

Important! Do not define the NT Authority\System user in the list. Define a local administrative user account.

ADV_POLICY_MNGT_CLIENT={1 | 0}

Configures the local computer for advanced policy management (1).

Default: 1

If this option is set to 1, specify the following:

- **APMS_HOST_NAME=\"***name***\"**

  Defines the name of the server where the advanced policy management components are installed.

COMMAND=*keyword*

Defines the command required for accepting the license agreement and silently installing the CA ControlMinder. The actual *keyword* is found at the bottom of the license agreement that is available when running the graphical installation program.

Default: *none*

DIST_SERVER_NAME=\"*name*\"

Defines the fully qualified name of the Distribution Server host that the SAM Agent and Report Agent communicate with (for example, test.company.com).

Default: *none*

DIST_SERVER_PORT=\"*port*\"

Defines the port number that the SAM Agent and Report Agent use for communication with the Distribution Server.

Default: 7243

DOMAIN_LIST=\"*domains*\"

Defines a space-separated list of your network DNS domain names for CA ControlMinder to add to host names.

Default: *none*

ENABLE_STOP={1 | 0}

Specifies whether the stack overflow protection (STOP) feature is enabled (1).

Default: 0 (disabled).

Note: STOP support is applicable to x86 and x64 installations only.

HOSTS_LIST=\"*hosts*\"

Defines a space-separated list of computers from which administrators can administer the CA ControlMinder database (CA ControlMinder terminals).

Default: The current computer.

IMPORT_NT={Y | N}

Specifies whether to support primary (enterprise) user stores. If you specify N, primary user stores are supported. If you specify Y, primary user stores are not supported and you can specify one or more of the following options to import Windows users and groups into the CA ControlMinder database:

- **IMPORT_USERS={1 | 0}**

  Specifies whether to import Windows users to the database.

- **IMPORT_GROUPS={1 | 0}**

  Specifies whether to import Windows groups to the database.

- **IMPORT_CONNECT_USERS={1 | 0}**

  Specifies whether to add the imported users to the appropriate imported groups in the database.

- **IMPORT_CHANGE_OWNER={1 | 0} NEW_OWNER_NAME=***name*

  Specifies someone other than you as an owner of the imported data.

- **IMPORT_FROM_DOMAIN={1 | 0} IMPORT_DOMAIN_NAME=***name*

  Specifies whether to import the accessor data from the defined domain.

Note: By default, all of these options are not specified (equivalent to a value of 0).

INSTALLDIR=\"*location*\"

Defines the location where CA ControlMinder installs.

Default: C:\Program Files\CA\AccessControl

MAINFRAME_PWD_SYNC={1 | 0}

Specifies whether the mainframe password synchronization feature is installed (1).

Default: 0 (not installed)

NEW_KEY=\"*name*\"

Defines the SSL key that authenticates communication between the Distribution Server and the SAM Agent and Report Agent.

PMDB_CLIENT={1 | 0}

Specifies whether the local CA ControlMinder database is subscribed to a parent Policy Model database.

Default: 0 (no)

If you specify this option and set it to 1, specify the following:

- **PMDB_PARENTS_STR=\"***parents***\"**

  Defines a comma-separated list of parent Policy Model databases the local CA ControlMinder database is subscribed to. Specify _NO_MASTER_ as a parent PMDB to indicate that the local database accepts updates from any PMDB.

  Default: *none*

- **PWD_POLICY_NAME=\"***name***\"**

  Defines the name of the password Policy Model.

  Default: *none*

PMDB_PARENT={1 | 0}

Specifies whether a Policy Model parent database is created. If you specify this option and set it to 1, specify the following:

- **PMDB_NAME=\"***name***\"**

  Defines the name of the PMDB to create.

  Default: pmdb

- **PMDB_SUBSCRIBERS_STR=\"***subs***\"**

  Defines a space-separated list of subscriber databases to which the PMDB specified with the PMDB_NAME option propagates changes to. Essentially, these are the subscriber databases for the installed PMDB parent.

PUPM_INTEGRATION={1 | 0}

Specifies whether the SAM Agent is installed (1).

Default: 0 (not installed)

If you specify this option and set it to 1, specify DIST_SERVER_NAME, DIST_SERVER_PORT, and USE_SECURE_COMM.

REPORT_AGENT={1 | 0}

Specifies whether the Report Agent is installed (1).

Default: 0 (not installed)

If you specify this option and set it to 1, specify DIST_SERVER_NAME, DIST_SERVER_PORT, USE_SECURE_COMM, and the following parameters:

- **AUDIT_ROUTING={1 | 0}**

  Specifies whether the Audit Routing feature is installed (1).

  Default: 0 (not installed)

- **REPORT_DAYS_SCHEDULE=***days*

  Defines a comma-separated list of days on which the Report Agent runs.

  Values: Sun, Mon, Tue, Wed, Thu, Fri, Sat

  Default: *none*

- **REPORT_TIME_SCHEDULE={***hh*:*mm***}**

  Defines the time at which the Report Agent runs on designated days (for example, 14:30).

  Limits: *hh* is a number in the range 0-23 and *mm* is a number in the range 0-59

  Default: *none*

TASK_DELEGATION={1 | 0}

Specifies whether the task delegation feature is enabled.

Default: 1 (enabled).

UNICENTER_INTEGRATION={1 | 0}

Specifies whether the Unicenter Integration feature is enabled (1). This feature is only available if you have Unicenter NSM installed on this computer.

Default: 0 (not enabled)

If you specify this option and set it to 1, specify the following:

- **SEND_DATA_TO_TNG={1 | 0}**

  Specifies if audit data is sent to Unicenter NSM (1).

  Default: 1 (data is sent)

- **OTHER_TNG_HOST_NAME=\"***name***\"**

  Defines the host to which the audit data is sent to.

  Default: Host name specified in Unicenter NSM

- **SUPPORT_TNG_CALENDAR= {1 | 0}**

  Specifies if the Unicenter NSM calendar is supported (1).

  Default: 1 (supported)

- **TNG_REFRESH_INTERVAL=\"***mm***\"**

  Defines the refresh interval in minutes. Verify that you also set SUPPORT_TNG_CALENDAR=1.

  Default: 10

- **UNICENTER_MIGRATION={1 | 0}**

  Specifies if Unicenter security data is migrated to CA ControlMinder (1).

  Default: 1 (migrated)

USE_SECURE_COMM={1 | 0}

Specifies whether the SAM Agent and the Report Agent use secure communication (1).

Default: 0 (no)

If you specify this option and set it to 1, then specify the value of the SSL key in NEW_KEY.

USE_SSL={1 | 0}

Specifies whether to set up SSL for communication encryption.

Default: 0 (no)

If you specify this option and set it to 1, then specify the following:

- **CERT_OPTION={1 | 2}**

  Specifies which certification option to use.

  Values: 1—Generate CA ControlMinder certificate; **2**—Use an existing installed certificate.

  Default: 1

- **GENERATE_OPTION={1 | 2}**

  Specifies how to generate the CA ControlMinder certificate. Verify that you set CERT_OPTION=1.

  Values: 1—Use default root certificate; **2**—Specify root certificate.

- **SERVER_PRIV_KEY_PWD=\"***password***\"**

  Defines the password for the private key for the generated CA ControlMinder certificate. Verify that you set CERT_OPTION=1.

- **GEN_ROOT_CERT=\"***file***\"**

  Defines the fully qualified file name of the root certificate file (.pem). Verify that you set CERT_OPTION=1 and GENERATE_OPTION=2.

- **GEN_ROOT_PRIVATE=\"***file***\"**

  Defines the fully qualified file name of the root private key file (.key). Verify that you set CERT_OPTION=1 and GENERATE_OPTION=2.

- **ROOT_PRIV_KEY_PWD=\"***password***\"**

  Defines the password for the root private key. Verify that you set CERT_OPTION=1 and GENERATE_OPTION=2.

- **EXIST_ROOT_CERT=\"***file***\"**

  Defines the fully qualified file name of the root certificate file (.pem). Verify that you set CERT_OPTION=2.

- **EXIST_SERVER_CERT=\"***file***\"**

  Defines the fully qualified file name of the server certificate file (.pem). Verify that you set CERT_OPTION=2.

- **EXIST_PRIVATE_KEY=\"***file***\"**

  Defines the fully qualified file name of the server private key file (.key). Verify that you set CERT_OPTION=2.

- **EXIST_PRIV_KEY_PWD=\"***password***\"**

  Defines the password for the server private key. Verify that you set CERT_OPTION=2.

USE_SYMT_KEY={1 | 0}

Specifies whether to set up symmetric key encryption for communication. If USE_SSL=0, this parameter is set to 1.

Default: 1

If you specify this option and set it to 1, then you also specify the following:

- **ENCRYPTION_METHOD={Default | DES | 3DES | 256AES | 192AES | 128AES}**

  Specifies the encryption method to use for communications.

  Default: 256AES

- **CHANGE_ENC_KEY={1 | 0}**

  Specifies to change the default encryption key (1).

  Default: 1 (yes)

- **NEW_ENCRYPT_KEY=\"***key***\"**

  Defines the encryption key if you select to change the default encryption key. Also set CHANGE_ENC_KEY=1.

Example: Use the setup Command to Set Installation Defaults

The following example sets the installation directory, defines installation log file defaults for the CA ControlMinder installation, then opens the graphical installation program.

```
setup.exe /s /v"INSTALLDIR="C:\Program Files\CA\AccessControl" /L*v
%SystemRoot%\eACInstall.log"
```

Examples: Use the setup Command to Specify Encryption Settings

The following examples install CA ControlMinder in silent mode with various encryption settings. In each example, the command also installs CA ControlMinder, installs the default Report Agent and Task Delegation features, enables SSL, and defines the path and name of the installation log file:

- This example generates a server certificate from the default CA ControlMinder root certificate and defines the password for the server private key:

  ```
  setup.exe /s /v"qn COMMAND=proceed USE_SSL=1 CERT_OPTION=1 GENERATE_OPTION=1
  SERVER_PRIV_KEY_PWD=\"P@ssw0rd\" /l*v C:\AC_silent.log"
  ```

- This example generates a server certificate from a third-party root certificate. The root private key is password-protected:

  ```
  setup.exe /s /v"qn COMMAND=proceed USE_SSL=1 CERT_OPTION=1 GENERATE_OPTION=2
  GEN_ROOT_CERT=\"C:\Crypto\example.pem\"
  GEN_ROOT_PRIVATE=\"C:\Crypto\example.key\" ROOT_PRIV_KEY_PWD=\"P@ssw0rd\" /l*v
  C:\AC_silent.log"
  ```

- This example specifies that CA ControlMinder uses third-party root and server certificates. The server private key is password-protected:

  ```
  setup.exe /s /v"qn COMMAND=proceed USE_SSL=1 CERT_OPTION=2
  EXIST_ROOT_CERT=\"C:\Crypto\example.pem\"
  EXIST_SERVER_CERT=\"C:\Crypto\server.pem\"
  EXIST_PRIVATE_KEY=\"C:\Crypto\server.key\" EXIST_PRIV_KEY_PWD=\"P@ssw0rd\"
  /l*v C:\AC_silent.log"
  ```

More information:

Communication Encryption (see page 453)

Upgrade a Windows Endpoint

When you upgrade an endpoint, the CA ControlMinder installation program upgrades the core CA ControlMinder functionality and any features that are already installed on the endpoint. You can choose to install new features after you upgrade the core CA ControlMinder functionality.

Note: You may have to reboot the computer to complete the upgrade. For information about which releases of CA ControlMinder require a reboot when you upgrade, see the *Release Notes*.

To upgrade an endpoint

1. Log into the Windows system as a user with Windows administrative privileges (that is, as the Windows administrator or a member of the Windows Administrators group.)
2. Close any applications that are running on your Windows system.
3. Insert the CA Access Control Endpoint Components for Windows DVD into your optical disc drive.

   If you have autorun enabled, the Product Explorer automatically appears. Otherwise, navigate to the optical disc drive directory and double-click the PRODUCTEXPLORERX86.EXE file.
4. From the Product Explorer main menu, expand the Components folder, select CA Access Control for Windows (*my_architecture*), then click Install.

   Note: The installation option that matches the architecture of the computer is highlighted to show that there is an existing installation of CA ControlMinder on the computer.

   A dialog appears asking if you want to perform an upgrade of CA ControlMinder.
5. Click Yes.

   The CA ControlMinder installation program starts loading and, after a short while, the Introduction screen appears.
6. Follow the instructions on the installation screens.

   The installation program upgrades CA ControlMinder. When the upgrade is complete, you are given the choice of restarting Windows now or later.
7. (Optional) Select Yes to restart your computer now.

   The computer reboots and the upgrade completes.

8. (Optional) Install additional CA ControlMinder features, as follows:
   a. Click Start, Control Panel, Add or Remove Programs.
   b. Scroll through the program list and select CA ControlMinder, and click Change.

      The CA ControlMinder installation program starts loading and, after a short while, the Program Maintenance screen appears.
   c. Select Modify and follow the instructions on the installation screens to install the features.

      During the installation, the installation program prompts you to supply information. For the information that you need when installing the features, refer to the installation worksheets (see page 149). You may need to reboot your computer for the installation to complete.

Starting and Stopping CA ControlMinder

By default, CA ControlMinder services start automatically whenever you start Windows.

Stop CA ControlMinder

You use the secons utility to stop CA ControlMinder on local and remote computers. You do not require any specific Windows privileges to stop CA ControlMinder, but you must have the ADMIN or OPERATOR attribute in CA ControlMinder.

Note: You cannot stop CA ControlMinder while it is running from Windows Services Manager. You must use the secons utility to stop CA ControlMinder before you modify a CA ControlMinder service in Windows Services Manager.

To stop CA ControlMinder

1. Open a command prompt window and navigate to the directory containing the CA ControlMinder binaries.

   By default, the CA ControlMinder binaries are located at C:\Program Files\CA\AccessControl\bin.

2. Enter the following command:

   `secons -s [hosts | ghosts]`

   -s [*hosts* | *ghosts*]

   Shuts down the CA ControlMinder services on the defined, space-separated, remote hosts. If you do not specify any hosts, CA ControlMinder shuts down on the local host.

   You can define a group of hosts by entering the name of a ghost record. If you use this option from a remote terminal, the utility requests password verification. You also need admin privileges on both the remote and local computers, and write permission to the local computer on the remote host database.

   When you stop CA ControlMinder on a local computer, the following message appears:

   `CA ControlMinder is now DOWN`

   When you stop CA ControlMinder on remote hosts, CA ControlMinder reports whether the remote host shutdown was successful. An attempt is made to shut down each host on the list, even if the remote host preceding it was not shut down successfully.

Start CA ControlMinder Manually

Typically, you start CA ControlMinder by starting Windows.

If you stopped CA ControlMinder, you can also restart it manually by issuing commands from the command prompt.

To start CA ControlMinder manually

1. Be sure you are logged in to the Windows system as a user with Windows administrative privileges (that is, as the Windows administrator or a member of the Windows Administrators group).
2. In a command prompt window, change to the directory containing the CA ControlMinder binaries (by default, C:\Program Files\CA\AccessControl\bin on your system directory).
3. Start CA ControlMinder by entering:

   ```
   seosd -start
   ```

Checking Your Installation

If you have installed CA ControlMinder successfully, you will notice the following changes:

- A new key is added to the Windows registry:

  ```
  HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl
  ```

  While CA ControlMinder is running, the CA ControlMinder keys and sub-keys are protected and you can modify the keys only through CA ControlMinder Endpoint Management or by using selang commands. However, you do not need to use CA ControlMinder Endpoint Management or selang commands to read the keys and values.

- When you restart your computer, several new CA ControlMinder services start automatically. These services include the Watchdog, Engine, and Agent, which are always installed. Other services, such as Task Delegation, exist depending on the options you chose during installation. The Display name for all CA ControlMinder services begins with "CA ControlMinder". You can check what services are installed, and verify that these services are running, using Windows Services Manager.

Displaying Login Protection Screen

By default, after you install CA ControlMinder, every time a user logs in interactively (GINA) and CA ControlMinder services are running, a protection screen appears, telling the user that this computer is protected by CA ControlMinder.

The splash screen displays for four seconds and closes automatically.

To disable this protection message, change the HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\AccessControl\SplashEnable registry key value from 1 to 0.

Configure an Endpoint for Advanced Policy Management

Once you install the advanced policy management server components, you need to configure each endpoint in your enterprise for advanced policy management. In doing so, you configure the endpoint to send information to and receive information from the server components.

Note: This procedure shows you how to configure an existing installation of CA ControlMinder for advanced policy management. If you specified this information when you installed CA ControlMinder on the endpoint you do not need to configure the endpoint again.

To configure an endpoint for advanced policy management, open a command window and enter the following command:

`dmsmgr -config -dhname dhName`

dhName

Defines a comma-separated list of Distribution Host (DH) names you want the endpoint to work with.

Example: DH__@centralhost.org.com

This command configures the endpoint for advanced policy management and sets it to work with the defined DH.

Note: For more information, see the dmsmgr -config command in the *Reference Guide*.

Configure a Windows Endpoint for Reporting

Once you have CA ControlMinder Endpoint Management and the Report Portal installed and configured, you can configure your endpoints to send data to the Distribution Server for processing by enabling and configuring the Report Agent.

Note: When you install CA ControlMinder, it lets you configure the endpoint for reporting. This procedure illustrates how you configure an existing endpoint for sending reports if you did not configure this option at install time.

To configure a Windows endpoint for reporting

1. Click Start, Control Panel, Add or Remove Programs.

   The Add or Remove Program dialog appears.

2. Scroll through the program list and select CA ControlMinder.

3. Click Change.

   The CA ControlMinder installation wizard appears.

4. Follow the wizard prompts to modify the CA ControlMinder installation so that you enable the Report Agent feature.

Note: After you enable the Report Agent, you can modify CA ControlMinder configuration settings to change performance-related settings. For more information on Report Agent configuration settings, see the *Reference Guide*.

Customizing CA ControlMinder for Cluster Environments

To use CA ControlMinder in a cluster environment, you must install CA ControlMinder on each node of the cluster. Define the same set of rules (quorum disk or network if you use network interception) for common resources on each node as well.

CA ControlMinder can detect that it is running in a cluster environment. If CA ControlMinder detects that the cluster has its own network with separate network adapters used for cluster internal communications only, network interception is disabled for these network adapters. For network interfaces that connect the cluster to the rest of the enterprise, network interception works as usual.

Note: This feature is not enabled if the cluster uses the same network interface for cluster internal communications *and* communication to the rest of the network.

Example

Suppose you have two nodes:

- NODE1 that has two IP addresses:
  - 10.0.0.1 is an internal cluster network IP address.
  - 192.168.0.1 is an outside network connection.
- NODE2 has also two IP addresses
  - 10.0.0.2 is an internal cluster network IP address.
  - 192.168.0.2 is an outside network connection.

  The cluster itself has an additional IP address of 192.168.0.3.

Network interception does not prevent NODE1 from connecting to NODE2 and vice versa as long as they do their communications using the internal cluster network IP addresses.

Network interception acts as defined by CA ControlMinder rules if NODE1 or NODE2 are contacted using outside network IP addresses.

In addition, network interception acts as defined by CA ControlMinder rules if the cluster is contacted at its 192.168.0.3 IP address.

Uninstallation Methods

You can use the following methods to uninstall CA ControlMinder from a Windows endpoint:

- Regular uninstallation—This method uses a graphical interface to uninstall CA ControlMinder and provides interactive feedback.
- Uninstall silently—This method uses the command line to uninstall CA ControlMinder without interactive feedback.

Uninstall CA ControlMinder

Be sure you are logged in to the Windows system as a user with Windows administrative privileges (that is, as the Windows administrator or a member of the Windows Administrators group).

To uninstall CA ControlMinder

1. (Optional) Shut down CA ControlMinder (see page 169).

   Note: If you do not do this manually, the installation program shuts CA ControlMinder down for you.

2. Choose Start, Settings, Control Panel.

   The Windows Control Panel appears.

3. Double-click Add/Remove Programs.

   The Add/Remove dialog appears.

4. Select CA ControlMinder from the installed programs list and click Add/Remove.

5. In the message box confirming that you want to remove CA ControlMinder, click Yes.

6. When uninstall is complete, click OK.

7. Reboot the computer to remove all CA ControlMinder components.

Uninstall CA ControlMinder Silently

To uninstall CA ControlMinder without interactive feedback, you can uninstall CA ControlMinder silently using the command line. Be sure you are logged in to the Windows system as a user with Windows administrative privileges (that is, as the Windows administrator or a member of the Windows Administrators group).

To uninstall CA ControlMinder r12.5 silently, enter the following command:

```
Msiexec.exe /x{822BFADC-E040-4F5C-A00A-B8E558A2D616} /qn insert_params_here
```

The *<insert_params_here>* variable specifies the installation settings you want to pass to the installation program. For example, this command uninstalls CA ControlMinder creates an uninstall log in c:\ac_uninst.log:

```
Msiexec.exe /x{822BFADC-E040-4F5C-A00A-B8E558A2D616} /qn /l*v c:\ac_uninst.log
```

Note: If you do not do this manually, the installation program shuts CA ControlMinder down for you.

Chapter 8: Installing and Customizing a UNIX Endpoint

This chapter guides you through the CA ControlMinder UNIX endpoint installation process. When you have finished installing CA ControlMinder following the instructions in this chapter, your system contains a copy of the CA ControlMinder endpoint software and an elementary CA ControlMinder database. The chapter then explains how to start CA ControlMinder and how to use its commands. Later, by editing the database, you can define access rules to protect your system.

This section contains the following topics:

Before You Begin

Before you can install CA ControlMinder, you must make sure that the preliminary requirements are met and that you have all of the necessary information.

Operating System Support and Requirements

You can install CA ControlMinder on any one of the supported UNIX operating systems.

Note: For more information, check the *Release Notes*.

Administration Terminals

You can administer CA ControlMinder policy from a central place using CA ControlMinder Endpoint Management and CA ControlMinder Enterprise Management, or by connecting to the computer with command line (selang) and updating the access rules directly on the computer.

To update the computer's access rules directly, you need write access on the terminal you are managing from and the *admin* attribute on the computer policy in the CA ControlMinder database.

By default, CA ControlMinder installation sets up terminal authority only for the local computer terminal. You can change that by either disabling this option from a local terminal or adding more terminals that can manage remotely.

To add the administration option for the terminal *my_terminal* to the computer *my_machine* using the user *my_user*, write the following selang rules:

```
er terminal my_terminal owner(nobody) defaccess(r)
auth terminal my_terminal xuid(my_user) access(all)
```

These rules let everyone log in to this terminal (regular login, not CA ControlMinder management), and let enterprise user *my_uid* log in to the computer and use CA ControlMinder management tools (selang, CA ControlMinder Endpoint Management, and so on).

Note: If the administrators are using CA ControlMinder Endpoint Management to administer CA ControlMinder, you only need to define the computer where CA ControlMinder Endpoint Management is installed. You do not need to define the computer where the administrator opens the browser.

Installation Notes

When installing CA ControlMinder (whether for the first time or as part of an upgrade), note the following points:

- Read the *Release Notes*.

  This document contains information about supported platforms, known issues, considerations, and other important information. Read the *Release Notes* before installing CA ControlMinder.

- If your environment is set up with a PMDB hierarchy or you are setting such an environment, we recommend that you:

  - Install or upgrade the Deployment Map Server (DMS) computer first.

    This is only required if you are going to use advanced policy-based management, and ensures that the DMS registers each Policy Model node and its subscribers.

  - Install or upgrade each computer in your hierarchy bottom-up (subscribers first).

    Upgraded PMDBs having subscribers with an earlier version may result in erroneous commands being sent. This can happen as a result of new PMDBs containing classes and properties that do not exist in the earlier version PMDBs.

    Note: A PMDB hierarchy running on a single computer can be upgraded simultaneously.

  - Do *not* upgrade during PMDB or policy updates.

  - Back up subscriber and PMDB policies.

  Note: Earlier PMDB versions are permitted to have later versions of subscribers. As commands in earlier versions are supported in later versions, earlier PMDBs can propagate to CA ControlMinder r12.0 subscribers.

- If you are upgrading from a pre- r12.0 version:

  - Programs that should be bypassed by STOP are now defined as database rules; SPECIALPGM records of a *stop* type.

  - Programs that should be bypassed by SURROGATE are now defined as database rules; SPECIALPGM records of a *surrogate* type.

  Note: The upgrade process converts old definitions (kept in a file) to the new database rules. Add these new rules to any existing selang scripts.

- You can upgrade the existing seos.ini and pmd.ini files, or can create new ones.

  Either way, the installation script saves a copy of the old seos.ini file as seos_ini.back and a copy of each pmd.ini file as pmd_ini.back (in its respective Policy Model directory).

- CA ControlMinder backs up the following existing files during an upgrade: serevu.cfg, audit.cfg, trcfilter.init, and sereport.cfg.

  If you want to keep the changes you made to these files, use the backed up files.

- If you are upgrading an existing database, we recommend that you:

  - Back it up first.

    Use dbmgr -b to backup the database.

  - Ensure that there are no subscribers in *sync* mode.

    Use sepmd -L to verify subscriber's status.

- Unicenter security integration and migration is only available for AIX, HP-UX PA-RISC, Solaris SPARC, and Linux x86 platforms.

- Unicenter TNG and CA ControlMinder for UNIX

  If you have a version of Unicenter TNG installed earlier than Unicenter NSM 3.0, install the following Unicenter TNG fix to permit CA ControlMinder to get process information:

  - HP-UX users with Unicenter TNG 2.4, install fix QO01182.
  - Linux users with Unicenter TNG 2.4, install fix PTF LO91335.
  - Sun users with Unicenter TNG 2.4, install fix QO00890.

  Note: Users with AIX 5.x running Unicenter NSM 3.0 must contact the CA Technologies Unicenter support team for a compatibility patch. Install this compatibility patch before installing CA ControlMinder on the host.

- To install Unicenter related options (install_base options: -uni or -mfsd) on Linux s390, you must have korn shell (ksh) installed before you install CA ControlMinder.

  The setup script for CCI Standalone (CCISA) uses ksh which is not installed by default on Linux.

- To install CA ControlMinder 32-bit binaries on Linux x86 64-bit we recommend that you use the _LINUX_*xxx*.tar.Z or CAeAC-*xxxx*-*y*.*y*.*iiii*.i386.rpm installation packages. These installation packages install 32-bit CA ControlMinder binaries on Linux x86 64-bit systems. If you are upgrading, these packages maintain compatibility with the previous 32-bit CA ControlMinder installation. Before you install CA ControlMinder, ensure that the following operating system 32-bit libraries are installed:

- ld-linux.so.2
- libICE.so.6
- libSM.so.6
- libX11.so.6
- libXext.so.6
- libXp.so.6
- libXt.so.6
- libc.so.6
- libcrypt.so.1
- libdl.so.2
- libgcc_s.so.1
- libm.so.6
- libncurses.so.5
- libnsl.so.1
- libpam.so.0
- libpthread.so.0
- libresolv.so.2
- libstdc++.so.5
- libaudit.so.0 (RHEL5 and OEL 5)
- libaudit.so.1 (REHL6 and OEL6 and up only)

The following is a list of relevant RPM packages that are required:

- SLES 10: compat-libstdc++, glibc-32bit, libgcc, ncurses-32bit, pam-32bit, xorg-x11-libs-32bit
- SLES 9: glibc-32bit, libgcc, libstdc++, ncurses-32bit, pam-32bit, XFree86-libs-32bit
- RHEL 6: ksh, dos2unix, libgcc_s.so.1, libpthread.so.0, libstdc++.so.6
- RHEL 5 and OEL 5: audit-libs, compat-libstdc++, glibc, libgcc, libICE, libSM, libXext, libXp, libXt, ncurses, pam
- RHEL 4 and OEL 4: compat-libstdc++, glibc, libgcc, ncurses, pam, xorg-x11-deprecated-libs, xorg-x11-libs
- RHEL 3: glibc, libgcc, libstdc++, ncurses, pam, XFree86-libs

- To install CA ControlMinder 64-bit binaries on Linux x86 64-bit, use the _LINUX_X64_*xxx*.tar.Z or CAeAC-*xxxx*-*y*.*y*.*iiii*.x86_64.rpm installation packages. If you use these installation packages, you do not have to install any additional RPM packages.

  Note the following points before installing or upgrading CA ControlMinder 64-bit binaries on Linux x86 64-bit:

  - The 64-bit installation package does not support CA ControlMinder GUI utilities, such as selock and selogo.
  - If the install_base script can access both the 32-bit and 64-bit tar files in a new installation, the install_base script uses the 64-bit tar file by default. To override this behavior, specify the desired tar file when you run the install_base command. If you install the 64-bit RPM package, you install only 64-bit binaries and libraries. For example:

    ```
    ./install_base_LINUX_X64_125.tar.Z
    ```

  - Any applications that are built and linked to the API must be rebuilt for the 64-bit installation. Use the LINUX64 target to build 64-bit API samples. This target uses D64BIT and -D64BITALL (-m32 removed). You need -m elf_x86_64 to build libraries.
  - If you use the install_base script to upgrade to a 64-bit CA ControlMinder installation from a 32-bit installation, set the -force_install flag prior to installation. The installation fails if you do not set this flag.
  - To fully uninstall cawin after uninstalling CA ControlMinder, use rpm -e --allmatches to ensure that the uninstall process removes both 32-bit and 64-bit versions of cawin.

- To install CA ControlMinder on Linux s390x 64-bit, ensure that the following operating system 32-bit libraries are installed:
  - ld.so.1
  - libcrypt.so.1
  - libc.so.6
  - libdl.so.2
  - libICE.so.6
  - liblaus.so.1 (SLES 8, RHEL 3)
  - libaudit.so.0 (RHEL 4, RHEL 5)l
  - ibm.so.6l
  - ibnsl.so.1
  - libpam.so.0
  - libresolv.so.2
  - libSM.so.6
  - libX11.so.6
  - libXext.so.6
  - libXp.so.6
  - libXt.so.6

  The following RPM packages are required:
  - SLES 10: glibc-32bit, pam-32bit, xorg-x11-libs-32bit
  - SLES 9: XFree86-libs-32bit, glibc-32bit, pam-32bit
  - RHEL 5: audit-libs, libXp, glibc, libICE, libSM, libX11, libXext, libXt, pam
  - RHEL 4: audit-libs, glibc, pam, xorg-x11-deprecated-libs, xorg-x11-libs
  - RHEL 3: glibc, laus-libs, pam
- If you use the install using the install_base script CA ControlMinder on Linux s390x, specify to use the ca-lic-01.90.04-00.s390x.rpm package to install CA_LIC.
- If you install CA ControlMinder on Linux and Linux-IA64 platforms using the -all option, mfsd is not installed.
- If you install CA ControlMinder on Solaris, install the SUNWlibc (Sun Workshop Compilers Bundled libC) package.
- CA ControlMinder is installed to use the Solaris SMF service automatically.
- Before you install CA ControlMinder 32-bit binaries on a 32-bit or 64-bit Linux computer, verify that the libstdc++.so.5 32-bit library is installed. If you do not install this library, the ReportAgent daemon will not start after you install CA ControlMinder.

- Before you install CA ControlMinder on Linux, specify the home directory in the environment.
- Before you install CA ControlMinder on Solaris 8, verify that the libCstd library level is 1.2 or later.
- Before installing the Enterprise Management Server verify that CA ControlMinder Endpoint kernels are unloaded and not present in the system.

UNIX Installation Parameter File-Customize UNIX Installation

The UNIX parameters file contains installation parameters that you can customize for your requirements. The parameters file contains customizable parameters for specific areas of the CA Control Minder package. For a particular parameter to take effect the corresponding shell variable must be set.

The parameter files conform to shell syntax and must contain *key=value* pairs. Use the parameter files from the package you want to install.

This file has the following format:

ADMIN_USERS

Defines users as security administrators.

Note: Security administrators can assign access rights to authorized users, manage privilege user passwords, and report on user activities.

Values: A space-separated list of user IDs, none

Default: none (Only root is defined as a security administrator)

API_INSTALL

Specifies whether to install the API package.

Values: yes, no

Default: no

APMS_ADMIN_USERS

Defines administrators for Advanced Policy Management Server components other than the local host.

Values: A space-separated list of users, none

Default: none

APMS_DESKTOP

Defines Advanced Policy Management Server components administration computers other than the local host.

Values: A space-separated list of computers, none

Default: none

APMS_DIST_MODE

Defines whether an advanced policy management server is running in the distribution mode.

Values: yes, no

Default: no

AUDIT_BK

Specifies whether to keep time-stamped backups of the audit file.

Notes:

- Specify *yes* to send audit data to the Report Server.
- CA Control Minder backs up the audit file when the specified size limit is reached.

Values: yes, no

Default: no

AUDIT_GROUP

Specifies the name of the group reading CA Control Minder audit files.

Values: Any existing group name, none.

Default: none (only root can read audit files)

Note: The root user can read the audit files unless you deny access using CA Control Minder access rules.

CLIENT_INSTALL

Specifies whether to install the client package.

Values: yes, no

Default: yes

DH_NAME

Defines the name of the Distribution Hosts (DH) on the endpoint Advanced Policy Management Server components host.

Values: A space-separated DH list in the format *dh1@host1 dh2@host1,* none

Default: none

DIST_SRV_HOST

Defines the message queue host names.

Values: A comma-separated list of valid host names, none

Default: none

DIST_SRV_PORT

Defines the message queue port.

Values: 7243 (for a ssl protocol), 7222 (for a non-ssl protocol)

Default: 7243

DIST_SRV_PROTOCOL

Defines the message queue communication protocol.

Values: ssl, tcp

Default: ssl

DRDH_NAME

Defines the names of the endpoint Disaster Recovery Distribution Hosts (DR DH).

Values: A space-separated DR DH list in the format *dr_dh1@drhost dr_dh2@drhost,* none

Default: none

ENABLE_ELM

Specifies whether CA Control Minder sends endpoint audit data to the report server.

Note: If you specify *yes*, set CA Control Minder to keep audit backups (AUDIT_BK=*yes*).

Values: yes, no

Default: no

ENABLE_KBL

Specifies whether CA Control Minder enables the KBL audit records manager.

Values: yes, no

Default: no

ENCRYPTION_METHOD_SET

Defines whether to use symmetric encryption, asymmetric encryption (public key), or both.

Values: 1 (Symmetric key), 2 (Public key), 3 (Public key and Symmetric key)

Default: 1

Notes:

- For public key encryption, you need a root certificate.
- For symmetric encryption, choose an encryption method (TRIPLEDES, DES, or AES).
- To configure FIPS only encryption, set the FIPS_ONLY parameter to *yes*.

Important! The encryption method must be the same on all CA Control Minder hosts. Earlier CA Control Minder releases configured a simple symmetric encryption method by default.

ETC_SEOS_SYMLINK

Defines whether a link is created in the /etc directory that points to the CA Control Minder installation directory.

Values: yes, no

Default: yes

FIPS_ONLY

Specifies whether CA Control Minder works in the FIPS only mode.

Note: In this mode, all non-FIPS functions are disabled and the encryption method is set to FIPS only.

Values: yes, no

Default: no

FORCE_ENCRYPT

Specifies whether the installation warns you about using a nondefault encryption key.

Note: After the upgrade, your encryption key is set to the default.

Values: yes, no

Default: no

FORCE_INSTALL

Specifies whether to force installation over an existing installation of the same CA Control Minder version. FORCE_INSTALL also specifies if the installation directory is different from the installation directory set in the new CA Control Minder package.

Values: yes, no

Default: no

FORCE_KERNEL

Specifies whether the installation warns you when the old kernel module cannot be unloaded.

Note: If you specify *no*, reboot the system after the upgrade is complete.

Values: yes, no

Default: no

INST_PHASE1

Specifies whether to install the baseline security pack.

Notes:

- The baseline security pack defines basic rules that protect the operating system.
- You can install the baseline security pack after the installation using the *install_baseline.sh* utility.
- To activate the rule protection after an install test period (recommended), disable the warning mode.

Values: yes, no

Default: no

INSTALL_ACCOUNT_MNG

Specifies whether you want to configure endpoint JCS Management.

Note: To configure the AccountManager, set the Distribution Server parameters.

Values: yes, no

Default: no

INSTALL_APMC

Specifies whether to configure the endpoint for advanced policy management.

Note: Each CA Control Minder endpoint must be configured to receive updates from the advanced policy management server components.

Values: yes, no

Default: yes

INSTALL_APMS

Specifies whether to install the advanced policy management server components to centrally managed policy deployments.

Note: We recommend that you install advanced policy management server components on a central computer.

Values: yes, no

Default: no

INSTALL_PUPM

Specifies whether you want to configure the PUPM Agent.

Values: yes, no

Default: no

INSTALL_RA

Specifies whether you want to configure endpoint Message Queues.

Values: yes, no

Default: no

JAVA_HOME

Defines the path to the installed Java environment.

Note: The Java environment path depends on the version and the platform. For example, on IBM J2SE Version 5.0 installed on Linux390, JAVA_HOME=*/opt/ibm/java2-s390-50/jre*.

Values: path to the installed Java environment

Default: java_home (the value in accommon.ini is set during installation)

JCS_SERVER_DN

Specifies the JCS server Distinguished Name (DN).

Values: A valid DN format string

Default: dc=im,dc=etasa

JCS_SERVER_PORT

Specifies the JCS port.

Values: Port number

Default: 20411

JCS_SSL

Defines the JCS communication protocol.

Values: yes (for SSL connection), no

Default: yes

JCS_USER_DN

Specifies the JCS administrative user Distinguished Name (DN).

Values: Any valid DN format string

Default: cn=root,dc=etasa

JCS_USER_PSSWD

Specifies the JCS administrative user password.

Note: Wildcards (*)replace the JCS_USER_PSSWD after the installation.

Values: Any valid DN format string

Default: No default value

LANG

Defines the CA Control Minder installation language.

Example: To install CA Control Minder with Japanese EUC support, LANG=*ja_JP*. For a complete list of supported languages, use the command *locale -a*.

Notes:

- To install a localized HP-UX package, set this token.
- If you specify this parameter, the installer LANG environment variable is ignored.

Values: A supported language string

Default: English

LIB_ENCRYPTION

Defines the encryption method that is used to protect communication between <eCA> programs and CA Control Minder installed hosts.

Notes:

- The encryption method must be the same on all CA Control Minder hosts that communicate with each other.
- This option requires that SET_SYMMETRIC is set to *yes*.

Values: 99 (AES2526), 1 (SCRAMBLE), 2 (DES), 3 (TRIPLEDES), 4 (AES128), 5 (AES192)

Default: 99

LIC_CMD

Defines the command that accepts the license agreement.

Notes:

- This command can be found inside the license agreement in square brackets.
- The license agreement file is: eACLicenseAgreementUNIX_english_cp1252.txt

Important! The LIC_CMD command is required to install CA Control Minder.

LIC_INTALL_DIR

Defines the CA license installation location.

Values: Any absolute path name.

Default: /opt/CA/SharedComponents (Same as lic98 default)

LOG_FILE_NAME

Defines the installation log file name that is created in the $SEOSDIR.

Values: Any valid file name.

Default: AccessControl_install.log

MFSD_INSTALL

Specifies whether to install the Mainframe Synchronization Support Daemon.

Values: yes, no

Default: no

NO_TNG_INT

Specifies whether to set up the selogrd/TNG integration.

Values: yes (attempts to set up selogrd/TNG integration), no (selogrd/TNG integration does not take place)

Default: no

OS_USERS

Specifies OS database administrators.

Values: A space-separated list of users, none

Default: none

PARENT_PMD

Defines a list of Policy Model Databases (PMDBs) from which the computer accepts updates.

Note: The local CA Control Minder database rejects updates from any PMDB that is not specified in this list.

Values: _NO_MASTER_ (The local database accepts updated from any PMDB), A comma-separated list of PMDBs in the format *pmd1@host1, pmdb2@host1*, A path to a file that contains a line-separated list of PMDBs**,** none (The local database does not accept updates from any PMDBs).

Default: none

PASSWD_PMD

Specifies the Policy Model Database (PMDB) where sepass sends password updates.

Values: A PMDB in the format *pmd_name@hostname*, none

Default: none

Notes:

- Password updates support the password history checking.
- If you do not set the PASSWD_PMD, the value of the PARENT_PMD is inherited.
- The PARENT_PMD and PASSWORD_PMD tokens can have the same value.
- If the values of the PARENT_PMD and the PASSWORD_PMD are not the same, the PARENT_PMD database must be a child (subscriber) of the PASSWORD_PMD database.

POSTEXIT

Defines the full program or script path name that is executed after you run the post install script.

Values: yes, pathname

Default: no

PREINSTALL

Defines the full program or script path name that is executed before you run the post install script.

Values: yes, pathname

Default: no

PRIMARY_ENTM_NAME

Defines the Primary Enterprise Management server host name.

Values: string, none

Default: none

PROVIDE_OR_GEN_CERT

Specifies whether you generate a new subject certificate and key or provide an existing subject certificate and key.

Notes:

- To set up SSL, provide a subject certificate and key and a root certificate.
- The root certificate must be common among all computers using SSL communication.
- You can generate a subject certificate and key automatically from a default certificate or from a certificate you provide. You can also point CA Control Minder to an existing certificate.

Values: 1 (Generate a subject certificate and key), 2 (Provide an existing certificate and key)

Default: 1

PWFORCE

Defines the upgrade behavior when a PMDB update is in progress.

Notes:

- If you upgrade CA Control Minder, also upgrade the Policy Model Update files.
- If a *sepmd -n* command is running, the package installation aborts to let the sempd finish processing. You can set this parameter to *yes* to force the installation to proceed but the sepmd in progress may not complete properly.

Values: yes, no

Default: no

REPORT_SHARED_SECRET

Defines the shared secret for Message Queue SSL authentication.

Note: Wildcards(*) replace the shared secret after the installation.

Values: Any string

Default: Empty value

REPORT_SRV_QNAME

Defines the name of the queue where reports are sent.

Values: A string representing a queue name

Default: queue/snapshots

REPORT_SRV_SCHEDULE

Defines when reports are generated and sent to the report server.

Values: A string representing time and date in the format *time@day, day*

Example:19:22@Sun, Mon. (This example generates reports every Sunday and Monday at 19:22).

Default: 00:00@Sun, Mon, Tue, Wed, Thu, Fri, Sat

ROOT_CERT_KEY

Specifies the public key that is used for the subject key generation.

Values: The full path name to the subject certificate file, default

Default:default (the key that is provided with the installation package)

ROOT_CERT_PATH

Specifies the root certificate that is used for the subject certificate generation.

Values: The full path name to the subject certificate file, default

Default: default (The root certificate that is provided with the installation package)

SELINUX_POLICY

Specifies whether UNIX Authentication Broker activates the SELinux policy during installation.

Values: yes, no

Default: no

SEOS_GROUP

Defines the name of the group that owns the CA Control Minder files.

Values: Any existing group name.

Default: root

SERIAL_NUM

Defines the subject certificate serial number.

Note: To define a subject certificate serial number, CA Control Minder uses default values or accepts your input.

Values: A valid serial number, 0003ba39cc23

Limits: 3-247 characters

Default: 0003ba39cc23

SERVER_INSTALL

Specifies whether to install the server package.

Values: no, yes

Default: yes

SET_SYMMETRIC

Specifies whether to change the default symmetric encryption method.

Notes:

- Encryption protects communication between CA Control Minder programs and CA Control Minder installed hosts.
- The recommended (default) encryption method is a combination of public key and symmetric methods.
- In order to configure the symmetric encryption set the LIB ENCRYPTION.

Values: yes, no

Default: yes

SUBJECT_CERT_KEY_PATH

Specifies the public key location.

Values: The full path name to the subject certificate file

Default: SEOSDIR>/data/crypto/sub.key

SUBJECT_CERT_PATH

Specifies the subject certification location.

Note: To generate a subject certificate, specify the file location.

Values: The full path name to the subject certificate file

Default: SEOSDIR>/data/crypto/sub.pem

SUBJECT_EXP_DATE

Defines the subject certificate expiration date.

Note: To define a subject certificate expiration date, CA Control Minder uses default values or accepts your input.

Values: A date in the format *mm/dd/yy*

Default: 12/31/35

SUBJECT_NAME

Defines the subject certificate name.

Note: To define a subject certificate name, CA Control Minder uses default values or accepts your input.

Values: An LDAP format name, cn=any.string

Limits: 3-63 characters

Default: c=any.string

TNG_INSTALL

Specifies whether to install the Unicenter Integration and Migration packages.

Note: This package supports CA Control Minder integration and migration with CAUTIL, Workload Management, and Event Management components of Unicenter.

Values: yes, no

Default: no

UPDATE_ENCRYPT

Specifies whether to change the default encryption method which protects communication between CA Control Minder programs and CA Control Minder installed hosts.

Values: yes, no

Default: yes

UPDATE_PROFILE

Defines whether the CA_LIC updates the file */etc/*profile with *profile.ca loading*.

Values: yes, no

Default: yes

UPGRADE_KERNEL_UNLOAD

Specifies whether the installer will attempt to stop and unload the existing version of CA Control Minder when installing a different version.

Values: yes, no

Default: yes

USE_OSUSER

Enables OS user support.

Note: OS users are defined in the OS repository but not in the CA Control Minder database. If you enable OS users support, you can reference users not defined in the CA Control Minder database.

Values: yes, no

Default: yes

USE_STOP

Specifies whether to enable the STOP (Stack Overflow Protection) feature of CA Control Minder.

Values: yes, no

Default: no

USE_UXIMPORT

Specifies whether CA Control Minder imports native users and groups into the database.

Values: yes, no

Default: no

Note: The import process uses local host files or the local NIS maps as information sources. The time that is required to import users and groups depends on the number of users, groups, and hosts defined. You can also import this data into the CA Control Minder database after the installation using the UxImport utility.

UserBrandZone

(Solaris 10 only) Specifies that CA Control Minder is installed on a branded zone or that a branded zone with CA Control Minder installed is configured.

Note: If you set this value to *yes*, the installation changes the kernel communication mode to use iotcl instead of a sysscall.

Values: yes, no

Default: no

WITH_DNS

Specifies whether to use DNS to create the host look-alike database during installation.

Values: yes, no

Default: yes

Installation Considerations for Linux s390 Endpoints

If you want to use Message Queue functionality, to remotely manage UNAB on CA ControlMinder Linux s390 and use reporting capabilities on Linux IA64 you install J2SE version 5.0 or later on the endpoint.

Message Queue functionality lets you send report and audit data from CA ControlMinder endpoints to the Report Portal and CA User Activity Reporting Module, respectively. Remote management lets you use CA ControlMinder Enterprise Management to manage UNAB endpoints.

You can install J2SE before or after you install CA ControlMinder or UNAB on the endpoint. If you install J2SE after you install CA ControlMinder or UNAB, you must also configure the Java location on the endpoint.

How the Installation Interacts with Java

Valid on Linux s390, Linux s390x and Linux IA64

To use Message Queue functionality, to remotely manage UNAB Linux s390 endpoints and use reporting capabilities on Linux IA64 and Linux s390, you install a supported Java version on the endpoint.

When you install CA ControlMinder or UNAB on a Linux s390 or a Linux IA64 endpoint, the installation does the following:

1. Checks the following locations for a path to a valid Java environment, in order:
   a. The JAVA_HOME parameter in the installation input.

      Installation input includes the UNAB installation parameters file, the UNIX CA ControlMinder installation parameters file, customized packages for native installations, and user input from interactive CA ControlMinder installations.

   b. The JAVA_HOME environment variable.

   c. (Linux s390 and Linux s390x) The default installation path, /opt/ibm/java2-s390-50/jre

2. Sets the value of the java_home configuration setting in the global setting of the accommon.ini file to one of the following _values:
   - If the installation finds a path to a valid Java environment, it sets the value of the configuration setting to this path.
   - If the installation does not find a path to a valid Java environment, it sets the value of the configuration setting to *ACSharedDir*/JavaStubs.

     By default, *ACSharedDir* is /opt/CA/AccessControlShared.

Configure the Java Location on Linux s390 and Linux s390x Endpoints

Valid on Linux s390 and Linux s390x

To use Message Queue functionality and to remotely manage UNAB Linux s390 endpoints, you must install J2SE version 5.0 or later on the endpoint. If you install J2SE after you install CA ControlMinder or UNAB, you must perform additional configuration steps.

To configure the Java location on the Linux s390 and Linux s390x endpoint

1. Stop CA ControlMinder and UNAB if they are running.
2. Change the value of the java_home configuration setting in the global section of the accommon.ini file to the path of the Java installation.

   For example, java_home=/opt/ibm/java2-s390-50/jre
3. Start CA ControlMinder and UNAB.

   The Java location is configured.

Native Installations

CA ControlMinder offers native package formats for installing and managing CA ControlMinder natively on supported operating systems. Native packages let you manage your CA ControlMinder installation using native package management tools.

Native Packages

CA ControlMinder includes native packages for each supported native installation format. These packages let you use native package features to manage installation, update, and removal of CA ControlMinder components. Native packages are located in the NativePackages directory of the CA ControlMinder Endpoint Components for UNIX DVD.

The following are the packages and their descriptions:

ca-lic

(Linux only) Installs the CA Technologies license program which is a prerequisite for all other packages.

Note: Only available in RPM format for Linux.

CAeAC

Installs the core CA ControlMinder components. This is the main CA ControlMinder installation package and combines the server, client, documentation, TNG integration, API, and mfsd packages which are traditionally packaged separately.

Note: The UNAB package also installs the CAWIN shared component.

You need to know the name of the package to perform some native commands (such as removing a package with RPM). To determine the name of a package using the package file, enter the appropriate native package command. For example, for an RPM package enter:

```
rpm -q -p RPMPackage_filename
```

Additional Considerations for Native Installations

When installing CA ControlMinder using native packaging, note the following additional considerations:

- To install the CA ControlMinder RPM package you must have the license program package ca-lic-01.0080 or higher
- To prevent loading /etc/profile.CA to the environment, set the following environment variable before installing the CA_LIC package:

  ```
  setenv Update_Profile0
  ```

- To build a custom CA ControlMinder RPM native installation package (customize_eac_rpm), you must have the rpmbuild utility on your computer.
- To build a custom CA ControlMinder AIX native installation package (customize_eac_bff), you must install bos.adt.insttools on your computer.

  For AIX 5.2, the version of bos.adt.insttools should be 5.2.0.75 or newer.

- The AIX native packages are built with bos.rte.install 5.2.0.75. Therefore we recommend that you use bos.rte.install 5.2.0.75 or greater to let you work with native packaging without error.
- The HP-UX native package uses Perl during installation.
- The Solaris native package must be located in a public location with read access for group and world, such as, /var/spool/pkg.
- The Solaris native package command pkgadd -R is not supported for the CA ControlMinder package.

  Use the CA ControlMinder package customization script to modify the installation directory (customize_eac_pkg -i *install_loc*).
- To install a localized version of a HP-UX native package, you *must* set a value for the LANG setting in the parameters file you use for your customized package.

  Note: The parameters file already includes the LANG setting. To set it, remove the preceding comment character (#) and space and enter a value for it. You can find OS supported encoding values using the locale -a command.

How to Specify That CA ControlMinder Uses a Password-Protected Root Certificate

When you install CA ControlMinder, you can configure it to use a third-party password-protected root certificate.

After you install CA ControlMinder, you use the root certificate to create CA ControlMinder server certificates. The server certificates encrypt and authenticate communication between CA ControlMinder components.

To configure CA ControlMinder to use a third-party password-protected root certificate, you must perform some additional steps when you use native packages to install CA ControlMinder, as follows:

1. When you customize the params file as part of the native package installation, specify the following parameters in the file:
   - ENCRYPTION_METHOD_SET=2
   - ROOT_CERT_PATH=*root_cert_path*
   - ROOT_CERT_KEY=*root_key_path*

2. After you install CA ControlMinder, do the following:

   a. Create a CA ControlMinder server certificate from the root certificate, as follows, where *ACInstallDir* is the directory in which you installed CA ControlMinder:

      ACInstallDir/bin/sechkey -e -sub -in /opt/CA/AccessControl/crypto/sub_cert_info -priv *root_key_path* -capwd *password* [-subpwd *password*]

      -priv *root_key_path*

      Specifies the file that holds the private key for the root certificate.

      -ca *password*

      Specifies the password for the private key of the root certificate.

      -subpwd *password*

      Specifies the password for the private key of the server certificate.

   b. If you specified a password for the server key, verify that CA ControlMinder can use the stored password to open the key:

      ACInstallDir/bin/sechkey -g -verify

   c. Change the value of the communication_mode configuration setting in the crypto section to one of the following:

      all_modes

      Specify this value if you want to enable both symmetric and SSL encryption. This value lets the computer communicate with all CA ControlMinder components.

      use_ssl

      Specify this value to enable SSL encryption only. This value lets the computer communicate with only the CA ControlMinder components that use SSL encryption.

   d. Start CA ControlMinder.

      CA ControlMinder starts and uses the CA ControlMinder server certificate to encrypt and authenticate communication.

Note: For more information about the sechkey utility, see the *Reference Guide*.

How to Specify That CA ControlMinder Uses a Third-Party Password-Protected Server Certificate

You can use third-party password-protected server certificates to encrypt and authenticate communication between CA ControlMinder components.

To configure CA ControlMinder to use third-party password-protected server certificates, you must perform some additional steps when you use native packages to install CA ControlMinder, as follows:

1. When you customize the params file as part of the native package installation, specify the following parameters in the file:
   - ENCRYPTION_METHOD_SET=2
   - ROOT_CERT_PATH=*root_cert_path*
   - ROOT_CERT_KEY=*root_key_path*
   - PROVIDE_OR_GEN_CERT=2
   - SUBJECT_CERT_PATH=*server_cert_path*
   - SUBJECT_KEY_PATH=*subject_key_path*
2. After you install CA ControlMinder, do the following:
   a. Store the password for the private key on the computer, as follows, where *ACInstallDir* is the directory in which you installed CA ControlMinder:

      `ACInstallDir/bin/sechkey -g -subpwd password`

      -subpwd *password*

      Specifies the password for the private key of the server certificate.

   b. Verify that CA ControlMinder can use the stored password to open the key:

      `ACInstallDir/bin/sechkey -g -verify`

c. Change the value of the communication_mode configuration setting in the crypto section to one of the following:

all_modes

Specify this value if you want to enable both symmetric and SSL encryption. This value lets the computer communicate with all CA ControlMinder components.

use_ssl

Specify this value to enable SSL encryption only. This value lets the computer communicate with only the CA ControlMinder components that use SSL encryption.

d. Start CA ControlMinder.

CA ControlMinder starts and uses the third-party password-protected server certificate to encrypt and authenticate communication.

Note: For more information about the sechkey utility, see the *Reference Guide*.

RPM Package Manager Installation

The RPM Package Manager (RPM) is a command-line utility that lets you build, install, query, verify, update, and erase individual software packages. RPM is used on Linux platforms such as Fedora, Red Hat Enterprise Linux, and CentOS.

Note: For more information, see the RPM Package Manager website at http://www.rpm.org and the UNIX man pages for RPM.

Instead of a regular installation, you can use the RPM packages CA ControlMinder provides. This lets you manage your CA ControlMinder installation with all your other software installations performed using RPM.

Remove Existing RPM Packages from the RPM Database

If you have already installed a CA ControlMinder RPM package that you created yourself, you must remove it from the RPM database so that the database reflects which packages you have installed. If you do not remove the existing package and install the new package, the RPM database will show that both the old package and the new one are installed, but in your file system, files from the newer package overwrite existing files. For RPM to upgrade a package, it has to have the same name as the currently installed package.

Note: Removing the package does not remove any CA ControlMinder files and the native package installation performs an upgrade.

To remove a package from the RPM database, use the following command:

```
rpm -e --justdb your_ACPackageName
```

Customize the CA ControlMinder RPM Package

Before you can install CA ControlMinder using a native package, you must customize the CA ControlMinder package to specify that you accept the license agreement. You can also specify custom installation settings when you customize a package.

You customize a package by extracting the installation parameters file from the package, modifying it as required, and then loading it back into the package. Some commands are available in the customization script so that you do not have to modify the parameters file.

Note: We recommend that you *do not* modify the package manually. Instead, use the script as described in the following procedure to customize the CA ControlMinder package.

You can find the RPM packages for each of the supported Linux operating systems in the NativePackages/RPMPackages directory of the CA ControlMinder Endpoint Components for UNIX DVD.

Follow these steps:

1. Copy the package you want to customize to a temporary location on your file system.

   OS is the appropriate subdirectory name of your operating system.

   In the read/write location on the file system, the package can be customized as required.

2. Copy the customize_eac_rpm script file and the pre.tar file to a temporary location on your file system.

   The pre.tar file is compressed tar file containing installation messages and the CA ControlMinder license agreement.

   Note: You can find the customize_eac_rpm script file and the pre.tar file in the same location where the native packages are.

3. Display the license agreement:

   `customize_eac_rpm -a [-d pkg_location] pkg_filename`

4. Take note of the keyword that appears at the end of the license agreement inside square brackets.

   You specify this keyword in the next step.

5. Customize the CA ControlMinder package to specify that you accept the license agreement:

   `customize_eac_rpm -w keyword [-d pkg_location] pkg_filename`

   Important! You must customize the package to specify that you accept the license agreement using a keyword you can find inside the license agreement.

6. (Optional) Set the language of the installation parameters file:

   `customize_eac_rpm -r -l lang [-d pkg_location] pkg_filename`

7. (Optional) Upgrade from an eTrust Access Control r8 SP1 package:

   `customize_eac_rpm -u install_prefix [-d pkg_location] pkg_filename`

8. (Optional) Change the default encryption files:

   `customize_eac_rpm -s -c certfile -k keyfile [-d pkg_location] pkg_filename`

9. (Optional) Get the installation parameters file:

   `customize_eac_rpm -g -f tmp_params [-d pkg_location] pkg_filename`

10. (Optional) Edit the installation parameters file to suit your installation requirements.

    This file lets you set the installation defaults for the package. For example, activate the POSTEXIT setting (remove the preceding # character) and point it to a post-installation script file you want to run.

11. (Optional) Set the installation parameters in your customized package:

    `customize_eac_rpm -s -f tmp_params [-d pkg_location] pkg_filename`

    You can now use the package to install CA ControlMinder with the customized defaults.

Note: The actual commands you use vary depending on many variables, including whether you are upgrading or installing for the first time, or whether you want to install to the default directory.

Example: Specify That You Accept the License Agreement

To accept the license agreement when installing a native package, you customize the package. The following example shows you how you customize the x86 CA ControlMinder RPM package that you can find on the CA ControlMinder Endpoint Components for UNIX DVD (mounted to /mnt/AC_DVD) to accept the license agreement:

```
cp /mnt/AC_DVD/NativePackages/RPMPackages/LINUX/CAeAC*i386.rpm /tmp
cp /mnt/AC_DVD/NativePackages/RPMPackages/pre.tar /tmp
chmod 777 /tmp/CAeAC*i386.rpm
/mnt/AC_DVD/NativePackages/RPMPackages/customize_eac_rpm -w keyword -d /tmp
CAeAC*i386.rpm
```

You can now use the customized package in the /tmp directory to install CA ControlMinder.

More information:

customize_eac_rpm Command—Customize RPM Package (see page 208)

Install CA ControlMinder RPM Packages

To manage the CA ControlMinder installation with all your other software installations, install the customized CA ControlMinder RPM package.

Important! You must customize the package to specify that you accept the license agreement using a keyword you can find inside the license agreement.

Note: The actual command you use varies depending on many variables, including whether you are upgrading or installing for the first-time, or whether you want to install to the default directory. Some command examples are available in this topic.

To install CA ControlMinder RPM packages

1. Use the rpm command to install the ca-lic package.

   The license program installs.

2. Customize the CAeAC package (see page 203).

   You must customize the package to specify that you accept the license agreement using a keyword that you can find inside the license agreement. You can also customize the package to specify custom installation settings.

   Note: If you are upgrading CA ControlMinder, you do not need to customize the package to specify that you accept the license agreement.

3. Use the rpm command to install the CAeAC package.

   CA ControlMinder installs.

   Note: The UNAB package also installs the CAWIN shared component.

   Important! If you are upgrading an existing CA ControlMinder package, unload SEOS syscall before you try to install the new package. Otherwise, the installation fails.

Example: Install or Upgrade CA ControlMinder on Red Hat Linux

The following example shows how you can install the CA ControlMinder package that you can find on the CA ControlMinder Endpoint Components for UNIX DVD (mounted to /mnt/AC_DVD) on a Red Hat Linux x86 ES 4.0 computer. This can be a fresh installation of CA ControlMinder or an upgrade of a currently installed CA ControlMinder RPM package (without needing to remove the installed package first). To do this, you install the license program package and then customize the CA ControlMinder package to accept the license agreement and install it as follows:

```
cd /mnt/AC_DVD/NativePackages/RPMPackages/LINUX
rpm -U ca-lic*i386.rpm ca-cs-cawin*i386.rpm
cp CAeAC*i386.rpm /tmp
cp ../pre.tar /tmp
chmod 777 /tmp/CAeAC*i386.rpm
../customize_eac_rpm -w keyword -d /tmp CAeAC*i386.rpm
rpm -U /tmp/CAeAC*i386.rpm
```

Example: Upgrade from an eTrust Access Control r8 SP1 Package Installation

The following example shows how you can upgrade an eTrust Access Control r8 SP1 package, which is installed at /opt/CA/eTrustAccessControl, to the CA ControlMinder package that you can find on the CA ControlMinder Endpoint Components for UNIX DVD (mounted to /mnt/AC_DVD) on a Linux s390 SLES 9 computer. To do this, you install the license program package, CAWIN package, and the customized CA ControlMinder package (in that order) as follows:

```
cd /mnt/AC_DVD/NativePackages/RPMPackages/LINUX390
rpm -U ca-lic*rpm ca-cs-cawin*rpm
cp -R CAeAC*s390.rpm /tmp
cp ../pre.tar /tmp
chmod 777 /tmp/CAeAC*s390.rpm
../customize_eac_rpm -u /opt/CA  -d /tmp CAeAC*s390.rpm
../customize_eac_rpm -w keyword -d /tmp CAeAC*s390.rpm
rpm -U /tmp/CAeAC*s390.rpm
```

Example: Install CA ControlMinder and the Prerequisites to a Custom Directory

The following example shows how you can install the default CA ControlMinder and the prerequisite package that you can find on the CA ControlMinder Endpoint Components for UNIX DVD (mounted to /mnt/AC_DVD) to custom directories on a Red Hat Linux Itanium IA64 ES 4.0. To do this, use the following commands:

```
cd /mnt/AC_DVD/NativePackages/RPMPackages/LINUX_IA64
rpm -U --prefix /usr/CA/shared ca-lic*ia64.rpm
cp -R CAeAC*ia64.rpm /tmp
cp ../pre.tar /tmp
chmod 777 /tmp/CAeAC*ia64.rpm
../customize_eac_rpm -u /usr/CA  -d /tmp CAeAC*ia64.rpm
../customize_eac_rpm -w keyword -d /tmp CAeAC*ia64.rpm
rpm -U --prefix /usr/CA /tmp/CAeAC*ia64.rpm
```

CA ControlMinder installs into the custom directory /usr/CA/AccessControl, which, is a concatenation of the custom directory you provided and the name of the product (Access Control).

Note: The license program installs to the specified directory only if $CASHCOMP variable is not defined in the environment (it can be defined in /etc/profile.CA). Otherwise, the license program installs to $CASHCOMP. If $CASHCOMP is not defined and you do not specify -lic_dir, the license program installs to the /opt/CA/SharedComponents directory.

More information:

Additional Considerations for Native Installations (see page 198)
Customize the CA ControlMinder RPM Package (see page 203)
customize_eac_rpm Command—Customize RPM Package (see page 208)

customize_eac_rpm Command—Customize RPM Package

The customize_eac_rpm command runs the CA ControlMinder RPM package customization script.

You should consider the following when using this command:

- The script works on the CA ControlMinder RPM packages only.

  Note: The script is not intended for use with the license program package.

- To customize a package, the package must be in a read/write directory on your file system.

This command has the following format:

```
customize_eac_rpm -h [-l]
customize_eac_rpm -a [-d pkg_location] pkg_filename
customize_eac_rpm -w keyword [-d pkg_location] pkg_filename
customize_eac_rpm -r [-d pkg_location] [-l lang] pkg_filename
customize_eac_rpm -s [-f tmp_params] | -c certfile | -k keyfile} [-d pkg_location]
pkg_filename
customize_eac_rpm -g [-f tmp_params] [-d pkg_location] pkg_filename
customize_eac_rpm -u install_prefix [-d pkg_location] pkg_filename
customize_eac_rpm -t tmp_dir [-d pkg_location] pkg_filename
```

pkg_filename

Defines the file name of the CA ControlMinder package you want to customize.

Note: If you do not specify the -d option, you must define the full pathname of the package file.

-a

Displays the license agreement.

-c *certfile*

Defines the full pathname of the root certificate file.

Note: This option is applicable to the CAeAC package only.

-d *pkg_location*

(Optional) Specifies the directory where you placed your package on the file system. If you do not specify a directory where the package is located, the script assumes the full pathname to the package file is *pkg_filename*.

-f *tmp_params*

Specifies the full path and name of the installation parameters file to create or retrieve information from.

Note: If you do not specify a file when using the -g option, the installation parameters are directed to the standard output (stdout).

-g

Gets the installation parameters file and places it in the file specified by the -f option.

-h

Displays command usage. When used in conjunction with the -l option, displays the language code for supported languages.

-k *keyfile*

Defines the full pathname of the root private key file.

Note: This option is applicable to the CAeAC package only.

-l *lang*

Sets the language of the installation parameters file to *lang*. You can set the language only in conjunction with the -r option.

Note: For a list of supported language codes you can specify, run -l with the -h option. By default, the installation parameters file is in English.

-r

Resets the package to use default values as in the original package.

-s

Sets the specified package to use inputs from the customized installation parameters file specified by the -f option.

-t *tmp_dir*

Sets the temporary directory for installation operations.

Note: The default temporary directory is /tmp.

-u *install_prefix*

Defines the prefix for the location where you have an installation of an eTrust Access Control r8 SP1 package. The actual installation location is a concatenation of this prefix and the product's name. The r8 SP1 package had eTrust in the product name and was therefore installed into the eTrustAccessControl subdirectory. Newer versions install into the AccessControl subdirectory.

For example, if you had r8 SP1 installed in /opt/CA/eTrustAccessControl and you are upgrading to r12.0 SP1, enter the following before you use the rpm command to install the package:

```
./customize_eac_rpm -u /opt/CA  -d . CAeAC-1200-0.1106.i386.rpm
```

-w *keyword*

Defines the keyword that specifies that you accept the license agreement. You can find this keyword at the end of the license agreement (inside square brackets). To locate the license agreement file, use the -a option.

Uninstall the RPM Package

To uninstall a CA ControlMinder RPM package installation, you need to uninstall the CA ControlMinder packages in the reverse order of their installation.

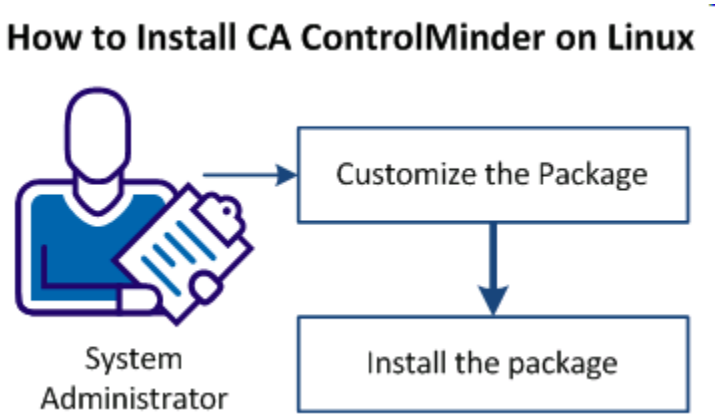
To uninstall the RPM package, run the following command:

```
rpm -e CAeAC-128SP0378
```

How to Install CA ControlMinder on Debian or Ubuntu Linux

The Debian Package Manager (dpkg) is a command-line utility that lets you install, query, verify, update, and remove software packages. It is used on Debian and Ubuntu Linux platforms.

The standard way to install CA ControlMinder on Debian or Ubuntu Linux is to use the native .deb packages that CA ControlMinder provides. This lets you manage your CA ControlMinder installation with all your other software installations performed using dpkg.



Follow these steps:

1. Customize the package (see page 211)
2. Install the package (see page 215)

Customize the CA ControlMinder .deb Package

Before you can install CA ControlMinder using a native package, you must customize the CA ControlMinder package to specify that you accept the license agreement. You can also specify custom installation settings when you customize a package.

You customize a package by extracting the installation parameters file from the package, modifying it as required, and then loading it back into the package. Some commands are available in the customization script so that you do not have to modify the parameters file.

Note: We recommend that you *do not* modify the package manually. Instead, use the script as described in the following procedure to customize the CA ControlMinder package.

Follow these steps:

1. Locate the .deb package in the NativePackages directory of the CA ControlMinder Endpoint Components for UNIX DVD.
2. Copy the .deb package to a temporary readable/writable location on your file system (*pkg_location*). Copy the customize_eac_deb file and the pre.tar file to the same location.

   The pre.tar file is a compressed tar file containing installation messages and the CA ControlMinder license agreement.
3. Display the license agreement:

   `customize_eac_deb -a [-d pkg_location] pkg_filename`
4. Take note of the *keyword* that appears at the end of the license agreement inside square brackets.

   You specify this keyword in the next step.
5. Customize the CA ControlMinder package to specify that you accept the license agreement:

   `customize_eac_deb -w keyword [-d pkg_location] pkg_filename`
6. (Optional) Set the language of the installation parameters file:

   `customize_eac_deb -r -l lang [-d pkg_location] pkg_filename`
7. (Optional) Upgrade from an eTrust Access Control r8 SP1 package:

   `customize_eac_deb -u install_prefix [-d pkg_location] pkg_filename`
8. (Optional) Change the default encryption files:

   `customize_eac_deb -s -c certfile -k keyfile [-d pkg_location] pkg_filename`
9. (Optional) Change the target installation directory to *target_location*:

   `customize_eac_deb -i target_location [-d pkg_location] pkg_filename`

   The default installation location is /opt/CA/.

10. (Optional) Configure other custom defaults for the package. Get the installation parameters file and save it as *tmp_params*:

    `customize_eac_deb -g -f tmp_params [-d pkg_location] pkg_filename`

    a. Edit the installation parameters file *tmp_params* to suit your installation requirements. For example, activate the POSTEXIT setting (remove the preceding # character) and point it to a post-installation script file you want to run.

    b. Assign the customized installation parameters to your customized package:

    `customize_eac_deb -s -f tmp_params [-d pkg_location] pkg_filename`

    You can now use the package to install CA ControlMinder with your customized default settings.

Example: Specify That You Accept the License Agreement

To accept the license agreement when installing a native package, you customize the package. The following example shows how you customize the 64-bit CA ControlMinder deb package to accept the license agreement. You find the package on the CA ControlMinder Endpoint Components for UNIX DVD which, in this example, is mounted to /mnt/AC_DVD.

```
cp /mnt/AC_DVD/NativePackages/_LINUX_X64_DEB_PKG_128.tar.Z /tmp
cp /mnt/AC_DVD/NativePackages/pre.tar /tmp
cd /tmp
zcat _LINUX_X64_DEB_PKG_128.tar.Z | tar -xvf -
chmod 777 caeac*.deb
/mnt/AC_DVD/NativePackages/customize_eac_deb -w keyword
    -d /tmp 128sp1-123_amd64.deb
```

You can now use the customized package to install CA ControlMinder.

customize_eac_deb Command—Customize .deb Package

Use the customize_eac_deb command to run the CA ControlMinder Debian package customization script before installing CA ControlMinder on Debian or Ubuntu Linux.

- The script works on CA ControlMinder Debian packages only.

  Note: The script is not intended for use with the license program package.

- Move the package to a read/write directory on your file system.

This command has the following format:

```
customize_eac_deb -h [-l lang]
customize_eac_deb -a [-d pkg_location] pkg_filename
customize_eac_deb -i target_location [-d pkg_location] pkg_filename
customize_eac_deb -w keyword [-d pkg_location] pkg_filename
customize_eac_deb -r [-d pkg_location] [-l lang] pkg_filename
customize_eac_deb -s [-f tmp_params] | -c certfile | -k keyfile} [-d pkg_location]
pkg_filename
customize_eac_deb -g [-f tmp_params] [-d pkg_location] pkg_filename
customize_eac_deb -t tmp_dir [-d pkg_location] pkg_filename
```

pkg_filename

Defines the file name of the CA ControlMinder package you want to customize.

Note: If you do not specify the -d option, you must define the full pathname of the package file.

-a

Displays the license agreement.

-c *certfile*

Defines the full pathname of the root certificate file.

Note: This option is applicable to the CAeAC package only.

-d *pkg_location*

(Optional) Specifies the directory where you placed your package on the file system. If you do not specify a directory where the package is located, the script assumes the full pathname to the package file is *pkg_filename*.

-f *tmp_params*

Specifies the full path and name of the installation parameters file to create or retrieve information from.

Note: If you do not specify a file when using the -g option, the installation parameters are directed to the standard output (stdout).

-g

Gets the installation parameters file and places it in the file specified by the -f option.

-h

Displays command usage. When used in conjunction with the -l option, displays the language code for supported languages.

-i *target_location*

Defines a custom target installation directory for the package.

Example: /opt/CA/

-k *keyfile*

Defines the full pathname of the root private key file.

Note: This option is applicable to the CAeAC package only.

-l *lang*

Sets the language of the installation parameters file to *lang*. You can set the language only in conjunction with the -r option.

Note: For a list of supported language codes you can specify, run -l with the -h option. By default, the installation parameters file is in English.

-r

Resets the package to use default values as in the original package.

-s

Sets the specified package to use inputs from the customized installation parameters file specified by the -f option.

-t *tmp_dir*

Sets the temporary directory for installation operations.

Note: The default temporary directory is /tmp.

-w *keyword*

Defines the keyword that specifies that you accept the license agreement. You can find this keyword at the end of the license agreement (inside square brackets). To locate the license agreement file, use the -a option.

Install the CA ControlMinder .deb Package

To install CA ControlMinder .deb package on the Linux platform, you use the dpkg -i command. The package file name contains the version number and has a .deb suffix. For example the "caeac-128sp0-246_amd64.deb" file installs the 64-bit version of CA ControlMinder 12.8, service pack 0, build 246.

Follow these steps:

1. Log on as the root user.
2. Install the CA ControlMinder package:
   ```
   dpkg -i caeac-xxxspx-xxx_amd64.deb
   ```
   The package is installed into the /opt/CA/ directory by default.
3. Verify that the package status is "OK installed".
   ```
   dpkg -s caeac-xxxspx-xxx
   ```

More information:

customize_eac_deb Command—Customize .deb Package (see page 213)

Uninstall the CA ControlMinder .deb Package

To remove a CA ControlMinder package from a Debian or Ubuntu Linux system, you use the dpkg -r and -P commands.

Follow these steps:

1. Find the full name of the CA ControlMinder package that you want to uninstall.
   ```
   dpkg -l | grep caeac
   ```
   The package name has the format caeac-xxxspx-xxx.
2. Remove and purge the CA ControlMinder package caeac-xxxspx-xxx:
   ```
   dpkg -r caeac-xxxspx-xxx
   dpkg -P caeac-xxxspx-xxx
   ```
3. Verify that the CA ControlMinder directory was removed from the installation directory:
   ```
   ls /opt/CA/
   ```

Verify CA ControlMinder Installation on Linux or Unix

(Optional) You can verify the installation by confirming that basic CA ControlMinder functionality works. You find the installation log in the installation directory under AccessControl/AccessControl_install.log.

Follow these steps:

1. Log on as root user.
2. Create a test file and give everyone read permissions:
   ```
   echo "##  This is my test file ##" > /tempfile
   chmod 666 /tempfile
   ```
3. Change into the CA ControlMinder bin directory. Load CA ControlMinder if it is not yet running:
   ```
   cd /opt/CA/AccessControl_128SP0_211/bin/
   ./seload
   ```
4. Run selang, create a *testuser*, and give it exclusive permission to access the test file.
   ```
   ./selang
   AC> eu testuser password(1)
   AC> ef /testfile owner(nobody)
   AC> auth FILE /testfile uid(testuser) acc(A)
   AC> exit
   ```
5. Verify that the root user cannot access the file ("permission denied"):
   ```
   cat /testfile
   ```

6. Log into the system as user *testuser*:
   `ssh localhost -l testuser`
7. Verify that *testuser* is able to access the file as expected:
   `cat /testfile`

Your CA ControlMinder installation is complete.

Solaris Native Packaging Installation

Solaris native packaging is provided as command-line utilities that let you create, install, remove, and report on individual software packages.

Note: For more information about Solaris native packaging, see the Sun Microsystems website and the man pages for pkgadd, pkgrm, pkginfo, and pkgchk.

Instead of a regular installation, you can use the Solaris native packages CA ControlMinder provides. This lets you manage your CA ControlMinder installation with all your other software installations performed using Solaris native packaging.

Important! To uninstall CA ControlMinder after a package installation, you must use the *pkgrm* command. Do not use uninstall_AC script.

Customize the Solaris Native Packages

Before you can install CA ControlMinder using a native package, you must customize the CA ControlMinder package to specify that you accept the license agreement. You can also specify custom installation settings when you customize a package.

You customize a package by extracting the installation parameters file from the package, modifying it as required, and then loading it back into the package. Some commands are available in the customization script so that you do not have to modify the parameters file.

Note: We recommend that you do not modify the package manually. Instead, use the script as described in the following procedure to customize the CA ControlMinder package.

You can find the Solaris native package for each of the supported Solaris operating systems in the NativePackages directory of the CA ControlMinder Endpoint Components for UNIX DVD.

To customize the Solaris native packages

1. Extract the package you want to customize to a temporary location on your file system.

   In the read/write location on the file system, you can customize the package as required.

   Important! When you extract the package, verify that file attributes for the entire directory structure of the package are preserved or Solaris native packaging tools will consider the package corrupt.

2. Copy the customize_eac_pkg script file and the pre.tar file to a temporary location on your file system.

   The pre.tar file is compressed tar file containing installation messages and the CA ControlMinder license agreement.

   Note: You can find the customize_eac_pkg script file and the pre.tar file in the same location where the native packages are.

3. Display the license agreement:

   `customize_eac_pkg -a [-d pkg_location] pkg_name`

4. Take note of the keyword that appears at the end of the license agreement inside square brackets.

   You specify this keyword in the next step.

5. Customize the CA ControlMinder package to specify that you accept the license agreement:

   `customize_eac_pkg -w keyword [-d pkg_location] [pkg_name]`

6. (Optional) Set the language of the installation parameters file:

   `customize_eac_pkg -r -l lang [-d pkg_location] [pkg_name]`

7. (Optional) Change the installation directory:

   `customize_eac_pkg -i install_loc [-d pkg_location] [pkg_name]`

8. (Optional) Change the default encryption files:

   `customize_eac_pkg -s -c certfile -k keyfile [-d pkg_location] [pkg_name]`

9. (Optional) Get the installation parameters file:

   `customize_eac_pkg -g -f tmp_params [-d pkg_location] [pkg_name]`

10. (Optional) Edit the installation parameters file to suit your installation requirements.

    This file lets you set the installation defaults for the package. For example, activate the POSTEXIT setting (remove the preceding # character) and point it to a post-installation script file you want to run.

11. (Optional) Set the installation parameters in your customized package:

    `customize_eac_pkg -s -f tmp_params [-d pkg_location] [pkg_name]`

    You can now use the package to install CA ControlMinder with the customized defaults.

Example: Specify That You Accept the License Agreement

To accept the license agreement when installing a native package, you customize the package. The following example shows you how you do customize the x86 CA ControlMinder Solaris package that you can find on the CA ControlMinder Endpoint Components for UNIX DVD (mounted to /mnt/AC_DVD) to accept the license agreement:

```
cp /mnt/AC_DVD/NativePackages/_SOLARIS_X86_PKG*.tar.Z /tmp
cp /mnt/AC_DVD/NativePackages/pre.tar /tmp
cd /tmp
zcat _SOLARIS_X86_PKG*.tar.Z | tar -xvf -
/mnt/AC_DVD/NativePackages/customize_eac_pkg -w keyword -d /tmp CAeAC
```

You can now use the customized package in the /tmp directory to install CA ControlMinder.

More information:

customize_eac_pkg Command—Customize Solaris Native Package (see page 269)
customize_eac_pkg Command—Customize Solaris Native Package (see page 222)

Install Solaris Native Packages

To manage the CA ControlMinder installation with all your other software installations, install the customized CA ControlMinder Solaris native package. The CA ControlMinder Solaris native packages let you install CA ControlMinder on Solaris easily.

Important! You must customize the package to specify that you accept the license agreement using a keyword you can find inside the license agreement.

To install the CA ControlMinder Solaris native packages

1. (Optional) Configure Solaris native installation defaults:

   a. Get a copy of the installation administration file to the current location:

      ```
      convert_eac_pkg -p
      ```

      The installation administration file is copied to the current location with the name *myadmin*.

      You can edit the installation administration file to change pkgadd installation defaults. You can then use the modified file for specific installations, such as CA ControlMinder, using the pkgadd -a option. However, this file is not specific to CA ControlMinder.

      Important! You must perform this step to upgrade an existing Solaris package installation from an older CA ControlMinder release.

   b. Edit the installation administration file (myadmin) as desired, then save the file.

      You can now use the modified installation settings for the CA ControlMinder native installation without affecting other installations.

   Note: Solaris native packaging may require user interaction by default. For more information about the installation administration file and how to use it, see the Solaris man page for pkgadd(1M) and admin(4).

2. Customize the CAeAC package (see page 217).

   You must customize the package to specify that you accept the license agreement using a keyword that you can find inside the license agreement. You can also customize the package to specify custom installation settings.

3. Install the package:

   ```
   pkgadd [-a dir/myadmin] -d pkg_location CAeAC
   ```

   -a *dir*/myadmin

   Defines the location of the myadmin installation administration file you created in step 1.

   If you do not specify this option, pkgadd uses the default installation administration file.

   pkg_location

   Defines the directory where the CA ControlMinder package (CAeAC) is located.

Important! The package must be located in a public location (that is, read access for group and world). For example, /var/spool/pkg

Note: You can find the Solaris native packages in the NativePackages directory of the CA ControlMinder Endpoint Components for UNIX DVD.

CA ControlMinder is now fully installed but not started.

Install Solaris Native Packages on Selected Zones

You can use Solaris native packaging to install CA ControlMinder to selected zones. However, you must also install CA ControlMinder on the global zone.

Note: We recommend that you use Solaris native packaging to install CA ControlMinder to *all* zones.

To install CA ControlMinder to selected zones

Important! Make sure you use the same CA ControlMinder version in all zones.

1. From the global zone, issue the command to install CA ControlMinder.

   `pkgadd -G -d pkg_location CAeAC`

   pkg_location

   Defines the directory where the customized CA ControlMinder package (CAeAC) is located.

   Important! The package must be located in a public location (that is, read access for group and world). For example, /var/spool/pkg

   This command installs CA ControlMinder only to the global zone.

2. In the global zone, enter the SEOS_load command to load the CA ControlMinder kernel module.

   Note: The CA ControlMinder kernel loads but CA ControlMinder does not intercept events in the global zone.

3. On each of the non-global zones where you want to install CA ControlMinder:

   a. Copy the CAeAC package to a temporary location on the non-global zone.

   b. Issue the following command from the non-global zone:

      `pkgadd -G -d pkg_location CAeAC`

      This command installs CA ControlMinder (using the package you copied in the previous step) on the non-global zone you are working from.

   You can now start CA ControlMinder on the internal zone.

Note: You must uninstall from all non-global zones before you remove CA ControlMinder from the global zone.

customize_eac_pkg Command—Customize Solaris Native Package

The customize_eac_pkg command runs the CA ControlMinder Solaris native package customization script.

- The script works on any of the available CA ControlMinder Solaris native packages.
- Move the package to a read/write directory on your file system.
- For localized script messages, you need to have pre.tar file in the same directory as the script file.

This command has the following format:

```
customize_eac_pkg -h [-l]
customize_eac_pkg -a [-d pkg_location] [pkg_name]
customize_eac_pkg -w keyword [-d pkg_location] [pkg_name]
customize_eac_pkg -r [-d pkg_location] [-l lang] [pkg_name]
customize_eac_pkg -i install_loc [-d pkg_location] [pkg_name]
customize_eac_pkg -s {-f tmp_params | -c certfile | -k keyfile} [-d pkg_location]
[pkg_name]
customize_eac_pkg -g [-f tmp_params] [-d pkg_location] [pkg_name]
customize_eac_pkg -t tmp_dir [-d pkg_location] [pkg_name]
```

pkg_name

(Optional) The name of the CA ControlMinder package you want to customize. If you do not specify a package, the script defaults to the main CA ControlMinder package (CAeAC).

-a

Displays the license agreement.

-c *certfile*

Defines the full pathname of the root certificate file.

Note: This option is applicable to the CAeAC package only.

-d *pkg_location*

(Optional) Specifies the directory where you placed your package on the file system. If you do not specify a directory where the package is located, the script defaults to /var/spool/pkg.

-f *tmp_params*

Specifies the full path and name of the installation parameters file to create or retrieve information from.

Note: If you do not specify a file when using the -g option, the installation parameters are directed to the standard output (stdout).

-g

Gets the installation parameters file and places it in the file specified by the -f option.

-h

Displays command usage. When used in conjunction with the -l option, displays the language code for supported languages.

-i *install_loc*

Sets the installation directory for the package to *install_loc*/AccessControl.

-k *keyfile*

Defines the full pathname of the root private key file.

Note: This option is applicable to the CAeAC package only.

-l *lang*

Sets the language of the installation parameters file to *lang*. You can set the language only in conjunction with the -r option.

Note: For a list of supported language codes you can specify, run -l with the -h option. By default, the installation parameters file is in English.

-r

Resets the package to use default values as in the original package.

-s

Sets the specified package to use inputs from the customized installation parameters file specified by the -f option.

-t *tmp_dir*

Sets the temporary directory for installation operations.

Note: The default temporary directory is /tmp.

-w *keyword*

Defines the keyword that specifies that you accept the license agreement. You can find this keyword at the end of the license agreement (inside square brackets). To locate the license agreement file, use the -a option. This option is required for new installations and upgrades.

convert_eac_pkg—Configure Solaris Native Installation

The default Solaris pkgadd behavior is determined by an installation administration file. To override default settings, you need to change the installation administration file (by default, /var/sadm/install/admin/default). For example, the CA ControlMinder package installs setuid executables and, optionally, lets you run a post-installation script (which will run as *root*). The default Solaris pkgadd behavior is to prompt you to confirm these operations.

Note: You can edit the installation administration file to change pkgadd installation defaults. You can then use the modified file for specific installations, such as CA ControlMinder, using the pkgadd -a option. However, this file is not specific to CA ControlMinder.

This command has the following format:

```
convert_eac_pkg -c [-d pkg_location] [pkg_name]
```

```
convert_eac_pkg -p [-f file]
```

-c

Converts an old-format package to the new format.

Note: Old-format packages were used in CA ControlMinder r8 SP1. You need to convert these before you upgrade.

You can convert information for an installed CA ControlMinder package or a spooled package. For a spooled package, use the -d option to indicate where the package is located.

-d *pkg_location*

Defines the directory where you placed your package on the file system

pkg_name

Defines the name of the package (CAeAC by default).

-p

Prepares a custom package configuration file named

-f *file*

Defines the location where you want to create the CA ControlMinder installation administration file.

If not specified, the command creates a file called *myadmin* in the current directory.

Example: Configure Solaris Native Installation for a Silent Installation

The following procedure shows how you configure Solaris native installation so that it does not prompt you to confirm installing setuid executables or running a post installation script:

1. Get a copy of the installation administration file to the current location:

   ```
   convert_eac_pkg -p
   ```

   This lets you modify the configuration settings for the CA ControlMinder native installation without affecting other installations.

2. Edit the following settings in your package configuration file (myadmin) as shown:

   ```
   setuid=nocheck
   action=nocheck
   ```

   Save the file.

3. Customize the package.

   As a minimum, you need to specify that you accept the license agreement.

4. Run the following command to install the customized CA ControlMinder package silently:

   ```
   pkgadd -n -a config_path\myadmin -d pkg_path CAeAC
   ```

Example: Upgrade a Solaris Native Installation that Uses an Old Format

The following procedure shows you how convert an existing installation of CA ControlMinder native package installation before you upgrade to a new release. To do this, run the following command:

```
convert_eac_pkg -c CAeAC
```

HP-UX Native Package Installation

HP-UX native packaging is provided as a set of GUI and command-line utilities that let you create, install, remove, and report on individual software packages. HP-UX native packaging also lets you install software packages on remote computers.

Note: For more information about the HP-UX native packaging, Software Distributor-UX (SD-UX), see the HP website at http://www.hp.com. You can also refer to the man pages for swreg, swinstall, swpackage, and swverify.

Instead of a regular installation, you can use the SD-UX native packages CA ControlMinder provides. This lets you manage your CA ControlMinder installation with all your other software installations performed using the SD-UX.

Important! To uninstall CA ControlMinder after a package installation, you must use the *swremove* command. Do not use the uninstall_AC script.

Customize the SD-UX Format Packages

Before you can install CA ControlMinder using a native package, you must customize the CA ControlMinder package to specify that you accept the license agreement. You can also specify custom installation settings when you customize a package.

You customize a package by extracting the installation parameters file from the package, modifying it as required, and then loading it back into the package. Some commands are available in the customization script so that you do not have to modify the parameters file.

Note: We recommend that you do not modify the package manually. Instead, use the script as described in the following procedure to customize the CA ControlMinder package.

You can find the Software Distributor-UX (SD-UX) format package for each of the supported HP-UX operating systems in the NativePackages directory of the CA ControlMinder Endpoint Components for UNIX DVD.

To customize the SD-UX format packages

1. Extract the package you want to customize to a temporary location on your file system.

   In the read/write location on the file system, the package can be customized as required.

   Important! When you extract the package, you must make sure that file attributes for the entire directory structure of the package are preserved or HP-UX native packaging tools will consider the package corrupt.

2. Copy the customize_eac_depot script file and the pre.tar file to a temporary location on your file system.

   The pre.tar file is compressed tar file containing installation messages and the CA ControlMinder license agreement.

   Note: You can find the customize_eac_depot script file and the pre.tar file in the same location where the native packages are.

3. Display the license agreement:

   ```
   customize_eac_depot -a [-d pkg_location] pkg_name
   ```

4. Take note of the keyword that appears at the end of the license agreement inside square brackets.

   You specify this keyword in the next step.

5. Customize the CA ControlMinder package to specify that you accept the license agreement:

   ```
   customize_eac_depot -w keyword [-d pkg_location] [pkg_name]
   ```

6. (Optional) Set the language of the installation parameters file:

   `customize_eac_depot -r -l lang [-d pkg_location] [pkg_name]`

7. (Optional) Change the installation directory:

   `customize_eac_depot -i install_loc [-d pkg_location] [pkg_name]`

8. (Optional) Change the default encryption files:

   `customize_eac_depot -s -c certfile -k keyfile [-d pkg_location] [pkg_name]`

9. (Optional) Get the installation parameters file:

   `customize_eac_depot -g -f tmp_params [-d pkg_location] [pkg_name]`

10. (Optional) Edit the installation parameters file to suit your installation requirements.

    This file lets you set the installation defaults for the package. For example, activate the POSTEXIT setting (remove the preceding # character) and point it to post-installation script file you want to run.

11. (Optional) Set the installation parameters in your customized package:

    `customize_eac_depot -s -f tmp_params [-d pkg_location] [pkg_name]`

    You can now use the package to install CA ControlMinder with the customized defaults.

Example: Specify That You Accept the License Agreement

To accept the license agreement when installing a native package, you customize the package. The following example shows you how you do customize the x86 CA ControlMinder SD-UX package that you can find on the CA ControlMinder Endpoint Components for UNIX DVD (mounted to /mnt/AC_DVD) to accept the license agreement:

```
cp /mnt/AC_DVD/NativePackages/_HPUX11_PKG_*.tar.Z /tmp
cp /mnt/AC_DVD/NativePackages/pre.tar /tmp
cd /tmp
zcat _HPUX11_PKG_*.tar.Z | tar -xvf -
/mnt/AC_DVD/NativePackages/customize_eac_depot -w keyword -d /tmp CAeAC
```

You can now use the customized package in the /tmp directory to install CA ControlMinder.

More information:

customize_eac_depot Command—Customize an SD-UX Format Package (see page 229)

Install HP-UX Native Packages

To manage the CA ControlMinder installation with all your other software installations, install the customized CA ControlMinder SD-UX format package. The CA ControlMinder SD-UX format packages let you install CA ControlMinder on HP-UX easily.

Important! You must customize the package to specify that you accept the license agreement using a keyword you can find inside the license agreement.

To install the CA ControlMinder HP-UX native packages

1. Log in as root.

   To register and install HP-UX native packages you need permissions associated with the root account.

2. Customize the CAeAC package (see page 226).

   You must customize the package to specify that you accept the license agreement using a keyword that you can find inside the license agreement. You can also customize the package to specify custom installation settings.

3. Register the customized package with SD-UX using the following command:

   `swreg -l depot` *`pkg_location`*

   pkg_location

   Defines the directory where the CA ControlMinder package (CAeAC) is located.

4. Install the CA ControlMinder package using the following command:

   `swinstall -s` *`pkg_location`* `CAeAC`

   SD-UX starts installing the CAeAC package from the *pkg_location* directory.

   CA ControlMinder is now fully installed but not started.

More information:

Additional Considerations for Native Installations (see page 198)
Customize the SD-UX Format Packages (see page 226)

customize_eac_depot Command—Customize an SD-UX Format Package

The customize_eac_depot command runs the CA ControlMinder native package customization script for SD-UX format packages.

You should consider the following when using this command:

- The script works on any of the available CA ControlMinder Solaris native packages.
- To customize a package, the package must be in a read/write directory on your file system.
- For localized script messages, you need to have pre.tar file in the same directory as the script file.

This command has the following format:

```
customize_eac_depot -h [-l]
customize_eac_depot -a [-d pkg_location] [pkg_name]
customize_eac_depot -w keyword [-d pkg_location] [pkg_name]
customize_eac_depot -r [-l lang] [-d pkg_location] [pkg_name]
customize_eac_depot -i install_loc [-d pkg_location] [pkg_name]
customize_eac_depot -s {-f tmp_params | -c certfile | -k keyfile} [-d pkg_location]
[pkg_name]
customize_eac_depot -g [-f tmp_params] [-d pkg_location] [pkg_name]
```

pkg_name

(Optional) The name of the CA ControlMinder package you want to customize. If you do not specify a package, the script defaults to the main CA ControlMinder package (CAeAC).

-a

Displays the license agreement.

-c *certfile*

Defines the full pathname of the root certificate file.

Note: This option is applicable to the CAeAC package only.

-d *pkg_location*

(Optional) Specifies the directory where you placed your package on the file system. If you do not specify a directory where the package is located, the script defaults to /var/spool/pkg.

-f *tmp_params*

Specifies the full path and name of the installation parameters file to create or retrieve information from.

Note: If you do not specify a file when using the -g option, the installation parameters are directed to the standard output (stdout).

-g

Gets the installation parameters file and places it in the file specified by the -f option.

-h

Displays command usage. When used in conjunction with the -l option, displays the language code for supported languages.

-i *install_loc*

Sets the installation directory for the package to *install_loc*/AccessControl.

-k *keyfile*

Defines the full pathname of the root private key file.

Note: This option is applicable to the CAeAC package only.

-l *lang*

Sets the language of the installation parameters file to *lang*. You can set the language only in conjunction with the -r option.

Note: For a list of supported language codes you can specify, run -l with the -h option. By default, the installation parameters file is in English.

-r

Resets the package to use default values as in the original package.

-s

Sets the specified package to use inputs from the customized installation parameters file specified by the -f option.

-w *keyword*

Defines the keyword that specifies that you accept the license agreement. You can find this keyword at the end of the license agreement (inside square brackets). To locate the license agreement file, use the -a option.

Uninstall HP-UX Packages

To uninstall a CA ControlMinder HP-UX package installation, you need to uninstall the CA ControlMinder packages in the reverse order of their installation.

To uninstall CA ControlMinder packages uninstall the main CA ControlMinder package:

```
swremove CAeAC
```

AIX Native Package Installation

AIX native packaging is provided as a set of GUI and command-line utilities that let you manage individual software packages. Instead of a regular installation, you can use the AIX native packages CA ControlMinder provides. This lets you manage your CA ControlMinder installation with all your other software installations performed using the AIX installp.

Note: While some AIX versions support several package formats (installp, SysV, RPM), CA ControlMinder provides the AIX native package format (installp) only.

Important! To uninstall CA ControlMinder after a package installation, you must use the *installp* command. Do not use the uninstall_AC script.

Customize the bff Native Package Files

Before you can install CA ControlMinder using a native package, you must customize the CA ControlMinder package to specify that you accept the license agreement. You can also specify custom installation settings when you customize a package.

You customize a package by extracting the installation parameters file from the package, modifying it as required, and then loading it back into the package. Some commands are available in the customization script so that you do not have to modify the parameters file.

Note: We recommend that you do not modify the package manually. Instead, use the script as described in the following procedure to customize the CA ControlMinder package.

You can find the installp format native packaging (AIX bff files) in the NativePackages directory of the CA ControlMinder Endpoint Components for UNIX DVD.

Follow these steps:

1. Log on as root.
2. Extract the package to a temporary location on your file system.

   In the read/write location on the file system, the package (a bff file) can be customized as required.

   Important! Verify that you have disk space that is at least twice the size of the package, so that it can hold temporary repackaging files.
3. Copy the customize_eac_bff script file and the pre.tar file to a temporary location on your file system.

   The pre.tar file is compressed tar file containing installation messages and the CA ControlMinder license agreement.

   Note: You can find the customize_eac_bff script file and the pre.tar file in the same location where the native packages are.

4. Display the license agreement:

   `customize_eac_bff -a [-d pkg_location] pkg_name`

5. Take note of the keyword that appears at the end of the license agreement inside square brackets.

   You specify this keyword in the next step.

6. Customize the CA ControlMinder package to specify that you accept the license agreement:

   `customize_eac_bff -w keyword [-d pkg_location] pkg_name`

7. (Optional) Set the language of the installation parameters file:

   `customize_eac_bff -r -l lang [-d pkg_location] pkg_name`

8. (Optional) Change the installation directory:

   `customize_eac_bff -i install_loc [-d pkg_location] pkg_name`

   Note: If you are setting up the CA ControlMinder package for installation into WPARs (Workload Partitions), change the installation location to an unshared file system using the -i option. By default /opt and /usr are shared file systems and cannot be used for WPAR installations of CA ControlMinder.

9. (Optional) Change the default encryption files:

   `customize_eac_bff -s -c certfile -k keyfile [-d pkg_location] pkg_name`

10. Get the installation parameters file:

    `customize_eac_bff -g -f tmp_params [-d pkg_location] pkg_name`

11. (Optional) Edit the installation parameters file to suit your installation requirements.

    This file lets you set the installation defaults for the package. For example, activate the POSTEXIT setting (remove the preceding # character) and point it to post-installation script file you want to run.

12. (Optional) Set the installation parameters in your customized package:

    `customize_eac_bff -s -f tmp_params [-d pkg_location] pkg_name`

You can now use the customized package to install CA ControlMinder.

Install AIX Native Packages

To manage the CA ControlMinder installation with all your other software installations, install the customized CA ControlMinder AIX native package. The CA ControlMinder AIX native packages (bff files) let you install CA ControlMinder on AIX easily.

Important! You must customize the package to specify that you accept the license agreement using a keyword you can find inside the license agreement.

Follow these steps:

1. Log in as root.

   To register and install AIX native packages, you need permissions associated with the root account.

2. Customize the CAeAC package (see page 231).

   You must customize the package to specify that you accept the license agreement using a keyword that you can find inside the license agreement. You can also customize the package to specify custom installation settings.

3. (Optional) Record the level (version) of the package that you want to install:

   `installp -l -d pkg_location`

   pkg_location

   Defines the directory where the CA ControlMinder package (CAeAC) is located.

   For each package in *pkg_location*, AIX lists the level of the package.

   Note: For more information about the AIX native packaging installation options, refer to the man pages for installp.

4. Install the CA ControlMinder package using the following command:

   `installp -ac -d pkg_location CAeAC [pkg_level]`

   pkg_level

   Defines the level number of the package you recorded earlier.

   Important: If you are installing into WPARs, specify an unshared file system for installation and install into the global environment.

   AIX starts installing the CAeAC package from the *pkg_location* directory. CA ControlMinder is now fully installed but not started.

5. (Optional) Install into specific WPAR *wparname.* (Use -A to install on all system WPARs).

   - From global environment:
     `syncwpar wpar_name`
   - Or from a WPAR:
     `syncroot`

More information:

Additional Considerations for Native Installations (see page 198)

customize_eac_bff Command—Customize a bff Native Package File

The customize_eac_bff command runs the CA ControlMinder native package customization script for bff native package files.

The script works on any of the available CA ControlMinder native packages for AIX. To customize a package, the package must be in a read/write directory on your file system.

Important! The location where you extract the package to should have enough space to contain at least twice the size of the package for intermediate repackaging results.

Note: For localized script messages, you need to have pre.tar file in the same directory as the script file.

This command has the following format:

```
customize_eac_bff -h [-l lang]
customize_eac_bff -a [-d pkg_location] pkg_name
customize_eac_bff -w keyword [-d pkg_location] pkg_name
customize_eac_bff -r [-d pkg_location] [-l lang] pkg_name
customize_eac_bff -i install_loc [-d pkg_location] pkg_name
customize_eac_bff -s {-f tmp_params | -c certfile | -k keyfile} [-d pkg_location]
pkg_name
customize_eac_bff -g [-f tmp_params] [-d pkg_location] pkg_name
customize_eac_bff -t temp_dir [-d pkg_location] [pkg_name]
```

pkg_name

The name of the CA ControlMinder package (bff file) you want to customize.

-a

Displays the license agreement.

-c *certfile*

Defines the full pathname of the root certificate file.

Note: This option is applicable to the CAeAC package only.

-d *pkg_location*

(Optional) Specifies the directory where you placed your package on the file system. If you do not specify a directory where the package is located, the script defaults to /var/spool/pkg.

-f *tmp_params*

Specifies the full path and name of the installation parameters file to create or retrieve information from.

Note: If you do not specify a file when using the -g option, the installation parameters are directed to the standard output (stdout).

-g

Gets the installation parameters file and places it in the file specified by the -f option.

-h

Displays command usage. When used in conjunction with the -l option, displays the language code for supported languages.

-i *install_loc*

Sets the installation directory for the package to *install_loc*/AccessControl.

-k *keyfile*

Defines the full pathname of the root private key file.

Note: This option is applicable to the CAeAC package only.

-l *lang*

Sets the language of the installation parameters file to *lang*. You can set the language only in conjunction with the -r option.

Note: For a list of supported language codes you can specify, run -l with the -h option. By default, the installation parameters file is in English.

-r

Resets the package to use default values as in the original package.

-s

Sets the specified package to use inputs from the customized installation parameters file specified by the -f option.

-t *tmp_dir*

Sets the temporary directory for installation operations.

Note: The default temporary directory is /tmp.

-w *keyword*

Defines the keyword that specifies that you accept the license agreement. You can find this keyword at the end of the license agreement (inside square brackets). To locate the license agreement file, use the -a option.

Uninstall AIX Packages

To uninstall a CA ControlMinder AIX package installation, you need to uninstall the CA ControlMinder packages in the reverse order of their installation.

To uninstall CA ControlMinder packages uninstall the main CA ControlMinder package:

```
installp -u CAeAC
```

AIX Workload Partitions (WPAR) Implementation

AIX provides virtualized operating system environments within a single instance of AIX called Workload Partitions (WPAR). Workload Partitions are software partitions that are created from and share the resources of a single instance of the AIX operating system. AIX contains a master partition called *global environment* and workload partitions that run alongside it.

You can protect each partition in your environment using CA ControlMinder. This lets you define different rules and policies for each partition, and therefore define different access restrictions for each partition.

Review the following considerations and limitations before you install CA ControlMinder on AIX WPAR:

- You can install CA ControlMinder on AIX 7.1or later only.
- Regular script installation (install_base) is not supported. Use the native package installation to install CA ControlMinder on AIX WPAR.
- If you select to use AIX WPAR in shared mode, where the /opt and /usr directories are shared by all partitions, use a private installation directory. For example: specify to install CA ControlMinder in /CA/AccessControl/ directory and not in /opt/CA/AccessControl.
- AIX WPAR Live Migration is not supported.
- To use the keyboard logger on the workload partitions using the keyboard logger, verify that CA ControlMinder is running and that the keyboard logger is enabled on the Global Environment and on each workload partition.
- CA ControlMinder file protection rules that are applied to the workload partitions do not protect from users access from the Global Environment. To protect the Global Environment, apply the file protection rules on the Global Environment.
- Before you can install CA ControlMinder on AIX WPAR 5.2 and up, you must customize the CA ControlMinder installation package. You cannot use the installation package that you customize to install CA ControlMinder on AIX WPAR 7.1 and up.
- CA ControlMinder PAM features that identify user login attempts (for example: segrace, serevu, and audit log records) are not supported on AIX WPAR 5.2.

Install CA ControlMinder AIX 7.1 WPAR Native Package in Shared Mode

Installing CA ControlMinder on the AIX WPAR default partition is similar to a regular installation except for using a non-default installation directory. In shared mode the /opt and /usr directories are shared between all Workload Partitions.

Follow these steps:

1. Log in to the Global Environment as root.

   To register and install AIX native packages, you need permissions associated with the root account.

2. Customize the CAeAC package (see page 231).

   You customize the package to specify that you accept the license agreement using a keyword that you can find inside the license agreement. You can also customize the package to specify custom installation settings.

   Important! Change the installation directory to specify a private directory.For example:

   ```
   customize_eac_bff -i /CA/AccessControl -d pwd CaeAC.12.6.1.*.bff
   ```

3. Install the CA ControlMinder package using the following command:

   ```
   installp -d pkg_location CAeAC
   ```

   AIX starts installing the CAeAC package from the *pkg_location* directory.

   CA ControlMinder is now fully installed but not started.

4. Synchronize CA ControlMinder with the AIX Workload Partitions using the following command:

   ```
   synchwpar <wpar_name>
   ```

   wpar_name

   Specifies the name of the AIX Workload Partition

   Note: To install CA ControlMinder on all partitions use the synchwpar -A command.

   CA ControlMinder is installed on the specified AIX Workload Partition.

Install CA ControlMinder AIX 7.1 WPAR Native Package in Detached Mode

Installing CA ControlMinder on an AIX Workload Partitions is similar to a regular installation. In Detached Mode each Workload Partition uses a local copy of the /opt and /usr directories.

Follow these steps:

1. Log in to the Global Environment as root.

   To register and install AIX native packages, you need permissions associated with the root account.

2. Customize the CAeAC package (see page 231).

   You customize the package to specify that you accept the license agreement using a keyword that you can find inside the license agreement. You can also customize the package to specify custom installation settings.

3. Install CA ControlMinder by executing the following command:

   `installp -d pkg_location CAeAC`

   AIX starts installing the CAeAC package from the *pkg_location* directory.

   CA ControlMinder is now fully installed but not started.

4. Copy the installation package to each of the detached Workload Partitions.

5. Log in to each Workload Partition as root and install CA ControlMinder

   CA ControlMinder is installed on the AIX Workload Partition.

Install AIX WPAR Native Package on AIX 5.2

If AIX 5.2 operating system is installed for one or more of the Workload Partitions, you can install CA ControlMinder on the workload partitions after you install CA ControlMinder on the Global Environment.

Important! You can install CA ControlMinder on AIX 7.1 WPAR Global Environment and up only.

Follow these steps:

1. Log in to the Global Environment as root.

   To register and install AIX native packages, you need permissions associated with the root account.

2. Customize the CAeAC package (see page 231).

   You customize the package to specify that you accept the license agreement using a keyword that you can find inside the license agreement. You can also customize the package to specify custom installation settings.

3. Install CA ControlMinder by executing the following command:

   `installp -d pkg_location CAeAC`

   AIX starts installing the CAeAC package from the *pkg_location* directory.

   CA ControlMinder is now fully installed but not started.

4. Copy the original CA ControlMinder installation package to each Workload Partition.

5. Log in to the Workload Partition as root.

6. Customize the CAeAC package for AIX 5.2 WPAR.

   Important! You customize the CA ControlMinder installation package for AIX 7.1 and AIX 5.2 environments separately to ensure compatibility with the installp program on each operating system.

7. Install CA ControlMinder on the Workload Partition.

   CA ControlMinder is installed on the specified AIX Workload Partition.

Uninstall CA ControlMinder AIX 7.1 WPAR Packages

You uninstall AIX 7.1 WPAR package by first removing CA ControlMinder from the Global Environment and then from each Workload Partition.

Follow these steps:

1. Stop all CA ControlMinder daemons on the Global Environment and on each of the Workload Partitions using the following command:

   ```
   secons -sk
   ```

2. Log in to the Global Environment as root.

3. Remove the CAeAC package using the following command:

   ```
   installp -u CAeAC
   ```

4. Synchronize the Workload Partitions using the following command:

   ```
   synchwpar <wpar_name>
   ```

   Note: To uninstall CA ControlMinder in detached partitions and from workload partitions running AIX 5.2, remove the installation package by running the uninstall command on each partition.

   CA ControlMinder is removed from the Global Environment and from each Workload Partition.

Regular Script Installations

CA ControlMinder offers the install_base script for installing CA ControlMinder on UNIX interactively or silently.

If you are using a regular script installation (not a native installation), you will need three files from the CA ControlMinder installation media:

- **install_base**—A script that installs CA ControlMinder from the tar file.
- ***_opSystemVersion_ACVersion*.tar.Z**—A compressed tar file containing all the CA ControlMinder files. For example, if you are installing CA ControlMinder r12.0 on IBM AIX version 5 then your tar file is _AIX5_120.tar.Z
- **pre.tar**—A compressed tar file containing messages for installation as well as the license agreement.

  After you read the license agreement file, you can continue the installation by entering the command found at the end of that file:

  - If you are running a silent install (using install_base -autocfg), you can use the -command option with the command that can be found at the bottom of the license agreement file.
  - If you are using a response file (-autocfg file_name), you do not need to use the -command option.

  To get the license file name and location, run install_base -h. You also get the file name and location if you enter the wrong command.

You can find these files in the /Unix/Access-Control directory of the CA ControlMinder Endpoint Components for UNIX DVD.

Install Using install_base Script

You can install CA ControlMinder on any supported OS using the install_base script. This is an interactive script but you can also run it silently.

Note: Before you run the install_base script, make sure you decide which functionality you want to install and review the install_base command (see page 243) so you know how to initiate the installation of this functionality. You may also want to learn first how the install_base script works (see page 249).

To install CA ControlMinder

1. If you already have CA ControlMinder installed and it is running, shut it down by logging in as an administrator and entering the following commands:

   ```
   ACInstallDir/bin/secons -sk
   ACInstallDir/bin/SEOS_load -u
   ```

2. Log in as *root*.

   To install CA ControlMinder, you need to have root permissions.

3. Mount the optical disc drive with the CA ControlMinder Endpoint Components for UNIX DVD.

   Important! If you are installing on HP from an optical disk drive, you need to ensure the proper reading of file names from the DVD. To prevent the file names from being forced into a shortened and all-uppercase format, enter the *pfs_mountd &* and the *pfsd &* commands and make sure that the following four daemons are invoked: pfs_mountd, pfsd.rpc, pfs_mountd.rpc, and pfsd. For more information, see the man pages of the particular pfs* daemons and commands.

4. Read the license agreement.

   To run the install_base script you need to accept the End User License Agreement. After you have read the license agreement, you can continue the installation by entering the command found at the end of that file. To get the license file name and location, run install_base -h.

5. Run the install_base script.

   The install_base script starts and, based on your choices, prompts you for the appropriate installation questions.

   Note: The installation script finds the appropriate compressed tar file, so typing the name the tar file for your platform is optional.

   Now the CA ControlMinder installation is complete; however, it is not yet running.

Example: Install the Client and Server Packages with Default Features

The following command shows how to initiate the install_base interactive script to install the client and server packages with all default CA ControlMinder features. During the installation you are asked to answer questions related to installing the client and server packages of CA ControlMinder.

```
/dvdrom/Unix/Access-Control/install_base
```

Note: As we did not specify a package to install, the install_base command installs both client and server packages.

Example: Install the Client Package with STOP Enabled to a Custom Directory

The following command shows how to initiate the install_base interactive script to install the client package to the /opt/CA/AC directory, and enable the Stack Overflow Protection option.

```
/dvdrom/Unix/Access-Control/install_base -client -stop  -d /opt/CA/AC
```

install_base Command—Run Installation Script

The install_base command runs the installation script and installs one or more of the CA ControlMinder packages with one or more of the selected installation options.

This command has the following format:

```
install_base [tar_file] [packages] [options]
```

tar_file

(Optional) Defines the name of the tar file containing the CA ControlMinder installation files for your platform. The installation script finds the appropriate compressed tar file automatically, so typing the name of your tar file is optional.

packages

(Optional) Defines the CA ControlMinder packages you want to install. If you do not specify any packages, the installation script installs both the client and server packages unless you are upgrading CA ControlMinder, in which case the installation script installs the same packages you already have installed.

Note: You must install the client package before you install any other package. You can, however, specify to install the client package together with any other package.

The following are the CA ControlMinder packages you can install:

-all

Installs all CA ControlMinder packages. These are the client package, server package, API package, and the MFSD package. It also enables STOP (-stop option).

-api

Installs the API package that includes API libraries and sample programs.

-client

Installs the client package that has the core CA ControlMinder functionality required for a standalone computer.

-mfsd

Installs the MFSD package that includes the mainframe synchronization daemon.

Note: You must install the server package before you install the MFSD package.

-server

Installs the server package, which includes more binaries and scripts (selogrcd, sepmd, sepmdd, sepmdadm, secrepsw). These complement the client package. For example, sepmdd lets you set up the computer with a Policy Model.

-uni

Installs the Unicenter security integration and migration package that supports CA ControlMinder integration with CAUTIL, Workload Management, and Event Management components of Unicenter, and the Unicenter EMSec API.

options

(Optional) Defines additional installation options you want to set.

Note: Installation options that affect CA ControlMinder functionality, (for example, -stop) can only be specified when you install the *client* package. Installation options that affect the installation process (for example, -verbose) can be specified with any package.

The following are the options you can specify:

-autocfg [*response_file*]

Runs the installation in silent mode (not in interactive mode). If a response file is specified, the installation uses the preferences stored in the file to automatically respond to the interactive installation process. If you do not specify a response file, or if the response file is missing any options, the installation uses preset defaults.

To create a response file:

- Use the *-savecfg* option.
- Edit an installation parameters file, which you can find inside parameters.tar

Important! If you do not specify a response file, you must use the *-command* option when using the *-autocfg* option.

When running a silent installation, consider the following:

- You cannot change the encryption key.
- Only the client and server packages are installed by default.

  To install any other package or feature, you must specify the appropriate option as you would in a normal installation.
- The install_base command does not print installation details on the screen during installation.

  To view installation messages on the screen during installation, use the *-verbose* option.
- For security reasons, you cannot specify the Shared Secret that that secures SSL communication between the Report Agent and the Distribution Server in a silent installation. To specify the Shared Secret you need to configure the Report Agent user (+reportagent) after installation.

-command *keyword*

Defines the command that specifies that you accept the license agreement. You can find this command at the end of the license agreement (inside square brackets) and you must use it when you use the -autocfg option. To locate the license agreement file, run *install_base -h*

Note: The license agreement is only available while the help is displayed. When you finish reading the help, the license agreement is deleted.

-d *target_dir*

Defines a custom installation directory. The default installation directory is /opt/CA/AccessControl/.

Important! You cannot put the CA ControlMinder database in a mounted network file system (NFS).

-dns | -nodns

Creates a lookaside database with or without DNS hosts. The -nodns option specifies that CA ControlMinder will not perform an nslookup on any hosts in the DNS during installation.

-fips

Specifies to activate FIPS-only public key (asymmetric) encryption.

-force

Forces the installation to ignore an active new subscriber update (*sepmd -n* and *subs <pmdb> newsubs(sub_name)*) and continue the installation. By default, the installation stops and asks you to finish the subscriber update first.

Note: If you use this option, the new subscriber update will fail.

-force_encrypt

Forces the installation to accept a non-default encryption key without warning you.

Important! After the upgrade is complete, your encryption key is set to the default.

Note: CA ControlMinder also provides SSL, AES (128bit, 192bit, and 256bit), DES, and 3DES encryption options that you can choose.

-force_install

Forces the new installation over the already installed version. Use this option when you want to install over the same version.

-force_kernel

Forces the installation to continue without warning you it cannot unload your old kernel.

Note: You may need to reboot the computer after the installation is complete.

-g *groupname*

Defines the name of the group owner of CA ControlMinder files. The default value is 0.

-h | -help

Displays help for this command.

-ignore_dep

Specifies that the installation does *not* check for dependency with other products.

-key *encryption_key*

Restores your encryption key during an upgrade.

Note: During an upgrade you must use the same encryption key that you used before the upgrade.

-lang *lang*

Defines the language in which to install CA ControlMinder. For a list of supported languages and character sets, read the description for this option when you display the help (install_base -h).

-lic_dir *license_dir*

If the license program is not already installed, defines the license program installation directory.

Note: The license program installs to the specified directory only if $CASHCOMP variable is not defined in your or the computer's environment (it can be defined in /etc/profile.CA). Otherwise, the license program installs to $CASHCOMP. If $CASHCOMP is not defined and you do not specify -lic_dir, the license program installs to the /opt/CA/SharedComponents directory. CAWIN installs to the same directory as the license package.

-nolink

Specifies not to create a link to seos.ini in the /etc directory when you install CA ControlMinder to the default path (/opt/CA/AccessControl/).

CA ControlMinder creates a link to seos.ini in the /etc directory when you install CA ControlMinder to a non-default directory. This lets CA ControlMinder "detect" the Installation location. Use this option if you are installing to the default path and you do not want to update /etc (due to a security requirement).

-nolog

Specifies that a log is not kept for the installation process. By default, all transactions associated with the installation process are stored to *ACInstallDir*/AccessControl_install.log (where *ACInstallDir* is the installation directory for CA ControlMinder).

-no_tng_int

Specifies for the installation not to attempt to set up selogrd integration with Unicenter Event Management.

If you do not specify this option, the installation script checks whether Unicenter Event Management is installed. If the script finds that Unicenter Event Management seems to be installed, it sets up selogrd integration with Unicenter Event Management by adding the following line to selogrd.cfg:

`uni hostname`

-noprofile

Specifies not to load /etc/profile.CA to the user environment.

-post *program_name*

Specifies a program to run after the installation is complete.

-pre *program_name*

Specifies a program to run before the installation starts.

-rcert *certificate.pem*

Specifies the full path name to the root certificate file.

Note: When you use this option, the script extract the tar file and then repackages it with the file you provide replacing the default file (def_root.pem).

-rkey *certificate.key*

Specifies the full path name to the root key file.

Note: When you use this option, the script extract the tar file and then repackages it with the file you provide replacing the default file (def_root.key).

-rootprop

Specifies that sepass changes to the root password are sent to the Policy Model.

Note: You can set this after the installation is complete using the AllowRootProp token of the seos.ini file. For more information about the seos.ini initialization file, see the *Reference Guide*.

-savecfg *<response_file>*

Stores your responses to the interactive installation for later use by the *-autocfg* option.

-stop

Enables the use of the STOP (Stack Overflow Protection) feature.

-system_resolve

Specifies to use system functions, which define a bypass for network caching on your system.

Note: You cannot use this option on IBM AIX platforms.

-v

Displays the version of the CA ControlMinder package.

-verbose

Specifies that installation messages are displayed on the screen during installation. This is the default in an interactive installation and you only need to specify this option if you want to see these messages when you use the *-autocfg* option.

How the install_base Script Works

The install_base script performs the following steps:

1. Asks you whether you want to change the default installation directory.
2. Displays the installation options you supplied and asks that you to confirm that you want to continue with the installation.
3. Extracts the data from the tar.Z file into the installation location (default or as specified by *target_dir*).
4. Different platforms cause different actions:
   - For Sun Solaris, the script adds the CA ControlMinder *syscall* script to the file /etc/name_to_sysnum. The original file is saved as /etc/name_to_sysnum.bak. It then creates the file /etc/rc2.d/S68SEOS that forms part of the boot sequence.
   - For IBM AIX, the script loads the SEOS_syscall script.
5. Allocates, initializes, and formats the CA ControlMinder database and builds the seos.ini file. The database files are placed in the *ACInstallDir*/seosdb directory (*ACInstallDir* is the CA ControlMinder installation directory.)
6. Determines if the machine is NIS+
   - If it is, it sets the nis_env token in the [passwd] section to *nisplus*
   - If it is not and the machine is NIS, it sets the token to *nis*.

     In addition, if rpc.nisd is running, the script sets the NisPlus_server token in the [passwd] section to yes.
7. Under supported 32-bit platforms Sun Solaris, IBM AIX, HP-UX, and Linux, the script determines if the machine is running under NIS or DNS (using caching). If it is, the script automatically creates a lookaside database and sets two tokens in the [seosd] section of the seos.ini file to yes: under_NIS_server and use_lookaside.

   Note: On other platforms the script prompts you for whether you want to install a lookaside database and for the target installation directory.
8. Prompts you for the following additional information: (You can modify these settings any time after installation.)
   - The name for the group of auditors that can read the audit file.
   - Whether you want to add all your UNIX users, user groups, and hosts to the CA ControlMinder database now.
   - Whether you want your database to be subscribed to a PMDB; and if so, to which one.

     Your answer does not actually subscribe your database to a PMDB; it only lets the specified PMDB make updates to this database when you create the subscription later.

Two safe responses to this question include:

If you want to:	Respond with:
Allow your database to be subscribed to a specific PMDB	The name of the PMDB in the format *pmd_name@hostname*
Prevent your database from being subscribed to any PMDB (at least until you specify otherwise)	The Enter key.

A third response, _NO_MASTER_ , allows your database to be subscribed to any PMDB. However, this can be a dangerous response, because it removes the selection of the PMDB from your control.

- The password Policy Model name.
- What users will be security administrators for CA ControlMinder.
- Whether you want CA ControlMinder to support enterprise users; and if so, whether you want to define any as security administrators.
- If you chose a FIPS-only installation, whether you want to specify FIPS-only options related to encryption.
- If you did not choose FIPS-only encryption, whether you want to replace the default encryption method.

  CA ControlMinder provides you with symmetric, public key, and a combination of the two as encryption options that you can choose.
- If you choose public key encryption, CA ControlMinder lets you specify how you want to provide the subject certificate and root certificate.

  Depending on your choices, CA ControlMinder helps you set up SSL.
- If you choose symmetric encryption, whether you want to set a new encryption key.

  Note: See sechkey in the *Reference Guide* for information about encryption.
- Whether you want to install the Baseline Security rules.

  Baseline Security rules offer administrators an opportunity to install a package containing two sets of rules to better protect your system, password and log files. One set of rules applies to all platforms to protect CA ControlMinder files. The other set protects UNIX files and is specific to the Sun Solaris, HP-UX, IBM AIX, and Digital DEC UNIX platforms. You cannot install one set of rules without the other. Baseline Security rules install in Warning mode providing you with information but not actual protection. That is why we recommend that you remove the Warning mode as soon as you become familiar with the rules.
- Whether you want to be able to start CA ControlMinder from a remote host.

- Whether you want to enable the Report Agent, and if so, whether you want to enable CA User Activity Reporting Module.

  The Report Agent sends scheduled snapshots of the database to the Message Queue. You must define the Distribution Server host name, the port to use, and the queue name if you enable the Report Agent. If you enable CA User Activity Reporting Module, you can also specify to keep time-stamped backups of the audit log file.

- Whether you want to enable the SAM Agent.

  The SAM Agent configures the local computer for SAM, so that you can obtain privileged account passwords from this computer. You must define the Distribution Server host name, the port to use, and the queue name if you enable the SAM Agent.

- Whether you want to set up this endpoint for advanced policy management; and if so, the Distribution Host (DH) name to send calculation deviation results to.

  Define the DH host name using the format *dhName@hostName* For example, if you installed the Distribution Server on a host named host123.comp.com, you should use the following: DH__@host123.comp.com

Configure Post-Installation Settings

Once the installation is complete, you need to configure CA ControlMinder for your environment.

Follow these steps:

1. Append the *ACInstallDir*/bin directory to your PATH environment variable

   By default, the installation directory is /opt/CA/AccessControl/

2. Check the seos.ini (see page 259) file tokens to make sure that the settings meet your requirements.

   If necessary, modify the settings.

3. To give yourself access to the CA ControlMinder man pages, add the directory *ACInstallDir*/man to your MANPATH.

   For example, if you are using csh shell, for the duration of the current session, enter the command:

   ```
   setenv MANPATH $MANPATH:/opt/CA/AccessControl//man
   ```

   For future sessions add a similar line to your .login, .profile, or .cshrc file.

Start CA ControlMinder

Assuming you are working in an X Windows environment, invoke CA ControlMinder, verify that it is correctly installed on your system, and perform the following steps to initiate important protection:

1. Open two windows under root (superuser) authority.
2. In either window, enter the command:

   ```
   seload
   ```

   Wait while the seload command starts three CA ControlMinder daemons: Engine, Agent, and Watchdog.
3. After you have started the daemons, go to the other window and enter the command:

   ```
   secons -t+ -tv
   ```

   CA ControlMinder accumulates a file of messages reporting operating system events. The secons -tv command displays the messages on the screen as well.
4. In the first window, where you gave the seload command, enter the following command:

   ```
   who
   ```

   Watch the second window, where CA ControlMinder is writing the trace messages, to see whether CA ControlMinder intercepts the execution of the who command and reports on it. CA ControlMinder is correctly installed on your system if it reports interception of the who command.
5. If you want, enter more commands to see how CA ControlMinder reacts to them.

   The database does not yet contain any rules for blocking access attempts. Nevertheless, CA ControlMinder monitors the system so that you can see how the system behaves with CA ControlMinder installed and running, and which events CA ControlMinder intercepts.
6. Shut down the seosd daemon, by entering the following command:

   ```
   secons -s
   ```

   The following message displays on the screen:

   ```
   CA ControlMinder is now DOWN !
   ```

Configure an Endpoint for Advanced Policy Management

Once you install the advanced policy management server components, you need to configure each endpoint in your enterprise for advanced policy management. In doing so, you configure the endpoint to send information to and receive information from the server components.

Note: This procedure shows you how to configure an existing installation of CA ControlMinder for advanced policy management. If you specified this information when you installed CA ControlMinder on the endpoint you do not need to configure the endpoint again.

To configure an endpoint for advanced policy management, open a command window and enter the following command:

`dmsmgr -config -dhname` *dhName*

dhName

Defines a comma-separated list of Distribution Host (DH) names you want the endpoint to work with.

Example: DH__@centralhost.org.com

This command configures the endpoint for advanced policy management and sets it to work with the defined DH.

Note: For more information, see the dmsmgr -config command in the *Reference Guide*.

Configure a UNIX Endpoint for Reporting

Once you have CA ControlMinder Endpoint Management and the Report Portal installed and configured, you can configure your endpoints to send data to the Distribution Server for processing by enabling and configuring the Report Agent.

Note: When you install CA ControlMinder, it lets you configure the endpoint for reporting. This procedure illustrates how you configure an existing endpoint for sending reports if you did not configure this option at install time.

To configure a UNIX endpoint for reporting

1. Run *ACSharedDir*/lbin/report_agent.sh:

   `report_agent config -server hostname [-proto {ssl|tcp}] [-port port_number [-rqueue queue_name]`

   If you omit any configuration options, the default setting is used.

   Note: For more information on the report_agent.sh script, see the *Reference Guide*.

2. Create a *+reportagent* user in database.

   This user should have ADMIN and AUDITOR attributes and *write* access to local terminal. You should also set epassword to the Report Agent Shared Secret (which you defined when you installed the Distribution Server).

3. Create a SPECIALPGM for the Report Agent process.

   The SPECIALPGM maps the root user to the +reportagent user.

Note: After you enable the Report Agent, you can modify CA ControlMinder configuration settings to change performance-related settings. For more information on Report Agent configuration settings, see the *Reference Guide*.

Example: Configure a UNIX Endpoint for Reporting Using selang

The following selang commands show you how, assuming you enabled and configured the Report Agent, you create the required Report Agent user and specify special security privileges for the Report Agent process:

```
eu +reportagent admin auditor logical epassword(Report_Agent) nonative
auth terminal (terminal101) uid( +reportagent) access(w)
er specialpgm (/opt/CA/AcessControl/bin/ReportAgent) Seosuid(+reportagent) \
Nativeuid(root) pgmtype(none)
```

Customizing CA ControlMinder

Implementing full-scale security using CA ControlMinder requires the definition of the security policies you want enforced. The time taken to make these definitions depends on the size of your site and the way you choose to manage security.

For instance, at a university you would probably not define most students to CA ControlMinder; they would get access based solely on resource _default settings. At a bank, however, you would probably define every user to CA ControlMinder and set access lists for every resource to allow specific users access to specific resources. Thus, for the same number of users, implementing CA ControlMinder at the university would take less time than implementing it at a bank.

As security administrator, you must define the objectives of the project. Decisions regarding site policy must be made carefully. CA ControlMinder includes several files that you can customize to help you implement the security policies of your site.

Trusted Programs

A trusted program is one that can be executed only as long as it has not been altered. Ordinarily it is a setuid/setgid program. CA ControlMinder also allows you to specify regular programs as trusted. When you are sure that the program has not been tampered with, register it in the PROGRAM class, where CA ControlMinder can guard its integrity.

You may want to use trusted programs together with *program pathing*, so users can perform certain tasks only by means of trusted programs.

Note: For more information about program pathing, see the *Endpoint Administration Guide for UNIX*.

CA ControlMinder can help you with a script to register a whole collection of setuid and setgid programs as trusted.

1. To save yourself the effort of remembering all your setuid and setgid programs, use the seuidpgm program that follows. It scans your file system, locates all setuid and setgid programs, and creates a script of selang commands that will register them all in the PROGRAM class.

   Issue this command:

   ```
   seuidpgm -q -l -f / > /opt/CA/AccessControl//seuid.txt
   ```

   Run as shown, seuidpgm does the following:

   - Scans the entire file system (starting from /).
   - Remains quiet (the -q option suppresses the “cannot chdir” messages).
   - Ignores any symbolic links (-l).
   - Registers the programs in both the FILE and PROGRAM classes (-f).
   - Outputs the commands to file /opt/CA/AccessControl//seuid.txt.

   Note: For a complete description of seuidpgm, see the *Reference Guide*.

2. Using a text editor, check the seuid.txt file to be sure that it includes all the setgid/setuid programs that you want to have trusted, and no other programs. Edit the file if necessary.

3. Use selang to run the edited file of commands. If the seosd daemon is not running, include the -l switch.

   ```
   selang [-l] -f /opt/CA/AccessControl//seuid.txt
   ```

   It may take a few minutes for selang to finish.

4. Restart the seosd daemon if it is not already running. Then check whether your system works as expected and whether setuid programs can be invoked.

5. It is advisable to change the default access of the PROGRAM class to NONE to prevent new untrusted setuid or setgid programs from being added and run without the knowledge of the security administrator.

   Enter the following selang command to set that default access value:

   ```
   chres PROGRAM _default defaccess(none)
   ```

Note: Veteran CA ControlMinder users will remember the UACC class in this connection. That class still exists and can be used to specify the default access of a resource. However, for ease of use we recommended that for specifying the default access of a class, you use the class's _default record instead. The _default specification overrides any UACC specification for the same class.

The records in the PROGRAM class representing the setuid, setgid, and regular programs that you have registered store the following attributes of the executable files.

- Device-number
- Inode
- Owner
- Group
- Size
- Creation Date
- Creation Time
- Last-Modification Date
- Last-Modification Time
- MD5 Signature
- SHA1 Signature
- Checksum CRC (Cyclical Redundancy Check)

The most important attribute of each program you register is that the program is *trusted*. That is, the program is considered OK to run. Any change in any of the attributes listed previously causes the program to lose its trusted status, and then CA ControlMinder can prevent the program from running.

Monitor Use of Unregistered Programs

If you are not sure whether you have successfully registered all the appropriate programs in the database, use the following command to watch for unregistered programs:

```
chres PROGRAM _default warning
```

The warning property puts the PROGRAM class into Warning mode, meaning that a special audit record appears as a warning each time an unregistered setuid or setgid program is used but the use of such programs *is not prevented*.

Review the Audit Log

You can search for untrusted records manually in the audit log, or you can set special notification instructions to be informed when certain programs become untrusted. The special notification is especially helpful so that users do not have to contact you to use a program that has become untrusted; instead, you can check the file as soon as you receive a notification that it has become untrusted.

Note: To set up special audit notifications, see the *Endpoint Administration Guide*.

Protection

To prevent execution of setuid and setgid commands that are not trusted, issue the following command:

Note: CA ControlMinder automatically includes the user “nobody” in the database.

```
newres PROGRAM _default defaccess(none) \
owner(nobody) audit(all)
```

CA ControlMinder then protects you against back doors and Trojan horses by requiring approval from you before allowing any new or changed program to run.

Now suppose, for example, that you have received a new, useful program that is a setuid program. You are sure it is not a Trojan horse, and you want all users to be able to execute it. To register the program as trusted, issue the following command:

```
newres PROGRAM program-pathname \ defaccess(EXEC)
```

Retrust Untrusted Programs

If a program has been untrusted by CA ControlMinder because of a change in its size, its modification date, or any other monitored property, the program will run again only if you *retrust* it, registering a new approval for it in the database. To retrust a program:

```
editres PROGRAM progam_name trust
```

Note: You can also retrust a program with the seretrust utility. For more information about this utility and its options, see the *Reference Guide*.

Initialization Files

This section describes various files that CA ControlMinder reads at initialization time. By default, CA ControlMinder places the initialization files in the directory containing the file seos.ini, which is the installation directory for CA ControlMinder.

seos.ini

The seos.ini file sets global parameters.

Note: For information about the structure of the file and supported tokens see the *Reference Guide*.

The seos.ini file, as installed, is protected and cannot be updated while CA ControlMinder is running, though all users can always access it on a READ basis. Enter the following command to let an authorized user update the file while CA ControlMinder is running:

```
newres FILE ACInstallDir/seos.ini owner(authUser) defacc(read)
```

ACInstallDir is the installation directory for CA ControlMinder, by default /opt/CA/AccessControl/.

This command establishes that the default access for the file is READ; however, only the owner of the file, *authUser*, can update the file.

Note: It is important that the default access for the seos.ini file be READ because many utilities access seos.ini during their processing. If they cannot read the file, they will fail.

Trace Filter File

This optional file contains entries that specify filter masks for filtering out CA ControlMinder trace messages of any kind.

The trace filter file specifies the trace messages that are to be filtered out (that is, those messages that are not to appear in the trace file). Each line specifies a mask that identifies a group of messages to be suppressed. For example, the following file suppresses all messages that begin with WATCHDOG or INFO and all messages that end with BYPASS.

```
WATCHDOG*
*BYPASS
INFO*
```

By default, CA ControlMinder uses a trace filter file named trcfilter.init. You can change the name and location of the trace filter file by editing the value of the trace_filter token in the [seosd] section of the seos.ini file.

To filter trace records, edit the file as required. To add remarks (comment lines) to the file, place a semicolon (;) at the beginning of the line.

The trcfilter.init file does not filter audit records generated by user traces. To filter these audit records, edit the audit.cfg file.

Note: For more information, see the seosd utility in the *Reference Guide*.

Advanced Policy Management

Multiple-rule 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 policy versions and then assign those to hosts or group host. Once assigned, policies are queued for deployment. Alternatively, you can deploy and undeploy policy versions directly onto hosts or group hosts.

Note: For more information about advanced policy management, see the *Enterprise Administration Guide*.

Configure Advanced Policy Management

If you are setting your enterprise to use advanced policy-based management, you need to install a DMS and a DH in a central location and then configure each endpoint for advanced policy management (see page 260).

To configure your hierarchy for advanced policy management post-installation, use the dmsmgr utility.

Note: For more information about the dmsmgr utility, see the *Reference Guide*.

Configure an Endpoint for Policy Deviation Calculations

Each endpoint must be configured to allow policy deviation calculation. Normally, you do this during the installation. This procedure is aimed at achieving this post-installation instead.

To configure an endpoint for policy deviation calculations, enter the following selang command:

`so dms+(DMS@host)`

DMS@host

Defines the name of your DMS specified in the shown format.

sesu and sepass Utilities

We recommend that you use sepass instead of the operating system's passwd command and sesu instead of the su command. To do this, you need to save the original system binaries and replace them with symbolic links to sepass and sesu respectively. Once this is done, you need to make sure you can always use these utilities.

On most operating systems, the sepass and sesu utilities run even when CA ControlMinder is not loaded. However, on some operating systems (for example, AIX) these utilities do not work when CA ControlMinder is not loaded. For these operating systems, CA ControlMinder provides wrapper scripts.

sesu and sepass Wrapper Scripts

The sesu and sepass wrapper scripts are found in the following directory:

ACInstallDir/samples/wrappers

This directory contains the following files:

File	Description
sesu_wrap.sh	Wrapper script for sesu
sepass_wrap.sh	Wrapper script for sepass
README	A text file with usage and conceptual information for these wrappers

Use the Wrapper Script to Run sesu

Using the wrapper scripts to run the sesu utility lets you run it on operating systems where it does not work when CA ControlMinder is not loaded.

Note: You only need to follow this procedure if the sesu utility does not run when CA ControlMinder is not loaded.

To use wrapper scripts to run sesu

1. Open the sesu_wrap.sh script in a text editor.

   The wrapper script displays in the text editor.

2. If necessary, change the following two variables:

   SEOSDIR

   Defines the CA ControlMinder installation directory. By default, this is set to the default installation directory:

   /opt/CA/AccessControl/

   SYSSU

   Defines the name of the original su system binary that you need to replace. By default, this is set to:

   /usr/bin/su.orig

3. Replace the su symbolic link to point to the sesu_wrap.sh wrapper script rather than to the sesu utility.

   Whenever you run su, the sesu wrapper script runs the sesu utility.

Use the Wrapper Script to Run sepass

Using the wrapper scripts to run the sepass utility lets you run it on operating systems where it does not work when CA ControlMinder is not loaded.

Note: You only need to follow this procedure if the sepass utility does not run when CA ControlMinder is not loaded.

To use wrapper scripts to run sepass

1. Open the sepass_wrap.sh script in a text editor.

   The wrapper script displays in the text editor.

2. If necessary, change the following two variables:

   SEOSDIR

   Defines the CA ControlMinder installation directory. By default, this is set to the default installation directory:

   `/opt/CA/AccessControl/`

   SYSPASSWD

   Defines the name of the original sepass system binary that you need to replace. By default, this is set to:

   `/usr/bin/passwd.orig`

3. Replace the passwd symbolic link to point to the sepass_wrap.sh wrapper script rather than to the sepass utility.

   Whenever you run passwd, the sepass wrapper script runs the sepass utility.

Maintenance Mode Protection (Silent Mode)

CA ControlMinder has a maintenance mode, also known as silent mode, for protection when the CA ControlMinder daemons are down for maintenance. In this mode, CA ControlMinder denies events while these daemons are down.

When CA ControlMinder is running, it intercepts security sensitive events and checks whether the event is allowed. Without activating maintenance mode, all events are permitted when CA ControlMinder services are down. With active maintenance mode, events are denied when CA ControlMinder daemons are down, stopping user activity while the system is maintained.

Maintenance mode can be tuned, and it is disabled by default.

When the CA ControlMinder security services are down:

- If maintenance mode is active, all security sensitive events are denied, except for special cases and for events executed by the maintenance user.
- If maintenance mode is disabled, CA ControlMinder does not intervene and execution is passed to the operating system.

When maintenance mode is activated and security is down, the prevented events are not logged in the audit log file.

To enable maintenance mode, follow these steps:

Important! If root is not the maintenance user, make sure you have an open session for the maintenance user as you will not be able to log in otherwise.

1. Make sure the CA ControlMinder daemons are down.
2. Using seini utility, change the token silent_deny value to *yes*.

   The token is located under SEOS_syscall section.

   ```
   seini -s SEOS_syscall.silent_deny yes
   ```

3. Change the token silent_admin value to the numeric UNIX UID that you want to let access the computer while CA ControlMinder daemons are down.

   ```
   seini -s SEOS_syscall.silent_admin <maintenance_UID>
   ```

   Note: *root* is the default maintenance mode user (UID 0).

   Important! If the maintenance user is not *root*, you must make the CA ControlMinder authorization daemon setuid to the root user so that you can start CA ControlMinder in maintenance mode. To make this change enter the following command:
   chmod 6111 seosd

4. Start CA ControlMinder daemons with seload command.

   Note: If the maintenance mode user is not root, start CA ControlMinder daemons with seosd command.

How to Install on Solaris Zones

Installing CA ControlMinder on Solaris 10 zones is no different than a regular installation. The recommended way of installing CA ControlMinder on Solaris 10 is using Solaris native packaging (pkgadd and pkgrm) commands.

Important: For CA ControlMinder to work in any nonglobal zone, install it in the global zone first.

Depending on whether you want to install CA ControlMinder on all zones, or only on selected zones, use *one* of the following methods:

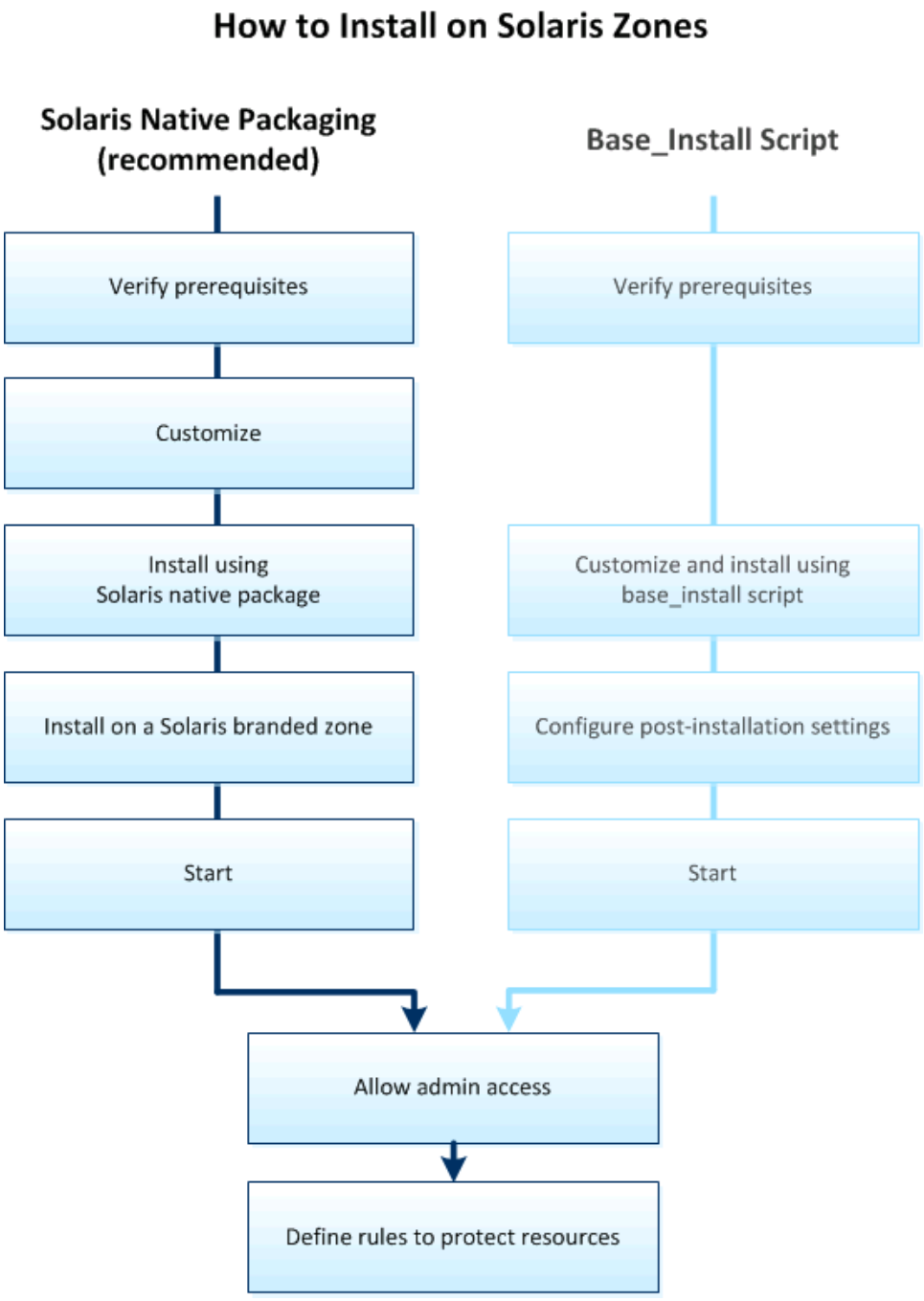
- Install CA ControlMinder using Solaris native packaging (see page 266)

  We recommend using the Solaris native package installation. You can either:

  - Install CA ControlMinder on all zones (see page 217).
  - Install CA ControlMinder on the global zone and selected zones (see page 221).

- Install CA ControlMinder on a selected zone using the install_base script (see page 276)

  The install_base script installs CA ControlMinder in the zone you are executing the script in. Install CA ControlMinder in the global zone first.


How to Install on Solaris Zones
Solaris Native Packaging (recommended)
Base_Install Script
Verify prerequisites
Customize
Install using Solaris native package
Install on a Solaris branded zone
Start
Verify prerequisites
Customize and install using base_install script
Configure post-installation settings
Start
Allow admin access
Define rules to protect resources

Follow these steps:

1. Install CA ControlMinder using *one* of the following methods:
   - Install CA ControlMinder using Solaris native packaging (see page 266) (recommended)
     a. Verify prerequisites (see page 267)
     b. Customize the Solaris native package (see page 268)
     c. Install Solaris Native Package (see page 272)
     d. Install on a Solaris Branded Zone (see page 272)
     e. Use ioctl for communication (see page 273)
     f. Start CA ControlMinder (see page 274)
   - Install CA ControlMinder in each zone using the install_base script (see page 276)
     a. Verify prerequisites (see page 276)
     b. Customize and install using install_base script (see page 276)
     c. Configure post-installation settings (see page 251)
     d. Start CA ControlMinder (see page 252)
2. Allow admin access using zlogin (see page 279)
3. Define rules to protect resources (see page 279)

Note: Due to a Solaris 11 limitation, the CA ControlMinder package is not propagated into nonglobal zones during installation. We recommend you to install CA ControlMinder in each zone individually using the Solaris native packaging tool (pkgadd).

Install Using Solaris Native Packaging

Solaris native packaging is provided as command-line utilities that let you create, install, remove, and report on individual software packages.

Note: For more information about Solaris native packaging, see the Sun Microsystems website and the man pages for pkgadd, pkgrm, pkginfo, and pkgchk.

Instead of a regular installation, you can use the Solaris native packages CA ControlMinder provides. This lets you manage your CA ControlMinder installation with all your other software installations performed using Solaris native packaging.

Important! To uninstall CA ControlMinder after a package installation, you must use the *pkgrm* command. Do not use uninstall_AC script.

If you install CA ControlMinder using Solaris native packaging on all zones, CA ControlMinder also automatically installs on any zones you create after the original installation. However, while the post-installation CA ControlMinder procedure scripts need to run from within the non-global zone, for new zones, these scripts can only run once the new zone configuration is complete. Specifically, you must run the "zlogin -C *zonename*" command (which, completes the configuration of the name service, the root password, and so on).

Important! If you do not run the "zlogin -C *zonename*" command, or if you boot and log in to the new zone very quickly, CA ControlMinder installation will be incomplete as the post-installation scripts did not run.

Note: For more information on setting up a new zone correctly, see Sun's *System Administration Guide: Solaris Containers--Resource Management and Solaris Zones*, which is available at Sun Microsystems Documentation website.

Verify Prerequisites

You find the Solaris native package for each of the supported Solaris operating systems in the NativePackages directory of the CA ControlMinder Endpoint Components for UNIX DVD.

- pre.tar
- _Solaris_PKG*.tar.Z
- convert_eac_pkg
- customize_eac_pkg

The _Solaris_PKG*.tar is the native package for Solaris. The pre.tar file is a compressed tar file containing installation messages and the CA ControlMinder license agreement.

Follow these steps:

1. Copy the installation files from the media to a temporary directory *$PACKAGE_DIR* (readable for group and world). For example, /tmp.

   ```
   cp /mnt/AC_DVD/NativePackages/_Solaris_PKG*.tar.Z $PACKAGE_DIR
   cp /mnt/AC_DVD/NativePackages/pre.tar             $PACKAGE_DIR
   cp /mnt/AC_DVD/NativePackages/*_eac_pkg           $PACKAGE_DIR
   ```

2. Unpack the tar archive in *$PACKAGE_DIR*.

   ```
   cd $PACKAGE_DIR
   zcat _Solaris_PKG*.tar.Z | tar -xvf -
   ```

   Important: Ensure that file attributes for the entire directory structure of the package are preserved during extraction, or Solaris native packaging tools will consider the package corrupt.

3. Verify that your system supports the correct versions of the C++ library.

   ```
   pvs -d /usr/lib/libCstd.so.1
           libCstd.so.1;
           SUNW_1.1.1;
           SUNW_1.1;
           SUNW_1.2;
           SUNW_1.3;
           SUNW_1.3.1;
   ```

Customize the Solaris Native Packages

Before you can install CA ControlMinder using a native package, you must customize the CA ControlMinder package and specify that you accept the license agreement. You can also specify custom installation settings when you customize a package.

You customize a package by extracting the installation parameters file from the package, modifying it as required, and then loading it back into the package. Some commands are available in the customization script so that you do not have to modify the parameters file.

Note: We recommend that you do not modify the package manually. Instead, use the script as described in the following procedure to customize the CA ControlMinder package.

Follow these steps:

1. Display the license agreement:

   `customize_eac_pkg -a -d $PACKAGE_DIR CAeAC`

2. Take note of the keyword that appears at the end of the license agreement inside square brackets.

   You specify this keyword in the next step.

3. Provide the *keyword* to specify that you accept the license agreement:

   `customize_eac_pkg -w keyword -d $PACKAGE_DIR CAeAC`

4. (Optional) Change the language of the installation parameters file to *lang.* By default, the installation parameters file is in English.

   `customize_eac_pkg -r -l lang -d $PACKAGE_DIR CAeAC`

5. (Optional) Change the default encryption files.

   `customize_eac_pkg -s -c certfile -k keyfile -d $PACKAGE_DIR CAeAC`

6. Change the target installation directory from /tmp to a custom path, for example /opt/CA/:

   `customize_eac_pkg -i /opt/CA -d $PACKAGE_DIR CAeAC`

7. Generate a response file "paramtemplate" with default values:

   `customize_eac_pkg -g -f $PACKAGE_DIR/paramtemplate -d $PACKAGE_DIR CAeAC`

8. Modify the default values in the paramtemplate file with data specific to your environment.

   The paramtemplate file lets you set the installation defaults for the package. For example, activate the POSTEXIT setting (remove the preceding # character) and point it to a post-installation script file you want to run.

customize_eac_pkg Command—Customize Solaris Native Package

The customize_eac_pkg command runs the CA ControlMinder Solaris native package customization script.

You should consider the following when using this command:

- The script works on any of the available CA ControlMinder Solaris native packages.
- To customize a package, the package must be in a read/write directory on your file system.
- For localized script messages, you need to have pre.tar file in the same directory as the script file.

This command has the following format:

```
customize_eac_pkg -h [-l]
customize_eac_pkg -a [-d pkg_location] [pkg_name]
customize_eac_pkg -w keyword [-d pkg_location] [pkg_name]
customize_eac_pkg -r [-d pkg_location] [-l lang] [pkg_name]
customize_eac_pkg -i install_loc [-d pkg_location] [pkg_name]
customize_eac_pkg -s {-f tmp_params | -c certfile | -k keyfile} [-d pkg_location]
[pkg_name]
customize_eac_pkg -g [-f tmp_params] [-d pkg_location] [pkg_name]
customize_eac_pkg -t tmp_dir [-d pkg_location] [pkg_name]
```

pkg_name

(Optional) The name of the CA ControlMinder package you want to customize. If you do not specify a package, the script defaults to the main CA ControlMinder package (CAeAC).

-a

Displays the license agreement.

-c *certfile*

Defines the full pathname of the root certificate file.

Note: This option is applicable to the CAeAC package only.

-d *pkg_location*

(Optional) Specifies the directory where you placed your package on the file system. If you do not specify a directory where the package is located, the script defaults to /var/spool/pkg.

-f *tmp_params*

Specifies the full path and name of the installation parameters file to create or retrieve information from.

Note: If you do not specify a file when using the -g option, the installation parameters are directed to the standard output (stdout).

-g

Gets the installation parameters file and places it in the file specified by the -f option.

-h

Displays command usage. When used in conjunction with the -l option, displays the language code for supported languages.

-i *install_loc*

Sets the installation directory for the package to *install_loc*/AccessControl.

-k *keyfile*

Defines the full pathname of the root private key file.

Note: This option is applicable to the CAeAC package only.

-l *lang*

Sets the language of the installation parameters file to *lang*. You can set the language only in conjunction with the -r option.

Note: For a list of supported language codes you can specify, run -l with the -h option. By default, the installation parameters file is in English.

-r

Resets the package to use default values as in the original package.

-s

Sets the specified package to use inputs from the customized installation parameters file specified by the -f option.

-t *tmp_dir*

Sets the temporary directory for installation operations.

Note: The default temporary directory is /tmp.

-w *keyword*

Defines the keyword that specifies that you accept the license agreement. You can find this keyword at the end of the license agreement (inside square brackets). To locate the license agreement file, use the -a option.

Note: Ensure that the parameters for cryptographic options of the DH are the same as those in the environment where install_base is installed.

Install Solaris Native Package

To manage the CA ControlMinder installation with all your other software installations, install the customized CA ControlMinder Solaris native package. Make sure you use the same CA ControlMinder version in all zones.

Solaris native packaging may require user interaction by default, and we recommend to configure the installation as follows to run silently.

Note: For more information about the installation administration file ("myadmin") and how to use it, see the Solaris man page for pkgadd(1M) and admin(4).

Follow these steps:

1. Generate the installation administration file in *$CONFIG_DIR* to activate silent installation:

   ```
   convert_eac_pkg -p
   ```

   The file "myadmin" is created from a generic template.

2. Edit the myadmin file and modify the following settings:

   ```
   setuid = nocheck
   action = nocheck
   ```

   You have configured the installation administration file to run silently.

3. Install your customized CA ControlMinder package silently using the -n option.

   Do *one* of the following:

   - To install on all zones, run the following command from the global zone:

     ```
     pkgadd -n -a $CONFIG_DIR\myadmin -d $PACKAGE_DIR CAeAC
     ```

   - Install on selected zones:

     Run the following command from the global zone:

     ```
     pkgadd -G -n -a $CONFIG_DIR\myadmin -d $PACKAGE_DIR CAeAC
     ```

     Run the following command on each of the selected non-global zones:

     ```
     pkgadd -n -a $CONFIG_DIR\myadmin -d $PACKAGE_DIR CAeAC
     ```

The installation is complete. You can now start CA ControlMinder.

Install on a Solaris Branded Zone

Solaris pkgadd does not support propagation of applications installed in the Solaris 10 global zone into branded zones. CA ControlMinder must use an ioctl instead of a syscall to communicate with the kernel module.

Note: The installation parameter file also lets you install on branded zones automatically when you install on the global zone.

Follow these steps:

1. Edit the *$PACKAGE_DIR/*paramtemplate file, and change the following setting:
   `UseBrandZone = "yes"`
2. Edit the seos.ini file and modify the following line:
   `SEOS_use_ioctl = 1`

   CA ControlMinder is configured to use ioctl.
3. Install CA ControlMinder in the Solaris 10 branded zone using pkgadd.
   `customize_eac_pkg -s -f $PACKAGE_DIR/paramtemplate -d $PACKAGE_DIR CAeAC`
   `pkgadd -G -a $PACKAGE_DIR/myadmin -d $PACKAGE_DIR CAeAC`
4. Install CA ControlMinder in the Solaris 8 and 9 branded zones using pkgadd.
   `customize_eac_pkg -s -f $PACKAGE_DIR/paramtemplate -d $PACKAGE_DIR CAeAC`
   `pkgadd -n -a $PACKAGE_DIR/myadmin -d $PACKAGE_DIR CAeAC`

   Ignore the warnings and confirm with 'y' when prompted.

The installation is complete. You can now start CA ControlMinder in the branded zone.

Important! If SEOS_use_ioctl is set to 0, you need to modify CA ControlMinder to use ioctl for communication in all zones. Once you make this change and reboot all zones, the installation is complete.

Use ioctl for Communication

If you want to install CA ControlMinder in Solaris branded zones, you must use an ioctl instead of a syscall to communicate with the kernel module.

Follow these steps:

1. Stop CA ControlMinder in the global zone and all non-global zones.

   Stop the last zone to disable event interception and prepare the kernel module for unloading.
   `zlogin -z zone_name /opt/CA/AccessControl/bin/secons -sk`
2. Unload the CA ControlMinder kernel module in the global zone:
   `SEOS_load -u`

   Note: The SEOS_load -u command ensures that CA ControlMinder is not running on any non-global zone before unloading it.

3. In each zone where CA ControlMinder is installed (global, non-global, and branded zones), set the seos.ini entry to 1 (by default, this is set to 0).
   `SEOS_use_ioctl = 1`
4. Load the kernel module in the global zone.
   `SEOS_load`

   This installs a pseudo device to let CA ControlMinder communicate with its kernel module via ioctl, and identifies zones that require a reboot so that they can utilize the ioctl.
5. Reboot each non-global and brand zone where CA ControlMinder is installed.

Starting and Stopping CA ControlMinder in a Zone

Starting and stopping CA ControlMinder in Solaris 10 zones is generally done in the same way you would normally start and stop CA ControlMinder on any Solaris computer.

The following exceptions apply to starting CA ControlMinder in zones:

- You can load the CA ControlMinder kernel module (SEOS_load) from the global zone only.
- You must load the CA ControlMinder kernel module in the global zone before you can start CA ControlMinder in any non-global zone.

  Once the CA ControlMinder kernel module is loaded in the global zone, you can then start and stop CA ControlMinder in any non-global zone and in any order.

The following exceptions apply to stopping CA ControlMinder in zones:

- You cannot unload the CA ControlMinder kernel module when one or more zones has maintenance mode (see page 262) enabled.
- You can stop CA ControlMinder in all zones in any order by issuing the *secons -s* command in each zone.
- You can stop CA ControlMinder in all zones at the same time by adding all zones to a GHOST record and then issuing the secons -s *ghost_name* command from the global zone.

  This is useful, for example, when you want to upgrade CA ControlMinder across all zones.
- You should stop the last zone with the *secons -sk* to disable event interception and prepare the CA ControlMinder kernel module for unloading.
- You can unload the CA ControlMinder kernel module (SEOS_load -u) from the global zone only.

  Note: The SEOS_load -u command ensures that CA ControlMinder is not running on any non-global zone before unloading it.

Start CA ControlMinder in A Non-global Zone

You can start CA ControlMinder from any non-global zone just as you would normally, but you must first load the CA ControlMinder kernel module in the global zone.

Follow these steps:

1. In the global zone, enter the SEOS_load command to load the CA ControlMinder kernel module.

   The CA ControlMinder kernel loads and you can now start CA ControlMinder in any zone.

   Note: The CA ControlMinder kernel loads but CA ControlMinder does not intercept events in the global zone.

2. In the non-global zone, enter the seload command to start CA ControlMinder in that zone.

   The non-global zone is protected by CA ControlMinder.

   Note: You can also start CA ControlMinder in the non-global zone remotely. For more information, see the seload command in the *Reference Guide*.

Install Using the Install_Base Script

Verify Prerequisites (Install_Base)

CA ControlMinder offers the install_base script for installing CA ControlMinder on UNIX interactively or silently.

If you are using a regular script installation (not a native installation), you will need three files from the CA ControlMinder installation media:

- **install_base**—A script that installs CA ControlMinder from the tar file.
- ***_opSystemVersion_ACVersion*.tar.Z**—A compressed tar file containing all the CA ControlMinder files. For example, if you are installing CA ControlMinder r12.0 on IBM AIX version 5 then your tar file is _AIX5_120.tar.Z
- **pre.tar**—A compressed tar file containing messages for installation as well as the license agreement.

  After you read the license agreement file, you can continue the installation by entering the command found at the end of that file:

  - If you are running a silent install (using install_base -autocfg), you can use the -command option with the command that can be found at the bottom of the license agreement file.
  - If you are using a response file (-autocfg file_name), you do not need to use the -command option.

  To get the license file name and location, run install_base -h. You also get the file name and location if you enter the wrong command.

You can find these files in the /Unix/Access-Control directory of the CA ControlMinder Endpoint Components for UNIX DVD.

Customize and Install Using Install_Base Script

You can install CA ControlMinder using the install_base script. This is an interactive script but you can also run it silently.

To install CA ControlMinder

1. If you already have CA ControlMinder installed and it is running, shut it down by logging in as an administrator and entering the following commands:
   `ACInstallDir/bin/secons -sk`
   `ACInstallDir/bin/SEOS_load -u`
2. Log in as *root*.

   To install CA ControlMinder, you need to have root permissions.
3. Mount the optical disc drive with the CA ControlMinder Endpoint Components for UNIX DVD.

4. Read the license agreement.

   To run the install_base script you need to accept the End User License Agreement. After you have read the license agreement, you can continue the installation by entering the command found at the end of that file. To get the license file name and location, run install_base -h.

5. (Optional) Customize the installation.

   Note: To decide which optional functionality you want to install, review the options of the install_base command (see page 243) in the *CA ControlMinder Implementation Guide*.

   Example: The following customized command shows how to initiate the install_base interactive script to install the client package to the /opt/CA/AC directory, and enable the Stack Overflow Protection option:
   `/dvdrom/Unix/Access-Control/install_base -client -stop -d /opt/CA/AC`

6. Install the client and server packages.

   Example: The following command initiates the install_base interactive script to install the client and server packages with all default CA ControlMinder features:
   `/dvdrom/Unix/Access-Control/install_base`

   The install_base script starts. During the installation you are prompted to answer questions related to installing the client and server packages of CA ControlMinder. As we did not specify a package to install in this example, the install_base command installs both client and server packages.

The CA ControlMinder installation is complete; however, it is not yet running.

Configure Post-Installation Settings

Once the installation is complete, you need to configure CA ControlMinder for your environment.

Follow these steps:

1. Append the *ACInstallDir*/bin directory to your PATH environment variable

   By default, the installation directory is /opt/CA/AccessControl/

2. Check the seos.ini (see page 259) file tokens to make sure that the settings meet your requirements.

   If necessary, modify the settings.

3. To give yourself access to the CA ControlMinder man pages, add the directory *ACInstallDir*/man to your MANPATH.

   For example, if you are using csh shell, for the duration of the current session, enter the command:

   ```
   setenv MANPATH $MANPATH:/opt/CA/AccessControl//man
   ```

   For future sessions add a similar line to your .login, .profile, or .cshrc file.

Start CA ControlMinder

Assuming you are working in an X Windows environment, invoke CA ControlMinder, verify that it is correctly installed on your system, and perform the following steps to initiate important protection:

1. Open two windows under root (superuser) authority.
2. In either window, enter the command:

   ```
   seload
   ```

   Wait while the seload command starts three CA ControlMinder daemons: Engine, Agent, and Watchdog.

3. After you have started the daemons, go to the other window and enter the command:

   ```
   secons -t+ -tv
   ```

   CA ControlMinder accumulates a file of messages reporting operating system events. The secons -tv command displays the messages on the screen as well.

4. In the first window, where you gave the seload command, enter the following command:

   ```
   who
   ```

   Watch the second window, where CA ControlMinder is writing the trace messages, to see whether CA ControlMinder intercepts the execution of the who command and reports on it. CA ControlMinder is correctly installed on your system if it reports interception of the who command.

5. If you want, enter more commands to see how CA ControlMinder reacts to them.

   The database does not yet contain any rules for blocking access attempts. Nevertheless, CA ControlMinder monitors the system so that you can see how the system behaves with CA ControlMinder installed and running, and which events CA ControlMinder intercepts.

6. Shut down the seosd daemon, by entering the following command:

   ```
   secons -s
   ```

   The following message displays on the screen:

   ```
   CA ControlMinder is now DOWN !
   ```

Allow Admin Access Using zlogin

The zlogin utility lets an administrator enter a zone. You should add a LOGINAPPL resource for this utility to control who can log in to any non-global zone.

CA ControlMinder comes with a predefined LOGINAPPL resource for protecting the zlogin utility.

Define Rules to Protect Resources

CA ControlMinder protects Solaris 10 zones in the same way it protects any computer. Each zone is protected in isolation from any other zones, with each rule you define in CA ControlMinder applying only to users working in that zone. Rules you apply in the global zone, even those that cover resources that are visible in a non-global zone, only apply to users who access them from the global zone.

Note: Make sure you protect non-global zone resources in both the non-global and the global zone as necessary.

Example: Global Zone Rules and Non-Global Zone Rules

In the following example, we define rules to protect a non-global zone (myZone1) file. All system files are always visible from the global zone.

The file we want to protect is /myZone1/root/bin/kill (path from global zone). To protect this file, we define the following CA ControlMinder rules:

- In the global zone:

```
nu admin_pers owner(nobody)
nr FILE /myZone1/root/bin/kill defaccess(none) owner(nobody)
authorize FILE /myZone1/root/bin/kill uid(admin_pers) access(all)
```

- In myZone1 (the non-global zone):

```
nu admin_pers owner(nobody)
nr FILE /bin/kill defaccess(none) owner(nobody)
authorize FILE /bin/kill uid(admin_pers) access(all)
```

Using these rules in both the global and non-global zones, we defined a user (admin_pers), defined our file as resource to be protected, and authorized our user to access the file. Without doing this in both zones, we would leave the resource exposed.

Uninstalling CA ControlMinder

Before you uninstall CA ControlMinder from Solaris zones, consider the following requirements.

- Uninstall from all non-global zones first before you remove CA ControlMinder from the global zone.
- If you installed using Solaris native packaging, use the native packaging command *pkgrm* to uninstall CA ControlMinder from all zones.

  Important! Do not use uninstall_AC script in this case.
- If you installed CA ControlMinder using the install_base script, you can uninstall it from individual nonglobal zones. However, the CA ControlMinder kernel can be uninstalled only from the global zone *and* only after CA ControlMinder has been stopped in all zones.

  Important! If you uninstall CA ControlMinder from the global zone using install_base before you uninstall from all zones, users may be locked out of the zones. We recommend you to use the Solaris native packaging to install and uninstall CA ControlMinder on Solaris zones.

Start CA ControlMinder Automatically

After you have tested CA ControlMinder and experimented with its features, you are ready to implement CA ControlMinder protection.

To arrange for the seosd daemon to start automatically upon boot, so that your resources are protected immediately, use the *ACInstallDir*/samples/system.init/*sub-dir* directory, where *sub-dir* is the directory for your operating system. Each sub-directory contains a README file with instructions for performing this task on the respective operating system.

Using the Service Management Facility to Manage CA ControlMinder

Valid on Solaris 10

You can use the Solaris Service Management Facility (SMF) utility to manage the CA ControlMinder daemons. Using the SMF utility, you control the authorization daemon (seosd), that manages the watchdog daemon (seoswd) and the seagent daemon. You use SMF-specific commands instead of the seload and secons commands.

Note: You can use the Service Management Facility utility to manage CA ControlMinder immediately after you install CA ControlMinder on Solaris 10.

Note: For more information about the seload and secons commands, refer to the *Reference Guide*.

The SMF commands have the following format:

```
#svcadm enable daemon

#svcadm disable daemon

#svcadm restart daemon

#svcadm refresh daemon

#svcs daemon

#svcs -l daemon

#svcadm clear daemon
```

Example: Start the seosd daemon

The following example shows how you start the seosd daemon:

```
#svcadm enable seosd
```

Note: This command is equivalent to using the seload command.

Example: Stop the seosd daemon

The following example shows you how to stop the seosd daemon:

```
#svcadm disable seosd
```

Note: This command is equivalent to using the secons -sk command.

Example: Restart the sesod daemon

The following example shows you how to restart the seosd daemon:

```
#svcadm restart seosd
```

Example: Reload the seosd configuration

This example shows you how to reload the seosd daemon configuration:

```
#svcadm refresh seosd
```

Note: This command is equivalent to using the secons -rl command.

Example: Display the status of the seosd daemon

The following example shows you how to list the status of the seosd daemon:

```
#svcs -l seosd
```

Example: Clear the maintenance state of the seosd daemon

The following example shows you how to clear the maintenance service state of the seosd daemon:

```
#svcadm clear seosd
```

Chapter 9: Installing and Customizing a UNAB Host

This section contains the following topics:

The UNAB Host

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, letting them log in to all platforms with the same user name and password.

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 in the same location that you also manage Windows users and groups.

Note: UNAB does not replace any of the existing PAM modules when installed. UNAB PAM is inserted into the existing PAM stack.

How to Implement UNAB

Before you start implementing UNAB, we recommend that you review the following steps to customize, install, and configure UNAB in your enterprise.

1. Verify that the UNIX computer name resolves (see page 300).
2. Check for system compliance (see page 296).

   The uxpreinstall utility verifies that the system is compatible with the UNAB requirements.

3. Customize the UNAB installation package (see page 301).

   Note: You do not need to customize the UNAB installation package for every UNIX host that you plan to install UNAB on. Customize the installation package for each operating system once and use it to install UNAB in your enterprise.

4. Configure UNAB to work with CA ControlMinder Enterprise Management (see page 306).

   Use the CA ControlMinder Enterprise Management server user interface to manage the UNAB endpoints.

5. Install the UNAB package on the UNIX hosts.

   Note: For more information about system requirements and operating system support, see the *Release Notes*.

6. Register the UNIX host with Active Directory (see page 342).

7. Start UNAB (see page 345).

   This step starts the UNAB daemon (uxauthd).

8. Create login authorization policies in CA ControlMinder Enterprise Management and assign the policy to the UNAB endpoints.

   A login policy defines which enterprise users and groups are permitted or denied access to the UNIX host.

   Note: For more information about login policies, see the *Enterprise Administration Guide.*

9. Activate UNAB on the UNIX host (see page 345).

   Activating UNAB lets enterprise users login to UNIX hosts.

10. (Optional) Implement UNAB in full integration mode (see page 346).

    In full integration mode, UNAB uses Active Directory to both authenticate and authorize users.

Before You Begin

Before you can install UNAB, make sure the preliminary requirements are met and that necessary information is available. We recommend that you review the steps that you need to complete to implement UNAB and perform the preliminary verifications.

Installation Modes

UNAB supports two installation modes:

- **Full integration**—In full integration mode the UNIX host relies on the Active Directory server for both authentication and authorization of users.
- **Partial integration**—In partial integration mode the UNIX host relies on the Active Directory server for authentication only, and uses a UNIX-based user store for authorization purposes. Use partial integration mode if you want to maintain the UNIX user store.

Active Directory Site Support

Before you install UNAB, you should understand how UNAB implements Active Directory site support. Active Directory site support helps to optimize network traffic, increase connection speed, and decrease response time.

When you register a UNAB endpoint with Active Directory, by default the uxconsole utility does the following:

- Discovers the Active Directory site that is closest to the physical location of the endpoint.
- Writes the name of the Active Directory site to the ad_site configuration setting in the ad section of the uxauth.ini file.

After registration, the UNAB endpoint communicates only with the domain controllers (DCs) in the discovered Active Directory site. If the endpoint cannot communicate with a DC in this site, the status of the UNAB endpoint changes to offline.

We recommend that you do not change the default behavior. However, when you customize the UNAB installation package, you can specify a list of DCs that the UNAB endpoint communicates with and a list of DCs that the UNAB endpoint ignores (the lookup_dc_list and the ignore_dc_list parameters, respectively). The DCs that you specify in these lists interact with Active Directory site support in the following ways:

- lookup_dc_list—The UNAB endpoint communicates with the DCs listed in this configuration setting, and does not communicate with the DCs discovered by Active Directory site support or DNS query.
- ignore_dc_list—The UNAB endpoint communicates with any DC discovered by Active Directory site support or DNS query that is *not* listed in this configuration setting.

Note: After installation, you can use the uxconsole -register utility to manually set the Active Directory site with which the UNAB endpoint communicates. For more information about the uxconsole utility, see the *Reference Guide*.

Installation Considerations for 64-bit Linux Hosts

Before you install UNAB on a Linux 64-bit computer, you must make sure that the following operating system 32-bit libraries are installed:

ld-linux.so.2, libICE.so.6, libcrypt.so.1, libdl.so.2, libgcc_s.so.1, libm.so.6, libnsl.so.1, libpam.so.0, libpthread.so.0, libresolv.so.2, libstdc++.so.5 (and libstdc++.so.6 on kernel v2.6), libaudit.so.0 (RHEL5 and OEL 5 only).

The following is a list of relevant RPM packages that are required:

- SLES 10: compat-libstdc++, glibc-32bit, libgcc, pam-32bit
- SLES 9: glibc-32bit, libgcc, libstdc++, pam-32bit
- RHEL 5 and OEL 5: audit-libs, compat-libstdc++, glibc, libgcc, pam
- RHEL 4 and OEL 4: compat-libstdc++, glibc, libgcc, pam
- RHEL 3: glibc, libgcc, libstdc++, pam

Before you install UNAB on a Linux s390x 64-bit computer, you must make sure that the following operating system 32-bit libraries are installed:

ld.so.1, libcrypt.so.1, libc.so.6, libdl.so.2, liblaus.so.1 (RHEL 3), libaudit.so.0 (RHEL 4, RHEL 5), libm.so.6, libnsl.so.1, libpam.so.0, libresolv.so.2

The following is a list of relevant RPM packages that are required:

- SLES 10: compat-libstdc++, glibc-32bit, pam-32bit
- SLES 9: glibc-32bit, libstdc++, pam-32bit
- RHEL 5: audit-libs, compat-libstdc++, glibc, pam
- RHEL 4: audit-libs, compat-libstdc++, glibc, pam
- RHEL 3: glibc, laus-libs, libstdc++, pam

SSH PAM Configurations

Before you install UNAB verify that the operating system supports the following SSH server and statements required to enable PAM configurations.

Note: The SSH configuration file location may vary according to specific customer installation.

SSH Server and PAM configuration for AIX

The SSH server configuration files is located in the following directory:

```
/etc/ssh/
```

To use OpenSSH 3.6 or lower, modify the following entry in /etc/ssh/sshd_config:

```
PAM_AthenticationViaKbdint yes
```

To use OpenSSH 3.7 and above modify the following entries in /etc/ssh/sshd_config:

```
ChallengeResponseAuthentication yes
```

```
UsePAM yes
```

Example: pam.conf entries for OpenSSH on AIX

The following example is a snippet from the pam.conf that contains the relevant entries to support OpenSSH server on AIX:

```
# Entries for OpenSSH
sshd auth optional  /usr/lib/security/pam_seos.o
sshd auth optional  /usr/lib/security/pam_aix
sshd auth sufficient      /usr/lib/security/pam_uxauth.o
sshd auth required  /usr/lib/security/pam_aix try_first_pass
sshd account sufficient    /usr/lib/security/pam_uxauth.o
sshd account requisite     /usr/lib/security/pam_uxauth.o
sshd account required      pam_aix
sshd password sufficient   /usr/lib/security/pam_seos.o
sshd password sufficient   /usr/lib/security/pam_uxauth.o
sshd password required     pam_aix
sshd session sufficient    /usr/lib/security/pam_uxauth.o
create_homedir
sshd session required      pam_aix
```

The Tectia SSH Server 4.x configurations file sshd2_config is located in the following file:directory

```
/etc/ssh2/
```

To use the Tectia Server 4.x modify the following entries in /etc/ssh2/ssh2d_config:

```
AllowedAuthentications ,publickey,keyboard-interactive,password
```

```
AuthKbdint.Optional pam
```

Example: pam.conf entries for Tectia SSH Server 4.x on AIX:

The following example is a snippet from the pam.conf that contains the relevant entries to support Tectia SSH server 4.x on AIX:

```
# Entries for tectia (sshd2)
sshd2 auth optional /usr/lib/security/pam_seos.o
sshd2 auth optional /usr/lib/security/pam_aix
sshd2 auth sufficient     /usr/lib/security/pam_uxauth.o
sshd2 auth required /usr/lib/security/pam_aix try_first_pass
sshd2 account sufficient   /usr/lib/security/pam_uxauth.o
sshd2 account requisite    /usr/lib/security/pam_uxauth.o
sshd2 account required     pam_aix
sshd2 password sufficient  /usr/lib/security/pam_seos.o
sshd2 password sufficient  /usr/lib/security/pam_uxauth.o
sshd2 password required    pam_aix
sshd2 session sufficient   /usr/lib/security/pam_uxauth.o
create_homedir
sshd2 session required     pam_aix
```

The Tectia SSH Server 6.x SSH configurations file sshd-server-config.xml is located in the following directory:

```
/etc/ssh2/
```

To use the Tectia SSH Server 6.x modify the following in the /etc/ssh2/ssh-server-config.xml file:

```
<settings windows-logon-type="interactive"
pam-account-checking-only="yes" />
….
<pluggable-authentication-modules service-name="ssh-server-g3"
pam-calls-with-commands="no" />
….
<authentication name="authentication" action="allow">
…
<auth-publickey />
<auth-password />
<auth-keyboard-interactive >
      <submethod-pam />
</auth-keyboard-interactive>
</authentication>
</authentication-methods>
```

Example: pam.conf entries for Tectia SSH Server 6.x on AIX:

The following example is a snippet from the pam.conf that contains the relevant entries to support Tectia SSH server 6.x on AIX:

```
# Entries for Tectia (Tectia 6.x)
ssh-server-g3 auth optional      /usr/lib/security/pam_seos.o
ssh-server-g3 auth optional      /usr/lib/security/pam_aix
ssh-server-g3 auth sufficient    /usr/lib/security/pam_uxauth.o
ssh-server-g3 auth required      /usr/lib/security/pam_aix
try_first_pass
ssh-server-g3 account sufficient /usr/lib/security/pam_uxauth.o
ssh-server-g3 account requisite  /usr/lib/security/pam_uxauth.o
ssh-server-g3 account required   pam_aix
ssh-server-g3 password sufficient/usr/lib/security/pam_seos.o
ssh-server-g3 password sufficient/usr/lib/security/pam_uxauth.o
ssh-server-g3 password required  pam_aix
ssh-server-g3 session sufficient /usr/lib/security/pam_uxauth.o
create_homedir
ssh-server-g3 session required   pam_aix
```

SSH Server and PAM configuration for Solaris

The SSH server configuration file sshd_config is located in on the following directories:

```
/usr/local/etc/ssh/
```

```
/etc/ssh
```

To use Open SSH 3.9 and above modify the following in the sshd_config file:

```
ChallengeResponseAuthentication yes
UsePAM yes
UsePrivilegeSeparation no
```

To use SunSSH 1.1 and SunSSH 1.1.3 modify the following in the sshd_config file:

```
PAMAuthenticationViaKBDInt yes
```

To use SunSSH 1.1.1 modify the following in the sshd_config file:

```
ChallengeResponseAuthentication yes
UsePAM yes
```

SSH Server and PAM configuration for Linux

The Tectia SSH Server 6.x configuration file ssh-server-config.xml is located in the following directory:

```
/etc/ssh2/
```

Modify the following entries in the configuration file:

```
<settings windows-logon-type="interactive"
pam-account-checking-only="yes" />
<auth-keyboard-interactive>
      <submethod-pam />
</auth-keyboard-interactive>
```

Modify the following in the /etc/pam.d/ssh-server-g3 file:

```
auth      include    system-auth
account   required   pam_nologin.so
account   include    system-auth
password  include    system-auth
session   optional   pam_keyinit.so force revoke
session   include    system-auth
session   required   pam_loginuid.so
```

Installation Considerations for Linux s390 Endpoints

If you want to use Message Queue functionality, to remotely manage UNAB on CA ControlMinder Linux s390 and use reporting capabilities on Linux IA64 you install J2SE version 5.0 or later on the endpoint.

Message Queue functionality lets you send report and audit data from CA ControlMinder endpoints to the Report Portal and CA User Activity Reporting Module, respectively. Remote management lets you use CA ControlMinder Enterprise Management to manage UNAB endpoints.

You can install J2SE before or after you install CA ControlMinder or UNAB on the endpoint. If you install J2SE after you install CA ControlMinder or UNAB, you must also configure the Java location on the endpoint.

How the Installation Interacts with Java

Valid on Linux s390, Linux s390x and Linux IA64

To use Message Queue functionality, to remotely manage UNAB Linux s390 endpoints and use reporting capabilities on Linux IA64 and Linux s390, you install a supported Java version on the endpoint.

When you install CA ControlMinder or UNAB on a Linux s390 or a Linux IA64 endpoint, the installation does the following:

1. Checks the following locations for a path to a valid Java environment, in order:
   a. The JAVA_HOME parameter in the installation input.

      Installation input includes the UNAB installation parameters file, the UNIX CA ControlMinder installation parameters file, customized packages for native installations, and user input from interactive CA ControlMinder installations.

   b. The JAVA_HOME environment variable.

   c. (Linux s390 and Linux s390x) The default installation path, /opt/ibm/java2-s390-50/jre

2. Sets the value of the java_home configuration setting in the global setting of the accommon.ini file to one of the following _values:
   - If the installation finds a path to a valid Java environment, it sets the value of the configuration setting to this path.
   - If the installation does not find a path to a valid Java environment, it sets the value of the configuration setting to *ACSharedDir*/JavaStubs.

     By default, *ACSharedDir* is /opt/CA/AccessControlShared.

Configure the Java Location on Linux s390 and Linux s390x Endpoints

Valid on Linux s390 and Linux s390x

To use Message Queue functionality and to remotely manage UNAB Linux s390 endpoints, you must install J2SE version 5.0 or later on the endpoint. If you install J2SE after you install CA ControlMinder or UNAB, you must perform additional configuration steps.

To configure the Java location on the Linux s390 and Linux s390x endpoint

1. Stop CA ControlMinder and UNAB if they are running.
2. Change the value of the java_home configuration setting in the global section of the accommon.ini file to the path of the Java installation.

   For example, java_home=/opt/ibm/java2-s390-50/jre
3. Start CA ControlMinder and UNAB.

   The Java location is configured.

Configure the Java Location on Linux IA64 Endpoint

Valid on Linux IA64

To use Message Queue functionality and reporting capabilities on CA ControlMinder Linux IA 64 endpoints, you install J2SE version 6.0 or later on the endpoint. If you install J2SE after you install CA ControlMinder you perform additional configuration steps.

To configure the Java location on the Linux IA64 endpoint

1. Stop CA ControlMinder if running.
2. Change the value of the java_home configuration setting in the global section of the accommon.ini file to the path of the Java installation.

   For example, java_home=/usr/share/java016.0/jre
3. Start CA ControlMinder.

   The Java location is configured.

Kerberos and SSO Considerations

You can install and register UNAB on a Kerberos enabled endpoint to leverage the Kerberos Single Sign On (SSO) service to authenticate once and log into multiple endpoints with the same user credentials. If not configured, you enable SSO functionality on the endpoint by installing and configuring Kerberized network services and applications.

Because configurations differ between systems, we strongly recommend that you do the following before you enable Kerberos and SSO on the endpoint:

- Read the system man pages and release specific options of native application service binaries, that you plan to use in SSO, especially the following:
  - sshd(1M)
  - telnetd
  - in.telnetd
  - inetd
  - pam.conf
  - inetd.sec
- Verify the PATH variable of the Kerberos supported versions of network applications. For example, on most Linux systems Kerberos tools are located under the /usr/Kerberos directory.
- Verify that the following Kerberos supported applications are configured as follow:
  - SSH—support credentials delegation, for example, set the GSSAPIDelegateCredentials token to yes
  - SSHD—support and enable GSSAPIAuthentication token
  - Telnet—on Solaris, PAM stack configured and Kerberos configuration and keytab files made available. Create a symbolic link or environment variable KRB5_CONFIG and KRB5_KTNAME to make the keytab files available
  - rlogin—install a Kerberos supported version of the application.

Note: For more system-specific Kerberos and SSO configuration, see your system documentation.

Example: Configure Kerberos on Solaris

The following example shows you the configuration required to configure Kerberos on Solaris. In this example, you install and configure Solaris packages to enable Kerberos.

Important! You may need to install and configure additional packages to configure the system you are using for Kerberos.

- Install the SUNWcry package to enable strong encryption
- On Solaris 10, SSH does not support GSSAPIDelegateCredentials
- Enable svc:/network/shell:kshell, svc:/network/login:klogin, svc:/network/telnet:default to use rsh, rlogin, and telnet services
- Modify the /etc/pam.conf file to handle Kerberos authentication.

The following is a snippet from the /etc/pam.conf file displays the added sections that enable Kerberos authentication for rlogin, rsh and telnet:

```
# Kerberized rlogin service
#
krlogin auth required           pam_unix_cred.so.1
krlogin auth required           pam_krb5.so.1
#
# rsh service (explicit because of pam_rhost_auth,
# and pam_unix_auth for meaningful pam_setcred)
#
rsh     auth sufficient         pam_rhosts_auth.so.1
rsh     auth required           pam_unix_cred.so.1
#
# Kerberized rsh service
#
krsh    auth required           pam_unix_cred.so.1
krsh    auth required           pam_krb5.so.1
#
# Kerberized telnet service
#
ktelnet auth required           pam_unix_cred.so.1
ktelnet auth required           pam_krb5.so.1
```

How UNAB Registration Works in a Kerberos Enabled Environment

When you register the host in Active Directory, UNAB creates user tickets in the same location as native Kerberos. The user can then transparently proceed to using kerberized application without having to acquire a Ticket Granting Ticket (TGT) manually.

The UNAB registration process in a Kerberos enabled host is as follows:

1. You run the uxconsole -register command and specify the -sso argument to register UNAB in Active Directory.

   The -sso argument forces the uxconsole to use the host Kerberos files and not the uxauth.ini file.

2. uxconsole verifies that UNAB can use the host Kerberos file for configuration purposes. *One* of the following occurs:

   a. uxconsole identifies that the file contains the required domain information to register UNAB.

   b. uxconsole identifies that the file does not contain the required information to register.

3. If the file does not contain the information, UNAB creates a backup of the original file and sets the kerberos_configuration token to internal.

   Note: If you remove UNAB from Active Directory using the uxconsole -deregister command, the Kerberos configuration file is not modified nor is the backup file removed.

4. If the file contains the required information, the uxconsole sets the kerberos_configuration token to standard.

5. The uxconsole continues with the registration process.

   Note: For more information about the uxconsole -register command and the seos.ini kerberos_configuration token, refer to the *Reference Guide*.

Important! If the Kerberos file on the host does not contain the required information to register UNAB, the registration fails.

Enable a UNAB Host for SSO

You can configure UNAB host for SSO to enable Active Directory users logged in to one UNAB host to log in to another UNAB host with their user names. In SSO enabled mode, UNAB maintains the keys it generated in the UNIX repository. Kerberos enabled applications use the keys to authenticate users when they log into another host.

Important! Verify that each host that you enable UNAB in SSO mode on is Kerberos enabled. Use the uxpreinstall utility to check for system compliance before you begin this procedure.

To enable a UNAB host for SSO

1. Log in to the UNIX host as root.
2. Register UNAB with Active Directory in SSO mode. Run the following command:

   ```
   ./uxconsole -register -d<active_directory_domain> -sso
   ```

   Note: You do not need to de-register UNAB before you register UNAB in SSO mode.
3. Activate UNAB to enable users to log in to the UNIX host. Run the following command:

   ```
   ./uxconsole -activate
   ```
4. Verify that the Kerberos mode is set to Standard using the -status -detail arguments. For example:

   ```
   ./uxconsole -status -detail | grep Kerberos

       Kerberos configuration - standard
   ```

   You have configured the UNAB host for SSO.

Check for System Compliance

The uxpreinstall utility verifies that a UNIX computer complies with UNAB system requirements. We strongly recommend that you use uxpreinstall to check for system compliance, and that you resolve any errors or conflicts that the utility identifies, before you start and activate UNAB. Resolving these errors helps prevent UNAB operational problems.

Important! The uxpreinstall utility informs you of real or potential problems but does not correct them. You cannot use the utility to configure the operating system or UNAB.

You can use uxpreinstall before or after you install UNAB. uxpreinstall does not modify the endpoint or the UNAB installation, but diagnoses possible problems and suggests solutions for the problems. Any problems that uxpreinstall identifies are problems on the endpoint, not problems with uxpreinstall.

Note: To run uxpreinstall before you install UNAB, copy the utility from another endpoint on which UNAB is installed. For more information about the uxpreinstall utility, see the *Reference Guide*.

To check for system compliance

1. Log in to the UNIX computer as a superuser.
2. Run uxpreinstall with a verbosity level of 0.

   uxpreinstall runs and displays a summary of the checks it performs and any errors or conflicts it identifies.
3. If uxpreinstall identifies any errors or conflicts, run uxpreinstall again with a verbosity level of 2 or higher.

   uxpreinstall displays more information about the errors and conflicts that it identifies.
4. Resolve the errors and conflicts.
5. Repeat Steps 2-4 until uxpreinstall does not identify any errors or conflicts.

   When the uxpreinstall output does not display any errors or conflicts, the computer complies with UNAB requirements. You can now start and activate UNAB.

Example: Run the uxpreinstall Utility

This example runs the uxpreinstall utility with the credentials of the administrator user against the Active Directory domain domain.com with a verbosity level of 3:

```
./uxpreinstall -a administrator -w admin -d domain.com -v 3
```

Troubleshoot Active Directory Issues using Uxconsole and Microsoft Utilities

During the implementation process, you can encounter various issues with Active Directory, such as registration and activation issues. The uxpreinstall utility can help you gather, identify and evaluate all the contributing factors. To enhance your ability to troubleshoot Active Directory, you can use the dcdiag (Domain Controller Diagnostics) and the netdiag (Network Diagnostics) utilities from Microsoft

Important! If you are using Windows Server 2003, you can find the dcdiag.exe and netdiag.exe utilities in the Support Tools software bundle. For more information, see Microsoft Knowledge Base articles: KB247811, KB265706, KB321708.

Use the following procedure to troubleshooting Active Directory:

1. Run uxpreinstall with a verbosity level of 0.

   uxpreinstall runs and displays a summary of the checks it performs and any errors or conflicts it identifies.

2. If uxpreinstall identifies any errors or conflicts, run uxpreinstall again with a verbosity level of 2 or higher.

   uxpreinstall displays more information about the errors and conflicts that it identifies.

   Note: We recommend that you be cautious when using –l (system logger check) and –k (Single Sign On readiness check) arguments, due to a large amount of output.

3. To log the uxpreinstall output, run uxpreinstall -f.
4. To log the Microsoft dcdiag utility output, run dcdiag /f.

   Note: The netdiag utility automatically creates the following log file: NetDiag.log.

5. Review the log files to failure, error messages; or warnings. If exist, run the uxpreinstall and the dcdiag utility with a higher verbosity level.
6. Review the log files again to locate actions that were not completed successfully and warning messages.

   Errors can be logged as warnings and not as error messages, due to user preferences.

7. Run the dcdiag /test:DNS /v /e to troubleshoot the domain controllers parameters.
8. Review the output, starting form the end of the log file.
9. Continue troubleshooting until you resolve all warning and error messages.

Example: Use dsquery to query users and groups

The following example shows you how to use the dsquery utility to query for users and groups:

```
dsquery user -name user1
dsquery group -name grp1
dsquery * "CN=Users,DC=example,DC=com" -scope base -attr *
```

Example: Use dnscmd utility to retrieve DNS settings

The following example shows you how to use the dnscmd to retrieve DNS settings:

```
dnscmd /enumzones
dnscmd /zoneprint <zonename>
```

Example: Use dsquery utility to discover Active Directory sites

The following example shows you how to use the dsquery utility to discover Active Directory sites:

```
dsquery subnet –name 192.168.*
dsquery site -o dn
dsquery subnet -o rdn -site <mysite>
nltest /DSGETSITECOV
```

Verify that the UNIX Computer Name Resolves Correctly

For UNAB to work, both the UNIX computer and the Active Directory computer must resolve the IP address of the UNIX computer to the same computer name, including the domain name.

To verify that the UNIX computer name resolves correctly, run the uxpreinstall utility.

Example: Verify that the Name of a UNIX Computer Resolves Correctly using uxpreinstall utility

This example shows you the result running the uxpreinstall with verbosity level 3 on a Linux for a computer named computer.caom on both a Windows, Active Directory server and UNIX computer:

```
Locating Active Directory services in domain <DOMAIN.COM>
Locating '_ldap._tcp.DOMAIN.COM.' records in DNS ...
computer.com:389 [100:0] (_ldap)
computer.com:389 [100:0] (_ldap)
Found LDAP services:
   computer:389
Performing name resolution on <computer.com>
Running command "host computer.com" ...
   DNS server reply:
      computer.com has address 192.168.1.1
Name <computer.com> was resolved to IP address <1192.168.1.1>
```

Example: Verify that the Name of a UNIX Computer Resolved Correctly using nslookup command

This example shows you the result of a forward nslookup resolution command on Linux for a computer named acctdept on both a Windows, Active Directory server and UNIX computer:

```
# nslookup acctdept
Server:         172.24.789.0
Address:        172.24.789.0#53

Name:   acctdept.parallel.com
Address: 172.24.123.110
```

UNAB Installation Parameters File—Customize UNAB Installation

The UNAB parameters file contains installation parameters that you can customize for your requirements.

This file has the following format:

AUDIT_BK

Specifies whether to keep time stamped backups of the audit file.

Note: Set the value to yes if you want to send audit data to the Distribution Server. If you set the value to yes, CA ControlMinder backs up the audit file when it reaches the size limit specified by the audit_size configuration settings and time stamps the file. This ensures that all audit data is available to the Report Agent.

Limits: yes, no

Default: no

COMPUTERS_CONTAINER

Defines the container name in the Active Directory under which the UNIX computer is registered.

Default: cn=Computers

DIST_SRV_HOST

Specifies the Distribution Server host name.

Limits: any valid host name.

Default: none

DIST_SRV_PORT

Specifies the Distribution Server port number.

Limits: SSL: 7243, TCP: 7222

Default: 7243

DIST_SRV_PROTOCOL

Specifies the Distribution Server communication protocol.

Limits: tcp, ssl

Default: ssl

ENABLE_ELM

Specifies whether the Report Agent sends endpoint audit data to the Distribution Server. This lets you integrate with CA User Activity Reporting Module.

Note: If you set the value to yes, set CA ControlMinder to keep audit backups (AUDIT_BK=yes).

Limits: yes, no

Default: no

GROUP_CONTAINER

Defines the name of the Active Directory container that holds the definitions of UNIX groups.

IGNORE_DC_LIST

Specifies which Active Directory Domain Controllers UNAB ignores when establishing LDAP connection.

Note: You can specify Domain Controllers from both the current and trusted domains.

Limits: none, comma separated list

Default: none

IGNORE_DOMAIN_LIST

Specifies which Active Directory domains UNAB ignores when querying for users and groups.

Limits: none, UNAB queries the current and all trusted domains; all, UNAB queries only the current domain; a comma separated list of domains to ignore

Default: none

IGNORE_USER_CONTAINER

Specifies the user containers to ignore when searching Active Directory.

Containers are defined by their distinguished names (DN) separated by semicolon. If the container DN does not contain domains names, it is applied to all queried domains.

Limits: list of container DN separated by semicolon, none

Default: none

IGNORE_GROUP_CONTAINER

Specifies the group containers to ignore when searching Active Directory.

Containers are defined by their distinguished names (DN) separated by semicolon. If the container DN does not contain domains names, it is applied to all queried domains.

Limits: list of container DN separated by semicolon, none

Default: none

INTEGRATION_MODE

Specifies the UNAB integration mode.

Limits: 1, partial integration; 2, full integration

Default: 2

JAVA_HOME

(Linux s390) Specifies the full pathname to the installed Java environment, depending on the Java version and operating system.

Specify this parameter only if the Java environment is not installed in the default location. If the Java environment is installed in the default location, the installation program sets the value of this parameter.

LANG

Specifies the installation language.

LIC_CMD

Specifies the license acceptance command.

LOCAL_POLICY

Specifies the login policy usage options.

Limits: yes, use UNAB policy and local login file, no, use UNAB login policy only.

Default: no

LOOKUP_DC_LIST

Specifies the Active Directory Domain Controllers (DCs) to establish LDAP connection with.

Note: You can specify DCs from both the current and trusted domains. If you specify the DCs to use, UNAB retrieves the list of DCs from Active Directory. If you do not specify the DCs to use, UNAB discovers the Active Directory site that is closest to the physical location of the endpoint and communicates with DCs in the discovered site.

Limits: none, comma separated list.

Default: none

NTP_SRV

Defines the name or IP address of the Network Time Protocol (NTP) server.

REPORT_SHARED_SECRET

Specify the shared secret that the Report Agent uses to authenticate against the Distribution Server.

Limits: Any valid string.

Default: none

Note: You must specify the same shared secret that you defined when you installed the Distribution Server.

REPORT_SRV_QNAME

Specifies the name of the queue that snapshots are sent to.

Limits: A string representing the queue name.

Default: queue/snapshots

REPORT_SRV_SCHEDULE

Defines when the Report Agent generates reports and sends them to the Distribution Server.

This token uses the following format: time@day[,day2] [...]

Default: 00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat

RENAME_KRB_TKT

Specifies whether to rename the Kerberos ticket that was generated during user login.

Note: Use this option to support SSO login if the user Kerberos ticket name consists of random strings.When enabled this token the script /etc/profile.d/uxauth_rename_krb_tkt.sh renames the user ticket and set the corresponding value of environment variable KRB5CCNAME.

Limits: yes, no

Default: no

SSO

Specifies whether UNAB supports Kerberos-based Single Sign On (SSO)

Limits: yes, no

Default: no

TIME_SYNCH

Specifies whether UNAB synchronizes system time with an NTP (Network Time Protocol) server.

Note: If you set this value to yes, you must specify a value for the NTP_SRV token. If you set this value to no, UNAB uses the UNIX mechanism for system time that is defined in /etc/ntp.conf.

Limits: yes, no

Default: no

USER CONTAINER

Defines the Active Directory container name holding the definitions of UNIX users.

UXACT_ADMINISTRATOR

Defines the user name of the Active Directory administrator.

UXACT_ADMIN_PASSWORD

Defines the account password of the Active Directory administrator.

UXACT_DOMAIN

Defines the domain that the UNIX computer is part of.

UXACT_RUN

Specifies whether to execute the uxconsole -register command during installation.

Limits: yes, no

Default: no

Note: The uxconsole -register command registers the UNIX computer in the Active Directory server under the Computers container.

UXACT_RUN_AGENT

Specifies whether to start UNAB daemon at the end of the installation process.

Limits: yes, no

Default:yes

UXACT_SERVER

Defines the name of the Active Directory server.

UXACT_VERB_LEVEL

Defines the verbosity level.

Limits: 0-7

Manage UNAB with CA ControlMinder Enterprise Management

You can use CA ControlMinder Enterprise Management to manage UNAB endpoints. This lets you view UNAB endpoints from the World View, create and assign login and configuration policies, and resolve conflicts that were discovered in the migration process. For CA ControlMinder Enterprise Management to manage UNAB endpoints, you register UNAB with CA ControlMinder Enterprise Management. Customize the UNAB installation package to modify the package parameters.

Note: Complete this procedure before you install UNAB.

To manage UNAB with CA ControlMinder Enterprise Management

1. Extract the installation parameters from the UNAB package into a temporary file.
2. Open the temporary file in a text editor.
3. Modify the following parameters for your enterprise:

   DISTRIBUTION_SRV_HOST

   Specifies the Distribution Server host name.

   Limits: any valid host name.

   Default: none

   DISTRIBUTION_SRV_PROTOCOL

   Specifies the Distribution Server communication protocol.

   Limits: tcp, ssl

   Default: ssl

   DISTRIBUTION_SRV_PORT

   Specifies the Distribution Server port number.

   Limits: ssl: 7243, tcp: 7222

   Default: 7243

4. Set the installation parameters in the customized package.

5. Install UNAB using the customized package.

   UNAB is installed with the customized settings.

6. Use the acuxchkey utility to set the Message Queue password you specified during the Enterprise Management Server installation to the UNAB host. For example:

   ```
   acuxchkey -t pwd "password"
   ```

   After the installation is complete and the Message Queue password set on the UNAB host, use CA ControlMinder Enterprise Management to manage UNAB endpoints.

   Note: For more information about the acuxcheky utility, refer to the *Reference Guide*.

Integration with CA ControlMinder

If you intend to install UNAB and CA ControlMinder on the same endpoint, you can leverage some UNAB capabilities to display UNAB specific information in CA ControlMinder. For example, you can display the enterprise user name instead of the UNIX account name in audit records. The seos.ini configuration file contains tokens that you enable when you want to integrate UNAB with CA ControlMinder

Important! Before you integrate UNAB with CA ControlMinder, verify that CA ControlMinder version r12.5 or later is installed on the endpoint.

The following tokens in the [seosd] section control the integration of UNAB with CA ControlMinder:

use_unab_db

Specifies that seosd uses the UNAB database to resolve user and groups names. This token enables CA ControlMinder to detect changes in UNAB, such as a new user login.

use_mapped_user_name

Specifies whether seosd uses the user enterprise name in audit records. When enabled, the seaudit utility displays the enterprise user name rather than the UNIX account name.

The following tokens in the [OS_User] section control the integration of UNAB with CA ControlMinder:

nonunix_unabgroup_enabled

Specifies whether CA ControlMinder supports non UNIX groups of users in the UNAB database. When enabled, CA ControlMinder supports users from non UNIX groups.

osuser_enabled

Specifies whether enterprise users and groups are enabled.

The following tokens in the [seos] section control the integration of UNAB with CA ControlMinder:

auth_login

Determines the login authority method. This token enables password checks to authenticate users, for example, sesudo, sesu, and sepass.

pam_enabled

Specifies whether the local host enables use of PAM for authentication and password changes in the LDAP database.

The following tokens in the [passwd] section control the integration of UNAB with CA ControlMinder:

nis_env

Specifies whether the local host is an NIS or NIS+ client.

change_pam

Specifies whether the local host uses PAM for password authentication and changes in the LDAP database. Use this token to enable sepass to work with external pam stores, for example UNAB.

The following tokens in the [pam_seos] section control the integration of UNAB with CA ControlMinder:

PamPassUserInfo

Specifies whether pam_seos sends user information to seosd.

pam_login_events_enabled

Specifies whether pam_seos sends login events to seosd.

pam_surrogate_events_enabled

Specifies whether pam_seos sends surrogate events to seosd.

Note: For more information about the seos.ini tokens, see the *Reference Guide*.

Integration with RSA SecurID

If your organization uses RSA SecurID to authenticate users, you can use the capabilities of RSA SecurID to authenticate users login to UNAB endpoints. You can install UNAB on a host that has an RSA SecurID client installed and manage user login policies in Active Directory.

If UNAB is running on a host that has RSA SecurID installed, UNAB does not authenticate users on login. UNAB detects that users authentication is done by a third-party program. UNAB is then able to manage users activities on the endpoint, for example, enforce local and enterprise security policies and generate audit messages.

How UNAB Integrates With the RSA SecurID

UNAB integrates with the RSA SecurID by leveraging PAM stack capabilities. PAM stack capabilities allow you to set which authentication program to use for users authentication during the login process and the order in which the authentication occurs.

The following process explains UNAB integration with RSA SecurID:

1. Install UNAB on an endpoint that has RSA SecurID client installed.
2. Configure the PAM stack in the order by which you want users authentication to occur. For example, you configure the PAM stack to call the RSA SecurID to authenticate the user passcode and PIN number and if unsuccessful, use UNAB to authenticate the user Active Directory credentials.
3. When a user attempts to log into the UNAB host the following occurs:

   Using RSA SecurID authentication and UNAB authentication:

   a. RSA SecurID prompts the user for a passcode and PIN number.

   b. The user enters the passcode and PIN number.

   c. The RSA SecurID attempts to authenticate the user passcode and PIN number. The following occurs:

      - The RSA SecurID validates the user passcode and PIN number and enables the user to login. The authentication process ends and this point and user account management process starts.
      - The RSA SecurId rejects the user passcode or PIN number.
      - UNAB prompts the user for a Active Directory user account or local account credentials.
      - UNAB attempts to authenticate the user credentials and if authenticated the authentication process ends and the user account management process starts.

Example: Using RSA SecurID authentication in Red Hat Advanced Server 5.3

The following snippet from the /etc/pam.d/system-auth file indicates that users authentication to the Red Hat Linux Advanced Server 5.3 is done by RSA SecurID only:

```
auth required pam_securid.so
```

Example: Using RSA SecurID, local UNIX and UNAB authentication in Red Hat Linux Advanced Server 5.3

The following snippet from the /etc/pam.d/system-auth file indicates that users authentication to the Red Hat Linux Advanced Server 5.3 is done by RSA SecurdID, local UNIX and UNAB:

```
auth sufficient   pam_securid.so
auth sufficient   pam_unix.so
auth sufficient   pam_uxauth.so
```

In this example the /etc/pam.d/system-auth file is configured to call the RSA SecurID (pam_securid.so) module to attempts and authenticate the user credentials. If unsuccessful, the local UNIX PAM module (pam_unix.so) attempts to authenticate the user credentials. If unsuccessful, the UNAB PAM stack module (pam_uxauth.so) attempts to authenticate the user credentials. In this example, when the UNAB PAM module attempts to authenticate the user credentials, UNAB does not prompt the user for a password. The local UNIX PAM module provides the UNAB PAM stack module with the password.

Note: The authentication process can end with either of the PAM stack modules.

Example: Using UNAB authentication and RSA SecurID authentication in Red Hat Advanced Server 5.3

The following snippet from the /etc/pam.d/system-auth file indicates that users authentication to the Red Hat Advanced Server 5.3 is done using UNAB authentication and RSA SecurID authentication:

```
auth optional     pam_unix.so
auth sufficient   pam_uxauth.so
auth sufficient   pam_securid.so
```

In this example the /etc/pam.d/system-auth file is configured to use the UNAB PAM stack (pam_uxauthd.so) to attempt and authenticate the user Active Directory credentials before using the RSA SecurID PAM stack (pam_securid.so) to authenticate the user passcode. The local UNIX PAM stack module (pam_unix.so) is set to optional. This indicates that the local UNIX PAM stack does not authenticate the user but rather prompts the user for password and forwards the password to the PAM stack.

Note: In this example the authentication process can end with either the RSA SecurID or UNAB modules successful authentication without using local UNIX authentication.

RPM Package Manager Installation

The RPM Package Manager (RPM) is a command-line utility that lets you build, install, query, verify, update, and delete individual software packages. It is intended for use on Linux platforms.

Note: For more information, see the RPM Package Manager website at http://www.rpm.org and the UNIX man pages for RPM.

You can use the RPM package CA ControlMinder provides for UNAB to manage your UNAB installation with all your other software installations performed using RPM.

Install UNAB RPM Packages

To log in to a UNIX computer using Active Directory user accounts, you need to install UNAB on each UNIX computer that you want to access. You use UNAB RPM packages to install UNAB on a Linux computer.

To install UNAB RPM packages

1. Log in to the Linux computer as root.
2. Copy the compressed tar file appropriate for the server platform from the /UNAB directory of the CA ControlMinder Endpoint Components for UNIX DVD to a temporary location on your file system.

   In the read/write location on the file system, the package can be customized as required. The compressed tar file contains the UNAB package and installation files.
3. Navigate to the temporary directory, uncompress, and extract the contents from the compressed tar file. For example, the following commands uncompress and extract the contents from a file named _LINUX_Ux_PKG_125.tar.Z:

   ```
   gunzip _LINUX_Ux_PKG_125.tar.Z
   tar xvf _LINUX_Ux_PKG_125.tar
   ```
4. Use the rpm command to install the ca-lic package. ca-lic is a CA Technologies license program that is a prerequisite for all other packages. For example:

   ```
   rpm -U ca-lic-0.0080-04.i386.rpm
   ```

   The ca-lic package installs.
5. Customize the UNAB package (see page 312).

   You must customize the package to specify that you accept the license agreement using a keyword that you can find inside the license agreement. You can also customize the package to specify custom installation settings.

6. Use the rpm command to install the UNAB package. For example:

   ```
   rpm -U uxauth-125-3.0.1517.i386.rpm
   ```

   The installation process begins.

   A message informs you that the installation process completed successfully.

   Note: The UNAB package also installs the CAWIN shared component.

7. Review the installation log file, uxauth_install.log, for information about the installation process.

   You can find the log file in the UNAB installation directory, which by default is at the following location:

   ```
   /opt/CA/uxauth
   ```

8. Verify that the installation completed successfully (see page 316).

Customize the UNAB RPM Package

Before you can install UNAB, you must customize the RPM package to specify that you accept the license agreement. You can also specify custom installation settings when you customize a package.

We recommend that you do not modify the package manually. Instead, use the customize_uxauth_rpm script as described. To build a custom UNAB rpm installation package, you must have the rpmbuild utility on your computer.

To customize the UNAB package

1. If you have not already done so, do the following:

   a. Copy the compressed tar file appropriate for the server platform from the /UNAB directory of the CA ControlMinder Endpoint Components for UNIX DVD to a temporary location on your file system.

      In the read/write location on the file system, the package can be customized as required.

   b. Navigate to the temporary directory, uncompress and extract the contents from the compressed tar file.

      The compressed tar file contains the UNAB installation files.

2. Enter the following command to extract the uxpreinstall utility from the installation package:

   ```
   customize_uxauth_rpm -e uxpreinstall -f tmp_params [-d pkg_location]
   pkg_filename
   ```

   Use the uxpreinstall utility to check for system compliance before you install UNAB.

3. (Optional) Enter the following command to set the language of the installation parameters file:

   `customize_uxauth_rpm -r -l lang [-d pkg_location] pkg_filename`

4. Enter the following command to display the license agreement:

   `customize_uxauth_rpm -a [-d pkg_location] pkg_filename`

5. Take note of the keyword that appears at the end of the license agreement inside square brackets.

   You specify this keyword in the next step.

6. Enter the following command:

   `customize_uxauth_rpm -w keyword [-d pkg_location] pkg_filename`

   This command specifies that you accept the license agreement.

7. Enter the following command to get the installation parameters file:

   `customize_uxauth_rpm -g -f tmp_params [-d pkg_location] pkg_filename`

8. Edit the installation parameters file to suit your installation requirements (see page 301).

   This file lets you set the installation defaults for the package.

9. Enter the following command:

   `customize_uxauth_rpm -s -f tmp_params [-d pkg_location] pkg_filename`

   This command sets the installation parameters in your customized package.

   You can now use the package to install UNAB with the customized defaults.

Example: Customize the UNAB RPM Package

The following examples show you how to customize a UNAB RPM package named uxauth-125-3.0.1517.i386.rpm that is located in the /unab_tmp directory.

- This example displays the license agreement and keyword:

  `./customize_uxauth_rpm -a /unab_tmp/uxauth-125-3.0.1517.i386.rpm`

- This example accepts the license agreement. The keyword in this example is agreement:

  `./customize_uxauth_rpm -w agreement /unab_tmp/uxauth-125-3.0.1517.i386.rpm`

- This example gets the installation parameters file and places it in the parameters.txt file in the same directory:

  ```
  ./customize_uxauth_rpm -g -f parameters.txt
  /unab_tmp/uxauth-125-3.0.1517.i386.rpm
  ```

- This example sets the installation parameters from the parameters in the parameters.txt file:

  ```
  ./customize_uxauth_rpm -s -f parameters.txt
  /unab_tmp/uxauth-125-3.0.1517.i386.rpm
  ```

customize_uxauth_rpm Command—Customize the UNAB RPM Package

The customize_uxauth_rpm command runs the UNAB RPM package customization script.

Note: To customize a package, the package must be in a read/write directory on your file system.

This command has the following format:

```
customize_uxauth_rpm -h [-l]
customize_uxauth_rpm -a [-d pkg_location] pkg_filename
customize_uxauth_rpm -w keyword [-d pkg_location] pkg_filename
customize_uxauth_rpm -r [-d pkg_location] [-l lang] pkg_filename
customize_uxauth_rpm -s -f tmp_params [-d pkg_location] pkg_filename
customize_uxauth_rpm -g [-f tmp_params] [-d pkg_location] pkg_filename
customize_uxauth_rpm -e uxpreinstall [-d pkgdir] [pgn_name]
customize_uxauth_rpm -t tmp_dir [-d pkg_location] pkg_filename
```

pkg_filename

Defines the file name of the UNAB package you want to customize.

Note: If you do not specify the -d option, you must define the full pathname of the package file.

-a

Displays the license agreement.

-e uxpreinstall

Specifies to extract the uxpreinstall utility from the installation package.

-w *keyword*

Defines the keyword that specifies that you accept the license agreement. You can find this keyword at the end of the license agreement (inside square brackets). To locate the license agreement file, use the -a option.

-d *pkg_location*

(Optional) Specifies the directory where you placed your package on the file system. If you do not specify a directory where the package is located, the script assumes the full pathname to the package file is included in *pkg_filename*.

-f *tmp_params*

Specifies the full path and name of the installation parameters file to create or retrieve information from.

Note: If you do not specify a file when using the -g option, the installation parameters are directed to the standard output (stdout).

-g

Gets the installation parameters file and places it in the file specified by the -f option.

-h

Displays command usage. When used in conjunction with the -l option, displays the language code for supported languages.

-l *lang*

Sets the language of the installation parameters file to *lang*. You can set the language only in conjunction with the -r option.

Note: For a list of supported language codes you can specify, run customize_uxauth_rpm -l -h. By default, the installation parameters file is in English.

-r

Resets the package to use default values as in the original package.

-s

Sets the specified package to use inputs from the customized installation parameters file specified by the -f option.

-t *tmp_dir*

Sets the temporary directory for installation operations.

Note: The default temporary directory is /tmp.

Verify That the Installation Completed Successfully

After you finish installing UNAB, you should verify that the installation completed successfully.

To verify that the installation completed successfully enter the following command:

`rpm -q unab_package_name`

unab_package_name

Defines the name of the UNAB native package.

If you successfully installed UNAB, a message informs you that the package is installed.

Example: Verify That the Installation Completed Successfully

The following example verifies that the installation completed successfully for a UNAB native package named uxauth:

```
rpm -q uxauth
```

Upgrade the UNAB RPM Package

If an existing version of UNAB is installed and you want to install a new version, you can upgrade the existing version of UNAB without removing the installed version. You use UNAB RPM packages to upgrade UNAB on a Linux computer.

Note: You do not need to manually upgrade ca-lic.

To upgrade the UNAB RPM package

1. Log in to the Linux computer as root.
2. Copy the compressed tar file appropriate for the server platform from the /UNAB directory of the CA ControlMinder Endpoint Components for UNIX DVD to a temporary location on your file system.

   The compressed tar file contains the installation and upgrade files.

3. Navigate to the temporary directory, uncompress and extract the contents from the compressed file. For example, the following commands uncompress a file named _LINUX_Ux_PKG_125.tar.Z:

   ```
   unzip _LINUX_Ux_PKG_125.tar.Z
   tar xvf _LINUX_Ux_PKG_125.tar
   ```

   The compressed package contains the UNAB installation and upgrade files.

4. Use the rpm command to upgrade UNAB. For example:

   ```
   rpm -U uxauth-125-3.0.1517.i386.rpm --verbose
   ```

   The upgrade process begins.

   A message informs you that the upgrade process completed successfully.

Uninstall the UNAB RPM Package

To uninstall UNAB you need to remove the RPM package from the UNIX computer where you installed it.

To uninstall UNAB, log in as root and enter the following command:

`rpm -e` *`unab_package_name`*

unab_package_name

Defines the name of the UNAB native package.

The uninstall process begins.

A message informs you that the process completed successfully.

Solaris Native Packaging Installation

Solaris native packaging is provided as command-line utilities that let you create, install, remove, and report on individual software packages.

Note: For more information about Solaris native packaging, see the Sun Microsystems website and the man pages for pkgadd, pkgrm, pkginfo, and pkgchk.

Important! To uninstall UNAB after a package installation, you must use the *pkgrm* command.

Customize the UNAB Solaris Native Packages

Before you install UNAB using Solaris native packaging customize the installation package and accept the license agreement. You can also specify custom installation settings when you customize a package.

Follow the steps in this procedure to customize any of the UNAB packages. We recommend that you do not modify the packages manually. Instead, use the customize_uxauth_pkg script as described.

To customize the Solaris native packages

1. Extract the package you want to customize from the /UNAB directory of the CA ControlMinder Endpoint Components for UNIX DVD to a temporary location on your file system.

   In the read/write location on the file system, the package can be customized as required.

   Important! When you extract the package, you must verify that file attributes for the entire directory structure of the package are preserved or the Solaris native packaging tools will consider the package corrupt.

2. (Optional) Copy the customize_uxauth_pkg script file and the pre.tar file to a temporary location on your file system.

   Place the pre.tar file in the same directory as the script file to receive script messages in all languages. The pre.tar file is a compressed tar file containing installation messages and the UNAB license agreement.

   Note: You can find the customize_uxauth_pkg script file and the pre.tar file in the same location where you extracted the package to.

3. Enter the following command to extract the uxpreinstall utility from the installation package:

   `customize_uxauth_pkg -e uxpreinstall -f tmp_params [-d pkg_location] [pkg_name]`

   Use the uxpreinstall to check for system compliance before you install UNAB.

4. (Optional) Enter the following command:

   `customize_uxauth_pkg -r -l lang [-d pkg_location] [pkg_name]`

   The language of the installation parameters file is set.

5. Enter the following command:

   `customize_uxauth_pkg -a [-d pkg_location] pkg_name`

   This command displays the license agreement.

6. Take note of the keyword that appears at the end of the license agreement inside square brackets.

   You specify this keyword in the next step.

7. Enter the following command:

   `customize_uxauth_pkg -w keyword [-d pkg_location] [pkg_name]`

   This command specifies that you accept the license agreement.

8. (Optional) Enter the following command:

   `customize_uxauth_pkg -i install_loc [-d pkg_location] [pkg_name]`

   This command changes the installation directory.

9. Enter the following command to get the installation parameters file:

   `customize_uxauth_pkg -g -f tmp_params [-d pkg_location] [pkg_name]`

10. Edit the installation parameters file to suit your installation requirements. (see page 301)

    This file lets you set the installation defaults for the package.

11. Enter the following command to set the installation parameters in your customized package:

    `customize_uxauth_pkg -s -f tmp_params [-d pkg_location] [pkg_name]`

    You can now use the package to install UNAB with the customized defaults.

customize_uxauth_pkg Command—Customize Solaris Native Package

The customize_uxauth_pkg command runs the UNAB Solaris native package customization script.

You should consider the following when using this command:

- The script works on any of the available UNAB Solaris native packages.
- To customize a package, the package must be in a read/write directory on your file system.
- For localized script messages, you need to have pre.tar file in the same directory as the script file.

This command has the following format:

```
customize_uxauth_pkg -h [-l]
customize_uxauth_pkg -a [-d pkg_location] [pkg_name]
customize_uxauth_pkg -w command [-d pkg_location] [pkg_name]
customize_uxauth_pkg -r [-d pkg_location] [-l lang] [pkg_name]
customize_uxauth_pkg -i install_loc [-d pkg_location] [pkg_name]
customize_uxauth_pkg -s -f tmp_params [-d pkg_location] [pkg_name]
customize_uxauth_pkg -g [-f tmp_params] [-d pkg_location] [pkg_name]
customize_uxauth_pkg -e uxpreinstall [-d pkg_location] [pkg_name]
customize_uxauth_pkg -t tmp_dir [-d pkg_location] [pkg_name]
```

pkg_name

(Optional) The name of the UNAB package you want to customize. If you do not specify a package, the script defaults to the main UNAB package (uxauth).

-a

Displays the license agreement.

-e uxpreinstall

Specifies to extract the uxpreinstall utility from the installation package.

-w *keyword*

Defines the keyword that specifies that you accept the license agreement. You can find this keyword at the end of the license agreement (inside square brackets). To locate the license agreement file, use the -a option.

-l *lang*

Sets the language of the installation parameters file to *lang*. You can set the language only in conjunction with the -r option.

Note: For a list of supported language codes you can specify, run -l with the -h option. By default, the installation parameters file is in English.

-d *pkg_location*

(Optional) Specifies the directory where you placed your package on the file system. If you do not specify a directory where the package is located, the script defaults to /var/spool/pkg.

-f *tmp_params*

Specifies the full path and name of the installation parameters file to create or retrieve information from.

Note: If you do not specify a file when using the -g option, the installation parameters are directed to the standard output (stdout).

-g

Gets the installation parameters file and places it in the file specified by the -f option.

-h

Displays command usage. When used in conjunction with the -l option, displays the language code for supported languages.

-i *install_loc*

Sets the installation directory for the package to *install_loc/*uxauth.

-r

Resets the package to use default values as in the original package.

-s

Sets the specified package to use inputs from the customized installation parameters file specified by the -f option.

-t *tmp_dir*

Sets the temporary directory for installation operations.

Note: The default temporary directory is /tmp.

Install UNAB Solaris Native Packages

The UNAB Solaris native packages let you install UNAB on Solaris easily.

Note: The following procedure installs UNAB with the default settings. You can customize the UNAB package before installing it.

To install UNAB Solaris native packages

1. (Optional) Configure Solaris native installation defaults:
   a. Enter the following command:

      ```
      convert_uxauth_pkg -p
      ```

      The installation administration file is copied to the current location with the name *myadmin*.

      You can edit the installation administration file to change pkgadd installation defaults. You can then use the modified file for specific installations, such as UNAB, using the pkgadd -a option. However, this file is not specific to UNAB.

   b. Edit the installation administration file (myadmin) as desired, then save the file.

      You can now use the modified installation settings for the UNAB native installation without affecting other installations.

   Note: Solaris native packaging may require user interaction by default. For more information about the installation administration file and how to use it, see the Solaris man page for pkgadd(1M) and admin(4).

2. Enter the following command:

   pkgadd [-a *dir*/myadmin] -d *pkg_location* uxauth

   -a *dir*/myadmin

   Defines the location of the myadmin installation administration file you created in step 1.

   If you do not specify this option, pkgadd uses the default installation administration file.

   pkg_location

   Defines the directory where the UNAB package (uxauth) is located.

   Important! The package must be located in a public location (that is, read access for group and world). For example, /var/spool/pkg

   Note: You can find the Solaris native packages in the UNAB directory of the CA ControlMinder Endpoint Components for UNIX DVD.

   UNAB is now fully installed but not started.

Install UNAB Solaris Native Packages on Selected Zones

You can use Solaris native packaging to install UNAB to selected zones. However, you must also install UNAB on the global zone.

Note: We recommend that you use Solaris native packaging to install UNAB to *all* zones.

To install UNAB to selected zones

Important! Make sure you use the same UNAB version in all zones.

1. From the global zone, enter the following the command.

   `pkgadd -G -d pkg_location uxauth`

   pkg_location

   Defines the directory where the UNAB package (uxauth) is located.

   Important! The package must be located in a public location (that is, read access for group and world). For example, /var/spool/pkg

   This command installs UNAB only to the global zone.

2. On each of the non-global zones where you want to install UNAB, do the following:

   a. Copy the uxauth package to a temporary location on the non-global zone.

   b. Enter the following command from the non-global zone:

      `pkgadd -G -d pkg_location uxauth`

      This command installs UNAB (using the package you copied in step number 1) on the non-global zone you are working from.

   You can now start UNAB on the internal zone.

Note: You must uninstall from all non-global zones before you remove UNAB from the global zone.

Upgrade UNAB on Solaris

The UNAB Solaris native packages let you upgrade and existing version UNAB on Solaris to a newer version of UNAB.

To upgrade UNAB on Solaris

1. Stop all UNAB daemons.
2. (Optional) Configure Solaris native installation defaults:
   a. Enter the following command:

      `convert_uxauth_pkg -p`

      The installation administration file is copied to the current location with the name *myadmin*.

      You can edit the installation administration file to change pkgadd installation defaults. You can then use the modified file for specific installations, such as UNAB, using the pkgadd -a option. However, this file is not specific to UNAB.

   b. Edit the installation administration file (myadmin) as desired, then save the file.

      You can now use the modified installation settings for the UNAB native installation without affecting other installations.

   Note: Solaris native packaging may require user interaction by default. For more information about the installation administration file and how to use it, see the Solaris man page for pkgadd(1M) and admin(4).
3. Enter the following command:

   `pkgadd [-a dir/myadmin] –v -d . UNAB`

   -a *dir*/myadmin

   Defines the location of the myadmin installation administration file you created in step 1.

   If you do not specify this option, pkgadd uses the default installation administration file.

   UNAB

   Defines the name of the UNAB native package.

   Note: If you installed the previous version of UNAB in a directory that is not the default directory, specify the full path to the UNAB directory by running the following command:

   `./customize_eac_pkg -i previous-path -d ./ CAeAC`

   -i *Previous-path*

   Defines the full path to the existing UNAB directory.

   Note: Verify that the full path name does not contain a slash character (/) at the end.

The new version of UNAB is now installed but not started.

Uninstall UNAB Solaris Native Package

To uninstall a UNAB Solaris package installation, uninstall the UNAB package.

To uninstall the main UNAB package, enter the following command:

pkgrm *unab_package_name*

unab_package_name

Defines the name of the UNAB native package.

UNAB is removed from the computer.

HP-UX Native Package Installation

HP-UX native packaging is provided as a set of GUI and command-line utilities that let you create, install, remove, and report on individual software packages. HP-UX native packaging also lets you install software packages on remote computers.

Note: For more information about the HP-UX native packaging, Software Distributor-UX (SD-UX), see the HP website at http://www.hp.com. You can also refer to the man pages for swreg, swinstall, swpackage, and swverify.

Important! To uninstall UNAB after a package installation, you must use the *swremove* command.

Customize the UNAB SD-UX Format Packages

Before you can install UNAB using a native package, you must customize the UNAB package and accept the license agreement. You can also specify custom installation settings when you customize a package.

We recommend that you do not modify the package manually. Instead, use the script as described in the following procedure to customize the UNAB package.

You can find the Software Distributor-UX (SD-UX) format package for each of the supported HP-UX operating systems in the UNAB directory of the CA ControlMinder Endpoint Components for UNIX DVD.

To customize the SD-UX format packages

1. Extract the package you want to customize to a temporary location on your file system.

   In the read/write location on the file system, the package can be customized as required.

   Important! When you extract the package, you must make sure that file attributes for the entire directory structure of the package are preserved or HP-UX native packaging tools will consider the package corrupt.

2. Copy the customize_uxauth_depot script file and the pre.tar file to a temporary location on your file system.

   The pre.tar file is compressed tar file containing installation messages and the UNAB license agreement.

   Note: You can find the customize_uxauth_depot script file and the pre.tar file in the following directory:

   `/uxauth/FILESET/opt/CA/uxauth/lbin`

3. Enter the following command to extract the uxpreinstall utility from the installation package

   `customize_exauth_depot -e uxpreinstall -f tmp_params [-d pkg_location] [pkg_name]`

   Use the uxpreinstall to check for system compliance before you install UNAB

4. Enter the following command:

   `customize_uxauth_depot -a [-d pkg_location] [pkg_name]`

   This command displays the license agreement.

5. Take note of the keyword that appears at the end of the license agreement inside square brackets.

   You specify this keyword in the next step.

6. Enter the following command:

   `customize_uxauth_depot -w keyword [-d pkg_location] [pkg_name]`

   This command specifies that you accept the license agreement

7. (Optional) Enter the following command:

   `customize_uxauth_depot -r -l lang [-d pkg_location] [pkg_name]`

   This command sets the language of the installation parameters file

8. (Optional) Enter the following command:

   `customize_uxauth_depot -i install_loc [-d pkg_location] [pkg_name]`

   This command changes the installation directory.

9. (Optional) Enter the following command to get the installation parameters file:

   `customize_uxauth_depot -g -f tmp_params [-d pkg_location] [pkg_name]`

10. (Optional) Edit the installation parameters file to suit your installation requirements (see page 301).

    This file lets you set the installation defaults for the package.

11. (Optional) Enter the following command:

    `customize_uxauth_depot -s -f tmp_params [-d pkg_location] [pkg_name]`

    This command sets the installation parameters in your customized package

    You can now use the package to install UNAB with the customized defaults.

Example: Specify That You Accept the License Agreement

To accept the license agreement when installing a native package, you customize the package. The following example shows you how you do customize the x86 UNAB SD-UX package that you can find on the directory where you extracted the package files into in order to accept the license agreement:

```
cp /mnt/AC_DVD/UNAB/_HPUX11_Ux_PKG_1*.tar.Z /tmp
cd /tmp
zcat _HPUX11_Ux_PKG_1*.tar.Z | tar -xvf -
/uxauth/FILESET/opt/CA/uxauth/lbin/customize_eac_depot -w keyword -d /tmp uxauth
```

You can now use the customized package in the /tmp directory to install UNAB.

More information:

customize_eac_depot Command—Customize an SD-UX Format Package (see page 229)

customize_uxauth_depot Command—Customize an SD-UX Format Package

The customize_uxauth_depot command runs the UNAB native package customization script for SD-UX format packages.

You should consider the following when using this command:

- The script works on any of the available UNAB HP-UX native packages.
- To customize a package, the package must be in a read/write directory on your file system.
- For localized script messages, you need to have pre.tar file in the same directory as the script file.

This command has the following format:

```
customize_uxauth_depot -h [-l]
customize_uxauth_depot -a [-d pkg_location] [pkg_name]
customize_uxauth_depot -w keyword [-d pkg_location] [pkg_name]
customize_uxauth_depot -r [-l lang] [-d pkg_location] [pkg_name]
customize_uxauth_depot -i install_loc [-d pkg_location] [pkg_name]
customize_uxauth_depot -s -f tmp_params [-d pkg_location] [pkg_name]
customize_uxauth_depot -e uxpreinstall [-d pkg_location] [pkg_name]
customize_uxauth_depot -g [-f tmp_params] [-d pkg_location] [pkg_name]
```

pkg_name

(Optional) The name of the UNAB package you want to customize. If you do not specify a package, the script defaults to the main UNAB package (uxauth).

-a

Displays the license agreement.

-e uxpreinstall

Specifies to extract the uxpreinstall utility from the installation package.

-d *pkg_location*

(Optional) Specifies the directory where you placed your package on the file system. If you do not specify a directory where the package is located, the script defaults to /var/spool/pkg.

-f *tmp_params*

Specifies the full path and name of the installation parameters file to create or retrieve information from.

Note: If you do not specify a file when using the -g option, the installation parameters are directed to the standard output (stdout).

-g

Gets the installation parameters file and places it in the file specified by the -f option.

-h

Displays command usage. When used in conjunction with the -l option, displays the language code for supported languages.

-i *install_loc*

Sets the installation directory for the package to *install_loc*/uxauth.

-l *lang*

Sets the language of the installation parameters file to *lang*. You can set the language only in conjunction with the -r option.

Note: For a list of supported language codes you can specify, run -l with the -h option. By default, the installation parameters file is in English.

-r

Resets the package to use default values as in the original package.

-s

Sets the specified package to use inputs from the customized installation parameters file specified by the -f option.

-w *keyword*

Defines the keyword that specifies that you accept the license agreement. You can find this keyword at the end of the license agreement (inside square brackets). To locate the license agreement file, use the -a option.

Install UNAB HP-UX Native Packages

To manage the UNAB installation with all your other software installations, install the customized UNAB SD-UX format package. The UNAB SD-UX format packages let you install UNAB on HP-UX easily.

Important! You must customize the package to specify that you accept the license agreement using a keyword you can find inside the license agreement.

To install the UNAB HP-UX native packages

1. Log in as root.

   To register and install HP-UX native packages you need permissions associated with the root account.

2. Customize the UNAB package (see page 325).

   You must customize the package to specify that you accept the license agreement using a keyword that you can find inside the license agreement. You can also customize the package to specify custom installation settings.

3. Register the customized package with SD-UX using the following command:

   `swreg -l depot` *`pkg_location`*

   pkg_location

   Defines the directory where the UNAB package is located.

4. Install the UNAB package using the following command:

   `swinstall -s` *`pkg_location`* `uxauth`

   SD-UX starts installing the package from the *pkg_location* directory.

   UNAB is now fully installed but not started.

More information:

Additional Considerations for Native Installations (see page 198)
Customize the SD-UX Format Packages (see page 226)

Uninstall HP-UX Packages

To uninstall a UNAB HP-UX package installation, you need to uninstall the UNAB packages in the reverse order of their installation.

To uninstall CA ControlMinder packages uninstall the main UNAB package:

`swremove` *`unab_package_name`*

unab_package_name

Defines the name of the UNAB native package.

AIX Native Package Installation

AIX native packaging is provided as a set of GUI and command-line utilities that let you manage individual software packages.

Note: While some AIX versions support several package formats (installp, SysV, RPM), UNAB provides the AIX native package format (installp) only.

Important!

- To uninstall UNAB after a package installation, you must use the *installp* command.
- UNAB uses the Pluggable Authentication Mode (PAM) and not the AIX Loadable Authentication Module (LAM) to authenticate users. Configure the AIX system to enable PAM before installing UNAB.
- To prevent application failure, verify that the user IDs and primary group IDs do not originate from different user stores. For example, if the user ID originates from /etc/passwd and the primary group originates from Active Directory.

Pluggable Authentication Module (PAM) on AIX

By default, AIX uses the Loadable Authentication Module (LAM) for identification and authentication purposes. To enable UNAB to authenticate users accessing the system, you must configure AIX to use PAM. Configure the AIX system to use PAM before you customize and install UNAB.

Note: You can enable PAM on AIX versions 5.3 and above.

Example: Configuring AIX to use PAM

The following example shows you how to configure AIX version 5.3 and above to use PAM, used by UNAB for authentication purposes.

1. Create a PAM configuration file.

   AIX does not provide a default /etc/pam.conf file.

2. Open the pam.conf file and include the basic module stack, then save the file. For example:

```
#
# Authentication
#
ftp     auth    required        /usr/lib/security/pam_aix
imap    auth    required        /usr/lib/security/pam_aix
login   auth    required        /usr/lib/security/pam_aix
rexec   auth    required        /usr/lib/security/pam_aix
rlogin  auth    required        /usr/lib/security/pam_aix
snapp   auth    required        /usr/lib/security/pam_aix
su      auth    required        /usr/lib/security/pam_aix
telnet  auth    required        /usr/lib/security/pam_aix
OTHER   auth    required        /usr/lib/security/pam_aix
#
# Account Management
#
ftp     account required        /usr/lib/security/pam_aix
login   account required        /usr/lib/security/pam_aix
rexec   account required        /usr/lib/security/pam_aix
rlogin  account required        /usr/lib/security/pam_aix
rsh     account required        /usr/lib/security/pam_aix
su      account required        /usr/lib/security/pam_aix
telnet  account required        /usr/lib/security/pam_aix
OTHER   account required        /usr/lib/security/pam_aix
#
# Password Management
#
login   password  required      /usr/lib/security/pam_aix
rlogin  password  required      /usr/lib/security/pam_aix
su      password  required      /usr/lib/security/pam_aix
telnet  password  required      /usr/lib/security/pam_aix
OTHER   password  required      /usr/lib/security/pam_aix
#
# Session Management
#
ftp     session required        /usr/lib/security/pam_aix
imap    session required        /usr/lib/security/pam_aix
login   session required        /usr/lib/security/pam_aix
rexec   session required        /usr/lib/security/pam_aix
rlogin  session required        /usr/lib/security/pam_aix
```

```
rsh     session required        /usr/lib/security/pam_aix
snapp   session required        /usr/lib/security/pam_aix
su      session required        /usr/lib/security/pam_aix
telnet  session required        /usr/lib/security/pam_aix
OTHER   session required        /usr/lib/security/pam_aix
```

3. Navigate to /lib/security and open the methods.cfg file for editing.
4. Enable PAM authentication by adding the following lines, then save the file:

```
PAM:
        program = /usr/lib/security/PAM
PAMfiles:
        options = auth=PAM,db=BUILTIN
```

5. Navigate to /etc/security and open the login.cfg file for editing.
6. Configure the authentication type to PAM, then save the file: auth_type = PAM_AUTH

   For example:

```
chsec -f /etc/security/login.cfg -s usw -a auth_type=PAM_AUTH
```

7. Navigate to /etc/ssh/ and open the sshd_config file for editing.
8. Enable SSH PAM authentication by adding the following parameters, then save the file:

```
UsePAM yes
```

   Note: Verify that you use a PAM supported version of OpenSSH (version 3.9p1 and above). To verify the version use the following command:

```
lslpp -i openssh.base.server
```

9. Navigate to /etc and open the pam.conf file for editing.
10. Add SSH PAM authentication by adding the following lines, then save the file:

```
sshd    auth            required        /usr/lib/security/pam_aix
OTHER   auth            required        /usr/lib/security/pam_aix
sshd    account         required        /usr/lib/security/pam_aix
OTHER   account         required        /usr/lib/security/pam_aix
sshd    password        required        /usr/lib/security/pam_aix
OTHER   password        required        /usr/lib/security/pam_aix
sshd    session         required        /usr/lib/security/pam_aix
OTHER   session         required        /usr/lib/security/pam_aix
```

11. Restart the computer.

    AIX is configured to use PAM for authentication purposes. You can now customize the AIX native package and install UNAB.

Customize the bff Native Package Files

Before you install UNAB using a native package, customize the UNAB package to specify that you accept the license agreement. You can also specify custom installation settings when you customize a package.

We recommend that you do not modify the package manually. Instead, use the script as described in the following procedure to customize the UNAB package.

You can find the installp format native packaging (bff files) for each of the supported AIX operating systems in the UNAB directory of the CA ControlMinder Endpoint Components for UNIX DVD.

Important! Before you install UNAB, verify that you have configured AIX to use PAM for authentication purposes.

To customize the bff native package files

1. Extract the package you want to customize to a temporary location on your file system.

   In the read/write location on the file system, the package (a bff file) can be customized as required.

   Important! This location needs to have disk space that is at least twice the size of the package, so that it can hold temporary repackaging files.

2. Copy the customize_uxauth_bff script file and the pre.tar file to a temporary location on your file system.

   The pre.tar file is compressed tar file containing installation messages and the UNAB license agreement.

   Note: You can find the customize_uxauth_bff script file and the pre.tar file in the same location where the native packages are.

3. Enter the following command to extract the uxpreinstall utility from the installation package

   `customize_uxauth_bff -e uxpreinstall -f tmp_params [-d pkg_location] pkg_name`

   Use the uxpreinstall to check for system compliance before you install UNAB

4. Enter the following command:

   `customize_uxauth_bff -a [-d pkg_location] pkg_name`

   This command displays the license agreement.

5. Take note of the keyword that appears at the end of the license agreement inside square brackets.

   You specify this keyword in the next step.

6. Enter the following command:

   `customize_uxauth_bff -w keyword [-d pkg_location] pkg_name`

   This command specifies that you accept the license agreement

7. (Optional) Enter the following command

   `customize_uxauth_bff -r -l lang [-d pkg_location] pkg_name`

   This command sets the language of the installation parameters file:

8. (Optional) Enter the following command:

   `customize_uxauth_bff -i install_loc [-d pkg_location] pkg_name`

   This command changes the installation directory.

9. Enter the following command to get the installation parameters file:

   `customize_uxauth_bff -g -f tmp_params [-d pkg_location] pkg_name`

10. (Optional) Edit the installation parameters file to suit your installation requirements (see page 301).

    This file lets you set the installation defaults for the package.

11. (Optional) Enter the following command to set the installation parameters in your customized package:

    `customize_uxauth_bff -s -f tmp_params [-d pkg_location] pkg_name`

    You can now use the package to install UNAB with the customized defaults.

customize_uxauth_bff Command—Customize a bff Native Package File (UNAB)

The customize_uxauth_bff command runs the <uxauth> native package customization script for bff native package files.

The script works on any of the available <uxauth> native packages for AIX. To customize a package, the package must be in a read/write directory on your file system.

Important! The location where you extract the package to should have enough space to contain at least twice the size of the package for intermediate repackaging results.

Note: For localized script messages, you need to have pre.tar file in the same directory as the script file.

This command has the following format:

```
customize_uxauth_bff -h [-l]
customize_uxauth_bff -a [-d pkg_location] pkg_name
customize_uxauth_bff -w keyword [-d pkg_location] pkg_name
customize_uxauth_bff -r [-d pkg_location] [-l lang] pkg_name
customize_uxauth_bff -i install_loc [-d pkg_location] pkg_name
customize_uxauth_bff -s -f tmp_params [-d pkg_location] pkg_name
customize_uxauth_bff -e uxpreinstall [-d pkg_location] pkg_filename
customize_uxauth_bff -g [-f tmp_params] [-d pkg_location] pkg_name
```

pkg_name

The name of the UNAB package (bff file) you want to customize.

-a

Displays the license agreement.

-e uxpreinstall

Specifies to extract the uxpreinstall utility from the installation package.

-c *certfile*

Defines the full pathname of the root certificate file.

Note: This option is applicable to the CAeAC package only.

-d *pkg_location*

(Optional) Specifies the directory where you placed your package on the file system. If you do not specify a directory where the package is located, the script defaults to /var/spool/pkg.

-f *tmp_params*

Specifies the full path and name of the installation parameters file to create or retrieve information from.

Note: If you do not specify a file when using the -g option, the installation parameters are directed to the standard output (stdout).

-g

Gets the installation parameters file and places it in the file specified by the -f option.

-h

Displays command usage. When used in conjunction with the -l option, displays the language code for supported languages.

-i *install_loc*

Sets the installation directory for the package to *install_loc/*uxauth.

-l *lang*

Sets the language of the installation parameters file to *lang*. You can set the language only in conjunction with the -r option.

Note: For a list of supported language codes you can specify, run -l with the -h option. By default, the installation parameters file is in English.

-r

Resets the package to use default values as in the original package.

-s

Sets the specified package to use inputs from the customized installation parameters file specified by the -f option.

-w *keyword*

Defines the keyword that specifies that you accept the license agreement. You can find this keyword at the end of the license agreement (inside square brackets). To locate the license agreement file, use the -a option.

Install UNAB AIX Native Package

To manage the UNAB installation with all your other software installations, install the customized UNAB AIX native package. The UNAB AIX native packages (bff files) let you install UNAB on AIX easily.

Important! You must customize the package to specify that you accept the license agreement using a keyword you can find inside the license agreement. If you want to manage the UNAB endpoint through CA ControlMinder Enterprise Management, you must register the UNAB endpoint with CA ControlMinder Enterprise Management *before* you install UNAB.

To install the UNAB AIX native packages

1. Log in as root.

   To register and install AIX native packages, you need permissions associated with the root account.

2. Customize the UNAB package (see page 334).

   You must customize the package to specify that you accept the license agreement using a keyword that you can find inside the license agreement. You can also customize the package to specify custom installation settings.

3. (Optional) Record the level (version) of the package that you want to install:

   `installp -l -d pkg_location`

   pkg_location

   Defines the directory where the UNAB package (uxauth) is located.

   For each package in *pkg_location*, AIX lists the level of the package.

   Note: For more information about the AIX native packaging installation options, refer to the man pages for installp.

4. Install the UNAB package using the following command:

   `installp -ac -d pkg_location uxauth[pkg_level]`

   pkg_level

   Defines the level number of the package you recorded earlier.

   AIX starts installing the UNAB package from the *pkg_location* directory.

   UNAB is now fully installed but not started.

More information:

Additional Considerations for Native Installations (see page 198)

Uninstall AIX Packages

To uninstall a UNAB AIX package installation, you need to uninstall the UNAB packages in the reverse order of their installation.

To uninstall UNAB packages uninstall the main UNAB package:

`installp -u unab_package_name`

unab_package_name

Defines the name of the UNAB native package.

AIX Workload Partitions (WPAR) Native Package Installation

AIX provides virtualized operating system environments within a single instance of AIX called Workload Partitions (WPAR). Workload Partitions are software partitions that are created from and share the resources of a single instance of the AIX operating system. AIX contains a master partition called *global environment* and workload partitions that run alongside it.

Review the following considerations and limitations before you install UNAB on AIX WPAR:

- You can install UNAB on AIX 7.1 WPAR or later only.
- If you select to use AIX WPAR in shared mode, where the /opt and /usr directories are shared by all partitions, use a private installation directory. For example: specify to install UNAB in /CA/uxauth/ directory and not in /opt/CA/uxauth directory.
- AIX WPAR Live Migration is not supported.
- You cannot install UNAB on AIX 5.2 WPAR.
- Enable the use_time_sych option (set to 'yes') on the AIX Global Environment only. Disable this option on the Workload Partition instances of UNAB (set to 'no').

Install UNAB AIX 7.1 WPAR Native Package in Shared Mode

Installing UNAB on the AIX WPAR default partition is similar to a regular installation except that you specify a non-default installation directory. In shared mode the /opt and /usr directories are shared between all Workload Partitions.

Important! You must customize the package to specify that you accept the license agreement using a keyword you can find inside the license agreement.

Follow these steps:

1. Log in to the Global Environment as root.

   To register and install AIX native packages, you need permissions associated with the root account.

2. Customize the UNAB package (see page 334).

   You must customize the package to specify that you accept the license agreement using a keyword that you can find inside the license agreement. You can also customize the package to specify custom installation settings.

   Important! Change the installation directory to specify a private directory. For example:

   ```
   customize_eac_bff -i /CA/uxauth -d pwd uxauth.12.6.1.*.bff
   ```

3. Install UNAB by executing the following command:

   ```
   installp -d 'pwd' -a uxauth
   ```

   AIX starts installing the UNAB package.

   UNAB is now fully installed but not started.

4. Synchronize UNAB with the AIX Workload Partitions using the following command:

   synchwpar *<wpar_name>*

   wpar_name

   Specifies the name of the AIX Workload Partition

   Note: To install UNAB on all partitions use the synchwpar -A command.

   UNAB is installed on the specified AIX Workload Partition. You can now manage UNAB on the Global Environment and on each Workload Partition separately.

Install UNAB AIX 7.1 WPAR Native Package in Detached Mode

Installing UNAB on an AIX Workload Partitions is similar to a regular installation. In Detached Mode each Workload Partition uses a local copy of the /opt and /usr directories.

Follow these steps:

1. Log in to the Global Environment as root.

   To register and install AIX native packages, you need permissions associated with the root account.

2. Customize the UNAB package (see page 334).

   You must customize the package to specify that you accept the license agreement using a keyword that you can find inside the license agreement. You can also customize the package to specify custom installation settings.

3. Install UNAB by executing the following command:

   ```
   installp -d 'pwd' -a uxauth
   ```

   AIX starts installing the uxauth package from the *pkg_location* directory.

   UNAB is now fully installed but not started.

4. Copy the installation package to each of the detached Workload Partitions.

5. Log in to each Workload Partition as root and install UNAB

   UNAB is installed on the AIX Workload Partition.

Uninstall UNAB AIX 7.1 WPAR Package

You uninstall AIX 7.1 WPAR package by first removing UNAB from the Global Environment and then from each Workload Partition.

Follow these steps:

1. Log in to the Global Environment as root.

2. Remove the uxauth package using the following command:

   ```
   installp -u uxauth
   ```

3. Synchronize the Workload Partitions using the following command:

   ```
   synchwpar <wpar_name>
   ```

   Note: To uninstall UNAB in detached partitions remove the installation package by running the uninstall command on each partition.

   CA ControlMinder is removed from the Global Environment and from each Workload Partition

Post-Installation Tasks

The following topics describe the post-installation tasks that you need to perform to configure the UNAB endpoint and activate UNAB.

Register a UNIX Host in Active Directory

To let users defined in Active Directory log in to UNIX computers, register on the Active Directory server each UNIX computer on which you installed UNAB.

Note: You can configure the UNAB installation parameters file to specify that the installation process registers the UNIX endpoint on Active Directory during UNAB installation.

To register a UNIX host in Active Directory

1. Verify that the time on the UNIX host and Active Directory server is synchronized.
2. Log in to the UNIX computer as a superuser.

   Note: You must activate UNAB before Active Directory users can log on to the UNIX computer.
3. If you use Microsoft Services for UNIX (SFU), specify the attribute names in the map section of the uxauth.ini file.

   If you do not specify the attribute names in the uxauth.ini file, users that are defined only in SFU cannot log in to UNAB hosts.

   Note: For more information about the uxauth.ini file, see the *Reference Guide*.
4. Navigate to the UNAB bin directory. By default the directory is:

   `/opt/CA/uxauth/bin`
5. Run the uxconsole -register utility.

   UNAB registers the UNIX computer in Active Directory and starts the uxauthd daemon.

   Note: For more information about uxconsole -register, see the *Reference Guide.*

Example: Register a UNIX Host in Active Directory

This example shows you how to register a UNIX computer in Active Directory. You type in the user name (-a administrator) and password (-w admin), define the Active Directory host name (-d Active_Directory_Host), set the verbosity level (-v 3), specify that the UNAB agent does not run at the end of the installation (-n), and define the name of the container in Active Directory (-o OU=COMPUTERS). The container must exist before you register the UNIX computer in Active Directory:

```
./uxconsole -register -a administrator -w admin -d Active_Directory_Host –v 3 -n -o
OU=COMPUTERS
```

Example: Delegating an Active Directory User the Privileges to Register a UNIX Host

If you do not want to specify an administrator user name and password when you run the uxconsole -register command, you can specify the user name and password of a user with delegated privileges for registering the UNIX host in Active Directory. The following example shows you how to delegate the privileges for registering a UNIX host in Active Directory to an Active Directory user.

1. On the Active Directory computer, click Start, Programs, Administrative Tools, Active Directory Users and Computers.

   The Active Directory Users and Computers management console opens.

2. Right-click the Computers folder and select Delegate Control.

   The Delegation Control Wizard opens.

3. Click Next.

   The wizard starts.

4. Complete the installation wizard using the following table, and click Finish:

Information	Action
Users and Groups	Specifies the user to which you want to delegate control to. Select Add and search for the user you want to delegate control to.
Tasks to Delegate	Defines the tasks to delegate to the selected users or groups. Select "Create a custom task to delegate"

Information	Action
Active Directory Object Type	Defines the scope of the task to delegate. Do the following: ■ Select "This folder, existing objects in this folder, and creation of new objects in this folder". ■ Select "Create Computer objects permission from the list".
Permissions	Defines the permissions to delegate to the user. Select "Creation/delegation of specific child objects ".

The wizard closes.You have delegated permission to create computer objects in Active Directory to the user. The user now has sufficient privileges to register a UNIX host in Active Directory.

Configure UNAB

The uxauth.ini file specifies the actions UNAB takes during startup and run time. The uxauth.ini file contains a default set of values that you can change to meet your specifications.

To configure UNAB

1. Log in to the UNIX host that is running UNAB.
2. Open the uxauth.ini file that is located by default in the following directory:

   `/opt/CA/uxauth`
3. Review the settings and change as required.

Note: For more information about uxauth.ini configuration settings, see the *Reference Guide*.

Note: You can use CA ControlMinder Enterprise Management to configure the uxauth.ini file.

Configure UNAB for Reporting

Once you have UNAB installed and configured, you can configure it to send data to the Distribution Server for processing by enabling and configuring the Report Agent. If you did not configure the Report Agent settings when you installed UNAB, configure the Report Agent when you enable it.

Note: This procedure illustrates how you configure an existing UNAB endpoint for sending reports. If you installed CA ControlMinder and UNAB on the same computer, you only need to configure the Report Agent settings once.

To configure UNAB for reporting run *ACSharedDir*/lbin/report_agent.sh:

```
report_agent config {-server hostname [-proto {ssl|tcp}] [-port port_number] [-rqueue
queue_name] -schedule <time@day> [,day2][...] > [-audit] | [-silent] ]
```

If you omit any configuration options, the script sets the default value for that option.

Note: For more information about the report_agent.sh script, and the Report Agent configuration settings, see the *Reference Guide*.

Start UNAB

For users from Active Directory log into the UNIX computer, start up UNAB.

To start UNAB

1. Log in to the UNIX computer as a superuser.
2. Locate the UNAB lbin directory.
3. Enter the following command:

   ```
   ./uxauthd.sh start
   ```

   The UNAB daemon starts.

Activate UNAB

After you have registered the UNIX host in Active Directory, you need to activate UNAB. Activation is the final step in the implementation process of UNAB. Once UNAB is activated it authenticates users based on their Active Directory password.

To activate UNAB

1. Log in to the UNIX computer as a superuser.
2. Navigate to the UNAB bin directory. By default the directory is:

   ```
   /opt/CA/uxauth/bin
   ```

3. Run the following command:

   ```
   ./uxconsole -activate
   ```

   -activate

   Specifies that login is activated for Active Directory users

   UNAB is activated

Note: Activating UNAB lets local users that have an Active Directory account to continue logging into the UNIX host.

Note: For more information about the uxconsole utility, see the *Reference Guide*.

Example: Login to UNAB after activation

The following example shows you how you can log in to a UNIX computer using an Active Directory account after you installed UNAB in partial mode and registered it.

1. Open a terminal window.
2. Connect to the UNIX host:

   ```
   telnet computer.com
   ```

   You are connected to the UNIX computer and a UNIX shell opens.
3. Enter the user name and password of an Active Directory account.

   If successful, a message is displayed, informing you of your last login details.

How to Implement Full Integration Mode

In full integration mode, the UNAB endpoint relies on the Active Directory server to both authenticate and authorize users.

To implement UNAB in full integration mode

1. Implement UNAB.

   This step installs and activates UNAB on UNIX endpoints.
2. Install a tool that lets you manage the UNIX attributes of Active Directory users.

   Because Active Directory Users and Computers does not expose UNIX attributes, you must install an additional tool to view and modify these attributes. For example, you can use the CA ControlMinder UNIX Attributes plug-in, Microsoft Identity Management for UNIX, ADSI Edit, or a simple LDAP client to view and modify UNIX attributes.

3. Migrate the attributes of users and groups on UNAB endpoints to Active Directory. Do *one* of the following:
   - Use the UNAB migration tool to copy the properties of UNAB endpoint users and groups to Active Directory.
   - Use the tool that you installed in Step 2 to manually configure the attributes of UNAB endpoint users and groups on Active Directory.

   This step lets you use Active Directory to control access to the endpoints. UNAB is now implemented in full integration mode.
4. (Optional) Delegate permission to manage privileges for UNAB users and groups to UNIX administrators on Active Directory.
5. Use the tool that you installed in Step 2 to update the UNIX attributes of Active Directory as needed.

   For example, an administrator uses the tool to update a user's default login shell.

UNAB Interactions with Active Directory

In full integration mode, the following UNIX user and group attributes are stored on Active Directory:

- UID
- GID
- Home directory
- Login shell
- GECOS

UNAB uses the Windows 2003 R2 schema to store these attributes. Generally UNAB reads these attributes, but does not write to them. UNAB writes to Active Directory attributes only if you use the uxconsole -migrate utility to migrate UNIX users and groups to Active Directory.

UNAB does not extend the Active Directory schema.

Install the CA ControlMinder UNIX Attributes Plug-in

The CA ControlMinder UNIX Attributes plug-in lets you manage UNIX attributes for UNAB users on Active Directory. The plug-in does not install an NIS server. Other tools that you can use to manage UNIX attributes for UNAB users include Microsoft Identity Management for UNIX, ADSI Edit, or simple LDAP clients.

By default, the plug-in uses the Active Directory 2003 R2 schema to read and write Active Directory data. If the R2 schema is not present, you can configure the plug-in to use different attributes.

Note: Provide the Active Directory administrator password during installation. The password is required as the Active Directory schema is modified. CA ControlMinder does not save the Active Directory administrator password.

Install the plug-in on the server that users use to manage Active Directory, but you do not need to install the plug-on on the Active Directory domain controller (DC).

Follow these steps:

1. Insert the CA ControlMinder Endpoint Components for UNIX DVD into an optical disc drive on the server.
2. Browse to the following directory:

   `ADTools\UnixADTabExt`
3. Choose the directory that suites the operating system you are using.
4. Double-click the setup.exe file.

   The CA ControlMinder UNIX Attributes plug-in installation wizard opens.
5. To install the CA ControlMinder UNIX Attributes plug-in, follow the instructions.

   The CA ControlMinder UNIX Attributes plug-in is installed on the Active Directory host.
6. (Optional) Configure the Active Directory attributes that the plug-in uses.

   Complete this step if the Active Directory schema is not Windows 2003 R2.

Configure the Attributes That the Plug-in Uses

The CA ControlMinder UNIX Attributes plug-in uses the Active Directory 2003 R2 schema to read and write Active Directory data. If your Active Directory server does not use the 2003 R2 schema, you can configure the plug-in to use attributes from a different schema.

If you configure the plug-in to use attributes from a different schema, you must also configure the UNAB endpoints to use the same attributes. You use the map section of the uxauth.ini file to configure the attributes that UNAB endpoints use.

To configure the attributes that the plug-in uses, change the value of the following registry entries. The entries are located in the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\uxauth
```

Entry	Default Value	Field Name in Plug-in
user_uid_attr_name	uidNumber	UID
user_loginshell_attr_name	loginShell	Login Shell
user_homedir_attr_name	unixHomeDirectory	Home Directory
user_gecos_attr_name	gecos	GECOS
user_gid_attr_name	gidNumber	Primary Group Name/GID
group_gid_attr_name	gidNumber	GID (Group ID)

Note: For more information about the uxauth.ini file, see the *Reference Guide*.

Uninstall the CA ControlMinder UNIX Attributes Plug-in

The CA ControlMinder UNIX Attributes plug-in lets you manage UNIX attributes for users and groups on Active Directory.

To uninstall the CA ControlMinder UNIX Attributes plug-in

1. Click Start, Control Panel, Add or Remove Programs.

   The Add or Remove Program dialog appears

   Note: On Windows Server 2008 click Start, Control Panel, Programs and Features.

2. Scroll through the program list and select CA Access Control UNIX Attributes Snap-in.

3. Click Change\Remove or Uninstall depending on the operating system you use.

   The uninstall process removes the CA ControlMinder UNIX Attributes plug-in from the system.

4. Delete the following registry key:

   `HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\uxauth`

5. Delete the ACUnixAttributesShellExt.dll file from the computer.

   The CA ControlMinder UNIX Attributes plug-in is uninstalled.

Example: Uninstall ACUnixAttributesShellExt.dll

The following example uninstalls the CA ControlMinder UNIX Attributes plug-in from the directory C:\WINDOWS\system32:

```
regsvr32 /u %WINDIR%\system32\ACUnixAttributesShellExt.dll
```

Users and Groups Migration

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. After you migrate UNIX users into Active Directory you control access to the UNIX hosts and no longer need to maintain the password or shadow files on each UNIX host.

After you migrate users and groups from the UNIX hosts to Active Directory (full integration mode), Active Directory performs authentication and authorization of users.

More information:

How Migration Works (see page 351)
Migrate UNIX Users and Groups to Active Directory (see page 352)

How Migration Works

When you start the migration process on a UNIX host, UNAB performs the following tasks:

1. Retrieves the list of local users and NIS/NIS+ users.

   Inspects Active Directory for each user name on the list and does one of the following for each user:

   - If the user exists in Active Directory and the user UNIX attributes are identical to the attributes that appear in the UNIX host, the user account is migrated.
   - If the user exists in Active Directory and several of the user UNIX attributes are missing, UNAB does not migrate the user and logs the missing properties.
   - If the user exists in Active Directory and the user does not have any UNIX attributes, UNAB migrates the user and adds the missing attributes.
   - If the user does not exist in Active Directory, UNAB does not create the user account in Active Directory.

2. Retrieves the list of local groups and NIS/NIS+ groups.

   Inspects the Active Directory for the groups name and for each group does one of the following:

   - If the group exist in Active Directory and the group UNIX attributes are identical to the attributes of the UNIX host, the group is migrated.
   - If the groups exist in Active Directory and the group ID is different to the ID on the UNIX host, UNAB does not migrate the group including its members to Active Directory.
   - If the group exists in Active Directory and the group IDs are identical but several UNIX attributes are missing, UNAB migrates the group to Active Directory and completes the missing attributes.
   - If the group does not exist in Active Directory, UNAB creates a group and migrates the groups to Active Directory.

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.

Note: If you select to migrate the root user to Active Directory, the root account is authenticated locally and in Active Directory on login. As a result, you can experience a long authentication process.

Migrate UNIX Users and Groups to Active Directory

You migrate users from the local UNIX host into Active Directory to manage access to the host from a single location.

To migrate UNIX users and groups to Active Directory

1. Log in to the UNIX computer as the root user.
2. Navigate to the UNAB installation bin directory, by default:

   `/opt/CA/uxauth/bin`
3. Run the -uxconsole -migrate utility.

   The uxconsole program migrates the UNIX users and groups to Active Directory. A message appears informing you that the operation completed successfully.

Note: For more information about resolving migration conflicts, see the *Enterprise Administration Guide*. For more information about the uxconsole utility, see the *Reference Guide.*

Delegating UNIX Administrators the Privileges to Manage UNIX Users and Groups Attributes

For UNIX administrators to manage UNIX users and groups attributes in Active Directory, you can delegate specific management privileges over to UNIX administrators. Delegating the management privileges enables the UNIX administrators to continue managing the UNIX users and groups attributes after they are migrated to Active Directory.

Before you delegate the management privileges, verify that you installed a tool that lets you manage the UNIX attributes of Active Directory users. We recommend that you delegate management privileges to a group, rather than to individual users.

Example: Delegating UNIX administrators the privileges to manage UNIX users and groups attributes

The following example shows you how to delegate the privileges for managing UNIX users and groups in Active Directory to a group of UNIX administrators.

1. On the Active Directory computer, click Start, Programs, Administrative Tools, Active Directory Users and Computers.

   The Active Directory Users and Computers management console opens.
2. Right click the Organizational Unit (OU) and select Properties.

   The Organizational Unit properties window opens.

3. Select the Security tab.

   Note: If you do not see the Security tab, verify that the Advanced Features option, under the View tab, is highlighted.

4. Click Advanced, then click the Add button.

   The Select User, Computer or Group window opens.

5. Enter the name of the group or users to delegate management privileges to. Click OK.

   The Permission Entry window opens.

6. Click the Properties tab.

   You assign permissions to the group or users in this window.

7. From the Apply Onto menu, select Group Objects.
8. Select the Read gidNumber and Write gidNumber options from the Allow column.
9. Click OK.

   You have delegated management attributes over UNIX groups to the UNIX administrators group.

10. Repeat Steps 1-6 to delegate management privileges over UNIX users.
11. From the Apply Onto menu, select Users Objects.
12. Select the following attributes from the Allow column:
    - Read Gecos
    - Write Gecos
    - Read gidNumber
    - Write gidNumber
    - Read uid
    - Write uid
    - Read uidNumber
    - Write uidNumber
    - Read unixHomeDirectory
    - Write unixHomeDirectory
    - Read loginShell
    - Write LoginShell
13. Click OK.

    You have delegated management attributes over UNIX users to the UNIX administrators group.

Configure UNIX Attributes for an Active Directory User

This procedure describes how to use the CA ControlMinder UNIX Attributes plug-in to manage the attributes of UNIX users on Active Directory. You can use other tools to manage UNIX attributes on Active Directory, such as Microsoft Identity Management for UNIX, ADSI Edit, or a simple LDAP client.

Note: When you define user account properties, you do not need to specify the computers that this user can log on to. These settings do not apply to UNIX hosts.

Configure the UNIX attributes for an Active Directory user

1. Select Start, Programs, Administrative Tools, Active Directory Users and Computers.

   The Active Directory Users and Computers window opens.

2. Double-click a user account.

   The user account properties appear.

3. Click the CA ControlMinder UNIX Attributes tab.

   The CA ControlMinder UNIX Attributes tab appears.

4. Complete the following fields:

   Enable UNIX Attributes

   Specifies if UNIX attributes are enabled on the user account. You must select this checkbox to enable UNIX attributes for the user.

   UID

   Defines the user ID number on the UNIX computer. Click Generate to find the next available UID.

   Home Directory

   Defines the user home directory on the UNIX computer.

   Example: /home/user

   Important! Verify that the parent directory of the home directory exists before you configure the user home directory.

   Login Shell

   Defines the user account login shell

   Example: /bin/sh

   GECOS

   Specifies the user GECOS information.

Primary Group Name/GID

Defines the primary group name or GID that the user is a member of.

Example: UNIXUsers

Important! You must assign a valid group name/GID when defining the user account.

5. Click OK.

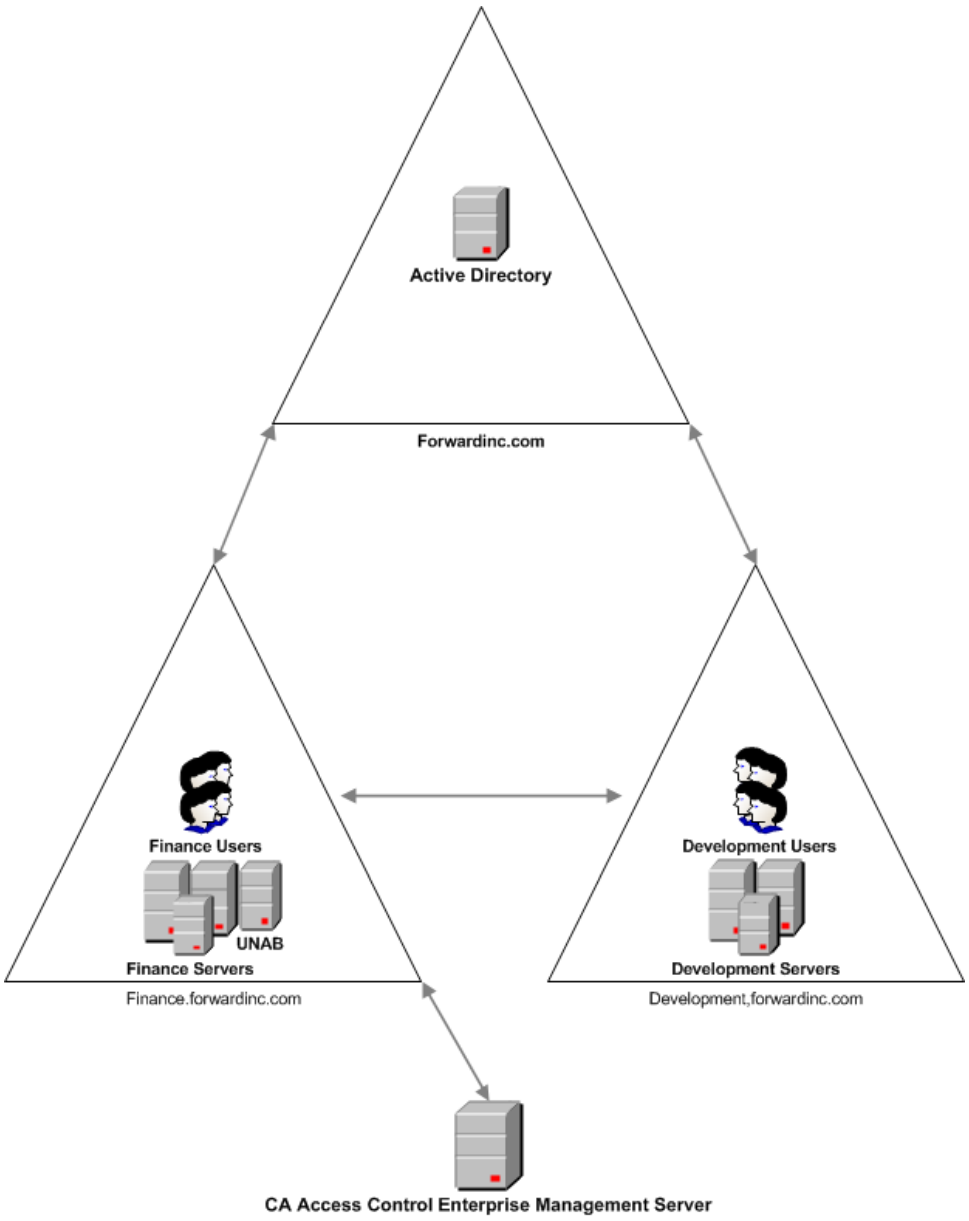
   The user UNIX attributes are configured.

Implementing UNAB in a Trusted Domains Environment

When you install UNAB, you specify the parameters of the domain UNAB will register with. After installing, registering and activating UNAB, you migrate users and groups into the domain.

If the domain that you specified has established trust relationships with other domains, users from those domains can potentially have access to computers in the domain that UNAB is a member of.

This diagram displays a UNAB implementation in a trusted domains environment:



In the previous diagram UNAB is installed in a domain that has established a trust connection with other domains. In this environment, users from a trusted domain can access the other domain although these users are not members of that domain.

Consider the following before you install UNAB in a trusted domains environment:

- The UNAB login policy controls access to computer in the domain based on user names. If multiple users have identical user names and are defined in more than one domain, UNAB cannot distinguish the domain of origin of the users and grants access to the domain.
- You can generate reports only for the domain that UNAB is a member of. You cannot generate reports for the trusted domains.
- You can migrate users to Active Directory that are defined in the domain UNAB is a member of.

We recommend that you maintain unique user and group names to prevent access from unauthorized users of trusted domains.

How to Register a UNIX Host in a One-Way Trust Domain Environment

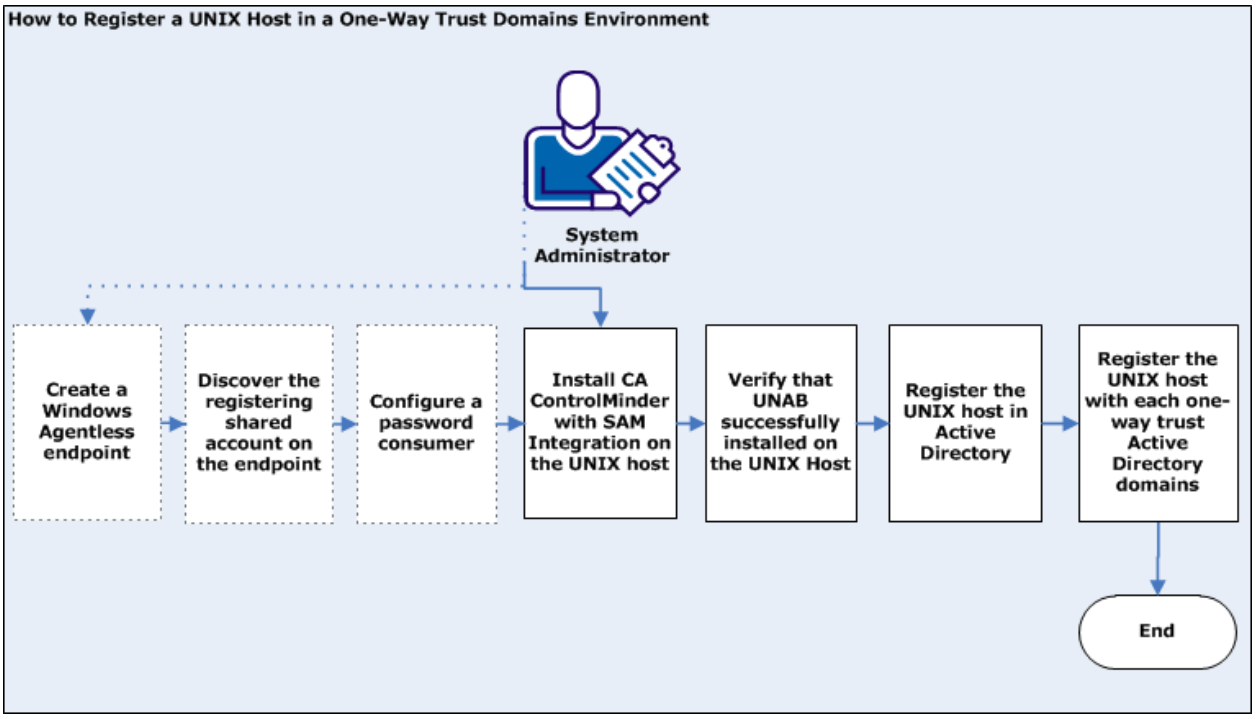
When you register the UNIX host in Active Directory, you use a user account with privileges to retrieve users and groups details from Active Directory. If you register the UNIX host in a two-way trust domains environment, you can use a single user account to retrieve users and groups from every Active Directory domain.

In a one-way trust domain environment the Active Directory account that you use to register a UNIX host cannot retrieve data from other Active Directory domains. In a one way trust domains environment, you register the UNIX host with a regular user account from each Active Directory domain.

Further, you can register a UNIX host with an Active Directory shared account and use SAM to manage the account. The user account must have sufficient permissions to retrieve the user and groups attributes from all every Active Directory domain.

To register a UNIX using a domain account, you use SAM integration. Integrating with SAM enables you to manage the registering user account, for example, apply the domain security policy, change the account password automatically and more.

The following diagram illustrates how to register a UNIX host in a one-way trust domain environment:



Note: Dotted lines indicate optional steps.

Follow these steps:

1. (Optional) To use a shared account to register the UNIX host, follow these steps:
   a. Create a Windows Agentless endpoint (see page 361).

      You specify the connection details of the Active Directory domain that you use to register each UNIX host.

   b. Discover the registering shared account on the endpoint (see page 362).

      You run the account discovery wizard on the Windows Agentless endpoint that you created.

   c. Define a password consumer (see page 365).

      You specify the UNAB endpoint as an SDK password consumer to enable the endpoint to obtain the registering user account password.

2. Install CA ControlMinder with SAM integration on each UNIX host that has UNAB installed (see page 367).

   The SAM integration configures the local computer for Shared Accounts Management (SAM). Set the INSTALL_PUPM option to yes to install SAM on the endpoint. For more information about SAM, see the *Enterprise Administration Guide*.

3. Verify that UNAB installation successfully completed. Do the following:
   a. Locate the accommon.ini file. By default, the file is located in the following directory:

      ```
      /opt/CA/AccessControlShared
      ```

   b. Locate the Distribution_Server token under the communication section.

   c. Define the Distribution Server URL. For example:

      ```
      tcp://ds_dr.comp.com:7222
      ```

      Note: For more information about the accommon.ini file, see the *Reference Guide*.

   d. Use the sechkey utility to set the communication password.

   e. Open a selang command-prompt window and enter the following commands:

      ```
      er ACVAR unab value("/opt/CA/uxauth/bin/uxauthd")
      er ACVAR unab value+("opt/CA/uxauth/bin/uxconsole")
      ```

4. Do *one* of the following:

   - To use a regular account to register the UNIX host, follow these steps:

     a. Start CA ControlMinder.

     b. register the UNIX host in each Active Directory domain (see page 371).

     c. Activate UNAB (see page 373).

     d. Register the UNIX host with each Active Directory in the one-way trust domain environment using the uxconsole -register- ows command.

     e. Start UNAB (see page 374).

   - To use a shared account to register the UNIX host, follow these steps:

     a. Start CA ControlMinder.

     b. Register a UNIX host in Active Directory (see page 371).

     c. Activate UNAB (see page 373).

     d. Register the UNIX host with each Active Directory in the one-way trust domain environment using the uxconsole -register- ows command..

     e. Start UNAB (see page 374).

     Note: For more information about the uxconsole utility, see the *Reference Guide*

Creating a Windows Agentless Endpoint

SAM can manage domain users on the Active Directory. To manage the Active Directory accounts, define a Windows Agentless Endpoint and provide the following information:

User Login

Defines the name of an administrative user who manages the endpoint. SAM uses this account to perform administrative tasks on the endpoint, for example, to connect to the endpoint, discover accounts, and change passwords.

Specify the *user name* in this field. Do not use the *computer name/user name* format or the *domain name/user name* format.

Example: Administrator.

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

Password

Defines the password of the administrative user of the endpoint.

Note: If you use the Advanced option, do not supply a password.

Host

Defines the Active Directory DNS domain name.

Example: company.com

Note: SAM attempts to resolve the Active Directory domain controller from the domain name. If SAM fails to resolve this name, specify the Active Directory Domain Controller (DC) DNS name or IP address.

Host Domain

Specifies the domain name (NETBIOS name).

Example: domain1

Note: Do not use the DNS name (domain1.ca.com), use the NETBIOS name (domain1).

Is Active Directory

Select this option to specify the Active Directory.

User Domain

Specifies the domain name (NETBIOS domain name) of the user specified in the User Login field or in the Advanced field (in case Advanced is used).

Example: domain1

Note: Do not use the DNS name (domain1.ca.com), use the NETBIOS name (domain1).

Advanced

Specifies whether to use a previously defined privileged administrative account, to perform administrative tasks on the endpoint. For example, SAM uses the account defined in the Advanced field to manage this endpoint instead of using the account specified in the User Login field. This option is useful when using the same privilege account to manage multiple endpoints.

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

Disable Exclusive Sessions

This option specifies whether to disable the exclusive sessions check on this endpoint. When selected, SAM does not check for open sessions on the endpoint.

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 ControlMinder Enterprise Management presents the accounts that it discovers in a table, so that you can easily tell which accounts you already manage with SAM.

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

Follow these steps:

1. In CA ControlMinder 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 ControlMinder Enterprise Management. Known accounts include ones that CA ControlMinder Enterprise Management already manages and the administrator account CA ControlMinder Enterprise Management uses to manage the endpoint.

Is Endpoint Administrator

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

Important! Be cautious when selecting the endpoint administrator account. CA ControlMinder 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, SAM 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 ControlMinder 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 ControlMinder 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 ControlMinder 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 ControlMinder Enterprise Management submit the task and creates the selected privileged accounts if there are no errors.

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 ControlMinder on the SAM endpoint with the SAM 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.

Follow these steps:

1. In CA ControlMinder 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 ControlMinder 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 SAM 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, SAM 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 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 ControlMinder 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 ControlMinder 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 ControlMinder Enterprise Management creates the password consumer.

Install CA ControlMinder RPM Packages

To manage the CA ControlMinder installation with all your other software installations, install the customized CA ControlMinder RPM package.

Important! You must customize the package to specify that you accept the license agreement using a keyword you can find inside the license agreement.

Note: The actual command you use varies depending on many variables, including whether you are upgrading or installing for the first-time, or whether you want to install to the default directory. Some command examples are available in this topic.

Follow these steps:

1. Use the rpm command to install the ca-lic package.

   The license program installs.

2. Customize the CAeAC package (see page 203).

   You must customize the package to specify that you accept the license agreement using a keyword that you can find inside the license agreement. You can also customize the package to specify custom installation settings.

   Note: If you are upgrading CA ControlMinder, you do not need to customize the package to specify that you accept the license agreement.

3. Use the rpm command to install the CAeAC package.

   CA ControlMinder installs.

   Note: The UNAB package also installs the CAWIN shared component.

   Important! If you are upgrading an existing CA ControlMinder package, unload SEOS syscall before you try to install the new package. Otherwise, the installation fails.

Customize the CA ControlMinder RPM Package

Before you can install CA ControlMinder using a native package, you must customize the CA ControlMinder package to specify that you accept the license agreement. You can also specify custom installation settings when you customize a package.

You customize a package by extracting the installation parameters file from the package, modifying it as required, and then loading it back into the package. Some commands are available in the customization script so that you do not have to modify the parameters file.

Note: We recommend that you *do not* modify the package manually. Instead, use the script as described in the following procedure to customize the CA ControlMinder package.

You can find the RPM packages for each of the supported Linux operating systems in the NativePackages/RPMPackages directory of the CA ControlMinder Endpoint Components for UNIX DVD.

Follow these steps:

1. Copy the package you want to customize to a temporary location on your file system.

   OS is the appropriate subdirectory name of your operating system.

   In the read/write location on the file system, the package can be customized as required.

2. Copy the customize_eac_rpm script file and the pre.tar file to a temporary location on your file system.

   The pre.tar file is compressed tar file containing installation messages and the CA ControlMinder license agreement.

   Note: You can find the customize_eac_rpm script file and the pre.tar file in the same location where the native packages are.

3. Display the license agreement:

   `customize_eac_rpm -a [-d pkg_location] pkg_filename`

4. Take note of the keyword that appears at the end of the license agreement inside square brackets.

   You specify this keyword in the next step.

5. Customize the CA ControlMinder package to specify that you accept the license agreement:

   `customize_eac_rpm -w keyword [-d pkg_location] pkg_filename`

   Important! You must customize the package to specify that you accept the license agreement using a keyword you can find inside the license agreement.

6. (Optional) Set the language of the installation parameters file:

   `customize_eac_rpm -r -l lang [-d pkg_location] pkg_filename`

7. (Optional) Upgrade from an eTrust Access Control r8 SP1 package:

   `customize_eac_rpm -u install_prefix [-d pkg_location] pkg_filename`

8. (Optional) Change the default encryption files:

   `customize_eac_rpm -s -c certfile -k keyfile [-d pkg_location] pkg_filename`

9. (Optional) Get the installation parameters file:

   `customize_eac_rpm -g -f tmp_params [-d pkg_location] pkg_filename`

10. (Optional) Edit the installation parameters file to suit your installation requirements.

    This file lets you set the installation defaults for the package. For example, activate the POSTEXIT setting (remove the preceding # character) and point it to a post-installation script file you want to run.

11. (Optional) Set the installation parameters in your customized package:

    `customize_eac_rpm -s -f tmp_params [-d pkg_location] pkg_filename`

    You can now use the package to install CA ControlMinder with the customized defaults.

Note: The actual commands you use vary depending on many variables, including whether you are upgrading or installing for the first time, or whether you want to install to the default directory.

Example: Specify That You Accept the License Agreement

To accept the license agreement when installing a native package, you customize the package. The following example shows you how you customize the x86 CA ControlMinder RPM package that you can find on the CA ControlMinder Endpoint Components for UNIX DVD (mounted to /mnt/AC_DVD) to accept the license agreement:

```
cp /mnt/AC_DVD/NativePackages/RPMPackages/LINUX/CAeAC*i386.rpm /tmp
cp /mnt/AC_DVD/NativePackages/RPMPackages/pre.tar /tmp
chmod 777 /tmp/CAeAC*i386.rpm
/mnt/AC_DVD/NativePackages/RPMPackages/customize_eac_rpm -w keyword -d /tmp
CAeAC*i386.rpm
```

You can now use the customized package in the /tmp directory to install CA ControlMinder.

More information:

customize_eac_rpm Command—Customize RPM Package (see page 208)

Start CA ControlMinder

Assuming you are working in an X Windows environment, invoke CA ControlMinder, verify that it is correctly installed on your system, and perform the following steps to initiate important protection:

1. Open two windows under root (superuser) authority.

2. In either window, enter the command:

   ```
   seload
   ```

   Wait while the seload command starts three CA ControlMinder daemons: Engine, Agent, and Watchdog.

3. After you have started the daemons, go to the other window and enter the command:

   ```
   secons -t+ -tv
   ```

   CA ControlMinder accumulates a file of messages reporting operating system events. The secons -tv command displays the messages on the screen as well.

4. In the first window, where you gave the seload command, enter the following command:

   ```
   who
   ```

   Watch the second window, where CA ControlMinder is writing the trace messages, to see whether CA ControlMinder intercepts the execution of the who command and reports on it. CA ControlMinder is correctly installed on your system if it reports interception of the who command.

5. If you want, enter more commands to see how CA ControlMinder reacts to them.

   The database does not yet contain any rules for blocking access attempts. Nevertheless, CA ControlMinder monitors the system so that you can see how the system behaves with CA ControlMinder installed and running, and which events CA ControlMinder intercepts.

6. Shut down the seosd daemon, by entering the following command:

   ```
   secons -s
   ```

   The following message displays on the screen:

   ```
   CA ControlMinder is now DOWN !
   ```

Register a UNIX Host in Active Directory

To let users defined in Active Directory log in to UNIX computers, register on the Active Directory server each UNIX computer on which you installed UNAB.

Note: You can configure the UNAB installation parameters file to specify that the installation process registers the UNIX endpoint on Active Directory during UNAB installation.

Follow these steps:

1. Verify that the time on the UNIX host and Active Directory server is synchronized.
2. Log in to the UNIX computer as a superuser.

   Note: You must activate UNAB before Active Directory users can log on to the UNIX computer.
3. If you use Microsoft Services for UNIX (SFU), specify the attribute names in the map section of the uxauth.ini file.

   If you do not specify the attribute names in the uxauth.ini file, users that are defined only in SFU cannot log in to UNAB hosts.

   Note: For more information about the uxauth.ini file, see the *Reference Guide*.
4. Navigate to the UNAB bin directory. By default the directory is:

   `/opt/CA/uxauth/bin`
5. Run the uxconsole -register utility.

   UNAB registers the UNIX computer in Active Directory and starts the uxauthd daemon.

   Note: For more information about uxconsole -register, see the *Reference Guide.*

Example: Register a UNIX Host in Active Directory

This example shows you how to register a UNIX computer in Active Directory. You type in the user name (-a administrator) and password (-w admin), define the Active Directory host name (-d Active_Directory_Host), set the verbosity level (-v 3), specify that the UNAB agent does not run at the end of the installation (-n), and define the name of the container in Active Directory (-o OU=COMPUTERS). The container must exist before you register the UNIX computer in Active Directory:

`./uxconsole -register -a administrator -w admin -d` *`Active_Directory_Host`* `–v 3 -n -o OU=COMPUTERS`

Example: Delegating an Active Directory User the Privileges to Register a UNIX Host

If you do not want to specify an administrator user name and password when you run the uxconsole -register command, you can specify the user name and password of a user with delegated privileges for registering the UNIX host in Active Directory. The following example shows you how to delegate the privileges for registering a UNIX host in Active Directory to an Active Directory user.

1. On the Active Directory computer, click Start, Programs, Administrative Tools, Active Directory Users and Computers.

   The Active Directory Users and Computers management console opens.
2. Right-click the Computers folder and select Delegate Control.

   The Delegation Control Wizard opens.

3. Click Next.

   The wizard starts.

4. Complete the installation wizard using the following table, and click Finish:

Information	Action
Users and Groups	Specifies the user to which you want to delegate control to. Select Add and search for the user you want to delegate control to.
Tasks to Delegate	Defines the tasks to delegate to the selected users or groups. Select "Create a custom task to delegate"
Active Directory Object Type	Defines the scope of the task to delegate. Do the following: ■ Select "This folder, existing objects in this folder, and creation of new objects in this folder". ■ Select "Create Computer objects permission from the list".
Permissions	Defines the permissions to delegate to the user. Select "Creation/delegation of specific child objects ".

The wizard closes.You have delegated permission to create computer objects in Active Directory to the user. The user now has sufficient privileges to register a UNIX host in Active Directory.

Activate UNAB

After you have registered the UNIX host in Active Directory, you need to activate UNAB. Activation is the final step in the implementation process of UNAB. Once UNAB is activated it authenticates users based on their Active Directory password.

Follow these steps:

1. Log in to the UNIX computer as a superuser.
2. Navigate to the UNAB bin directory. By default the directory is:

   `/opt/CA/uxauth/bin`

3. Run the following command:

   ```
   ./uxconsole -activate
   ```

   -activate

   Specifies that login is activated for Active Directory users

   UNAB is activated

Note: Activating UNAB lets local users that have an Active Directory account to continue logging into the UNIX host.

Note: For more information about the uxconsole utility, see the *Reference Guide*.

Example: Login to UNAB after activation

The following example shows you how you can log in to a UNIX computer using an Active Directory account after you installed UNAB in partial mode and registered it.

1. Open a terminal window.
2. Connect to the UNIX host:

   ```
   telnet computer.com
   ```

   You are connected to the UNIX computer and a UNIX shell opens.
3. Enter the user name and password of an Active Directory account.

   If successful, a message is displayed, informing you of your last login details.

Start UNAB

For users from Active Directory log into the UNIX computer, start up UNAB.

Follow these steps:

1. Log in to the UNIX computer as a superuser.
2. Locate the UNAB lbin directory.
3. Enter the following command:

   ```
   ./uxauthd.sh start
   ```

   The UNAB daemon starts.

Chapter 10: Installing Endpoint Management

This section contains the following topics:

How to Prepare the Endpoint Management Server

Before you install CA ControlMinder Endpoint Management, you need to prepare the server.

Important! If you intend to install CA ControlMinder Enterprise Management on the same computer, you do not need to follow these steps. The installation program installs CA ControlMinder Endpoint Management as part of CA ControlMinder Enterprise Management installation.

To prepare the Endpoint Management server, do the following:

1. Install a supported Java Development Kit (JDK).

   Note: You can find prerequisite third-party software on the CA ControlMinder Third Party Components DVDs. For information about supported versions, see the *Release Notes*.

2. Install a supported JBoss version.

   We recommend that you run JBoss as a service. (daemon on UNIX).

   Note: You can find prerequisite third-party software on the CA ControlMinder Third Party Components DVDs. For information about supported versions, see the *Release Notes*.

3. Install CA ControlMinder.

   Note: Follow the instructions for installing a CA ControlMinder endpoint.

4. (Windows only) Restart the computer.
5. Stop CA ControlMinder services (secons -s).

   The server is now ready for CA ControlMinder Endpoint Management to be installed.

Install CA ControlMinder Endpoint Management on Windows

Valid on Windows

The graphical installation uses a wizard to support and guide you when installing CA ControlMinder Endpoint Management on a Windows computer.

To install CA ControlMinder Endpoint Management on Windows

1. Verify that you prepare the server correctly.
2. Insert the CA ControlMinder Server Components for Windows DVD into your optical disc drive.
3. Open the CA ControlMinder Product Explorer (ProductExplorerx86.EXE).

   The CA ControlMinder Product Explorer appears.
4. Expand the Components folder, select CA ControlMinder Endpoint Management, then click Install.

   The InstallAnywhere wizard starts loading.
5. Complete the wizard as required. The following installation inputs are not self-explanatory:

   JBoss Folder

   Defines the location where JBoss Application Server is installed.

   If you use the supplied JBoss version, this is the location where you extracted the contents of the JBoss zip file.

   Web Service Information

   Defines the *location* where you want to install the CA ControlMinder Web Service and the *port* you want this service to use (by default, 5248).

   Full computer name

   Defines the name of the application server (the local computer). This is the name you then need to use in the URL when you access the application.

   The installation is now complete.

Install CA ControlMinder Endpoint Management on Linux

You must use console installation to install CA ControlMinder Endpoint Management on a Linux computer.

To install CA ControlMinder Endpoint Management on Linux

1. Make sure that you prepare the server correctly.
2. Insert the CA ControlMinder Server Components for Solaris or Server Component for Linux DVD into your optical disc drive.
3. Mount the optical disc drive.
4. Open a terminal window and navigate to the EndPointMgmt directory on the optical disc drive.
5. Enter the following command:

   ```
   install_EM_r125.bin -i console
   ```

   The InstallAnywhere console appears after a few moments.
6. Complete the prompts as required. The following installation inputs are not self-explanatory:

   Choose Locale By Number

   Defines the number representing the locale you want to install in.

   Note: You need a localized operating system to install in any of the supported non-English languages.

   JBoss Folder

   Defines the location where JBoss Application Server is installed.

   If you use the supplied JBoss version, this is the location where you extracted the contents of the JBoss zip file.

   Web Service Information

   Defines the *location* where you want to install the CA ControlMinder Web Service and the *port* you want this service to use (by default, 5248).

   Full computer name

   Defines the name of the application server (the local computer). This is the name you then need to use in the URL when you access the application.

   The installation is now complete.

Uninstall CA ControlMinder Endpoint Management on Windows

Log in to the Windows system as a user with Windows administrative privileges (that is, the Windows administrator or a member of the Windows Administrators group).

To uninstall CA ControlMinder Endpoint Management on Windows

1. Stop JBoss if it is running.
2. Click Start, Control Panel, Add or Remove Programs.

   The Add or Remove Program dialog appears.
3. Scroll through the program list and select CA ControlMinder Endpoint Management.
4. Click Change/Remove.

   The Uninstall CA ControlMinder Endpoint Management wizard appears.
5. Follow the wizard's instructions to uninstall CA ControlMinder Endpoint Management.

   The uninstall completes and removes CA ControlMinder Endpoint Management from your computer.
6. Click Done to close the wizard.

Note: If you have installed prerequisite software in custom locations, remove the JBoss and JDK folders manually.

Uninstall CA ControlMinder Endpoint Management on Linux

If you want to remove CA ControlMinder Endpoint Management from your computer you need to use the uninstall program that CA ControlMinder Endpoint Management provides.

Follow these steps:

1. Stop JBoss by doing *one* of the following:
   - From the JBoss job windows, interrupt (Ctrl+C) the process.
   - From a separate window, type:

     `./JBoss_path/bin/shutdown -S`
2. Enter the following command:

   `"/ACEMInstallDir/Uninstall_EndpointManagement/Uninstall_CA_Access_Control_Endpoint_Management"`

   ACEMInstallDir

   Defines the installation directory of CA ControlMinder Endpoint Management. By default this path is:

   `/opt/CA/AccessControlServer/EndpointManagement/`

   InstallAnywhere loads the uninstall console.
3. Follow the prompts to uninstall CA ControlMinder Endpoint Management.

   The uninstall completes and removes CA ControlMinder Endpoint Management from your computer.

Start CA ControlMinder Endpoint Management

Once you install CA ControlMinder Endpoint Management you need to start CA ControlMinder and the web application server.

To start CA ControlMinder Endpoint Management

1. Start CA ControlMinder services.

   CA ControlMinder Endpoint Management requires that CA ControlMinder be running.

2. Start the following additional services, which do not load when you issue the seosd -start command:

   - CA ControlMinder Web Service
   - CA ControlMinder Message Queue (if present)

3. Start JBoss Application Server by doing either of the following:

   - Click Start, Programs, CA, Access Control, Start Task Engine.

     Note: The Task Engine may take some time to load the first time that you start it.

   - Start JBoss Application Server service from the Services panel.

     When JBoss Application Server completes loading, you can log in to the CA ControlMinder Endpoint Management web-based interface.

     Note: JBoss Application Server may take some time to load the first time that you start it.

   When JBoss Application Server completes loading, you can log in to the CA ControlMinder Endpoint Management web-based interface.

Open CA ControlMinder Endpoint Management

Once you install and start CA ControlMinder Endpoint Management you can open the web-based interface from a remote computer using the URL for CA ControlMinder Endpoint Management.

To open CA ControlMinder Endpoint Management

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

   http://*enterprise_host*:*port*/acem

2. Enter the following information:

   User Name

   Defines the name of the user that has privileges to perform CA ControlMinder administration tasks.

   Note: The user name you use to log in should include the computer name (for example, *myComputer**Administrator* on Windows or *root* on UNIX).

   Password

   Defines the password of the CA ControlMinder user.

   Host Name

   Defines the name of the endpoint you want to perform administrative tasks on. This can be either a host or a PMDB, specified in the format: *PMDB_name@host_name*

   Note: You must have permissions to manage the endpoint from the computer where CA ControlMinder Endpoint Management is installed (using the TERMINAL resource).

   Click Log In.

   CA ControlMinder Endpoint Management opens on the Dashboard tab.

Note: You can also open CA ControlMinder Endpoint Management from a Windows computer where you installed it by clicking Start, Programs, CA, Access Control, Endpoint Management.

Example: Open CA ControlMinder Endpoint Management

Enter the following URL into your web browser to open CA ControlMinder Endpoint Management from any computer on the network:

```
http://appserver123:18080/acem
```

The URL suggests that CA ControlMinder Endpoint Management is installed on a host named appserver123 and uses the default JBoss port 18080.

Chapter 11: Installing a High Availability Deployment

This section contains the following topics:

High Availability

CA Access Control Enterprise Management uses mirrored sites to provide high availability deployments. *Mirrored* sites are fully redundant facilities with full, real-time information mirroring and are identical to the primary site in all technical aspects. Data is processed and stored at the primary and mirrored sites simultaneously.

Mirrored sites employ an active-passive deployment for failover. An *active-passive* deployment includes two or more data centers, with one actively processing requests and the other ready to service requests if the active one fails. The clustering solution software that you select is responsible for controlling the active and passive servers and switching between them in case of failure.

In an active-passive deployment, the active server is referred to as the primary server, and the passive server is referred to as the secondary server.

Benefits and Limitations of a High Availability Deployment

A high availability deployment helps ensure that your CA ControlMinder Enterprise Management components continue to service requests if one or more components or servers fails. If the endpoints cannot connect to the primary environment, they connect to the secondary server until the primary environment is restored.

A high availability deployment has the following benefits:

- Prevents loss of privileged accounts, DMS datasource files and endpoints definitions if the primary Enterprise Management Server fails.
- Helps ensure uninterrupted use.

Consider the following limitations when planning a high availability deployment:

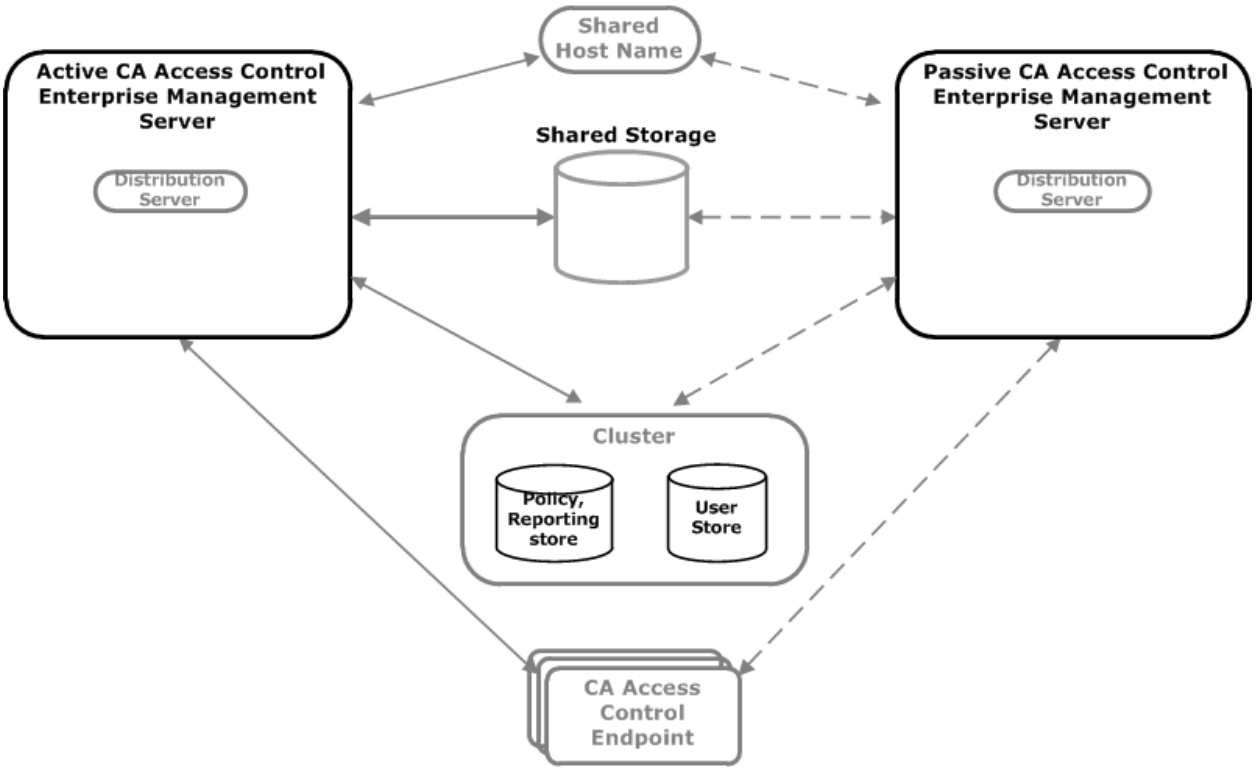
- The Enterprise Management Server does not support session continuity in an event of a failure. User sessions terminate if the active server fails to respond. Logged-in users must log in again.
- Only one active DMS is supported.
- Identical communication passwords used when installing the primary and secondary Enterprise Management Servers.
- The Java Connector Sever (JCS) on the primary and secondary servers must have the same name.

Note: We recommend that you use virtual DNS names that are controlled by the clustering software solution to seamlessly transition between the servers in case of failure.

For example, in case the primary Enterprise Management Server fails when a user session is open, the user can either type in the URL of the secondary Enterprise Management Server or, using a virtual DNS or load balancer, continue working using the same URL.

High Availability Deployment Architecture

The following diagram shows CA ControlMinder Enterprise Management in a high availability environment:



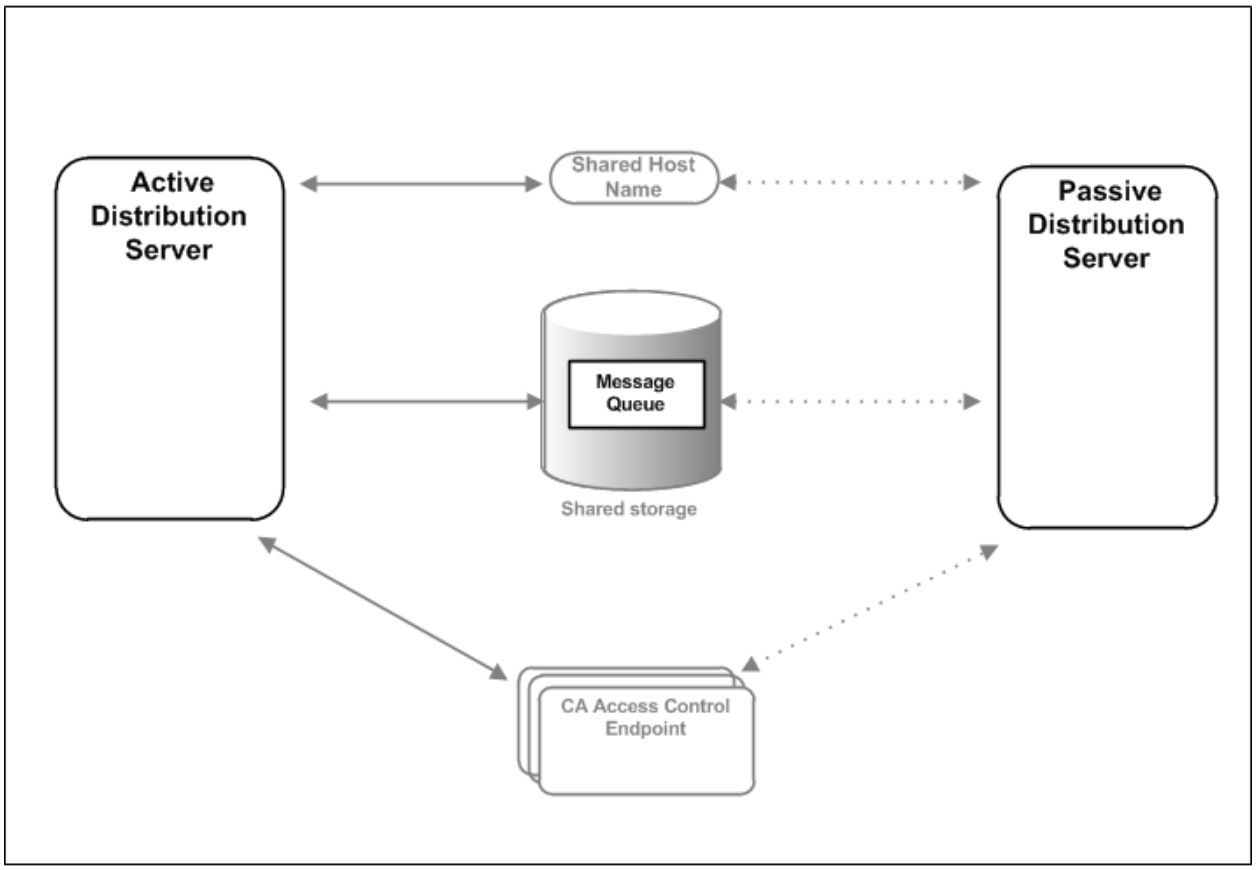
As illustrated in the preceding diagram, a high availability deployment has the following components:

- A primary Enterprise Management Server and at least one secondary Enterprise Management Server
- A clustered installation of a policy and reporting store and a user store
- Shared storage that is accessible by both the primary and secondary CA ControlMinder Enterprise Management servers
- A shared host name
- CA ControlMinder endpoints able to work with both the primary and secondary Enterprise Management Servers

Distribution Servers in a High Availability Environment Architecture

You can deploy additional Distribution Servers for high availability to prevent loss of audit events collected from the endpoints in an event of failure to the Distribution Server.

The following diagram shows an implementation of primary and secondary Distribution Servers in a high availability environment:



As illustrated in the previous diagram, a high availability implementation of the Distribution Server is based on the following:

- A primary Distribution Server and at least one secondary Distribution Server.
- A shared storage that holds the Message Queue data files and that is accessible by both the primary and secondary Distribution Servers.

  You place the Message Queue data files on the shared storage to verify that audit events messages that arrived form the endpoints are not lost if the Distribution Server fails.
- A shared host name.
- CA ControlMinder endpoints able to work with both the primary and secondary Distribution Servers.

Components of a High Availability Environment

You need the following to deploy CA ControlMinder in a high availability environment.

- Primary server:
  - Enterprise Management Server
- Secondary server:
  - Enterprise Management Server
- User repository
- Policy and reporting database
- Shared storage solution:
  - The cluster software
  - The shared storage

The Shared Storage

We recommend that you implement a shared storage solution using shared storage devices. The shared storage must be accessible to both the active and passive servers. Verify that the shared storage solution you use meets the following criteria:

- Write order—the shared storage solution must write data blocks to the shared storage in the same order as they occur in the buffer.
- Synchronous write persistence—upon return from a synchronous write call, the storage solution guarantees that all the data has been written to durable, persistent storage.

The following are examples of the software based shared storage solutions:

- Dual-Port SCSI device
- Storage Area Network (SAN)

Dual-Port SCSI and SAN solutions comply with the write order and synchronous write persistence requirements.

The Cluster Software

The cluster software enables servers across a network to work together in a computer cluster to provide application high availability.

Important! The steps described in this chapter apply to Microsoft cluster software and Active Directory only.

In a high availability deployment, the cluster software performs the following tasks:

- Monitors the status of the primary and secondary Enterprise Management Servers
- Verifies that only one instance, either the primary or secondary servers, is active at a time
- Manages the CA ControlMinder services on the Enterprise Management Servers
- Manages the shared host name that points the endpoints to the active server

What Happens In Case of a Failure?

In a high availability deployment, the clustering solution software queries the primary server for availability at a fixed interval. If the primary server fails to respond within the predefined period, the clustering solution software and CA ControlMinder do the following:

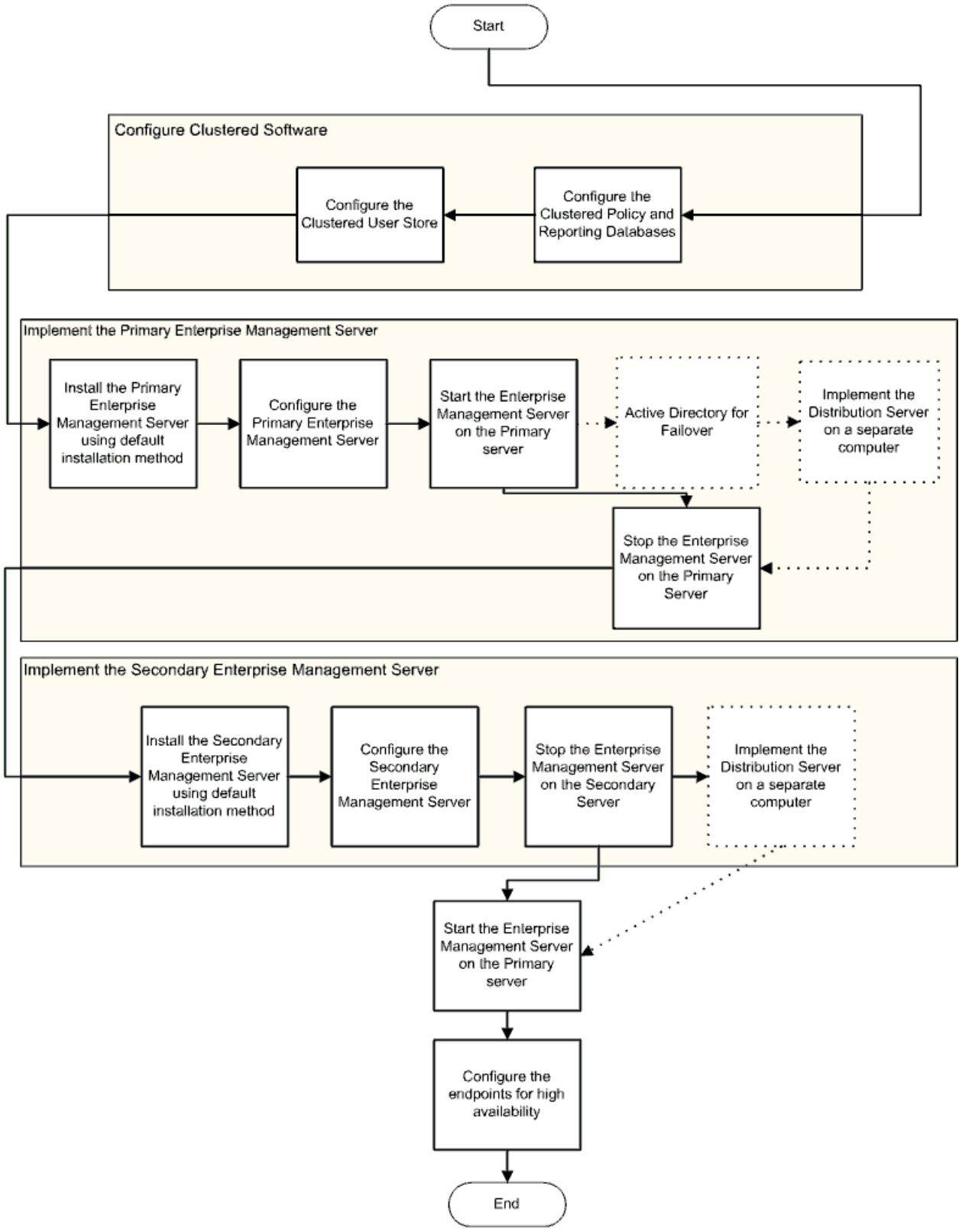
1. The clustering solution software stops all the Enterprise Management Server services running on the primary server.
2. The clustering solution software starts all the Enterprise Management Server services on the secondary server.
3. CA ControlMinder endpoints attempt to connect to the secondary server and continue working.
4. When the clustering software solution stops Enterprise Management Server services on the primary server, any users who are logged in to the application are logged out. To continue using the application, the users must log in to CA ControlMinder Enterprise Management again.

How to Configure CA ControlMinder Enterprise Management for High Availability

To correctly configure the high availability deployment, you must set up the primary and secondary Enterprise Management Servers in the correct order.

The following diagram shows the steps that you take to implement multiple Enterprise Management Servers in a high availability environment.

Note: Configuring Active Directory for failover and implementing the Distribution Servers on separate computers are optional steps.


Start
Configure Clustered Software
Configure the Clustered User Store
Configure the Clustered Policy and Reporting Databases
Implement the Primary Enterprise Management Server
Install the Primary Enterprise Management Server using default installation method
Configure the Primary Enterprise Management Server
Start the Enterprise Management Server on the Primary server
Active Directory for Failover
Implement the Distribution Server on a separate computer
Stop the Enterprise Management Server on the Primary Server
Implement the Secondary Enterprise Management Server
Install the Secondary Enterprise Management Server using default installation method
Configure the Secondary Enterprise Management Server
Stop the Enterprise Management Server on the Secondary Server
Implement the Distribution Server on a separate computer
Start the Enterprise Management Server on the Primary server
Configure the endpoints for high availability
End

More information:

How to Install the Enterprise Management Server Components (see page 62)
How to Set Up Reporting Service Server Components (see page 105)

Configure the Primary Enterprise Management Server

The primary Enterprise Management Server is the central management server and contains components and tools that let you deploy policies to endpoints, manage privileged accounts, and define resources, accessors, and access levels.

Follow these steps:

1. If you did not do so, install CA ControlMinder Enterprise Management on the primary server.

   All the web-based applications, the Distribution Server, the DMS, and CA ControlMinder are installed.

2. Stop all CA ControlMinder services.
3. Modify the services to start up manually and not automatically.
4. Copy the DMS and the DH to the shared storage as follows:

   a. Locate the DMS directory and copy it to the shared storage. This directory is located in the following location:

      `ACServerInstallDir/APMS/AccessControl/data/DMS__`

      ACServerInstallDir

      Defines the name of the directory where the Enterprise Management Server is installed.

   b. Locate the DH directory and copy it to the shared storage. This directory is located in the following location:

      `ACServerInstallDir/APMS/AccessControl/Data/DH__`

   c. Locate the DH__WRITER directory and copy it to the shared storage. By default this directory is located in the following location:

      `ACServerInstallDir/APMS/AccessControl/Data/DH__WRITER`

   d. Set the _pmd directory_ registry key configuration setting to the full pathname of the shared storage directory you copied the DMS and the DH to. For example: Z:\PMD.

   The primary server is configured to use the DMS and DH on the shared storage.

5. Configure the Message Queue to use the shared storage as follows:
   a. Move the following files to the shared storage: routes.conf, groups.conf, queues.conf, users.conf

      These files are located in the following directory:

      `ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data`

   b. Move the Message Queue datastore files to the shared storage. These files are located under the following directory: `ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data/datastore`

   c. Open the tibemsd.conf file for editing. This file is located by default in the following directory:

      `ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data`

      a. Set the location of the routes.conf, user.conf, groups.conf and queues.conf to the shared storage. For example: Z:/Tibco/users.conf

      b. Set the value of the "store" token to point to the directory on the shared storage where you copied the datastore files to. For example:Z:\PMD\DATASTORE

      c. Set the value of the "server" token to the cluster logical name in upper case without the suffix. For example: server=ENTMCLUSTER.

      d. Save and close the file.

   d. Open the queues.conf file for editing.

      a. Append a comma and add the word "store=$sys.failsafe" at the end of every queue definition line.

      b. Save and close the file.

6. Create a batch file to start all CA ControlMinder services when the primary Enterprise Management Server resumes operation, as follows:

```
seosd -start
net start acrptmq
net start "CA Access Control Web Service"
net start im_jcs
net start JBAS50SVC
```

7. Create a batch file to stop all CA ControlMinder service when the primary Enterprise Management Server fails, as follows:

```
secons -s

net stop acrptmq
net stop "CA Access Control Web Service"
net stop im_jcs
net stop JBAS50SVC
```

8. Configure the cluster software to run the scripts on failure.
9. Start all CA ControlMinder services

Example: Edit the queues.conf File

The following snippet from the queues.conf file is an example of how you amend the file to configure the Message Queue to use the shared storage.

```
queue/snapshots secure,store=$sys.failsafe
queue/audit secure,store=$sys.failsafe
ac_endpoint_to_server secure,store=$sys.failsafe
ac_server_to_endpoint secure,store=$sys.failsafe
```

Configure the Secondary Enterprise Management Server

The secondary Enterprise Management Server handles endpoint requests in an event of failure to the primary server.

Follow these steps:

1. If necessary, copy the FIPS key from the primary Enterprise Management Server to a temporary directory. The file is located in the following directory:

   `JBOSS_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/config/keys`

   JBOSS_HOME

   Defines the name of the directory where JBoss is installed.
2. Install the Enterprise Management Server on the secondary server from a Command Prompt window and specify the full pathname to the FIPS key on the primary Enterprise Management Server.

   All the web-based applications, the Distribution Server, the DMS, and CA ControlMinder are installed.
3. Stop all CA ControlMinder services.
4. Modify the services to start up manually and not automatically.
5. Set the *_pmd directory_* registry key configuration setting to the full pathname of the shared storage directory you copied the DMS and the DH to. For example: Z:\PMD.

   The secondary server is configured to use the DMS and DH on the shared storage.

6. Configure the Message Queue to use the shared storage. Do the following:

   a. Open the tibemsd.conf file for editing. This file is located by default in the following directory:

      ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

      ACServerInstallDir

      Defines the name of the directory where the Enterprise Management Server is installed.

      a. Set the location of the routes.conf, user.conf, groups.conf and queues.conf to the shared storage. For example: Z:/Tibco/users.conf

      b. Set the value of the "server" token to the cluster logical name in upper case without the suffix. For example: server=ENTMCLUSTER.

      c. Remove the following files: routes.conf, groups.conf, queues.conf, users.conf from the following directory:

      ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

      d. Set the value of the "*store*" token to point to the directory on the shared storage where you copied the datastore files to, for example: Z:\PMD.

      e. Save and close the file.

   b. Open the queues.conf file for editing.

   c. Append a comma and add the word "store=$sys.failsafe" at the end of every queue definition line, then save and close the file.

7. Verify that the CA ControlMinder services are not running.
8. Configure the DMS to authorize the secondary Enterprise Management Server, as follows:
   a. On the primary Enterprise Management Server, start the JCS, JBoss Application Server, CA ControlMinder and Message Queue services.
   b. Open a selang Command Prompt window and enter the following command:

      ```
      host DMS__@
      ```

      A message appears informing you that you are connected to the local host.
   c. Enter the following command to display the list of authorized terminals:

      ```
      sr TERMINAL *
      ```

      CA ControlMinder displays the details of the authorized terminals.
   d. Enter the following commands to add the secondary Enterprise Management Server to the authorized terminals list:

      ```
      newres TERMINAL
      <secondary_enterprise_management_server_full_DN> audit (f)
      owner(nobody)defacc(r)
      authorize TERMINAL
      <secondary_enterprise_management_server_full_DN>
      uid(+reportagent) access(write)
      authorize TERMINAL
      <secondary_enterprise_management_server_full_DN>
      uid(DOMAIN\Administrator) access(write,read)
      authorize TERMINAL
      <secondary_enterprise_management_server_full_DN>
      uid(ac_entm_pers) access(write,read)
      ```
9. Create a batch file to start all CA ControlMinder services in case the primary Enterprise Management Server fails, as follows:

   ```
   seosd -start
   net start acrptmq
   net start "CA Access Control Web Service"
   net start im_jcs
   net start JBAS50SVC
   ```
10. Create a batch file to stop all CA ControlMinder service when the primary Enterprise Management Server resumes operation, as follows:

    ```
    secons -s
    net stop acrptmq
    net stop "CA Access Control Web Service"
    net stop im_jcs
    net stop JBAS50SVC
    ```
11. Configure the Microsoft cluster software to run the scripts on failure.

    You have configured the secondary Enterprise Management Server.

Configure a Load Balancing Enterprise Management Server for High Availability

After you configure the primary and secondary Enterprise Management Servers for high availability, you can install and configure the Load Balancing Enterprise Management Servers for high availability.

Note: Verify that you can resolve the fully qualified DNS name of the cluster before you install the Load Balancing Enterprise Management Server.

To Install the Load Balancing Enterprise Management Server follow the procedure for installing the primary Enterprise Management Server.

Important! Select the Load Balancing Enterprise Management Server when prompted by the installation wizard. When prompted for the primary Enterprise Management Server information you must provide the cluster logical name. Do not specify an IP address.

Configure Active Directory for Failover

If you use Active Directory as the user store, you can configure the Enterprise Management Server to work with multiple Domain Controllers. If the primary Domain Controller fails, another Domain Controller takes over and continues to service client requests.

Follow these steps:

1. Enable the CA IdentityMinder Management Console (see page 87).

   You use the CA Identity Manager Management Console to configure the list of Domain Controllers in the environment.

2. Open the CA IdentityMinder Management Console (see page 88).

3. Click Directories, then select click ac-dir environment.

   The Directory Properties window appears.

4. Click Export and save the XML file.

5. Open the XML file for editing. Locate the <Connection host= *host_name*> tag. For example:

   ```
   <Connection host="primaryDir.com" port="389">
   ```

6. Append the string "**failover**" to the end of the line and specify the host name and port number of your Domain Controllers in a space separated list, then save the file. For example:

   ```
   <Connection host="ADserver1" port="389"
   failover="ADserver2:389"/>
   ```

7. In the Management Console, click Update.

   The Update Directory window opens.

8. Enter the full pathname of the XML file that you edited, or browse for the file, then click Finish.

   Status information is displayed in the Directory Configuration Output field.

9. Click Continue, and restart the environment.

   The Enterprise Management Server can now work with the primary and secondary Domain Controllers.

Configure CA ControlMinder Enterprise Management with Local DMS

Configuring the DMS on the Enterprise Management Server to connect to the DMS using "localhost" rather than the fully qualified domain name.

To configure CA ControlMinder Enterprise Management with local DMS

1. Log into CA ControlMinder Enterprise Management, then select System, DMS, Modify Connection.

   The Modify Connection:Search Connection windows appears.

2. Search for the default DMS connection and click Select.

   The Modify Connection:*ConnectionName* window opens.

3. Modify the Host Name to LocalHost, as follows:

   ```
   DMS__@localhost
   ```

4. Click Submit.

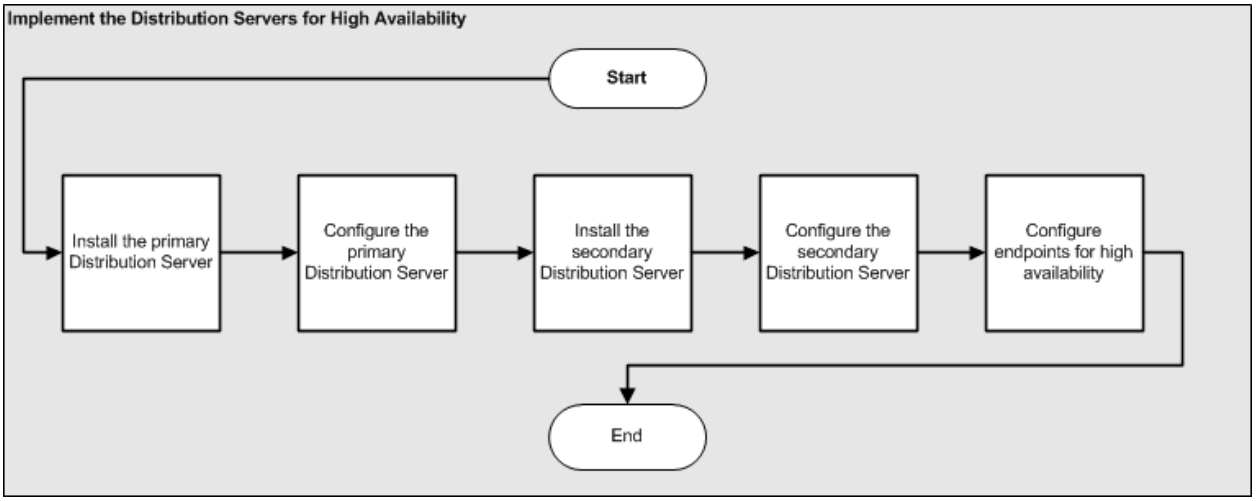
   The primary and secondary Distribution Hosts can now share the DMS computer.

How to Configure the Distribution Servers for High Availability

To correctly configure multiple Distribution Servers in a high availability environment, set up the primary and secondary Distribution Servers in the correct order.

The following diagram shows the steps that you take to set up multiple Distribution Servers to work with one Enterprise Management Server.

Important! Complete the following steps only if you integrate CA ControlMinder Enterprise Management with CA User Activity Reporting Module. Configure the Distribution Servers for high availability to avoid losing all the events that the failed Distribution Server collected and did not send to the Enterprise Management Server and to the CA User Activity Reporting Module.



More information:

Install the Distribution Server (see page 436)

Configure the Primary Distribution Server

The Distribution Server handles communication between the Application Server and the endpoints.

You should complete this procedure if you install standalone Distribution Servers only.

Follow these steps:

1. From the Services window, stop the JCS, CA ControlMinder and Message Queue Server services.
2. Modify the services to start up manually and not automatically.
3. Create the PMD directory on the shared storage.
4. Configure the Distribution Host to use the shared storage, as follows:
   a. Copy the DH directory to the shared storage. This directory is located in the following location:

      DistServerInstallDir/APMS/AccessControl/Data/DH__

      DistServerInstallDir

      Defines the name of the directory where you installed the Distribution Server.

   b. Copy the DH__WRITER directory to the shared storage. This directory is located in the following location:

      DistServerInstallDir/APMS/AccessControl/Data/DH__WRITER

   c. Copy the DMS__ directory to the shared storage. This directory is located in the following location:

      DistServerInstallDir/APMS/AccessControl/Data/DMS__

   d. Set the *_pmd_directory_* registry key, under *ComputerAssociates**AccessControl**PMD*, configuration setting to the full pathname of the shared storage directory you copied the DMS and DH to. For example: Z:\PMD.

   The primary server is configured to use the DMS and DH on the shared storage.

5. Configure the Message Queue to use the shared storage, as follows:
   a. Create a directory on the shared storage. For example: Z\MessageQueue
   b. Copy the Message Queue datastore files to the shared storage. These files are located in the following directory:

      DistServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

   c. Open the tibemsd.conf file for editing. This file is located in the following directory:

      DistServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

   d. Set the value of the "*store*" token to point to the directory on the shared storage where you copied the datastore files to. For example: F:\MessageQueue.
   e. Save and close the file.
   f. Open the queues.conf file for editing.
   g. Append a comma and add the word "store=$sys.failsafe" to the end of every queue definition line, then save the file.
6. Start the CA ControlMinder services.

Example: Edit the queues.conf File

The following snippet from the queues.conf file shows you how amend the file to configure the Message Queue to use the shared storage.

```
queue/snapshots secure,store=$sys.failsafe
queue/audit secure,store=$sys.failsafe
ac_endpoint_to_server secure,store=$sys.failsafe
ac_server_to_endpoint secure,store=$sys.failsafe
```

Configure the Secondary Distribution Server

The secondary Distribution Server handles communication between the Application Server and the endpoints in case the active Distribution Server fails to respond within a predefined interval.

Follow these steps:

1. Stop the JCS, CA ControlMinder and Message Queue Server services.
2. Modify the services to start up manually and not automatically.
3. Set the *_pmd_directory_* registry key, under *\ComputerAssociates\AccessControl\PMD*, configuration setting to the full pathname of the shared storage directory you copied the DMS and DH to. For example: Z:\PMD.

   The secondary Distribution Server can now access the DMS and DH files on the shared storage. You have configured the Distribution Host to use the shared storage.
4. Configure the Message Queue to use the shared storage, as follows:
   a. Open the tibemsd.conf file for editing. This file is located in the following directory:

      DistServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

      DistServerInstallDir

      Defines the name of the directory where you installed the Distribution Server.

   b. Set the value of the "*store*" token to point to the directory on the shared storage where you copied the datastore files to, for example: Z:\Datastore.
   c. Save and close the file.
   d. Open the queues.conf file for editing.
   e. Append a comma and add the word "store=$sys.failsafe" at the end of every queue definition line, then save the file.
5. Verify that the CA ControlMinder services on the secondary server are stopped.

Configure Endpoints for High Availability

After you installed and configured the primary and secondary Enterprise Management Servers, you set up the CA ControlMinder endpoints to work in a high availability environment.

To configure endpoints for high availability

1. Install CA ControlMinder with the Advanced Policy Management Client feature enabled on the endpoint.

   The CA ControlMinder endpoint is installed.

2. Open a command prompt window on the endpoint and enter the following command:

   `dmsmgr –config -dhname` *names*

   This command configures the endpoint to work with the comma-separated list of Distribution Hosts.

   Note:For more information about the dmsmgr utility, see the *Reference Guide*.

3. Set the *Distribution_Server* configuration setting to list the Distribution Servers, separated by a comma:

   `ssl://ds1.sample.com:7243, ssl://ds2.sample.com:7243`

4. Save the settings.

   You have configured a list of Distribution Hosts and Distribution Servers with which the endpoint can communicate. The endpoint can now work in a high availability environment.

Example: Configure a List of Distribution Servers

The following example shows you how to configure a list of Distribution Servers for high availability.

During the installation of the endpoint, you are asked to enter the parameters of the Distribution Server that the endpoint communicates with. By default, this is the Enterprise Management Server. For high availability, you configure the endpoint to use the secondary Distribution Server when the primary Distribution Server fails.

1. Enter the names of the primary and secondary Distribution Servers:

   ```
   dmsmgr -config -dhname DH__@node1.computer.com,DH__@node2.computer.com
   ```

   A message appears confirming the action.

2. Specify the list of primary and secondary Distribution Server URLs.
   - UNIX: Modify the Distribution_Server parameter in the [communication] section of accommon.ini file.
   - Windows: Modify the Distribution_Sever value the Windows Registry. This parameter is found in:

     ```
     HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\common\
     communication
     ```

More information:

Installing and Customizing a UNIX Endpoint (see page 175)
Installing and Customizing a Windows Endpoint (see page 143)

Oracle RAC Configuration for High Availability

If you are using Oracle as the policy and reporting database, you can configure Oracle for high availability using Oracle RAC.Oracle Real Applications Cluster (RAC) is a cluster database based on a shared disc architecture that provides high availability for Oracle databases.

Example: Configuring CA ControlMinder Enterprise Management for High Availability using Oracle RAC

The following example explains how you configure CA ControlMinder Enterprise Management to use Oracle RAC for high availability.

1. Prepare the Oracle database for Enterprise Management.

   You create a user account on the Oracle RAC server and assign the user privileges to install CA ControlMinder Enterprise Management.

2. Implement CA ControlMinder Enterprise Management for high availability.

   Install and configure the Primary and Secondary Enterprise Management Servers.

   Note: Specify the logical name of the Oracle RAC in the Host Name and the shared service name in the Service Name field.

3. Verify that the Oracle RAC host name resolves correctly.

   Map the host IP address to the logical name of the Oracle RAC. For example:

   ```
   11.11.111.11  Node1MachineName
   11.11.111.12  Node2MachineName
   11.11.111.11  Node1LogicalMachineName
   11.11.111.12  Node2LogicalMachineName
   ```

4. Modify the Primary and Secondary Enterprise Management Servers settings to use Oracle RAC. Do the following:

   a. Stop the JBoss application server.

   b. Navigate to the following path, where JBoss_HOME indicates the directory where you install JBoss:

      ```
      JBoss_HOME/server/default/deploy
      ```

5. Open the following files for editing:

   ```
   imauditdb-ds.xml
   imtaskpersistencedb-ds.xml
   imworkflowdb-ds.xml
   objectstore-ds.xml
   reportsnapshot-ds.xml
   ```

6. In each file, locate the <connection-url> tag and specify the host names and service name as follows:

   ```
   <connection-url>jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=off)(FAILOVER=on
   )(ADDRESS_LIST=(ADDRESS=(protocol=tcp)(host=Node1LogicalMachineName)(port=152
   1))(ADDRESS=(protocol=tcp)(host=
   Node2LogicalMachineName)()(port=1521)))(CONNECT_DATA=(SERVER=DEDICATED)(SERVI
   CE_NAME=SharedService)))</connection-url>
   ```

7. In each file, add the following line:

   ```
   <check-valid-connection-sql>select 1 from dual</check-valid-connection-sql>
   ```

8. Save and close the files.

9. Start the JBoss application server.

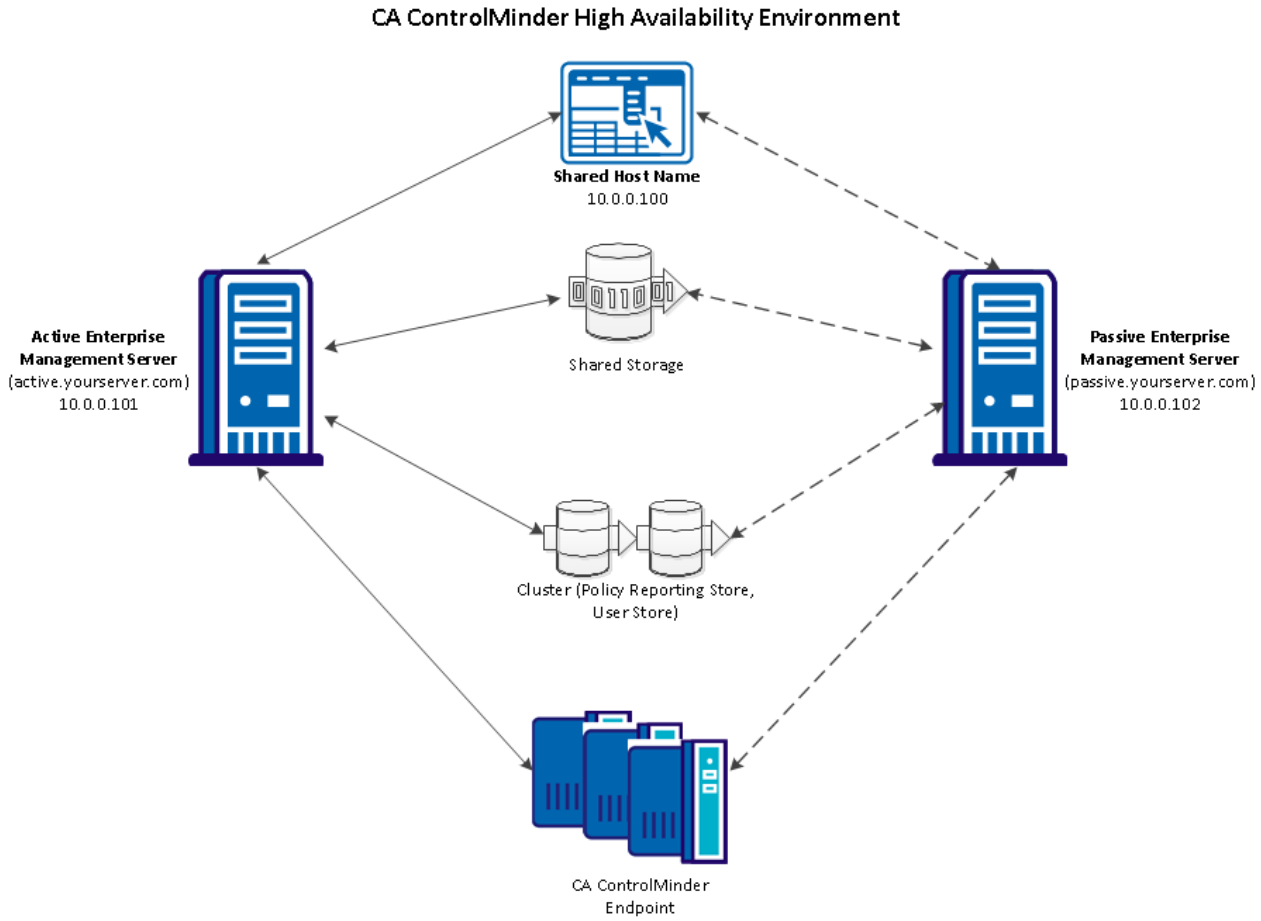
   You have configured the Primary and Secondary Enterprise Management Servers.

Implementing CA ControlMinder High Availability on Linux Using Veritas Cluster Server

A High Availability deployment ensures that your CA ControlMinder Enterprise Management components continue to service requests if one or more components or servers fail. If the endpoints cannot connect to the primary environment, they connect to a secondary server until the primary environment is restored.

Your primary and secondary CA ControlMinder Enterprise Management Servers are located in the same datacenter accessing the shared hostname. If the primary environment fails, then the Veritas Cluster software enables switching the services and the secondary environment takes control.

The following diagram shows CA ControlMinder Enterprise Management in a High Availability environment.

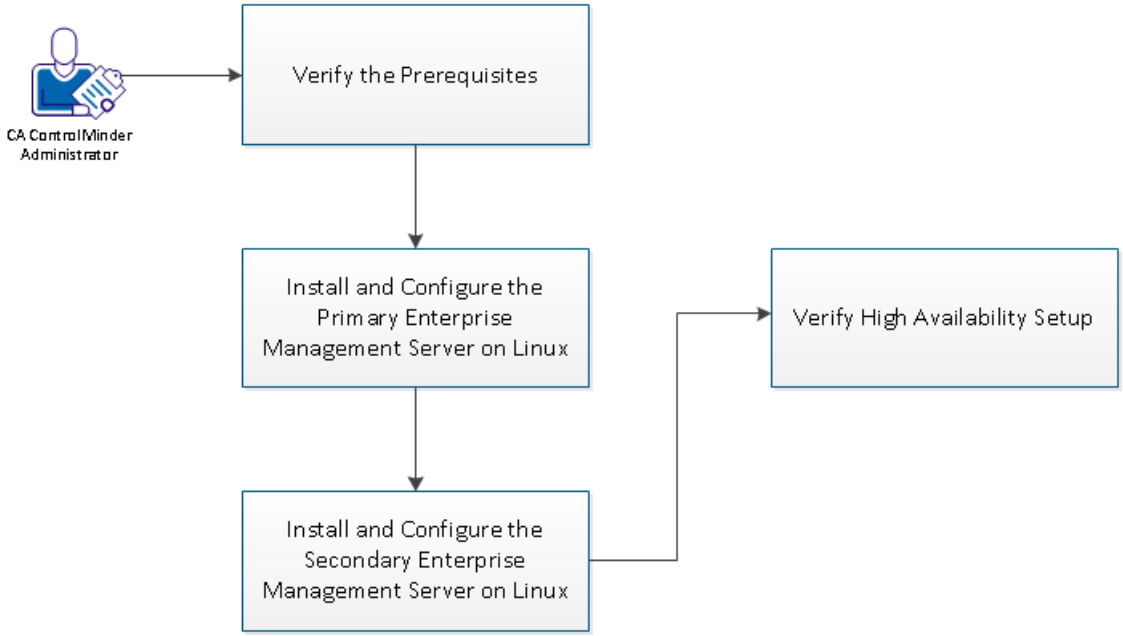


As illustrated in the preceding diagram, a High Availability deployment has the following components:

- A primary (active) Enterprise Management Server and at least one secondary(passive) Enterprise Management Server.
- A clustered installation of a policy and reporting store and a user store.
- Shared storage that is accessible by both the primary and secondary CA ControlMinder Enterprise Management Servers.
- A shared host name.
- CA ControlMinder endpoints able to work with both the primary and secondary Enterprise Management Servers.

The following diagram shows the process to configure CA ControlMinder High Availability on Linux using the Veritas Cluster Server.

Implementing CA ControlMinder High Availability on Linux Using Veritas Cluster Server



Perform the following steps:

1. Verify the prerequisites (see page 410).
2. Configure the Primary Enterprise Management Server on Linux (see page 411).
3. Configure the Secondary Enterprise Management Server on Linux (see page 419).
4. Verify the High Availability setup (see page 422).

Verify the Prerequisites

Verify the following prerequisites before implementing CA ControlMinder High Availability on Linux using the Veritas Cluster Server:

1. Two similar nodes with the supported OS version and 2 NICs (Network Interface Controller) are available.
2. Verify that the primary and secondary CA ControlMinder Enterprise Management Servers are installed.

   Note: For more information about installing the Enterprise Management Server on Linux, refer the Implementation Guide.
3. Verify that shared storage is accessible by each node. We recommend 4-5 disks or LUNs (Logical Unit Number) are shared across the two nodes.
4. Verify that the Linux Veritas Cluster Server is installed and the scripts ready for an automatic switch over.

   Note: For more information about installing the Veritas Cluster Server, see the Linux 5.1 Veritas Cluster Server Installation Guide on the Symantec website.

Configure the Primary Enterprise Management Server

The primary Enterprise Management Server is the central management server and contains components and tools that let you deploy policies to endpoints, manage privileged accounts, and define resources, accessors, and access levels.

Note: This procedure assumes that you have installed the primary Enterprise Management server and all the web-based applications, the Distribution Server, and the DMS.

Follow these steps:

1. Verify that CA ControlMinder services are started.

   CA ControlMinder Enterprise Management requires that CA ControlMinder is running.

2. Verify that JBoss Application Server service is started. If the JBoss Application Server services are not started, enter the following command:

   ```
   ./JBOSS_DIR/bin/run.sh -b 0.0.0.0
   ```

   When the JBoss Application Server completes loading, you can log in to the CA ControlMinder Enterprise Management web-based interface.

3. Configure the DMS to authorize the secondary Enterprise Management Server, as follows:

   a. On the primary Enterprise Management Server, start the JCS, JBoss Application Server, CA ControlMinder, and Message Queue daemons.

   b. Open a selang Command Prompt window and enter the following command:

      ```
      host DMS__@
      ```

      A message appears informing you that you are connected to the local host.

   c. Enter the following command to display the list of authorized terminals:

      ```
      sr TERMINAL *
      ```

      CA ControlMinder displays the details of the authorized terminals.

   d. Enter the following commands to add the secondary Enterprise Management Server to the authorized terminals list:

      ```
      newres TERMINAL
      <secondary_enterprise_management_server_full_DN> audit (f)
      owner(nobody)defacc(r)
      authorize TERMINAL
      <secondary_enterprise_management_server_full_DN>
      uid(+reportagent) access(write)
      authorize TERMINAL
      <secondary_enterprise_management_server_full_DN>
      uid(DOMAIN\Administrator) access(write,read)
      ```

```
authorize TERMINAL
<secondary_enterprise_management_server_full_DN>
uid(ac_entm_pers) access(write,read)
```

4. Run the following commands to modify the host name that CA ControlMinder uses to distribute policies:

   ```
   sepmd -u DH__WRITER DMS__@<node1 host name>
   sepmd -s DH__WRITER DMS__@<cluster shared DNS NAME>
   sepmd -u DMS__ DH__@<node1 host name>
   sepmd -s DMS__ DH__@<cluster shared DNS NAME>
   ```

5. Stop all CA ControlMinder daemons.
6. Modify the services to start up manually (see page 415) and not automatically.
7. Copy the DMS and the DH to the shared storage as follows:
   a. Copy the DMS directory to the shared storage, for example: /shared/AccessControlServer/. The directory is located in the following location:

      ACServerInstallDir/APMS/AccessControl/policies/DMS__

      ACServerInstallDir

      Defines the name of the directory where you installed the Enterprise Management Server.

   b. Copy the DH directory and to the shared storage. The directory is located in the following location:

      ACServerInstallDir/APMS/AccessControl/policies/DH__

   c. Copy the DH__WRITER directory to the shared storage. The directory is located in the following location:

      ACServerInstallDir/APMS/AccessControl/policies/DH__WRITER

   d. Open the seos.ini file for editing. This file is located in the following location:

      ACServerInstallDir/APMS/AccessControl

   e. Set the _pmd directory_ token configuration setting to the full pathname of the shared storage directory you copied the DMS and the DH to. For example: /shared/AccessControlServer/

   The primary server is configured to use the DMS and DH on the shared storage.
8. Configure the Message Queue to use the shared storage as follows:

a. Move the Message Queue datastore files to the shared storage. These files are located under the following directory:
ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data/datastore

The following is an example to copy Message Queue datastore files:

```
# cp -r
/opt/CA/AccessControlServer/MessageQueue/tibco/cfgmgmt/ems/
data /shared/MessageQueue/data/
```

b. Open the tibemsd.conf file for editing. This file is located by default in the following directory:

ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

a. Set the location of the routes.conf, user.conf, groups.conf, and queues.conf to the shared storage. For example: /shared/MessageQueue/data/users.conf

b. Set the value of the *store* token to point to the directory on the shared storage where you copied the datastore files to. For example: /shared/MessageQueue/data/datastore.

c. Set the value of the *server* token to the cluster logical name in upper case without the suffix. For example: server=ENTMCLUSTER.

d. Save and close the file.

c. Open the queues.conf file for editing.

a. Append a comma and add the word *store=$sys.failsafe* at the end of every queue definition line.

b. Save and close the file.

d. Open the routes.conf file for editing and comment the following:

```
# vi shared/MessageQueue/data/routes.conf

#[EMS-SERVER2]

# url=tcp://7022
```

e. Modify the Tibco folders so that Tibco users have read and write access.

a. Create the Tibco group with gid 65534. The following is an example to create the Tibco folder:

```
# groupadd -g 65534 tibco
```

b. Create the Tibco user with uid 65534. The following is an example to create the Tibco user:

```
# useradd -g 65534 -u 65534 tibco
```

c. Change ownership of MessageQueue directory and all subdirectories. The following is an example to change ownership of MessageQueue directory and all subdirectories:

```
#chown -R tibco /shared/MessageQueue
```

d. Change permissions of MessageQueue directory and all subdirectories. The following is an example to change permissions of MessageQueue directory and all subdirectories:

```
#chmod -R u=rwx,go= /shared/MessageQueue
```

e. Change Default Tibco directory permissions to allow rwx access only to the Tibco user. The following is an example to change the directory permissions to allow rwx access only to the Tibco user:

```
#chown -R tibco /opt/CA/AccessControlServer/MessageQueue/
```

```
#chmod -R u=rwx,go= /opt/CA/AccessControlServer/MessageQueue/
```

9. Modify the base URL (see page 416) to the cluster name in the CA Identity Minder Management Console.
10. Create a batch file to stop all CA ControlMinder services (see page 417) when the primary Enterprise Management Server fails.
11. Create a batch file to start all CA ControlMinder services (see page 417) when the primary Enterprise Management Server resumes operation.
12. Create a batch file to check the status of CA ControlMinder services (see page 418).
13. Configure the cluster software to run the scripts on failure.
14. Start all CA ControlMinder services.

You have configured the primary Enterprise Management Server. Proceed to configure the secondary Enterprise Management Server.

Modify Services to Start Manually

Modify the services to start manually by using the chkconfig command on the Primary and the Secondary Enterprise Management Servers. The following snippet is an example of the chkconfig script:

```
# chkconfig --list im_jcs

im_jcs          0:off   1:off   2:on    3:on    4:on    5:on    6:off

# chkconfig im_jcs off

# chkconfig --list im_jcs

im_jcs          0:off   1:off   2:off   3:off   4:off   5:off   6:off

# chkconfig --list ca-acrptmq

ca-acrptmq      0:off   1:off   2:on    3:on    4:on    5:on    6:off

# chkconfig ca-acrptmq off

# chkconfig --list ca-acrptmq

ca-acrptmq      0:off   1:off   2:off   3:off   4:off   5:off   6:off
```

--list *name*

This option lists all of the services which chkconfig knows about, and whether they are stopped or started in each run level. When you specify the *name*, the service name information is displayed.

Modify Base URL

Modify the base URL to the cluster name in the CA Identity Minder Management Console.

Follow these steps:

1. Verify that CA Identity Minder Management Console has been enabled.

   Note: For more information about enabling CA Identity Minder Management Console, see the Enable the CA Identity Minder Management Console topic in the Implementation Guide.

2. Open the CA Identity Minder Management Console, open a web browser, and enter the following URL, for your host:

   `http://enterprise_host:port/idmmanage`

   The CA Identity Minder Management Console opens.

3. Click Environments.

   The Environments page lists the Identity Manager environment.

4. Select the environment.

   The Environment Properties page opens.

5. Modify the Base URL to the Cluster name. For example, https://clusterentm.ca.com.

   Click Save.

Create Batch File to Stop CA ControlMinder Services

Create a batch file to stop all CA ControlMinder Services on the Primary and the Secondary Enterprise Management Servers.. The following example stops the Message Queue, Java Connector Service (JCS), and the JBoss:

```
#!/bin/sh
#To Stop the AccessControl Services
/opt/CA/AccessControlServer/APMS/AccessControl/bin/secons -sk

#To Stop the CA ControlMinder Message Queue
#/etc/init.d/ca-acrptmq stop
su - tibco -c "/etc/init.d/ca-acrptmq stop"

#To Stop the Web Services
/opt/CA/AccessControlServer/APMS/AccessControl/bin/secons -S
"eacws"

#To Stop Java Connector Service JCS
/etc/init.d/im_jcs stop

#To Stop JBOSS
cd /opt/jboss-4.2.3.GA/bin/
/opt/jboss-4.2.3.GA/bin/shutdown.sh -S &
sleep 60
```

Create Batch File to Start CA ControlMinder Services

Create a batch file to start all CA ControlMinder Services on the Primary and the Secondary Enterprise Management Servers. The following example starts the Message Queue, Java Connector Service (JCS), and the JBoss:

```
#!/bin/sh
#To Start the AccessControl Services
/opt/CA/AccessControlServer/APMS/AccessControl/bin/seload

#To Start the CA ControlMinder Message Queue
#/etc/init.d/ca-acrptmq start
su - tibco -c "/etc/init.d/ca-acrptmq start" &
sleep 10

#To Start Java Connector Service JCS
/etc/init.d/im_jcs start

#To Start JBOSS
cd /opt/jboss-4.2.3.GA/bin/
/opt/jboss-4.2.3.GA/bin/run.sh -b 0.0.0.0 &
sleep 9
```

Create Batch File to Check Status of CA ControlMinder Services

Create a batch file to check the status for all CA ControlMinder Services on the Primary and Secondary Enterprise Management Servers.

Note: Customize the script based on your requirement. The exit codes that are used in the example are based on the Veritas setup, for more information about the codes, refer the Symantec Support website.

The following is an example to check the status for all CA ControlMinder Services:

```
#!/bin/sh

a=1;
b=1;
c=1;
d=1;
#CA Control Minder Status check using the Process SEOSD status
ps -ef | grep -v grep| grep seosd >/dev/null 2>&1;
a=$?;

#JCS running status check
b=`/etc/init.d/im_jcs status`;
if [ "$b" == "jcs is running" ];
then
b=0;
else
b=1;
fi

#CA ControlMinder Message Queue status check
c=`/etc/init.d/ca-acrptmq status`
if [ "$c" = "CA ControlMinder Message Queue is running" ];
then
c=0;
else
c=1;
fi

#JBOSS running status check
ps -ef | grep -v grep| grep run.sh >/dev/null 2>&1;
d=$?

#echo "$a $b $c $d"  #To Check the Individual process Status All Zeros
Means All Services are up and running and All Ones Means All Services
are down

#Script status will return '110' when all the services are up and
running, will return '100' when all services are down and will return
'1' when anyone of the service is down
```

```
if [ "$a$b$c$d" = "0000" ];
then
exit 110

elif [ "$a$b$c$d" = "1111" ];
then
exit 100

else
exit 1
fi
```

Configure the Secondary Enterprise Management Server

The secondary Enterprise Management Server handles endpoint requests in an event of failure to the primary server.

Follow these steps:

1. Copy the FIPS key from the primary Enterprise Management Server to a temporary directory. The file is located in the following directory:

   `JBOSS_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/config/keys`

   JBOSS_HOME

   Defines the name of the directory where JBoss is installed.

2. Install the Enterprise Management Server on the secondary server from a Command Prompt window and specify the full pathname to the FIPS key on the primary Enterprise Management Server.

   Note: Verify that the same database and communication password details are the same as used for the primary Enterprise Management Server.

   All the web-based applications, the Distribution Server, the DMS, and CA ControlMinder are installed.

3. Stop all CA ControlMinder daemons.

4. Modify the services to start up manually (see page 415) and not automatically.

5. Set the *_pmd directory_* token configuration setting to the full pathname of the shared storage directory you copied the DMS and the DH to. For example: /shared/AccessControlServer/.

   The secondary server is configured to use the DMS and DH on the shared storage.

6. Configure the Message Queue to use the shared storage. Do the following:

   a. Open the tibemsd.conf file for editing. This file is located by default in the following directory:

      ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

      ACServerInstallDir

      Defines the name of the directory where you installed the Enterprise Management Server.

      The following is an example to copy Message Queue datastore files:

      ```
      # cp -r
      /opt/CA/AccessControlServer/MessageQueue/tibco/cfgmgmt/ems/
      data /shared/MessageQueue/data/
      ```

      a. Set the location of the routes.conf, user.conf, groups.conf and queues.conf to the shared storage. For example: /shared/MessageQueue/data/users.conf.

      b. Set the value of the *server* token to the cluster logical name in upper case without the suffix. For example: server=ENTMCLUSTER.

      Note: The installation writes the computer name as the original value. The value should be changed to a short name of the cluster, without the domain name, in upper case. If the cluster DNS name is “entmcluster.ca.com” then specify ENTMCLUSTER.

      c. Remove the following files: routes.conf, groups.conf, queues.conf, users.conf from the following directory:

      ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

      d. Set the value of the *store* token to point to the directory on the shared storage where you copied the datastore files to, for example: /shared/MessageQueue/datastore.

      e. Save and close the file.

b. Modify the Tibco folders so that Tibco users have read and write access.

   a. Create Tibco group with gid 65534. The following is an example to create Tibco folder:

   ```
   # groupadd -g 65534 tibco
   ```

   b. Create Tibco user with uid 65534. The following is an example to create Tibco user:

   ```
   # useradd -g 65534 -u 65534 tibco
   ```

   c. Change Default Tibco directory permissions to allow rwx access only to the Tibco user. The following is an example to change the directory permissions to allow rwx access only to the Tibco user:

   ```
   #chown -R tibco /opt/CA/AccessControlServer/MessageQueue/
   ```

   ```
   #chmod -R u=rwx,go= /opt/CA/AccessControlServer/MessageQueue/
   ```

7. Verify that the CA ControlMinder daemons are not running.
8. Create a batch file to start all CA ControlMinder services (see page 417) in case the primary Enterprise Management Server fails.
9. Create a batch file to stop all CA ControlMinder services (see page 417) when the primary Enterprise Management Server resumes operation.
10. Create a batch file to check the status of CA ControlMinder (see page 418) services.
11. Configure the cluster software to run the scripts on failure.

    You have configured the secondary Enterprise Management Server.

Verify High Availability Setup

Verify that the CA ControlMinder High Availability setup is working correctly.

Follow these steps:

1. Log in to the primary Enterprise Management Server and perform the following steps:
   a. Verify that CA ControlMinder, JBoss, and the Message Queue services are started and running.
   b. Verify that the DMS and Tibco resources are shared with the primary Enterprise Management Server.
   c. Open the server.log file and review it for errors:

      JBossInstallDir/server/default/log/server.log

      This file lists the actions that JBoss performs in the JBoss web application server environment.

      Note: JBoss creates to new server.log file each time you start it.
   d. Shut down the primary Enterprise Management Server by stopping the CA ControlMinder, JBoss, and Message Queue services.
2. Log in to the secondary Enterprise Management Server and perform the following steps:
   a. Verify that the shared resources are shared with the secondary Enterprise Management Server.
   b. Start the CA ControlMinder, JBoss, and Message Queue daemons.
   c. Open the server.log file and review it for errors:

      JBossInstallDir/server/default/log/server.log
3. Log in to CA ControlMinder Enterprise Management and perform the following steps:
   a. Verify that the primary and secondary Enterprise Management Servers are visible in the World View, Hosts section.
   b. Verify that the primary and secondary Enterprise Management Servers are visible in the Privileged Accounts, View Endpoint section.
   c. Verify that the primary and secondary Enterprise Management Servers are visible in the System, Connector Server, View Connector Server section.
4. Perform various actions on the secondary Enterprise Management Server and verify the event in the primary Enterprise Management Server.

If no errors occur, you have successfully configured CA ControlMinder High Availability.

Appendix A: Troubleshooting

This section contains the following topics:

Tibco User Cannot Start Tibco Services

Symptom:

The Tibco user is unable to start Tibco services.

Solution:

Verify the following conditions:

- The Tibco user exists on the Primary and Secondary Enterprise Management Servers.
- The Tibco user has rwx permissions for the /shared/MessageQueue folder and the /opt/CA/AccessControlServer/MessageQueue folder.
- The store value in the tibemsd.conf is mapped to the datastore in the /shared/MessageQueue/data/datastore folder.
- The users, groups, topics, queues, and routes are mapped to the /shared/MessageQueue/data folder.

JCS Cannot Connect to the Host

Symptom:

The JCS on the secondary Enterprise Management Server cannot connect to the Host.

Solution:

This issue occurs if you do not start JBoss after the installation on the secondary Enterprise Management Server. The JCS registration message expires and the Connector Server is not visible.

To resolve this issue, copy the Connector Server from the primary Enterprise Management Server and modify the host details.

JBoss Errors in the queues.conf File

Symptom:

The queues.conf file displays one of the following JBoss error messages:

```
Reconnect failed
```

```
javax.naming.NameNotFoundException
```

Solution:

These errors occur if the queues.conf file is not configured properly. To resolve this issue, verify that the queues.conf file is shared from the primary and secondary Enterprise Management Server.

Chapter 12: Installing a Disaster Recovery Deployment

This section contains the following topics:

Disaster Recovery Overview

Disaster recovery lets you restore your system after a subsystem crash or other catastrophic failure occurs.

The goal of disaster recovery is to restore as much data as possible, and to limit the resources needed during the backup and restore phases.

More information:

Disaster Recovery

A disaster recovery deployment makes it easier to restore the Enterprise Management Server in the event of a catastrophic system failure. If the CA ControlMinder and SAM endpoints cannot connect to the production environment, they connect to the disaster recovery environment until the production environment is restored.

A disaster recovery deployment has the following benefits:

- The database of the disaster recovery DMS is a duplicate of the production DMS database. This means that you have a copy of your policies if the production DMS database becomes corrupt.
- An endpoint can connect to the production or disaster recovery environment. If the production environment goes down, an endpoint sends data to the disaster recovery environment, so information about policy status and deviations is not lost in the event of a catastrophic system failure.
- You do not have to re-subscribe each endpoint after you have recovered from a disaster.

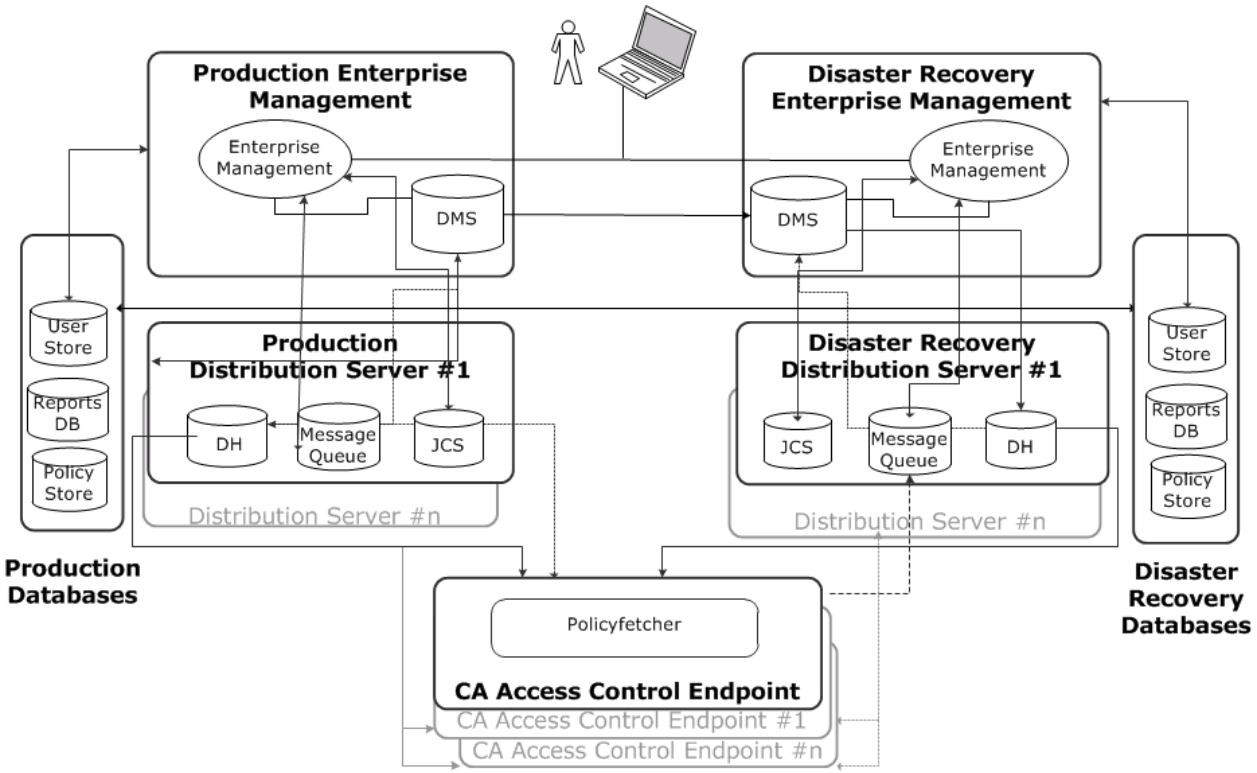
The following CA ControlMinder components are not backed up or restored during the disaster recovery process. Back up these components separately:

- Password policy models
- PMDBs
- RDBMSs
- CA ControlMinder Endpoint Management
- CA ControlMinder Enterprise Management
- data on the endpoints
- CA ControlMinder audit files
- The CA ControlMinder endpoints
- Reports
- Message Queue
- CA Business Intelligence

Note: The DMS audit file is saved when the DMS is backed up.

Disaster Recovery Architecture

The following diagram shows how you deploy CA ControlMinder in a disaster recovery configuration.



Components for Disaster Recovery

You need the following components to deploy CA ControlMinder in a disaster recovery configuration:

- For the production environment:
  - One installation of the Enterprise Management Server
  - Central database (RDBMS)
  - One or more installation of the Distribution Server.
- For the disaster recovery environment:
  - One installation of Enterprise Management Server
  - Central database (RDBMS)
  - One or more installation of the Distribution Server.

Consider the following points when planning a disaster recovery deployment:

- You can restore a DMS only from backup files saved on the same platform, operating system, and version of CA ControlMinder. For example, you cannot restore a DMS using CA ControlMinder r12.5 from backup files of a DMS using CA ControlMinder r12.0 SP1.
- You can set up clustering or other failover solution on your RDBMS.
- You should synchronize the data in the RDBMS between the production and disaster recovery server.
- You should synchronize Message Queue data stores between the production and disaster recovery servers.

How a Disaster Recovery Deployment on the Endpoint Works

A disaster recovery deployment creates a duplicate of your production Distribution Server database, helps ensure that data sent from endpoints is not lost in a system failure, and makes it easier to restore the production environment after a disaster.

The following process describes how a disaster recovery deployment on the endpoint works:

1. You configure the endpoint to work against a list of production and disaster recovery Distribution Servers.
2. At the specified time, the endpoint attempts to connect to the Distribution Server in the production environment.
    a. The endpoint attempts to connect to the first production Distribution Server in its list. If it does not connect, it tries to connect to that Distribution Server for a specified number of attempts. *One* of the following happens:
        - The endpoint connects to the production Distribution Server. The process ends at this step.
        - The endpoint can not connect to the production Distribution Server. The process goes to step b.

        Note: The number of times the endpoint attempts to connect to Distribution Server and the Distribution Servers to connect to is defined in the Distribution_Server configuration setting in the communication section and max_dh_command_retry configuration setting in the policyfetcher section.

    b. The endpoint attempts to connect to the second production Distribution Server in its list, then the third, and so on (for the same defined number of times, if necessary). *One* of the following happens:
        - The endpoint connects to a production Distribution Server. The process ends at this step.
        - The endpoint can not connect to any production Distribution Server, and the cycle ends. The process goes to step 3.

3. The endpoint repeats Step 2 for a specified number of cycles. *One* of the following happens:

   - The endpoint connects to a production Distribution Server. The process ends at this step.
   - The endpoint does not connect to a production Distribution Server. The process goes to the next step.

     Note: The number of times the endpoint attempts to connect to Distribution Server and the Distribution Servers to connect to is defined in the Distribution_Server configuration setting in the communication section and max_dh_command_retry configuration setting in the policyfetcher section.

4. The endpoint attempts to connect to the first disaster recovery Distribution Server in its list. If it does not connect to this Distribution Server, it tries to connect to the second disaster recovery Distribution Server in its list, then the third, and so on, until the endpoint connects to a disaster recovery Distribution Server.

   Note: If an endpoint cannot connect to a production or disaster recovery Distribution Server, it will not send a heartbeat to the DMS. To determine if an endpoint is online or offline, check what time the last heartbeat notification was sent to the DMS.

5. After it has connected to a disaster recovery Distribution Server, the endpoint continually tries to connect to a production Distribution Server. *One* of the following happens:

   - The endpoint connects to a production Distribution Server, and returns to the production environment.
   - The endpoint does not connect a production Distribution Server. The endpoint remains in the disaster recovery environment, and repeats Step 4.

   Note: For more information about the policyfetcher and communication sections, see the *Reference Guide*.

How to Install a Disaster Recovery Deployment

To verify that you correctly subscribe the disaster recovery components to each other, you setup the production and disaster recovery components in the order specified in the following process.

A disaster recovery configuration makes it easier to restore your Enterprise Management Server components in the event of a catastrophic system failure. You may need to back up other CA ControlMinder components separately, for example the central database (RDBMS).

Important!: You cannot restore a DMS from backup files that use another operating environment or version of CA ControlMinder. Verify that the production and disaster recovery environments are deployed on identical platforms, operating systems, and versions of CA ControlMinder.

Note: This process assumes that you installed the DMS and DH on separate hosts.

The following process describes how to install a disaster recovery deployment:

1. Set up the production Enterprise Management Sever (see page 430)
2. Set up the disaster recovery Enterprise Management Server (see page 432)
3. Configure databases replication between the production and disaster recovery servers
4. Configure DMS subscriptions (see page 434)
5. Synchronize the Message Queue servers data files (see page 450)
6. Set up an endpoint (see page 435).

Note: We recommend that you install the RDBMS over a cluster or any other method that allows data synchronization between sites.

Set Up the Production CA ControlMinder Enterprise Management

The production Enterprise Management Server contains the DMS. The DMS stores up-to-date information about policy versions, policy scripts, and the policy deployment status of each endpoint. You use the production DMS to deploy and manage your enterprise policies.

Because the production DHs and the disaster recovery DMS subscribe to the production DMS, set up the production DMS before you set up any other disaster recovery component. This helps ensure that the subscriptions are correctly configured later in the installation process.

To set up the production Enterprise Management Server

1. Implement the Enterprise Management Server.

   All the web-based applications, the Distribution Server, the DMS, and CA Access Control are installed.

2. (Optional) Implement the Distribution Server (see page 436).

   The Message Queue and the Java Connector Server are installed.

3. (Optional) If you want to remove the local DH from the Enterprise Management Server and use the DH on the Distribution Server, to maintain a separation between the management and distribution server, run the following command on the production Enterprise Management Server:

   `dmsmgr -remove -dh name`

   -dh *name*

   Removes a DH with the *name* specified on the local host.

   Example: *dmsmgr -remove -dh DH*

   The above example removed a DH named DH from the host.

   The production DMS is created with no subscribers.

4. Configure the Message Queue to work in failsafe mode. Do the following:

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

      ACServerInstallDir`/MessageQueue/tibco/cfgmgmt/ems/data`

   b. Open the queues.conf file for editing.

   c. Add the word "**failsafe**" at the end of every queue definition line, then save and close the file.

5. Configure CA ControlMinder Enterprise Management with local DMS (see page 399).

   You have installed and configured the production Enterprise Management Server. You can now configure the disaster recovery Enterprise Management Server.

Example: Edit the queues.conf File

The following snippet from the queues.conf file is an example of how you amend the file to configure the Message Queue to use the shared storage.

```
queue/snapshots secure,store=$sys.failsafe
queue/audit secure,store=$sys.failsafe
ac_endpoint_to_server secure,store=$sys.failsafe
ac_server_to_endpoint secure,store=$sys.failsafe
```

Set up the Disaster Recovery CA ControlMinder Enterprise Management

The disaster recovery Enterprise Management Server deploys and manages your enterprise policies in the event of a catastrophic system failure. Because the disaster recovery Enterprise Management Server is a subscriber of the production Enterprise Management Server, its database contains the same information about policy versions, policy scripts, and endpoint deployment status as the production Enterprise Management Server.

Note: Configure the production Enterprise Management Server before you set up the disaster recovery Enterprise Management Server.

To set up the disaster recovery Enterprise Management Server

1. Copy the FIPSKey.dat file from the production Enterprise Management Server to the disaster recovery server. The file is located in the following directory, where *JBoss_HOME* indicates the directory where you installed JBoss:

   ```
   JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/config/keys
   ```

2. Implement the Enterprise Management Server on the disaster recovery server.

   All the web-based applications, the Distribution Server, the DMS, and CA Access Control are installed.

   Important! Specify the FIPSKey.dat file you copied from the production Enterprise Management Server when you launch the installation process. For example:

   ```
   E:\EnterpriseMgmt\Disk1\InstData\NoVM\install_EntM_r125.exe
   -DFIPS_KEY=C:\tmp\FIPSkey.dat
   ```

3. (Optional) Implement the disaster recovery Distribution Server (see page 439).

   The Message Queue and Java Connector Server are installed.

4. (Optional) If you want to remove the local DH and use the DH on the Distribution Server, to maintain a separation between the management and distribution server, run the following command on the disaster recovery Enterprise Management Server:

   ```
   dmsmgr -remove -dh name
   ```

   -dh *name*

   Removes a DH with the *name* specified on the local host.

   Example: *dmsmgr -remove -dh DH*

   The disaster recovery DMS is created with no subscribers.

5. Configure the Message Queue to work in failsafe mode. Do the following:
   a. Navigate to the following directory, where *ACServerInstallDir* is the directory where you installed the Enterprise Management Server:

      ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

   b. Open the queues.conf file for editing.
   c. Add the word "**failsafe**" at the end of every queue definition line, then save and close the file.
6. Configure CA ControlMinder Enterprise Management with local DMS (see page 399).

You have installed and configured the disaster recovery Enterprise Management Server.

Example: Edit the queues.conf File

The following snippet from the queues.conf file is an example of how you amend the file to configure the Message Queue to use the shared storage.

```
queue/snapshots secure,store=$sys.failsafe
queue/audit secure,store=$sys.failsafe
ac_endpoint_to_server secure,store=$sys.failsafe
ac_server_to_endpoint secure,store=$sys.failsafe
```

Configure the DMS Subscription

The disaster recovery Enterprise Management Server is a subscriber of the production Enterprise Management Server. Therefore, its database contains the same information about policy versions, policy scripts, and endpoint deployment status as the production Enterprise Management Server.

You configure the database of the disaster recovery Enterprise Management Server as a subscriber of the production Enterprise Management Server to synchronize the two databases.

To configure the DMS subscription

1. Move to the disaster recovery Enterprise Management Server.
2. Define the production Enterprise Management Server as the parent of the disaster recovery Enterprise Management Server. Run the following command:

   `env pmd`

   `subs drpmd_name parentpmd(<pr_dms_pmdname>@pr_host)`

   drpmd_name

   Defines the name of the disaster recovery PMDB.
3. Move to the production Enterprise Management Server:
4. Run the following command:

   `sepmd -n prDMS_name drDMS_name`

   prDMS_name

   Defines the name of the production DMS.

   drDMS_name

   Defines the name of the disaster recovery DMS. Specify the disaster recovery DMS in the following format: *drDMS_name@hostname*.

The disaster recovery Enterprise Management Server is subscribed to and synchronized with the production Enterprise Management Server.

Set Up an Endpoint

Once you install the Enterprise Management Server in the production and disaster recovery environments, you need to configure each endpoint in your enterprise to work with the production and disaster recovery server components. In doing so, you configure the endpoint to send information to and receive information from the server components.

Note: Provide the Advanced Policy Management Server Component host name as part of the installation process. Enter the names of the production DHs in the following format: *prDH_name@hostname*[, *prDH_name@hostname*..]

To set up an endpoint

1. Install CA ControlMinder endpoint functionality, with the Advanced Policy Management Client Components enabled, on the endpoint host.

   CA ControlMinder endpoint functionality is installed on the host, and the endpoint is subscribed to the production DHs.

2. Open a selang command window on the endpoint.

3. Enter the following command:

   `so dh_dr+(drDH_name[, drDH_name...])`

   drDH_name

   Defines the names of the disaster recovery DH.Format: *drDH_name@hostname*.

   The endpoint is subscribed to the disaster recovery DHs.

4. Specify the list of production and disaster recovery Distribution Server URLs.

   - UNIX: Modify the Distribution_Server parameter in the [communication] section of accommon.ini file.
   - Windows: Modify the Distribution_Sever value the Windows Registry. This parameter is found in:

     `HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\common\communication`

   Note: For more information about the Distribution_Server value, see the *Reference Guide*.

   Note: You can also subscribe an endpoint to a disaster recovery DH by creating a policy with the stated selang command and deploying it to the endpoint. For more information about creating and deploying policies, see the *Enterprise Administration Guide*.

Additional Information for Installing a Disaster Recovery Deployment

The following topics describe additional configuration steps that you may need to perform to install a disaster recovery deployment.

Install the Distribution Server

When you configure CA ControlMinder to work in a disaster recovery or high availability environment, you install the Distribution Servers on separate computers and configure the Distribution Servers to propagate files between them.

To install the Distribution Server

1. Insert the appropriate CA ControlMinder Server Components DVD for your operating system into your optical disc drive.
2. Do either of the following:
   - On Windows:

     If you have autorun enabled, the Product Explorer automatically appears. Do the following:

     a. If the Product Explorer does not appear, navigate to the optical disc drive directory and double-click the ProductExplorerx86.EXE file.

     b. Expand the Components folder in the Product Explorer, select CA ControlMinder Distribution Server, then click Install.

     The InstallAnywhere installation program starts.
   - On UNIX:

     a. Mount the optical disc drive.

     b. Open a terminal window and navigate to the following directory on the optical disc drive:

     /DistServer/Disk1/InstData/NoVM

     c. Run the following command:

     ```
     ./install_DistServer.bin -i console
     ```

     The InstallAnywhere installation program starts.

3. Complete the wizard as required. The following installation inputs are not self-explanatory:

   Message Queue Settings

   Defines the Message Queue server administrator password (Communication Password).

   Limits: Minimum of six (6) characters

   Java Connector Server - Provisioning Directory Information

   Defines the password for the Java Connector Server.

   Note: The Java Connector Server provides CA ControlMinder Enterprise Management with privileged account management capabilities.

   The CA ControlMinder Distribution Server installation is complete.

   Note: You must complete additional steps if you install the Distribution Server as part of a disaster recovery implementation.

More information:

Set Up the Production Distribution Server (see page 437)
Set Up the Disaster Recovery Distribution Server (see page 439)

Set Up the Production Distribution Server

The production Distribution Server contains the DH. The DH distributes policy deployments made on the production DMS to the endpoints, and receives deployment status updates from the endpoints to send to the production DMS.

Because the production DHs and the disaster recovery DMS subscribe to the production DMS, set up the production DMS before you set up any other disaster recovery component. This helps ensure that the subscriptions are correctly configured later in the installation process.

To set up the production Distribution Server

1. Install the Distribution Server (see page 436) on the production Distribution Server computer.
2. Run the following command on the production Distribution Server to configure the DH:

   ```
   dmsmgr -remove -auto
   ```

   ```
   dmsmgr -create -dh name -parent name\
   [-admin user[,user...]] [-desktop host[,host...]]
   ```

   -dh *name*

   Creates a DH with the *name* specified on the local host.

   -parent *name*

   Defines the production DMS that the DH will send endpoint notifications to. Specify the production DMS in the following format: *DMS_name@hostname*.

   -admin *user*[,*user*...]

   (Optional) Defines internal users as administrators of the created DH.

   -desktop *host*[,*host*...]

   (Optional) Defines a list of computers that have TERMINAL access rights to the computer with the created DH.

   Note: Whether specified or not, the terminal running the utility is always granted administration rights for the created DH.

   The production DH is created and configured.

3. Run the following command:

   ```
   sepmd -n prDMS_name prDH_name
   ```

   prDMS_name

   Defines the name of the production DMS.

   prDH_name

   Defines the name of the production DHs. Specify the name in the following format: *prDH_name@hostname*.

   Example: DH__@prdh.com

   The DH is subscribed to and synchronized with the production DMS.

4. Set up Message Queue routing between the Distribution Server and the production DMS.
5. Repeat Steps 1-4 for each production Distribution Server.

Set Up the Disaster Recovery Distribution Server

Because the disaster recovery Distribution Server is a subscriber of the production Distribution Server, its database contains the same information about policy versions, policy scripts, and endpoint deployment status as the production Distribution Server.

Note: You must set up the production Distribution Server before you set up the disaster recovery Distribution Server.

To set up the disaster recovery Distribution Server

1. Install the Distribution Server (see page 436) on the disaster recovery Distribution Server computer.
2. Run the following command on the disaster recovery Distribution Server to configure the DH:

   ```
   dmsmgr -remove -auto
   ```

   ```
   dmsmgr -create -dh name -parent name\
   [-admin user[,user...]] [-admin user[,user...]]
   ```

   -dh *name*

   Creates a DH with the *name* specified on the local host.

   -parent *name*

   Defines the disaster recovery DMS that the DH will send endpoint notifications to. Specify the disaster recovery DMS in the following format: *drDMS_name@hostname*.

   -admin *user* [,*user*...]

   (Optional) Defines internal users as administrators of the created DH.

   -desktop *host*[,*host*...]

   (Optional) Defines a list of computers that have TERMINAL access rights to the computer with the created DH.

   Note: Whether specified or not, the terminal running the utility is always granted administration rights for the created DH.

   The disaster recovery DH is created and configured.

3. Run the following command on the disaster recovery Distribution Server:

   `sepmd -n drDMS_name drDH_name`

   drDMS_name

   Defines the name of the disaster recovery DMS.

   drDH_name

   Defines the name of the disaster recovery DH. Specify the name in the following format: *drDH_name@hostname*.

   Example: DH__@drdh.com

   The DH is subscribed to and synchronized with the disaster recovery DMS.

4. Set up Message Queue routing between the Distribution Server and the disaster recovery DMS.
5. Repeat Steps 1-4 for each disaster recovery Distribution Server.

The Disaster Recovery Process

The disaster recovery process has two stages: backup and restoration. In the backup stage, the data in the DMS database is copied into another directory. In the restoration stage, the dmsgmr utility uses the backup DMS files to restore an existing DMS, or create a DMS.

Note: A disaster recovery configuration makes it easier to restore your advanced policy management components in the event of a catastrophic system failure. You may need to back up other CA ControlMinder components separately.

More information:

Data That Can Be Restored (see page 441)
When to Restore a DMS (see page 441)
When to Restore a DH (see page 442)
How a DMS Is Restored (see page 442)
How a DH Is Restored (see page 443)

Data That Can Be Restored

When you restore a DMS, dmsmgr uses backup files from another DMS to create a new DMS. When you restore a DH, dmsmgr copies data from the DMS backup files to the DH Reader directory. In both cases you restore the same data.

The data that you restore is a duplicate of the data in the DMS database, and includes:

- Information about your enterprise policies, versions, and assignments
- Information about deployment and policy status, deployment deviation, and deployment hierarchy
- Host and host group definitions
- Configuration settings
- The updates.dat file
- Registry entries
- DMS audit file

Note: You do not need to restore the DH__Writer because it has a transient database.

When to Restore a DMS

When you restore a DMS, dmsmgr uses backup files from another DMS to create a new DMS. The following scenarios describe when to restore a production DMS:

- When a catastrophic production system failure has occurred.
- When the production DMS database is corrupt.
- When you need to set up a new production DMS on a different host.

The following scenarios describe when to restore a disaster recovery DMS:

- When the disaster recovery DMS is not in sync with the production DMS.
- When the disaster recovery DMS database is corrupt.
- When you need to set up a new disaster recovery DMS on a different host.

Note: You can restore a DMS over an existing DMS, or into a new directory where no DMS exists.

When to Restore a DH

When you restore a DH, dmsmgr copies data from the DMS backup files to the DH Reader directory. The following scenarios describe when to restore a DH:

- When a catastrophic production system failure has occurred.
- When the DH database is corrupt.
- When the DH is out of sync with its DMS.
- When you need to set up a new DH on a different host.

Note: You do not need to restore the DH Writer because it has a transient database. Check that the DH Writer is present in the existing DH file structure before you restore a DH.

How a DMS Is Restored

Understanding how the dmsmgr utility restores a DMS helps you diagnose any problems that may occur during the restoration process.

The following process describes how dmsmgr restores a DMS:

1. dmsmgr removes the existing DMS.
2. dmsmgr copies the backup DMS files from the location that you specified into the DMS directory.
3. dmsmgr deletes any subscribers to the DMS.
4. *One* of the following happens:
   - If you restore a production DMS, dmsmgr adds the disaster recovery DMS to the production DMS as its first subscriber, with an offset value equal to the last global offset stored in the backup files.
   - If you restore a disaster recovery DMS, dmsmgr re-subscribes the disaster recovery DMS to the production DMS, with an offset value equal to the last global offset stored in the backup files.
5. dmsmgr subscribes each DH to the DMS. Each DH has an offset value of 0 and out of sync status.

   Note: A DH cannot receive updates from the DMS when it is out of sync. To release the DH from out of sync status, restore the DH.

How a DH Is Restored

Understanding how the dmsmgr utility restores a DH helps you diagnose any problems that may occur during the restoration process.

The following process describes how dmsmgr restores a DH:

1. dmsmgr removes the existing DH.
2. dmsmgr copies the backup DH files from the location that you specified into the DH directory.
3. dmsmgr subscribes the DH to the DMS with an offset value equal to the last global offset stored in the backup files.
4. dmsmgr clears the out of sync flag on the DH.

Offset Values

The updates.dat file stores each command that the DMS deploys. When you create a new subscriber, the Policy Model sends the commands in the updates.dat file to the subscriber. Each command is indexed by an increasing number, called the *offset value*.

When you add a subscriber to the DMS, you can specify an offset of:

- **0**—The Policy Model sends all commands to the subscriber.
- **The last offset**—The Policy Model sends no commands to the subscriber.
- **An integer X between 0 and the last offset**—The Policy Model sends all commands between X and the last offset to the subscriber.

Out of Sync Subscribers

An *out of sync subscriber* is a subscriber that has not received any updates since the updates.dat file was last truncated. Flagging a subscriber as out of sync lets CA ControlMinder ignore the subscriber, and no commands are sent to this subscriber.

An out of sync subscriber does not receive any updates from its parent DMS or Policy Model. To clear the out of sync flag and let the subscriber receive updates, you must re-subscribe the subscriber to its parent.

If every subscriber to a parent DMS or Policy Model is out of sync, the parent effectively has no subscribers.

How to Recover from a Disaster

If a production system failure occurs, the endpoints work against the disaster recovery environment. When you recover from a disaster, you move operation from the disaster recovery environment back to the restored production environment.

The following process describes how to recover from a disaster:

1. Stop CA ControlMinder on the production Enterprise Management Server and the production Distribution Servers.
2. Stop all administrative work against the disaster recovery DMS, that is, stop CA ControlMinder Enterprise Management and the policydeploy utility.
3. (Optional) Auto-truncate the updates.dat file.
4. Back up the disaster recovery DMS. You can back up the DMS using either of the following methods:
   - local backup (see page 445)
   - remote backup (see page 446)
5. Restore the production database (RDBMS).
6. Restore the production DMS (see page 448) from the disaster recovery DMS backup files.
7. Start CA ControlMinder on the production DMS.
8. Back up the production DMS.You can back up the DMS using either of the following methods:
   - local backup (see page 445)
   - remote backup (see page 446)
9. Restore each production DH from the production DMS backup files.
10. Start CA ControlMinder on each production Distribution Server.
11. Move all administrative work to the production DMS, that is, start CA ControlMinder Enterprise Management and the policydeploy utility on the production CA ControlMinder Enterprise Management.

12. (Optional) If the disaster recovery DMS is out of sync with the production DMS, complete the following steps:
    a. Restore the disaster recovery DMS (see page 449) from the production DMS backup files.
    b. Back up the disaster recovery DMS.You can back up the DMS using either of the following methods:
        - the sepmd utility (see page 445)
        - selang commands (see page 446)
    c. Restore each disaster recovery DH from the disaster recovery DMS backup file.

Back Up the DMS Using sepmd

Backup the DMS to save copies of the policies that you deployed to the endpoints and reports snapshots that the Enterprise Management Server received from the endpoints.

When you back up the DMS, you copy the data from the DMS database to a specified directory.

The sepmd utility backs up the DMS only on a local host. You should store the backed up DMS files in a secure location, preferably protected by CA ControlMinder access rules. We recommend that you auto-truncate the updates.dat file before you back up the DMS.

Note: You can also use selang commands to back up a DMS on a local or remote host.

To back up the DMS using sepmd

1. Lock the DMS using the following command:

   `sepmd -bl dms_name`

   The DMS is locked, and cannot send any commands to its subscribers.

2. Back up the DMS database using the following command:

   `sepmd -bd dms_name [destination_directory]`

   dms_name

   Defines the name of the DMS that is backed up on the local host.

   destination_directory

   Defines the directory the DMS is backed up to.

   Default: (UNIX) *ACInstallDir*/data/policies_backup/dmsName

   Default: (Windows) *ACInstallDir*\data\policies_backup\dmsName

   The DMS database is backed up to the destination directory.

3. Unlock the DMS using the following command:

   `sepmd -ul dms_name`

   The DMS is unlocked, and can send commands to its subscribers.

Back Up the DMS Using selang

Back up the DMS to copy the data from the DMS database to a specified directory.

You can use selang commands to back up a DMS on a local or a remote host. You should store the backed up DMS files in a secure location, preferably protected by CA ControlMinder access rules. We recommend that you auto-truncate the updates.dat file before you back up the DMS.

Note: You can also use the sepmd utility to back up a DMS on a local host.

To back up the DMS using selang

1. (Optional) If you are using selang to connect to the DMS from a remote host, connect to the DMS host using the following command:

   `host dms_host_name`

2. Move to the PMD environment using the following command:

   `env pmd`

3. Lock the DMS using the following command:

   `pmd dms_name lock`

   The DMS is locked, and cannot send any commands to its subscribers.

4. Back up the DMS database using the following command:

   `backuppmd dms_name [destination(destination_directory)]`

   dms_name

   Defines the name of the DMS that is backed up on the local host.

   destination*(destination_directory)*

   Defines the directory the DMS is backed up to.

   Default: (UNIX) *ACInstallDir*/data/policies_backup/dmsName

   Default: (Windows) *ACInstallDir*\data\policies_backup\dmsName

   The DMS database is backed up to the destination directory.

5. Unlock the DMS using the following command:

   `pmd dms_name unlock`

   The DMS is unlocked, and can send commands to its subscribers.

Restore a DH

Restore a DH to copy data from the DMS backup files into the DH_Reader directory using the dmsmgr utility.You do not need to restore a DH Writer because it has a transient database. Check that the DH Writer is present in the existing DH file structure before you restore a DH.

Note: If the DH Writer is not present in the existing DH file structure, or you want to set up a new DH, use the dmsmgr -create function to create a new DH before you restore a DH.

Note: You must have full administrative access to the operating system to use the dmsmgr utility.

Follow these steps:

1. Remove the DH, if it exists.
2. Recreate the DH.

   The DH registers with the DMS automatically and downloads the database.

3. Run the following command on the DH host if synchronization with the DMS fails:
   `dmsmgr -sync self`

The DH is restored and the DH is subscribed to the DMS.

Restore the Production DMS

When you restore the production DMS, dmsmgr copies the data from the disaster recovery DMS backup files into the production DMS directory.

Note: You must have full administrative access to the operating system to use the dmsmgr utility.

To restore the production DMS, enter the following command on the production DMS host:

```
dmsmgr -restore -dms name -source path -replica name\
[-subscriber dhname[,dhname...]] [-admin user[,user...]]\
[-xadmin user[,user...]]
```

-admin *user*[,*user*...]

(UNIX) Defines internal users as administrators of the restored DMS or DH.

-dms *name*

Defines the name of the DMS that is restored on the local host.

-replica *name*

Defines the name of the disaster recovery DMS that is subscribed to the production DMS. Specify the disaster recovery DMS in the following format: *DMS_name@hostname*.

-subscriber *dh_name*[, *dh_name*...]

(Optional) Defines a comma-separated list of DHs that the restored DMS will send policy updates to. Specify each DH in the following format: *DH_name@hostname*.

-source *path*

Defines the directory that contains the backup files to restore.

-xadmin *user*[,*user*...]

(UNIX) Defines enterprise users as administrators of the restored DMS or DH.

The production DMS is restored.

Note: After you restore the production DMS, you must back up the production DMS and restore the production DHs from the backup file. This ensures that the production DMS and production DHs are synchronized.

Restore the Disaster Recovery DMS

When you restore the disaster recovery DMS, dmsmgr copies the data from the backup files into the disaster recovery DMS directory.

Note: You must have full administrative access to the operating system to use the dmsmgr utility.

To restore the disaster recovery DMS, enter the following command on the disaster recovery DMS host:

```
dmsmgr -restore -dms name -source path -parent name\
[-subscriber dhname[,dhname...]] [-admin user[,user...]]\
[-xadmin user[,user...]]
```

-admin *user*[,*user*...]

(UNIX) Defines internal users as administrators of the restored DMS or DH.

-dms *name*

Defines the name of the DMS that is restored on the local host.

-parent *name*

Defines the name of the production DMS that the restored disaster recovery DMS will subscribe to. Specify the production DMS in the following format: *DMS_name@hostname.*

-source *path*

Defines the directory that contains the backup files to restore.

-subscriber *dh_name*[, *dh_name*...]

(Optional) Defines a comma-separated list of DHs that the restored DMS will send policy updates to. Specify each DH in the following format: *DH_name@hostname*.

-xadmin *user*[,*user*...]

(UNIX) Defines enterprise users as administrators of the restored DMS or DH.

The disaster recovery DMS is restored and the disaster recovery DMS is subscribed to the production DMS.

Note: After you restore the disaster recovery DMS, you must back up the disaster recovery DMS and restore the disaster recovery DHs from the backup file. This ensures that the disaster recovery DMS and disaster recovery DHs are synchronized.

Back Up the Message Queue Server Data Files

Back up the Message Queue Servers data files to copy data from the production Message Queue Server to the disaster recovery Message Queue Server.

To back up the message queue server data files, copy the Message Queue Server data file from the production Distribution Server to the disaster recovery Distribution Server. By default, the data files are located in the following directory, where *ACServerInstallDir* is the directory in which you installed the Message Queue Server:

ACServerInstallDir/MessageQueue/tibco/ems/bin/datastore

Restore the Message Queue Server Data Files

Restore the Message Queue Servers data files to copy data from the disaster recovery Message Queue Server to the production Message Queue Server.

To restore the message queue server data files, copy the Message Queue Server data file from the disaster recovery Distribution Server to the production Distribution Server. By default, the data files are located in the following directory, where *ACServerInstallDir* is the directory in which you installed the Message Queue Server:

ACServerInstallDir/MessageQueue/tibco/ems/bin/datastore

How To Synchronize the Message Queue Servers Data Files

When you work in a disaster recovery environment, it is crucial to synchronize the production and disaster recovery Message Queue Servers. Synchronizing the servers helps ensure that the data on both the production and disaster recovery Message Queue Servers is updated and, if the production servers do not function, the disaster recovery servers can continue servicing the data without interruptions.

Note: The synchronization solution is based on a third-party replication tool. Verify that the storage solution writes the data blocks to a shared storage in the same order as they occur in the data buffer. Verify that upon return from a synchronous write call, the storage solution help ensure that all the data was written to durable, persistent storage.

To synchronize the data files of the Message Queue Servers, do the following:

1. On the production Distribution Server, set up message routing settings between the Message Queue Server and all the Message Queue Servers installed on the Enterprise Management Server.
2. Set up message routing settings between the Message Queue Servers on the disaster recovery Distribution Servers and the disaster recovery Enterprise Management Server.

3. Modify the queues.conf file on both the disaster recovery and production Message Queue Servers on the Enterprise Management Server and add a "fail-safe" line.

   For example:

   ```
   queue/snapshots secure,failsafe
   queue/audit secure, failsafe
   ac_endpoint_to_server secure, failsafe
   ac_server_to_endpoint secure,failsafe
   ```

   By default this file is located in the following directory, where *ACServerInstallDir* is the directory in which you installed the Enterprise Management Server:

   ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

4. Replicate the production Message Queue Server EMS data files on the Enterprise Management Server to the Message Queue Server on the disaster recovery Enterprise Management Server using a third-party replication tool.

   By default, the Message Queue Server EMS data files are located in the following directory, where *ACServerInstallDir* is the directory in which you installed Enterprise Management Server:

   ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data/datastore

   You have configured the Message Queue Servers EMS data files synchronization settings.

Appendix B: Changing Communication Encryption Methods

This section contains the following topics:

Communication Encryption

You can use the following methods to encrypt communication between CA ControlMinder components and to encrypt CA ControlMinder client/server communication:

- Symmetric encryption
- SSL

Note: On Windows, when you change the encryption mode (for example, to FIPS-only mode), restart CA ControlMinder services if you need to propagate passwords from a password PMDB.

Symmetric Encryption

CA ControlMinder uses encryption libraries to implement symmetric (standard) encryption. You can use the following methods to encrypt communication between CA ControlMinder components:

- Default (proprietary) encryption
- AES128
- AES192
- AES256
- DES
- 3DES

Note: The encryption method named default is not the default CA ControlMinder encryption method. The default encryption method is AES256.

When you install CA ControlMinder, the installer stores the encryption libraries in the following directory, where *ACInstallDir* is the directory in which you installed CA ControlMinder:

- (Windows) *ACInstallDir*\bin
- (UNIX) *ACInstallDir*/lib

On Windows, CA ControlMinder stores the full path of the encryption library that you use for symmetric encryption in the following configuration setting:

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl\Encryption Package
```

You use the sechkey utility to change the symmetric encryption key and the symmetric encryption method.

More information:

Change the Symmetric Encryption Key (see page 455)
Change the Symmetric Encryption Method (see page 456)

How sechkey Configures Symmetric Encryption

A symmetric encryption key is 55 characters long. sechkey automatically truncates longer keys and pads out shorter keys.

When you use sechkey to change an encryption key, sechkey changes the key in all programs in the CA ControlMinder database at once. When sechkey changes the symmetric key or symmetric encryption method, it decrypts then re-encrypts the following:

- Encrypted records for any Policy Model installed on the computer
- All encrypted passwords in the CA ControlMinder database, including CA ControlMinder Message Queue passwords and, if CA ControlMinder uses bi-directional passwords, USER passwords
- The server private key, if the key is not password-protected
- The password for the server private key, if the key is password-protected

In addition, whenever you use a CA ControlMinder API to create a program that communicates with CA ControlMinder, the communication for the new program is encrypted with the same key.

Change the Symmetric Encryption Key

Symmetric encryption keys protect communication between CA ControlMinder components. You use the sechkey utility to change the symmetric encryption keys. You can use sechkey in interactive or non-interactive mode.

Before you change the symmetric encryption key, note the following limitations:

- The password must be 1-55 characters long
- The password must not contain high ASCII characters
- The password must not contain double quotes (")

You must have the ADMIN attribute to use sechkey.

Important! To avoid communication problems, use the same encryption key on all computers that run CA ControlMinder components.

To change the symmetric encryption key

1. Stop CA ControlMinder.

   If you are changing the encryption settings on a CA ControlMinder Enterprise Management server, also stop the CA ControlMinder Web Service.

2. Run the sechkey utility in interactive mode:

   ```
   sechkey
   ```

   The utility prompts you to enter the existing key and the new key, and changes the symmetric encryption key.

3. Start CA ControlMinder.

   If you are changing the encryption settings on a CA ControlMinder Enterprise Management server, also start the CA ControlMinder Web Service.

   CA ControlMinder starts and encrypts communication with the new encryption key.

Example: Change the Symmetric Encryption Key in Non-interactive Mode

The following example changes the default CA ControlMinder symmetric key to a new key with the value newkey:

```
sechkey -d newkey
```

Note: For more information about the sechkey utility, see the *Reference Guide*.

Change the Symmetric Encryption Method

Symmetric encryption protects communication between CA ControlMinder components and is implemented by encryption libraries. You use the sechkey utility to change the encryption library, and therefore change the symmetric encryption method.

You must have the ADMIN attribute to use sechkey.

Note: If CA ControlMinder is operating in FIPS-only mode, you cannot change the symmetric encryption method. CA ControlMinder operates in FIPS-only mode when the value of the fips_only configuration token in the crypto section is 1. This restriction prevents you from changing the encryption method to a non-FIPS compliant method.

Important! To avoid communication problems, use the same encryption method on all computers that run CA ControlMinder components.

To change the symmetric encryption method

1. Stop CA ControlMinder.

   If you are changing the encryption settings on a CA ControlMinder Enterprise Management server, also stop the CA ControlMinder Web Service.

2. Use the sechkey utility to change the symmetric encryption method.

3. Start CA ControlMinder.

   If you are changing the encryption settings on a CA ControlMinder Enterprise Management server, also start the CA ControlMinder Web Service.

   CA ControlMinder starts and encrypts communication with the new encryption method.

Example: Change the Symmetric Encryption Method to 3DES

The following command changes the symmetric encryption method to 3DES:

```
sechkey -m -sym tripledes
```

Note: For more information about the sechkey utility, see the *Reference Guide*.

Multiple Symmetric Encryption Methods in an Enterprise Deployment

Endpoints can communicate with other CA ControlMinder components that use different encryption methods. The encryption_methods configuration setting in the crypto section specifies the symmetric encryption methods that the endpoint accepts.

By default the configuration setting lists the following encryption methods, in order:

- AES256
- AES192
- AES128
- DES
- 3DES

When the CA ControlMinder Agent decrypts incoming communication from another component, it attempts to use each method in the list, in turn, until the decryption is successful. The Agent uses the same encryption method to encrypt outgoing communication to that component.

Similarly, when the CA ControlMinder Web Service tries to connect to an endpoint, it attempts to use each method in the list, in turn, until it successfully communicates with the endpoint.

Multiple encryption methods let you easily upgrade an enterprise CA ControlMinder deployment. For example, you have an r12.5 deployment that uses DES encryption. You want to perform a staged upgrade to r12.5 SP4 and change the encryption method to AES256 for the upgraded components. You upgrade the Enterprise Management Server to r12.5 SP4; the server now uses AES256 encryption by default. However, because the r12.5 SP4 server can also communicate with CA ControlMinder components that use DES encryption, the Enterprise Management Server can continue to manage the r12.5 endpoints.

SSL, Authentication, and Certificates

Secure Sockets Layer (SSL), including TLS, provides communications between computer programs. SSL helps ensure that communications have the following properties:

- The participants in the communication are authenticated, that is, the participants in the communication are the programs, or users, that they purport to be.
- The data is securely encrypted, and only the participants can read it.

Participants authenticate each other by using X.509 certificates. An X.509 certificate is an electronic document that links the certificate owner's address with a public key. The certificate is not forgeable.

SSL works on a client/server model and uses PKI (public key infrastructure). When a client receives an X.509 certificate from a server, it checks if the certificate is valid. If the certificate is valid, the client knows that the server is the program or user that it purports to be, so the server is authenticated. Also, if the client uses the certificate's public key to encrypt data, only the server can decrypt that data, so the data is secure. Conversely, the server uses the X.509 certificate it receives from a client in the same way.

What a Certificate Contains

Programs send X.509 certificates to prove that their identity is bound to a public key. This lets other programs encrypt messages knowing that only the subject of the certificate can decrypt those messages.

The contents of an X.509 certificate are as follows:

- **Certificate data**—The most important certificate data fields are as follows:
  - The public identifier of the certificate subject (for example, a web address)
  - The period (start and end dates) for which the certificate is valid
- **Name of the Certificate Authority (CA) certifying the certificate**—The reader of the certificate can be sure that if the signature is valid, the CA validates that the public key is associated with the subject. This means that if readers of the certificate trust the CA, they can trust that data encrypted with the public key can only be read by the subject.
- **The subject's public key**—The reader of the certificate uses the public key to encrypt data to send to the certificate subject.
- **A digital signature**—The digital signature is a hashed encapsulation of all the other data in the certificate, encrypted with the CA's private key. (Note the contrast to the encryption case, in which the sender encrypts data with a public key.) Anyone with access to the CA's public key can read the signature and check that this matches the other data in the certificate. If any of the text in the certificate has been changed, the signature will no longer match the certificate text.

Associated with the certificate, but kept separate and secure, is the subject's private key. The subject uses the private key to decrypt messages that programs have encrypted with the public key.

What a Certificate Proves

A reader can validate the certificate signature by using the public key of the Certificate Authority (CA). If the decrypted signature matches the rest of the certificate, and the reader trusts the CA, this means the reader knows the following are true:

- That when the reader encrypts data using the public key, only the owner of the private key will be able to decrypt and read that data.
- That the owner of the certificate private key is the subject given in the certificate.

To be confident that the certificate is valid, the reader needs to trust the CA, and also needs to access the CA's public keys. In most cases the CA is a well known company and the program (and all popular web browsers) has copies of the CA's public keys, so the reader does not need to go online to check that the CA really did validate the certificate.

If the issuer is also the owner, the certificate is said to be self-signed, and trusting the issuer is more problematic.

To check that the program that sent the certificate is the certificate owner, the reader needs to use some other method. Usually the reader checks that the address it used to find the sender of the certificate is the same as the address that is in the certificate.

Root and Server Certificates

A root, or CA, certificate is a trusted X.509 certificate that is validated by a Certificate Authority (CA). You use this trusted certificate to create additional X.509 certificates named server, or subject, certificates. Each server certificate is signed by the private key of the root certificate. If a reader trusts the root certificate, the reader knows they can trust any server certificate that is created from the root certificate.

The root certificate generates and authenticates server certificates. You can use the following types of root certificate in CA ControlMinder:

- The default CA ControlMinder root certificate
- A third-party root certificate, including a password-protected certificate

The server certificate encrypts and authenticates CA ControlMinder client/server communication and communication between CA ControlMinder components. You can use the following types of server certificate in CA ControlMinder:

- The default CA ControlMinder server certificate
- A third-party server certificate, including a password-protected certificate
- A CA ControlMinder server certificate created from a third-party root certificate

Enable SSL Encryption

You configure encryption settings when you install CA ControlMinder. After installation, you can use the sechkey utility to change SSL encryption. You may also need to change the value of configuration settings.

Important! To avoid communication problems, use the same encryption method on all computers that run CA ControlMinder components.

To enable SSL encryption

1. Stop CA ControlMinder.

   If you are changing the encryption settings on a CA ControlMinder Enterprise Management Server, also stop the CA ControlMinder Web Service.

2. Change the value of the communication_mode configuration setting in the crypto section to *one* of the following:

   all_modes

   Specify this value if you want to enable both symmetric and SSL encryption. This value lets the computer communicate with all CA ControlMinder components.

   Note: If you specify this value, CA ControlMinder uses SSL encryption each time that it tries to communicate with another CA ControlMinder component. If SSL fails, it then uses symmetric encryption. This value lets you migrate your CA ControlMinder deployment from a symmetric encryption environment to an SSL encryption environment.

   use_ssl

   Specify this value to enable SSL encryption only. This value lets the computer communicate with only the CA ControlMinder components that use SSL encryption.

   Note: (Windows) If you are working with a third-party program that uses the CA ControlMinder SDK, the crypto section is located at the CA ControlMinder SDK registry path that you defined during installation.

3. (Recommended) Configure SSL communication to do *one* of the following:

   - Use third-party root and server certificates (see page 461).
   - Use a server certificate you generate from a third-party root certificate (see page 463).

   Note: If you do not configure SSL encryption further, you can use the default CA ControlMinder X.509 certificates to encrypt and authenticate communication between CA ControlMinder components. However, we recommend that you change the default certificates instead.

4. Start CA ControlMinder:
   - If you are changing the encryption settings on a CA ControlMinder Enterprise Management Server, also start the CA ControlMinder Web Service.
   - If you are working with a third-party program that uses the CA ControlMinder SDK, restart the process that uses the CA ControlMinder SDK.

   SSL encryption is enabled.

Use Third-Party Root and Server Certificates

If you use SSL encryption, you can use third-party root and server certificates to encrypt and authenticate communication between CA ControlMinder components.

You need the following files to use third-party root and server certificates:

- **root.pem**—Root certificate
- **server.pem**—Server certificate
- **server.key**—Private key for the server certificate

  If you use OU password-protected server certificates, you also need the password for the private key for the server certificate.

Note: Because the server certificates are already created, you do not need the private key for the root certificate.

To use third-party root and server certificates

1. Verify that CA ControlMinder services are stopped and that SSL is enabled.
2. Replace the root certificate. Do *one* of the following:
   - Copy the new root certificate to the location specified in the ca_certificate configuration setting in the crypto section.
   - Edit the value of the ca_certificate configuration setting in the crypto section to specify the full path to the new root certificate.

     Note: If you install the root certificate in a new directory, write CA ControlMinder FILE rules to protect the new directory.
3. Replace the server certificate. Do *one* of the following:
   - Copy the new server certificate to the location specified in the subject_certificate configuration setting in the crypto section.
   - Edit the value of the subject_certificate configuration setting in the crypto section to specify the full path to the new server certificate.

     Note: If you install the server certificate in a new directory, write CA ControlMinder FILE rules to protect the new directory.

4. Replace the server key. Do *one* of the following:
   - Copy the new server key to the location specified in the private_key configuration setting in the crypto section.
   - Edit the value of the private_key configuration setting in the crypto section to specify the full path to the new server key.

     Note: If you install the server key in a new directory, write CA ControlMinder FILE rules to protect the new directory.
5. If you use OU password-protected certificates do the following:
   a. Verify that the value of the fips_only configuration setting in the crypto section is 0.

      Note: You cannot use password-protected certificates if CA ControlMinder is operating in FIPS-only mode.

   b. Store the password for the server certificate private key on the computer as follows:

      ```
      sechkey -g -subpwd private_key_password
      ```

      Note: You must have the ADMIN attribute to use sechkey.

   c. Verify that CA ControlMinder can use the stored password to open the private key:

      ```
      sechkey -g -verify
      ```

      If CA ControlMinder cannot open the key, repeat Step b and specify the correct password.

   Note: For more information about the sechkey utility, see the *Reference Guide*.
6. Start CA ControlMinder:
   - If you are changing the encryption settings on a CA ControlMinder Enterprise Management Server, also start the CA ControlMinder Web Service.
   - If you are working with a third-party program that uses the CA ControlMinder SDK, restart the process that uses the CA ControlMinder SDK.

   SSL encryption is enabled.

Use a Server Certificate You Generate from a Third-Party Root Certificate

If you use SSL encryption, you can create server certificates from third-party root certificates. You use these certificates to encrypt and authenticate communication between CA ControlMinder components.

You can create a password-protected server certificate; if you do, CA ControlMinder uses a specified password to protect the private key for the server certificate.

You need the following files to create a server certificate from a third-party root certificate:

- **root.pem**—Root certificate
- **root.key**—Private key for the root certificate

To use a server certificate you generate from a third-party root certificate

1. Verify that CA ControlMinder services are stopped and that SSL is enabled.
2. If you use OU password-protected certificates, verify that the value of the fips_only configuration setting in the crypto section is 0.

   Note: You cannot use password-protected certificates if CA ControlMinder is operating in FIPS-only mode.
3. Delete every file *except* sub_cert_info in the following directory, where *ACInstallDir* is the directory in which you installed CA ControlMinder:

   ACInstallDir/data/crypto

   Important! Do not delete the sub_cert_info file.

   The default server certificate and default key for the server certificate are deleted.
4. Replace the root certificate. Do *one* of the following:
   - Copy the new root certificate to the location specified in the ca_certificate configuration setting in the crypto section.
   - Edit the value of the ca_certificate configuration setting in the crypto section to specify the full path to the new root certificate.

     Note: If you install the root certificate in a new directory, write CA ControlMinder FILE rules to protect that directory.
5. Use the sechkey utility to generate a server certificate.

   Note: For more information about the sechkey utility, see the *Reference Guide*. You must have the ADMIN attribute to use sechkey. If you are working with a third-party program that uses the CA ControlMinder SDK, append the -s option to the sechkey command when you run sechkey.

6. (Optional) Delete the private key for the root certificate.

   If you do not want to create another server certificate from the root certificate, you can delete the private key for the root certificate.

7. Start CA ControlMinder:

   - If you are changing the encryption settings on a CA ControlMinder Enterprise Management Server, also start the CA ControlMinder Web Service.
   - If you are working with a third-party program that uses the CA ControlMinder SDK, restart the process that uses the CA ControlMinder SDK.

   SSL encryption is enabled.

Example: Use sechkey to Create a Server Certificate

This example creates a server certificate from a third-party root certificate. This example uses the default CA ControlMinder certificate information file. The private key for the root certificate is named custom_root.key and located at /opt/CA/AccessControl/data/crypto:

```
sechkey -e -sub -in "/opt/CA/AccessControl/data/crypto/sub_cert_info" -priv
/opt/CA/AccessControl/data/crypto/custom_root.key
```

Password-Protected Server Certificates

You can configure CA ControlMinder to use a password-protected server certificate; if you do, CA ControlMinder uses a specified password to protect the private key for the server certificate. CA ControlMinder stores the password in the crypto.dat file in the *ACInstallDir*/Data/crypto directory, where *ACInstallDir* is the directory in which you installed CA ControlMinder. The crypto.dat file is hidden, encrypted, read-only, and protected by CA ControlMinder. If CA ControlMinder is stopped, only the superuser can access the password.

If you create a password-protected server certificate, sechkey does not encrypt the certificate. If you create a server certificate that is not password-protected, sechkey encrypts the certificate using AES256 and the CA ControlMinder encryption key.

Enterprise Management Server SSL Communication

Starting from 12.7, the Enterprise Management Server components use SSL for communication. You can modify the SSL communication setting for the following components:

- JBoss Application Server

  By default, JBoss is not installed with SSL support.

- Message Queue

  You can modify the Message Queue default SSL ports to prevent unauthorized access to well-known ports.

- CA ControlMinder Enterprise Management
- (Optional) Java Connector Server

  Import a new SSL certificate after you upgrade to CA ControlMinder r12.5 SP3 only if you used the default certificate.

SSL Communication for JBoss

Starting from 12.7, the JBoss application server is installed with SSL support.You can modify the JBoss SSL communication settings.

Note: For more information about how to configure SSL for JBoss, refer to the JBoss product documentation.

Example: Modify JBoss for SSL Communication on Windows

This example shows you how to configure the JBoss application server to use SSL for secure communication.

Important! This procedure describes how to configure JBoss to use SSL for secure communication using JBoss version 4.2.3 and JDK version 1.5.0.

Follow these steps:

1. Stop JBoss if it is running.
2. Open a command-prompt window and navigate to the following directory:

   JBoss_HOME\server\default\deploy\IdentityMinder.ear\custom\ppm\truststore

3. Enter the following command to change the default ssl, keystore password:

   `keytool -storepasswd -new <password> -keystore ssl.keystore -storepass secret`

   -storepasswd

   Specifies to change the keystore password. The password must be at least six (6) characters long.

   -keystore

   Specifies the keystore name to add the certificate.

   -keystore

   Specifies the keystore name.

   -storepass

   Defines the password that is used to protect the keystore.

4. Enter the following command to create a key for the Enterprise Management Server:

   `keytool -genkey -alias entm -keystore ssl.keystore -keyalg RSA`

   -genkey

   Specifies that the command generates a key pair (public and private keys).

   -alias

   Defines the alias to add an entry to the keystore.

   -keyalg

   Specifies the algorithm to generate the key pair.

   The keytool utility starts.

5. Enter the password *secret*.

6. Complete the prompts as required and press enter to verify the parameters that you entered.

   The certificate is added to the keystore.

   Note: The keystore and key alias must use identical passwords.

7. Enter the following command to encrypt the keystore password to a file:

   `java -cp C:/jboss-4.2.3.GA/server/default/lib/jbosssx.jar org.jboss.security.plugins.FilePassword welcometojboss 13 <password> keystore.password`

   Note: The Salt and IterationCount are the variables that define the strength of the encrypted password. In this example, "welcometojboss" is the salt and 13 is the iteration count.

8. Locate the file named server.xml in the following directory and open it for editing:

   JBossInstallDir`\server\default\deploy\jboss-web.deployer`

9. Locate the <Connector Port> tag in the following section:

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443
         This connector uses the JSSE configuration, when using APR, the
         connector should be using the OpenSSL style configuration
         described in the APR documentation -->
    <!--
    <Connector port="18443" protocol="HTTP/1.1" SSLEnabled="true"
               maxThreads="150" scheme="https" secure="true"
               clientAuth="false" sslProtocol="TLS" />
```

Note: The connector port number corresponds to the JBoss HTTPS Port number that you specified during the prerequisite or CA ControlMinder Enterprise Management installation process.

10. Uncomment the "<!--" above the <Connector port> tag.

    You can now edit this tag.

11. Add the following properties to the <Connector port> tag:

```
securityDomain="java:/jaas/encrypt-keystore-password"
SSLImplementation="org.jboss.net.ssl.JBossImplementation"
```

12. Save and close the server.xml file.

13. Navigate to the following directory to locate the jboss-service.xml file:

```
JBOss_HOME/server/default/deploy/jboss-web.deployer/META-INF
```

14. Add the following mbean between the <server> and </server> tags:

```
<mbean code="org.jboss.security.plugins.JaasSecurityDomain"
name="jboss.security:service=PBESecurityDomain">
      <constructor>
         <arg type="java.lang.String" value="encrypt-keystore-password"></arg>
      </constructor>
      <attribute
name="KeyStoreURL">${jboss.server.home.dir}/deploy/IdentityMinder.ear/custom/
ppm/truststore/ssl.keystore</attribute>
      <attribute
name="KeyStorePass">{CLASS}org.jboss.security.plugins.FilePassword:${jboss.se
rver.home.dir}/deploy/IdentityMinder.ear/custom/ppm/truststore/keystore.passw
ord</attribute>
<attribute name="Salt">welcometojboss</attribute>
<attribute name="IterationCount">13</attribute>
 </mbean>
```

Note: In the preceding example, welcometojboss is the salt and 13 is the iteration count.

15. Save and close the jboss-service.xml.
16. Start and open CA ControlMinder Enterprise Management.

    Note: After you complete this procedure, you can select to connect to JBoss, and CA ControlMinder Enterprise Management, in either SSL or non-SSL modes.

How You Configure CA ControlMinder Enterprise Management for SSL Communication

You can configure the Enterprise Management Server to use SSL when working with Active Directory or CA Directory.

Do the following:

1. Obtain the users directory certificate in a DER, CRT or CERT format.
2. Add the certificate to the keystore.
3. Configure CA ControlMinder Enterprise Management to use SSL communication.

More information:

Adding the Users Directory Certificate to the Keystore (see page 468)
Configure CA ControlMinder Enterprise Management for SSL Communication (see page 469)

Adding the Users Directory Certificate to the Keystore

Before you can configure CA ControlMinder Enterprise Management to use SSL communication, add the users directory certificate to the keystore.

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

Example: Adding the Active Directory Certificate to the Keystore

Important! This example shows you how to configure CA ControlMinder Enterprise Management to use SSL for secure communication with Active Directory using JBoss version 4.2.3 and JDK version 1.5.0. You must obtain the Active Directory certificate in a DER, CER or CERT encoded binary format before you begin this procedure.

1. Stop JBoss if it is running. Do *one* of the following steps:
   - From the JBoss job windows, interrupt (Ctrl+C) the process.
   - Stop the JBoss Application Server service from the Services Panel.
2. On the Enterprise Management Server, open a command prompt window and navigate to the following directory:

   jbossInstallDir/server/default/deploy/IdentityMinder.ear/custom/ppm/truststore

3. Enter the following command:

   `keytool -import -keystore ssl.keystore -alias ad -file <activedirectory.cert>`

   A password prompt appears.

   -import

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

   -alias

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

   -file

   Specifies the full pathname of the Active Directory certificate file.

4. Enter the password *secret*.
5. Navigate to the JBoss bin directory. By default this directory is found in:

   JbossInstallDir/bin

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

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

7. Save the file and start JBoss.

More information:

Configure CA ControlMinder Enterprise Management for SSL Communication (see page 469)

Configure CA ControlMinder Enterprise Management for SSL Communication

After you add the users directory certificate to the keystore, you can configure CA ControlMinder Enterprise Management to work with SSL communication.

Note: To configure CA ControlMinder Enterprise Management for SSL connection you must enable the CA IdentityMinder Management Console. For more information about the CA IdentityMinder Management Console, see the *CA IdentityMinder Management Console online help*.

To configure CA ControlMinder Enterprise Management for SSL communication

1. In the CA IdentityMinder Management Console, click Directories.
2. Click the ac-dir directory.

   The Directory Properties windows appears.

3. At the bottom of the properties window, click Export.
4. When prompted, save the XML file.
5. Open the XML file for editing.
6. Locate the <Provider userdirectory="ac-dir" type="LDAP"> tag.
7. Change the secure parameter to true. For example:

   ```
   <LDAP searchroot="DC=abc,DC=company,DC=com" secure="true">
   ```

8. Locate the <Connection host="COMPUTER.abc.company.com" port=" "> tag and change the port number to 636. For example:

   ```
   <Connection host="COMPUTER.abc.company.com" port="636">
   ```

9. Search for all appearances of the <Container objectclass="top,organizationalUnit" attribute="ou"/> tag and enter the *value* parameter at the end of each line. For example:

   ```
   <Container objectclass="top,organizationalUnit" attribute="ou" value=""/>
   ```

10. Save the file.
11. In the CA IdentityMinder Management Console, from the directory properties page, click Update.

    The Update Directory window appears.

12. Type the path and file name of the XML file for updating the Identity Manager directory, or browse for the file, then click Finish.

    Status information is displayed in the Directory Configuration Output field.

13. Click Continue, and restart the environment.

    CA ControlMinder Enterprise Management can now communicate with the users directory using SSL.

More information:

Enable the CA IdentityMinder Management Console (see page 87)
Open the CA IdentityMinder Management Console (see page 88)

Message Queue Server SSL Port Numbers

When you install CA ControlMinder Enterprise Management, the Message Queue Server is configured with the default SSL communication port numbers. You can modify the port numbers after you installed CA ControlMinder Enterprise Management, for example, to prevent unauthorized access from well-known ports.

Example: Modifying the Message Queue Server SSL Port Numbers

The following example explains how to modify the Message Queue Server SSL port numbers from the default port numbers.

To modify the Message Queue Server SSL Port Numbers

Note: Stop all the CA ControlMinder services or daemons before you modify the Message Queue Server settings.

1. In the CA ControlMinder Enterprise Management Server, navigate to the following directory:

   ACServer_InstallDir/AccessControlServer/MessageQueue/tibco/ems/bin

2. Open the routes.conf file for editing.
3. Locate the entry [PR_DMS_SERVER] and modify the port number value at the url field. For example:

   ```
   url = ssl://PR_DMS_SERVER:7777
   ```

4. Open the tibemsd.conf file for editing.
5. Locate the entry listen ports and modify the port number. For example:

   ```
   listen = ssl://7777
   ```

6. Open the tibcoems-service.xml file for editing.
7. Locate the section <!-- The JMS provider loader --> and modify the port number at the java.naming.provider.url line. For example:

   ```
   java.naming.provider.url=tibjmsnaming://localhost:7777
   ```

8. Open the factories.conf file for editing.
9. Locate the following sections: [SSLQueueConnectionFactory], [SSLTopicConnectionFactory], [SSLXAQueueConnectionFactory] and modify the port number at the url field. For example:

   ```
   [SSLQueueConnectionFactory]
     type                    = queue
     url                     = ssl://7777
     ssl_verify_host         = disabled

   [SSLTopicConnectionFactory]
     type                    = topic
     url                     = ssl://7777
     ssl_verify_host         = disabled

   [SSLXAQueueConnectionFactory]
     type                    = xaqueue
     url                     = ssl://7777
     ssl_verify_host         = disabled
   ```

10. Locate the following entry: org.jboss.naming.NamingAlias and modify the port number. For example:

    `tibjmsnaming://localhost:7777`

11. Start the CA ControlMinder services.

    The Message Queue Server SSL port numbers are now modified as required.

Configure the Servers to Use an Identical Encryption Key

When you install more than one Enterprise Management Server, each server uses its own encryption key with which to encrypt and decrypt data in the central database. If your environment uses multiple Enterprise Management Servers to write data to and read data from a single central database, each server must use an identical encryption key.

Important! Complete the following steps only if you did not specify the FIPS key that the primary Enterprise Management Server uses when you installed the secondary Enterprise Management Server, using the **-DFIPS_KEY** option.

To configure the servers to use an identical encryption key

1. Stop JBoss if it is running. Do *one* of the following:
   - Interrupt the JBoss application server window (Ctrl+C).
   - Stop the JBoss service from the Services panel.
2. Configure the Enterprise Management Servers to use an identical encryption key. Do as follows:
   a. Copy the FIPSKey.dat file in the following directory from the primary Enterprise Management Server:

      JBoss_HOME`/server/default/deploy/IdentityMinder.ear/config/com/netegrity/config/keys`

   b. Paste the FIPSKey.dat file in this directory on each secondary Enterprise Management Server.

      A message appears informing you that files by that name exists.

   c. Select to overwrite the existing file with the new file.

      The new files are placed in the directory. Each Enterprise Management Server now uses an identical encryption key.

3. Use the new encryption key to update the AES passwords on each secondary Enterprise Management Server. Do as follows:
   a. Encrypt the clear text password (see page 508).
   b. Locate the following files on each secondary Enterprise Management Server:

      JBoss_HOME/server/default/conf/login-config.xml

      JBoss_HOME/server/default/deploy/properties-service.xml

   c. Replace each AES password in the files with the new, encrypted password.
4. Start JBoss.

   The primary and secondary Enterprise Management Servers now encrypt and decrypt data with an identical encryption key.

Example: Encrypted AES Password

The following snippet of the login-config.xml file shows an encrypted AES password:

```
<application-policy name="imobjectstoredb">
        <authentication>
                <login-module
code="com.netegrity.jboss.datasource.PasswordEncryptedLogin"
                flag="required">
                        <module-option name="userName">user1</module-option>
                        <module-option name="password">
                        {AES}:/lxnvWwAEcYhSm0u3YT3ow==</module-option>
                        <module-option name="managedConnectionFactoryName">

        jboss.jca:name=jdbc/objectstore,service=NoTxCM</module-option>
                </login-module>
        </authentication>
</application-policy>
```

Change the CA ControlMinder Web Service URL

You use the CA ControlMinder Web Service to access CA ControlMinder Enterprise Management and CA ControlMinder Endpoint Management. The CA ControlMinder Web Service URL has the format HTTP:*hostname*:*port;* for example, http://entmserver:5248. By default, *hostname* is the name of the Enterprise Management Server.

When you change the CA ControlMinder Web Service URL, you change the IP address and port that the web service listens on. To increase security, you can change the host name to localhost; for example, http://127.0.0.1:5248. Using localhost helps to limit the exposure of the web service, because it helps to prevent scanners from detecting the web service from outside the immediate localhost environment.

Follow these steps:

1. Stop JBoss and CA ControlMinder services if they are running.
2. Change the host name in the URL, as follows:
   - (Windows) Change the value of the machineName registry value in the WebService registry key to the new host name.
   - (Linux) Change the value of the machineName configuration setting in the WebService section of the seos.ini file to the new host name.
3. (Optional) Change the port number in the URL, as follows:
   - (Windows) Change the value of the portNumber registry value in the WebService registry key to the new port number.
   - (Linux) Change the value of the portNumber configuration setting in the WebService section of the seos.ini file to the port number.
4. Open the following file, where *JBoss_home* is the home directory in which you installed JBoss:

   JBoss_home/server/default/conf/webservice.properties
5. Change the value of the webservice.url property to the new host name and port. For example:

   ```
   webservice.url=http://127.0.0.1:5248
   ```
6. Save and close the file.
7. Restart CA ControlMinder services, including the CA ControlMinder Web Service.
8. Restart JBoss.

   The CA ControlMinder Web Service URL is changed.

Modify the Microsoft SQL Server Database Connectivity Settings

When you install the Enterprise Management Server on a Microsoft SQL server, the authentication mode is set to SQL Server Authentication. You can modify the database authentication mode after the installation is complete to work in Windows Authentication mode.

When the SQL Server is working in Windows Authentication mode, the Enterprise Management Server uses the JBoss service account to administer the central database on the SQL Server. If you want to use a different JBoss service account, you change the account on the SQL Server database instance.

Important! To set the SQL Server to work in Windows Authentication mode requires you to install the SQL Server JDBC 4.0 driver.

Important! Verify that you assign the user you specify in the Microsoft SQL Server the dbowner database role.

To modify the SQL server database connectivity settings, do the following:

1. If you have not already done so, download and extract the SQL Server JDBC 4.0 driver files into a temporary folder.
2. Stop JBoss if it is running. Do one of the following:
   - Interrupt the JBoss application server window (Ctrl+C).
   - Stop the JBoss service from the Services panel.
3. Navigate to the JBoss lib directory. The directory is located under:

   JBossInstallDir/server/default/lib
4. Copy the file sqljdbc4.jar from the temporary directory to the JBoss lib directory.

   A message appears informing you that a file by that name exists.
5. Select to overwrite the existing file with the new file.

   The new file is placed in the directory.
6. Navigate to the JBoss bin directory. By default, this directory is located at:

   JBossInstallDir/bin
7. Copy the file sqljdbc_auth.dll (version x64) from the temporary directory to the JBoss bin directory.

   The new file is placed in the directory.
8. Navigate to the JBoss deploy directory. By default, this directory is located at:

   JBoss-directory/server/default/deploy
9. Open the following files:
   - imquartzdb-ds.xml
   - imauditdb-ds.xml
   - imtaskpersistencedb-ds.xml
   - imworkflowdb-ds.xml
   - objectstore-ds.xml
   - reportsnapshot-ds.xml
10. In each file, locate the <connection-url> tag and add the following code after the DatabaseName= parameter:

    ;integratedSecurity=true
11. From each file, delete the <security-domain> tag.

12. Save the files and restart JBoss.

    CA ControlMinder Enterprise Management can now work with the SQL server in Windows Authentication mode.

Example: Modifying the JBoss Configuration Files to Enable Windows Authentication Mode

This example shows you how to modify one of the JBoss configuration files to switch from SQL Authentication mode to Windows Authentication mode. In this example, the administrator modifies the file objectstore-ds.xml and specifies that the connection mode is Windows Authentication (;integratedSecurity=true). Next, the administrator removes the <security-domain> tag from the file as it is applicable only to SQL Authentication mode.

The following extract displays the objectsstore-ds.xml file after the administrator modified the connection settings:

```
<connection-url>jdbc:sqlserver://example.comp.com:1433;
selectMethod=cursor;DatabaseName=ACDB;
integratedSecurity=true</connection-url>
```

Windows Authentication Configuration For the Report Portal

Valid on Windows

When you install the Report Portal (CA Business Intelligence) and select to use Microsoft SQL Server as the CMS database, the authentication mode is set to SQL Server Authentication. Microsoft SQL Server authentication uses a SQL user account to authenticate database connections.

If Active Directory is used in your organization, you can modify the authentication method to Windows Authentication. In Windows Authentication, connections to the CMS database are authenticated using a Domain user account and not a local user account.

Authenticating connection in Windows Authentication provides a secured method of communication between all Report Portal components. You can remove clear text passwords from the report packages you deploy on the Report Portal because you configure an ODBC connection to the database that contains the user credentials.

Important! Windows Authentication requires that you use both Internet Information Server (IIS) and Microsoft SQL Server.

How to Configure the Report Portal to Work in Windows Authentication

Understanding the steps you take to modify the Report Portal database connection authentication mode helps you to implement the Report Portal in Windows Authentication.

Do the following to configure the Report Portal for Windows Authentication:

1. Prepare a supported version of Microsoft SQL Server database to use as the CMS database.
2. Prepare the CA Business Intelligence CMS database using the default user and collation.
3. Create a System DSN and specify to use SQL Server Authentication.

   The system DSN is used to connect to the Report Portal CMS database.
4. Add an Active Directory user to the local Administrators group.

   You specify this user to authenticate when you configure the report portal to work in Windows Authentication.
5. Set the ASP.NET Web Service Extension to Allowed.
6. Install the Report Portal (CA Business Intelligence) (see page 105). Do the following during the installation:
   a. Select to install CA Business Intelligence in custom mode.
   b. Specify Microsoft SQL Server 2005 as the database.
   c. Specify IIS as the web server.
7. Configure the Report Portal for Windows Authentication.

   You configure the CA Business Intelligence services to use the Active Directory user account to authenticate in Windows Authentication.
8. Create a System DSN for the CA ControlMinder reporting database using Windows Authentication.

   The System DSN is used to connect to the CA ControlMinder reporting portal.
9. Deploy the report packages on the Report Portal.

Configure the Report Portal for Windows Authentication

After you install the Report Portal, you can now configure the Report Portal to work in Windows Authentication. You configure the Report Portal to use the Active Directory user account and modify the system DSN connection parameters.

To configure the Report Portal for Windows Authentication

1. Log into the Report Portal host as the operating system administrator.
2. Modify the System DSN for the Report Portal CMS to Windows NT Authentication.
3. Select Start, Programs, BusinessObjects XI Release 2, Business Objects Enterprise, Central Configuration Manager.

   The Central Configuration Manager opens, displaying the CA Business Intelligence services.
4. Stop all CA Business Intelligence services.
5. Modify the services Log On As settings to the Active Directory user credentials. Do so to all the CA Business Intelligence services.

   Important! Do not change the settings of the WinHTTP Web Proxy Auto-Discovery and World Wide Web Publishing services.
6. Start all CA Business Intelligence services.

   The Report Portal is now configured to authenticate in Windows Authentication.

   Note: You can verify that the connections to the reporting database use the Active Directory user account from the Microsoft SQL Server Activity Monitor.

Example: Modify the CA Business Intelligence services Log On As connection settings

The following example shows you how to modify the CA Business Intelligence Connection Server service Log On As credentials from system account to an Active Directory account.

1. Right-click the Connection Server service from the list and select Properties.

   The Connection Server service properties window opens.
2. At the Log On As section, remove the mark from the System Account option.

   The connection settings fields are enabled.
3. Enter the Active Directory user name, password, and confirm the password.

   Example: Domain/username

   Click OK. The service connection settings are changed.
4. Exit the Central Configuration Manager.

System DSN Connection Configuration Example

System DSN connection settings define the parameters needed to connect to a database. In the following example, you create a system DSN that authenticates users connection in SQL Server Authentication, because the Report Portal only supports SQL Authentication when it is installed. You configure the CMS database system DSN before you install CA Business Intelligence.

In the following example, you create a System DSN for the Report Portal CMS database:

1. Select Start, Settings, Control Panel, Administrative Tools, Data Sources (ODBC).

   The ODBC Data Sources Administrator opens.

2. From the System DSN tab, select Create.

   The Select a New Data Source window opens.

3. Scroll down and select SQL Server, then click Finish.

   The Create a New Data Source to SQL Server wizard opens.

4. Enter the connection name, description and SQL server name. Click Next.
5. Select to use SQL Server Authentication.
6. Enter the administrator user credentials to connect to the SQL server. Click Next.
7. Select the Change the default database to option and select the Report Portal CMS database from the list. Click Next.
8. Click Finish. Select to test the connection, then click OK.

   The System DSN is created.

Deploy the Report Package on a Report Portal that Works in Windows Authentication

Valid on Windows

To make use of the standard CA ControlMinder reports, you need to import the report package file into BusinessObjects InfoView.

Note: This procedure describes how you deploy a report package on the Report Portal when no previous version of the same package is already deployed.

To deploy the report package on the Report Portal

1. Verify that the central database, Distribution Server, and Report Portal are set up.

   Note: Verify that the JAVA_HOME variable is set up on the Report Portal computer.

2. Create a System DSN for the CA ControlMinder reporting database and specify to use Windows NT Authentication.

   The system DSN you create is used to connect to the CA ControlMinder reporting database.You specify the system DSN when you configure the report package.

3. Insert the CA Business Intelligence for Windows DVD into your optical disc drive and navigate to the \Disk1\cabi\biconfig folder.

4. Copy the contents of the biconfig directory into a temporary directory.

5. Insert the appropriate CA ControlMinder Server Components DVD for your operating system into your optical disc drive and navigate to the \ReportPackages folder.

6. Copy the following file from the optical disc into the same temporary directory:

   - \ReportPackages*RDBMS**import_biar_config*.xml
   - \ReportPackages*RDBMS**AC_BIAR_File*.biar

   RDBMS

   Defines the type of RDBMS used for CA ControlMinder reporting.

   Value: MSSQL2005.

   ***import_biar_config*.xml**

   Defines the name of the import configuration file (.xml) for your RDBMS.

   Value: import_biar_config_mssql_2005.xml

   Note: If you use MS SQL Server 2008 as your central database, configure the import_biar_config_mssql_2005.xml file.

   ***AC_BIAR_File*.biar**

   Defines the name of the CA ControlMinder reports file (.biar) for your language and RDBMS.

   Note: The <biar-file name> property of the import configuration file for your RDBMS points to this file. It is set by default to the name of the English version for your RDBMS.

7. Edit your copy of the *import_biar_config*.xml file. Define the following XML properties:

   Important! Remove the user name, password and server fields from the file.

   <biar-file name>

   Defines the full pathname to the CA ControlMinder reports file (.biar). This is the file that you copied in the previous step.

   <networklayer>

   Defines the network layer supported by your RDBMS.

   Value: ODBC.

   <rdms>

   Defines the type of RDBMS used for CA ControlMinder reporting.

   Value: Generic ODBC datasource

   <datasource>

   Defines the DSN you created

   Important! Specify the name of the database used by CA ControlMinder for reporting and not the CA Business Intelligence CMS.

8. Open a command prompt window and enter the following command:

   System_Drive:\BO\biconfig.bat -h *host_name* -u *user_name* -p *password* -f *ac_biar_config*.xml

   host_name

   Defines the Report Portal host name.

   user_name

   Defines the Report Portal administrator you configured when you installed the Report Portal.

   password

   Defines the password for the Report Portal administrator.

   For example:

   ```
   biconfig.bat -h reportportal.comp.com -u Administrator -p P@ssw0rd -f
   C:\BO\import_biar_config_mssql_2005.xml
   ```

Example: Sample Microsoft SQL Server 2005 Import Configuration File Configured to use Windows Authentication

The following code snippet is an example of an edited import configuration file (import_biar_config_mssql2005.xml) for MS SQL Server 2005 you deploy on a Report Portal that works in Windows Authentication:

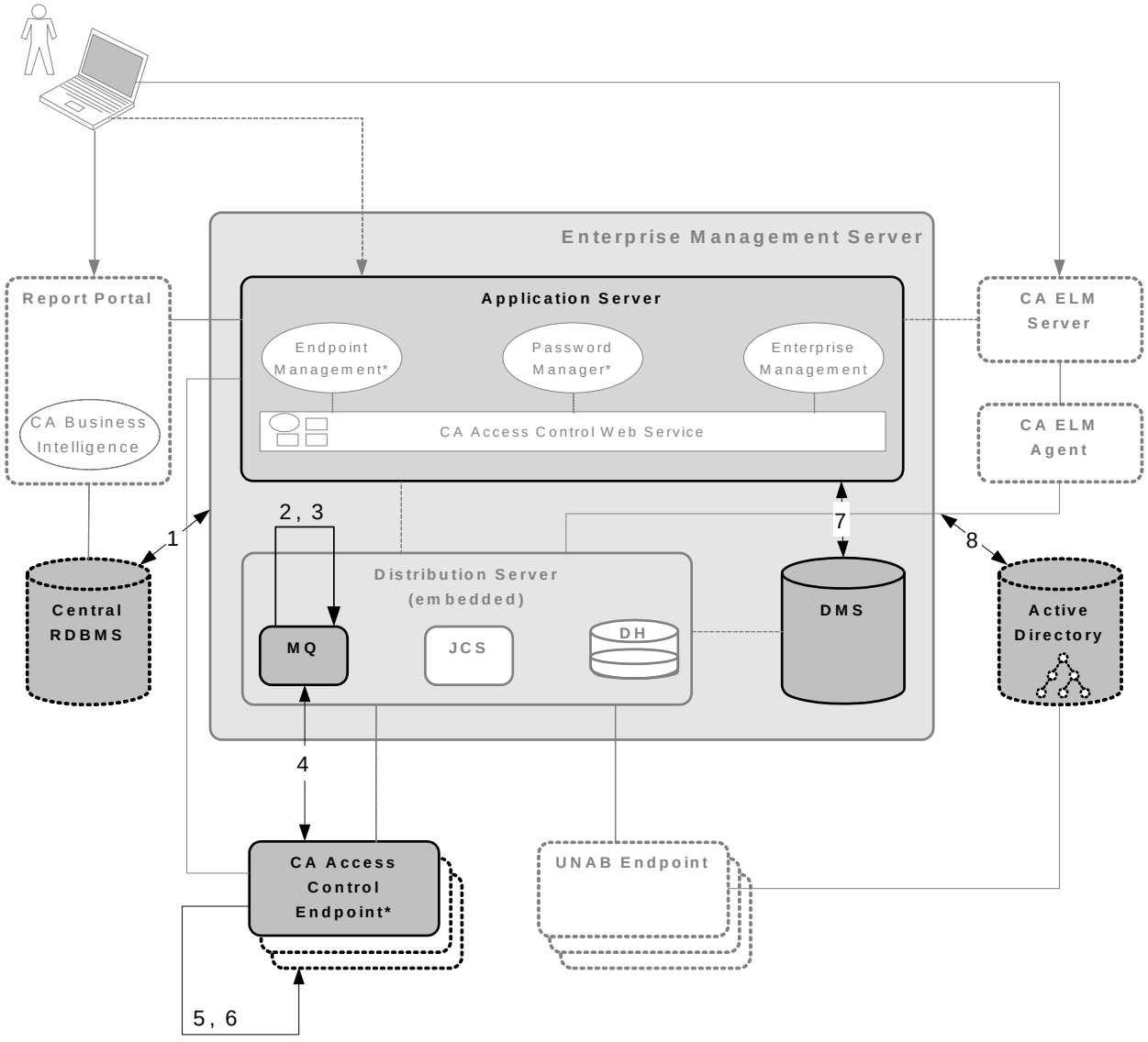
```
<?xml version="1.0"?>
<biconfig version="1.0">
        <step priority="1">
                <add>
                        <biar-file name="c:\temp\biconfig\
                        AccessControl_R12.5_EN_JP_KR_SQL_6_DEC_2009.biar">
                                <networklayer>ODBC</networklayer>
                                <rdms>Generic ODBC datasource</rdms>
                                <datasource>acdb</datasource>
                        </biar-file>
                </add>
        </step>
</biconfig>
```

Appendix C: Changing CA ControlMinder Service Account Settings

This section contains the following topics:

How CA ControlMinder Service Accounts Interact with CA ControlMinder Components

The following diagram shows how the service accounts interact with various CA ControlMinder components.



The numbers in the diagram correspond to the following service accounts:

1. RDBMS_service_user

   This account authenticates communication between the Enterprise Management Server and the RDMBS.

   Note: This account is not named RDBMS_service_user. You specify the name of this account when you create a user to prepare the database for CA ControlMinder Enterprise Management.

2. guest

   This account is the JNDI connection account that locates the message queue in the Message Queue server.

   Note: You can change the JNDI connection account after installation.

3. reportserver

   This account lets the DMS and CA ControlMinder Enterprise Management log in to the Message Queue.

4. +reportagent

   This account lets an endpoint log in to the Message Queue.

5. +policyfetcher

   This account executes the policyfetcher daemon or service on the endpoint.

6. +devcalc

   This account executes the policy deviation calculation on the endpoint.

7. ac_entm_pers

   This account authenticates communication between the Enterprise Management Server and the DMS.

8. ADS_LDAP_bind_user

   This account lets CA ControlMinder Enterprise Management perform LDAP queries against Active Directory.

   Note: This account is not named ADS_LDAP_bind_user. The name of this account is the User DN that you specify in the Active Directory Settings wizard page when you install CA ControlMinder Enterprise Management.

Service Account Passwords

In most cases, you set the password for CA ControlMinder service accounts when you install CA ControlMinder Enterprise Management. However, you may need to change the password for these accounts after installation. For example, you may be required to change the passwords each year to comply with your organization's security or password policies.

If a service account interacts with two CA ControlMinder components, you must change the password for the account on each component. If you change the password on only one component, the service account cannot log in to the other component.

Change the RDBMS_service_user Password

The RDBMS_service_user account authenticates communication between the Enterprise Management Server and the RDBMS. This account is not named RDBMS_service_user. You create this account when you prepare the database for CA ControlMinder Enterprise Management, and you provide the account name and password, along with other database information, when you install CA ControlMinder Enterprise Management.

You may need to regularly change the RDBMS_service_user password to comply with your organization's security and password policies. You must change the password on both the Enterprise Management Server and the RDBMS.

Before you change the password for this account, note the following:

- The default password for this account is the password that you specified when you created the user.
- The password has the following limitations:
  - Must be 1-50 characters long
  - Must not contain high ASCII characters
  - Must not contain double quotes (")
  - Must adhere to RDBMS password rules
- The password is stored in the following XML file, where *JBoss_home* is the directory in which you installed JBoss:

  JBoss_home/server/default/conf/login-config.xml

To change the RDBMS_service_user password

1. Change the password using your database tools.

   Note: For more information about how to change the password, see the MS SQL or Oracle documentation.

2. Change the password in the Enterprise Management Server:

   a. Stop JBoss Application Server.

   b. Encrypt the clear text password (see page 508).

   c. Change the password in the login-config.xml file (see page 510).

   d. Restart JBoss Application Server.

   e. Verify that you can log in to CA ControlMinder Enterprise Management.

      JBoss is successfully started and the password is changed in the Enterprise Management Server.

   The RDBMS_service_user password is changed in all locations.

Example: Change the Password in the login-config.xml File

This snippet of the login-config.xml file shows you one instance of the changed RDMBS_service_user password. The user is named caidb01. The password has been encrypted and is }>8:Jt^+%INK&i^v:

```
<application-policy name="imobjectstoredb">
        <authentication>
                <login-module
code="com.netegrity.jboss.datasource.PasswordEncryptedLogin"
                flag="required">
                        <module-option name="userName">caidb01</module-option>
                        <module-option name="password">
                        {AES}:}>8:Jt^+%INK&i^v==</module-option>
                        <module-option name="managedConnectionFactoryName">

        jboss.jca:name=jdbc/objectstore,service=NoTxCM</module-option>
                </login-module>
        </authentication>
</application-policy>
```

Change the reportserver Password

CA ControlMinder Enterprise Management and the DMS use the reportserver account to connect to the Message Queue.

CA ControlMinder Enterprise Management uses the reportserver account to do the following:

- Send reporting data to CA User Activity Reporting Module
- Send UNAB remote migration commands
- Provide privileged account passwords to the SAM Agent on SAM endpoints
- Receive reporting data from CA ControlMinder endpoints

The DMS uses the reportserver account to do the following:

- Send UNAB policies to UNAB endpoints
- Receive policy deployment status information that is sent from UNAB endpoints

You may need to regularly change the reportserver password to comply with your organization's security and password policies. You must change the password on the Distribution Server, Enterprise Management Server, and DMS.

Before you change the reportserver password, note the following:

- The default password for this account is the communication password that you specify when you install CA ControlMinder Enterprise Management.
- The password has the following limitations:
  - Must be 1–240 characters long
  - Must not contain high ASCII characters
  - Must not contain double quotes (")
- The password is stored in the Message Queue and the following XML files, where *JBoss_home* is the directory in which you installed JBoss:
  - *JBoss_home*/server/default/deploy/properties-service.xml
  - *JBoss_home*/server/default/conf/login-config.xml

Important! If you have more than one Distribution Server in your enterprise, first change the password on the Distribution Server installed on the Enterprise Management Server, then change the password on the other Distribution Servers in your enterprise.

To change the reportserver password

1. On the Distribution Server, set the Message Queue password for the reportserver user (see page 506).

   You have changed the reportserver password on the Distribution Server.

2. Change the password on the Enterprise Management Server, as follows:

   a. Stop JBoss Application Server.

   b. Encrypt the clear text password (see page 508).

   c. Change the password in the properties-service.xml file (see page 509).

   d. Change the password in the login-config.xml file (see page 510).

   e. Restart JBoss Application Server.

   f. Verify that you can log in to CA ControlMinder Enterprise Management.

      JBoss is successfully started and the password on the Enterprise Management Server is changed.

3. Use sechkey to change the reportserver password on the DMS (see page 505).

   The reportserver password is changed in all locations.

Example: Set the Message Queue Password For the reportserver User

This Tibco EMS Administration Tool command sets the Message Queue password for the reportserver user. The password is "secret", and must be in clear text and enclosed in double quotes:

```
ssl://localhost:7243> set password reportserver "secret"
Password of user 'reportserver' has been modified
ssl://localhost:7243>
```

Example: Change the Password in the properties-service.xml File

This snippet of the properties-service.xml file shows you the changed reportserver password. The password has been encrypted and is }>8:Jt^+%INK&i^v:

```
<attribute name="Properties">
      SamMDB.mdb-user=reportserver
      <!-- encoded tibco password -->
      SamMDB.mdb-passwd={AES}:}>8:Jt^+%INK&i^v==
</attribute>
```

Example: Change the Password in the login-config.xml File

This snippet of the login-config.xml file shows you the changed reportserver password. The password has been encrypted and is }>8:Jt^+%INK&i^v:

```
<application-policy name="JmsXATibcoRealm">
       <authentication>
          <login-module
code="com.netegrity.jboss.datasource.PasswordEncryptedLogin" flag="required">
             <module-option name="userName">reportserver</module-option>
            <module-option
name="password">{AES}:}>8:Jt^+%INK&i^v==</module-option>
                <module-option name="managedConnectionFactoryName">
                jboss.jca:service=TxCM,name=TibcoJmsXA</module-option>
          </login-module>
       </authentication>
    </application-policy>
```

Example: Use sechkey to Change the Message Queue Password on the DMS

This command changes the Message Queue password on the DMS. The password is "secret", and must be in clear text and enclosed in double quotes:

```
sechkey -t -server -pwd "secret"
```

Change the +reportagent Password

The +reportagent account lets an endpoint log in to the Message Queue. On each endpoint, the UNAB Agent, SAM Agent, and Report Agent use this account to communicate with the Message Queue.

You may need to regularly change the +reportagent password to comply with your organization's security and password policies. Change the password on both the Message Queue and the endpoints.

Before you change the +reportagent password, note the following:

- The default password is the communication password that you specify when you install CA ControlMinder Enterprise Management.
- The password has the following limitations:
  - Must be 1–240 characters long
  - Must not contain high ASCII characters
  - Must not contain double quotes (")
- The password is stored in the Message Queue and the CA ControlMinder database on the endpoint (seosdb).

Important! If you have more than one Distribution Server in your enterprise, first change the password on the Distribution Server installed on the Enterprise Management Server, then change the password on the other Distribution Servers in your enterprise. The Message Queue is part of the Distribution Server.

To change the +reportagent password

1. On the Distribution Server, set the Message Queue password for the +reportagent user (see page 506).

   The +reportagent password is changed on the Message Queue.

2. Use sechkey to change the password (see page 505) that ReportAgent uses to connect to the Message Queue on the endpoints.

   The changed +reportagent password is propagated to the endpoints.

   Note: You can also use selang to change the +reportagent password on the endpoints. However, you cannot use a policy to propagate the selang command, because you cannot use advanced policy management to set user passwords.

Example: Set the Message Queue Password For the +reportagent User

This Tibco EMS Administration Tool command sets the Message Queue password for the +reportagent user. The password is "secret", and must be in clear text and enclosed in double quotes:

```
ssl://localhost:7243> set password +reportagent "secret"
Password of user '+reportagent' has been modified
ssl://localhost:7243>
```

Example: Use sechkey to Change the Message Queue Password on the Endpoints

This command propagates the Message Queue password for the +reportagent user to the endpoints that are subscribed to the Distribution Server. The password is "secret", and must be in clear text and enclosed in double quotes:

```
sechkey -t -pwd "secret"
```

Change the +policyfetcher Password

The +policyfetcher account executes the policyfetcher daemon or service, which looks for deployment tasks on the DH, applies policy updates to the local CA ControlMinder database (seosdb), and sends a heartbeat to the DH at regular intervals. CA ControlMinder uses a SPECIALPGM rule to define +policyfetcher as a system user. +policyfetcher runs as the NT Authority\System user in Windows.

You may need to regularly change the +policyfetcher password to comply with your organization's security and password policies.

Before you change the +policyfetcher password, note the following:

- There is no default password for this account. CA ControlMinder does not set a password for +policyfetcher during installation.
- The password has the following limitations:
  - Must be 1–240 characters long
  - Must not contain high ASCII characters
  - Must not contain double quotes (")
- The password is stored in seosdb, the local CA ControlMinder database.

Important! To prevent this user from logging in to the CA ControlMinder database, we recommend that you do not set a password for this user.

To change the +policyfetcher password, use selang to change the password (see page 504).

Example: Change the +policyfetcher Password

This command changes the password for the +policyfetcher user. The password is "secret", and must be in clear text and enclosed in double quotes:

```
AC> cu +policyfetcher password("secret") grace- nonative
(localhost)
Successfully updated USER +policyfetcher
```

Change the +devcalc Password

The +devcalc account executes the policy deviation calculation, which calculates the difference between the expected access rules that will be deployed on an endpoint (as a result of policy deployment) and the actual rules that have been successfully deployed on the same endpoint. CA ControlMinder uses a SPECIALPGM rule to define +devcalc as a system user. +devcalc runs as the NT Authority\System user in Windows.

You may need to regularly change the +devcalc password to comply with your organization's security and password policies.

Before you change the +devcalc password, note the following:

- There is no default password for this account. CA ControlMinder does not set a password for +devcalc during installation.
- The password has the following limitations:
  - Must be 1–240 characters long
  - Must not contain high ASCII characters
  - Must not contain double quotes (")
- The password is stored in seosdb, the local CA ControlMinder database.

Important! To prevent this user from logging in to the CA ControlMinder database, we recommend that you do not set a password for this user.

To change the +devcalc password, use selang to change the password (see page 504).

Example: Change the +devcalc Password

This command changes the password for the +devcalc user. The password is "secret", and must be in clear text and enclosed in double quotes:

```
AC> cu +devcalc password("secret") grace- nonative
(localhost)
Successfully updated USER +devcalc
```

Change the ac_entm_pers Password

The ac_entm_pers account authenticates communication between the DMS and the Enterprise Management Server.

You may need to regularly change the ac_entm_pers password to comply with your organization's security and password policies. You must change the password on both the RDBMS and the DMS.

Before you change the ac_entm_pers password, consider the following:

- The default password is a password that is randomly generated by CA ControlMinder during installation.
- The password has the following limitations:
  - Must be 1-48 characters long
  - Must not contain double quotes (")
  - Must not contain high ASCII characters
- The password is stored in the RDBMS and the DMS.

To change the ac_entm_pers password

1. Use selang to change the ac_entm_pers password in the DMS (see page 504).
2. In CA ControlMinder Enterprise Management, configure the connection to the DMS and specify the new password.

   The ac_entm_pers password is changed in all locations.

   Note: For more information about configuring the connection to the DMS, see the *CA ControlMinder Enterprise Management Online Help*.

Example: Use selang to Change the ac_entm_pers Password

This command connects to the DMS and changes the password for the ac_entm_pers user. The password is "secret", and must be in clear text and enclosed in double quotes:

```
AC> eu ac_entm_pers admin auditor nonative password(secret) logical nonative grace-
```

Change the ADS_LDAP_bind_user Password

The ADS_LDAP_bind_user account lets CA ControlMinder Enterprise Management perform LDAP queries against Active Directory. This account is not named ADS_LDAP_bind_user. The name of this account is the User DN that you specify in the Active Directory Settings wizard page when you install CA ControlMinder Enterprise Management.

You may need to regularly change the ADS_LDAP_bind_user password to comply with your organization's security and password policies. You must change the password on both Active Directory and the RDBMS.

Before you change the ADS_LDAP_bind_user password, note the following:

- The default password is the password that you specify in the Active Directory Settings wizard page when you install CA ControlMinder Enterprise Management.
- The password has the following limitations:
  - Must be 7-120 characters long
  - Must not contain high ASCII characters
  - Must not contain a colon (:)
  - Must adhere to Active Directory password rules
- The password is stored in Active Directory and the RDBMS

To change the ADS_LDAP_bind_user password

1. Change the password in Active Directory, using Active Directory tools.

   Note: For more information about how to change the password, see the Active Directory documentation.

2. Change the user directory password in the CA IdentityMinder Management Console (see page 512).

   The ADS_LDAP_bind_user password is changed in all locations.

Change the JNDI Connection Account

The JNDI connection account is named guest and locates the message queue in the Message Queue server. By default, this account does not have a password.

You can change the account that JNDI uses to locate the message queue in the Message Queue server. The name of this account is stored in the Message Queue and the following XML file, where *JBoss_home* is the directory in which you installed JBoss:

JBoss_home/server/default/deploy/jms/tibco-jms-ds.xml

To change the JNDI connection account

1. Create a Message Queue user.
2. Change the JNDI connection account, as follows:
   a. Stop JBoss Application Server.
   b. Replace the account name in the tibco-jms-ds.xml file with the name of the Message Queue user you created.
   c. Restart JBoss Application Server.
   d. Verify that you can log into CA ControlMinder Enterprise Management.

      JBoss is successfully started and the JNDI connection account is changed.

Create a Message Queue User

You create a Message Queue user when you change the JNDI connection account.

To create a Message Queue user

1. Navigate to the following directory, where *DistServer* is the directory in which you installed the Distribution Server:

   DistServer/MessageQueue/tibco/ems/5.1/bin
2. (UNIX) Enter the following command:

   ```
   tibemsadmin
   ```

   The Tibco EMS Administration Tool starts.
3. (Windows) Enter the following command:

   ```
   tibemsadmin.exe
   ```

   The Tibco EMS Administration Tool starts.
4. Connect to the current environment, using one of the following commands:
   - If the Distribution Server listens for the Report Agent on port 7222 (the default port), use the following command:

     ```
     connect
     ```
   - If the Distribution Server listens for the Report Agent in SSL mode on port 7243, use the following command:

     ```
     connect SSL://7243
     ```
5. Enter your username and password.

   Note: The default username is admin and the password is the communication password that you specified when you installed CA ControlMinder Enterprise Management.

   You are connected to the Message Queue.

6. Enter the following command:

   `create user username`

   username

   Specifies the name of the new Message Queue user.

   The new user is created.

Example: Create a Message Queue User

This Tibco EMS Administration Tool command creates a Message Queue user named example:

```
> connect SSL://7243
Login name (admin): admin
Password:
Connected to: ssl://localhost:7243
ssl://localhost:7243> create user example
User 'example' has been created
ssl://localhost:7243>
```

Change the Account in the tibco-jms-ds.xml File

You change the account in the tibco-jms-ds.xml file when you change the JNDI connection account.

To change the account in the tibco-jms-ds.xml file

1. Stop JBoss Application Server if it is not already stopped.
2. Navigate to the following directory, where *JBoss_home* is the directory in which you installed JBoss:

   JBoss_home/server/default/deploy/jms
3. Open the tibco-jms-ds.xml file in a text-based editor.
4. Change the account name at the end of the following parameter:

   `java.naming.security.principal=`
5. Save and close the file.

Example: Change the Account Name in the tibco-jms-ds.xml File

This snippet of the tibco-jms-ds.xml file shows the changed JNDI connection account. The account is named example:

```
<!-- The JMS provider loader -->
        <mbean code="org.jboss.jms.jndi.JMSProviderLoader"
        name=":service=JMSProviderLoader,name=TibjmsProvider">
                <attribute name="ProviderName">TIBCOJMSProvider</attribute>
                <attribute name="ProviderAdapterClass">
                org.jboss.jms.jndi.JNDIProviderAdapter</attribute>
                <attribute
name="FactoryRef">SSLXAQueueConnectionFactory</attribute>
                <attribute
name="QueueFactoryRef">SSLXAQueueConnectionFactory</attribute>
                <attribute
name="TopicFactoryRef">SSLXATopicConnectionFactory</attribute>
                <attribute name="Properties">
                        java.naming.security.principal=example

        java.naming.factory.initial=com.tibco.tibjms.naming.TibjmsInitialContextF
actory
                        java.naming.provider.url=tibjmsnaming://localhost:7243
                        java.naming.factory.url.pkgs=com.tibco.tibjms.naming
                        com.tibco.tibjms.naming.security_protocol=ssl
                        com.tibco.tibjms.naming.ssl_enable_verify_host=false

                </attribute>
        </mbean>
```

Changing Message Queue Communication Settings

You can change the following Message Queue communication settings:

- The password for the Message Queue administrator
- The Message Queue server certificate
- The Message Queue URL
- The password for the Message Queue SSL keystore
- The password that endpoints use to connect to the Message Queue

  Note: Endpoints use the +reportagent service account to connect to the Message Queue.
- The password that CA ControlMinder Enterprise Management and the DMS use to connect to the Message Queue

  Note: CA ControlMinder Enterprise Management and the DMS use the reportserver service account to connect to the Message Queue.

More information:

Change the +reportagent Password (see page 491)
Change the reportserver Password (see page 488)

Change the Message Queue Administrator Password

The Message Queue administrator account is named *admin* and lets you perform administrative tasks in the Message Queue.

You may need to regularly change the admin password to comply with your organization's security and password policies.

Before you change the Message Queue administrator password, note the following:

- The default password for this account is the communication password that you specify when you install CA ControlMinder Enterprise Management.
- The password has the following limitations:
  - Must be 1-240 characters long
  - Must not contain high ASCII characters
  - Must not contain double quotes (")
  - Must not contain @ and $ signs
- The password is stored in the Message Queue.

Important! If you have more than one Distribution Server in your enterprise, first change the password on the Distribution Server installed on the Enterprise Management Server, then change the password on the other Distribution Servers in your enterprise. The Message Queue is part of the Distribution Server.

To change the Message Queue administrator password, set the Message Queue password for the admin user (see page 506).

Example: Set the Message Queue Password For the admin User

This Tibco EMS Administration Tool command sets the Message Queue password for the admin user. The password is "secret", and must be in clear text and enclosed in double quotes:

```
ssl://localhost:7243> set password admin "secret"
Password of user 'admin' has been modified
ssl://localhost:7243>
```

Change the Message Queue Server Certificate

The Message Queue uses the server certificate for SSL communication between the Message Queue and its clients. The Message Queue clients are CA ControlMinder endpoints and CA ControlMinder Enterprise Management.

To change the Message Queue server certificate

1. Stop the CA ControlMinder Message Queue.
2. Create an X.509 server certificate.

   We recommend that you create a .p12 format certificate.
3. Navigate to the following directory, where *DistServer* is the directory in which you installed the Distribution Server:

   `DistServer/MessageQueue/tibco/bin/ems`
4. Enter the following command:

   `tibemsadmin -mangle password`

   password

   Specifies the password for the server certificate.

   The password for the server certificate is encrypted.
5. Open the tibemsd.conf file in a text-based editor. The file is located in the following directory:

   `DistServer/MessageQueue/tibco/bin/ems`
6. Change the value of the following parameters:

   ssl_server_identity

   Specifies the full path to the server certificate.

   ssl_server_key

   Specifies the full path to the server certificate key.

   Note: Leave this parameter blank if you use a .p12 certificate.

   ssl_password

   Specifies the encrypted password for the server certificate.
7. Save and close the file.

   The Message Queue server certificate is changed.
8. Restart the CA ControlMinder Message Queue.

Example: The tibemsd.conf file

The following is an example of the Message Queue server parameters in the tibemds.conf file for a .p12 server certificate. The password has been encrypted and is }>8:Jt^+%INK&i^v, and the ssl_server_key parameter has no value:

```
ssl_server_identity     = "C:\Program
Files\CA\AccessControlServer\MessageQueue\conf\keystore.p12"
ssl_server_key          =
ssl_password            = }>8:Jt^+%INK&i^v
```

Change the Password for the Message Queue SSL Keystore

The Message Queue SSL keystore stores the server certificates that the Message Queue uses for SSL communication. When you change the password for the Message Queue SSL keystore, you update the public/private key pair that signs the server certificates.

You may need to regularly change the password for the Message Queue SSL keystore to comply with your organization's security and password policies.

Before you change the password for the Message Queue SSL keystore, note the following:

- The default password is the communication password that you specify when you install CA ControlMinder Enterprise Management.
- The password has the following limitations:
  - Must be 6-50 characters long
  - Must not contain high ASCII characters
  - Must not contain double quotes (")
- The password is stored in the following file, where *ACServer* is the directory in which you installed CA ControlMinder Enterprise Management:

  ACServer/MessageQueue/conf/keystore.p12

Important! If you have more than one Distribution Server in your enterprise, first change the password on the Distribution Server installed on the Enterprise Management Server, then change the password on the other Distribution Servers in your enterprise. The Message Queue is part of the Distribution Server.

To change the password for the Message Queue SSL keystore

1. Stop the CA ControlMinder Message Queue service.
2. Open a command prompt window and navigate to the following directory, where *JDK* is the directory in which you installed the Java Development Kit:

   JDK/bin

3. Run the following command:

   ```
   keytool -genkey -keyalg RSA -keysize 1024 -keystore "keystore.p12" -storetype
   PKCS12 -dname "cn=acmq" -alias acmq -storepass "password" -keypass "password"
   ```

   -genkey

   Specifies that the command creates a key pair (public and private keys).

   -keyalg RSA

   Specifies to use the RSA algorithm to generate the key pair.

   -keysize 1024

   Specifies that the size of the generated key is 1024 bits.

   -storetype PKCS12

   Specifies that the generated key is in the PKCS12 file format.

   -dname "cn=acmq"

   Specifies that X.500 distinguished name for the generated certificate is acmq. This name is used in the issuer and subject fields of the certificate.

   -alias acmq

   Specifies to update the keystore entry names acmq.

   -storepass "*password*"

   Specifies the password that protects the Message Queue SSL keystore. The password must be identical to the password that you specify for the -keypass parameter.

   -keypass "*password*"

   Specifies the password that protects the private key of the new key pair. The password must be identical to the password that you specify for the -storepass parameter.

   The keytool utility changes the password for the Message Queue SSL keystore.

4. Navigate to the following directory, where *DistServer* is the directory in which you installed the Distribution Server:

   ```
   DistServer/MessageQueue/tibco/bin/ems
   ```

5. Run the following command:

   ```
   tibemsadmin -mangle password
   ```

   The password for the SSL keystore is encrypted.

Change the Message Queue URL

The Message Queue uses the localhost as the URL.You can modify the URL to use the fully qualified distinguished name (FQDN) of the host by modifying the tibco-jms-ds.xml file.

The URL information is stored in the Message Queue in the following XML file, where *JBoss_HOME* is the directory where you installed JBoss:

JBoss_home/server/default/deploy/jms/tibco-jms-ds.xml

Follow these steps:

1. Stop the JBoss Application Server, the CA ControlMinder Message Queue service and all the CA ControlMinder services.
2. Back up the tibco-jms-ds.xml file that is placed at the following location:

   JBoss_home\server\default\deploy\jms
3. Open the tibco-jms-ds.xml file and perform the following steps:
   a. Locate *localhost*.
   b. Replace *localhost* with *FQDN*.
   c. Perform steps a and b for every instance of *localhost*.
   d. Save and close the file.
4. Browse to the following location to modify the communication key:

   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Common\commmunication
5. Locate the key value *Distribution_Server*.

   The default value is ssl://localhost:7243.
6. Replace the *ssl://localhost:7243* value with *ssl://<FQDN>:7243*.
7. Start all CA ControlMinder services, including the CA ControlMinder Message Queue service.
8. Start the JBoss service.

   The CA ControlMinder Message Queue URL is changed.

Password Change Procedures

The following procedures explain the different ways in which you can change CA ControlMinder passwords.

Use selang to Change a Password

You can use selang to change the password for the following service accounts:

- +policyfetcher
- +devcalc
- ac_entm_pers

You may need to regularly change the password for these accounts to comply with your organization's security and password policies.

When you use selang to change a password, note the following:

- You must enclose the password in double quotes.
- You cannot use advanced policy management to propagate password change commands.

Note: You may need to use more than one method to change the password on all components that the service account interacts with.

To use selang to change a password, run the following command:

```
cu user password("password") grace- nonative
```

user

Specifies the name of the user whose password you change.

password

Specifies the new password.

Note: If you cut and paste the password into the command, verify that the password does not contain carriage returns or line feeds.

Example: Change the +policyfetcher Password

This command changes the password for the +policyfetcher user. The password is "secret", and must be in clear text and enclosed in double quotes:

```
AC> cu +policyfetcher password("secret") grace- nonative
(localhost)
Successfully updated USER +policyfetcher
```

More information:

Change the +policyfetcher Password (see page 492)
Change the +devcalc Password (see page 493)

Use sechkey to Change a Message Queue Password

You can use sechkey to change the password for the following service accounts:

- reportserver
- +reportagent

You may need to regularly change the password for these accounts to comply with your organization's security and password policies. When you use sechkey to change a password, you must enclose the password in double quotes.

Note: You may need to use more than one method to change the password on all components that the service account interacts with.

To use sechkey to change a Message Queue password, run the following command on the Distribution Server:

```
{sechkey | acuxchkey} -t [-server] -pwd "password"
```

sechkey

Specifies to change the password on a CA ControlMinder endpoint.

acuxchkey

Specifies to change the password on a UNAB endpoint.

-server

Specifies to change the password on the DMS.

Note: This parameter is only valid with the sechkey parameter.

password

Specifies the new password.

Note: If you cut and paste the password into the command, verify that the password does not contain carriage returns or line feeds.

Example: Change the Message Queue Password on a UNAB Endpoint

This command propagates the Message Queue password to all UNAB endpoints that communicate with the Distribution Server. The password is "secret", and must be in clear text and enclosed in double quotes:

```
acuxchkey -t -pwd "secret"
```

Example: Change the Message Queue Password on the DMS

This command changes the Message Queue password on the DMS. The password is "secret", and must be in clear text and enclosed in double quotes:

```
sechkey -t -server -pwd "secret"
```

More information:

Change the +reportagent Password (see page 491)
Change the reportserver Password (see page 488)

Set a Message Queue Password

You set the Message Queue password to change the password for the following service accounts:

- reportserver
- +reportagent

You may need to regularly change the password for these accounts to comply with your organization's security and password policies. When you set a Message Queue password, you must enclose the password in double quotes.

Note: You may need to use more than one method to change the password on all components that the service account interacts with.

To set a Message Queue password

1. Navigate to the following directory, where *DistServer* is the directory in which you installed the Distribution Server:

   DistServer/MessageQueue/tibco/ems/5.1/bin

2. (UNIX) Enter the following command:

   ```
   tibemsadmin
   ```

   The Tibco EMS Administration Tool starts.

3. (Windows) Enter the following command:

   ```
   tibemsadmin.exe
   ```

   The Tibco EMS Administration Tool starts.

4. Connect to the current environment, using one of the following commands:

   - If the Distribution Server listens for the Report Agent on port 7222 (the default port), use the following command:

     ```
     connect
     ```

   - If the Distribution Server listens for the Report Agent in SSL mode on port 7243, use the following command:

     ```
     connect SSL://7243
     ```

5. Enter your username and password.

   Note: The default username is admin and the password is the communication password that you specify when you install CA ControlMinder Enterprise Management.

   You are connected to the Message Queue.

6. Run the following command:

   `set password` *`user`* "*`password`*"

   user

   Specifies the name of the user whose password you change.

   "***password***"

   Specifies the new password.

   The password for the user is changed on the Message Queue.

   Note: If you cut and paste the password into the command, verify that the password does not contain carriage returns or line feeds.

Example: Set the Message Queue Password for the reportserver User

This Tibco EMS Administration Tool command sets the Message Queue password for the reportserver user. The password is "secret", and must be in clear text and enclosed in double quotes:

```
> connect SSL://7243
Login name (admin): admin
Password:
Connected to: ssl://localhost:7243
ssl://localhost:7243> set password reportserver "secret"
Password of user 'reportserver' has been modified
ssl://localhost:7243>
```

More information:

Change the +reportagent Password (see page 491)
Change the reportserver Password (see page 488)

Encrypt a Clear Text Password

You encrypt clear text passwords for the following service accounts:

- RDBMS_service_user
- reportserver

You encrypt the passwords because they are stored in clear text XML files in the JBoss directory. You use the pwdtools utility to encrypt clear text passwords.

To avoid accidentally selecting carriage breaks in the encrypted password, we recommend that you direct the encrypted password (the output of the utility) to a text file. Otherwise, carriage breaks may occur if the encrypted password wraps over more than one line.

When you use pwdtools to encrypt a clear text password, you must enclose the password in double quotes.

To encrypt clear text passwords

1. Open a command prompt window.
2. Navigate to the following directory, where *ACServerInstallDir* is the directory in which you installed CA ControlMinder Enterprise Management:

   `ACServerInstallDir/IAM Suite/Access Control/tools/PasswordTool`
3. Run the following command:

   `pwdtools -FIPS -p "password" -k [filename]`

   password

   Specifies the clear text password.

   filename

   Specifies the name of the file to which pwdtools outputs the encrypted password.

   pwdtools encrypts the password.

Example: Encrypt a Clear Text Password

This command encrypts a clear text password and directs the encrypted password to the file pw.txt. The clear text password is "secret" and must be enclosed in double quotes:

```
C:\Program Files\CA\AccessControlServer\IAM Suite\Access
Control\tools\PasswordTool>
pwdtools.bat -FIPS -p "secret" -key
C:\jboss-4.2.3.GA\server\default\deploy\IdentityMinder.ear\config\com\netegrity\c
onfig\keys\FIPSkey.dat"
```

More information:

Change the reportserver Password (see page 488)
Change the RDBMS_service_user Password (see page 486)

Change the Password in the properties-service.xml File

You change the password in the properties-service.xml file to change the password for the reportserver account. You may need to regularly change the password for this account to comply with your organization's security and password policies.

Note: You may need to use more than one method to change the password on all components that the service account interacts with.

To change the password in the properties-service.xml file

1. Stop JBoss Application Server.
2. Navigate to the following directory, where *JBoss_home* is the directory in which you installed JBoss:

   JBoss_home/server/default/deploy
3. Open the properties-service.xml file in a text-based editor.
4. Change the password in the SamMDB.mdb-passwd parameter.
5. Save and close the file.

Example: Change the Password in the properties-service.xml File

This snippet of the properties-service.xml file shows you the changed reportserver password. The password has been encrypted and is }>8:Jt^+%INK&i^v:

```
<attribute name="Properties">
      SamMDB.mdb-user=reportserver
      <!-- encoded tibco password -->
      SamMDB.mdb-passwd={AES}:}>8:Jt^+%INK&i^v==
</attribute>
```

More information:

Change the reportserver Password (see page 488)

Change the Password in the login-config.xml File

You change the password in the login-config.xml file when you change the password for the following service accounts:

- RDBMS_service_user
- reportserver

You may need to regularly change the password for these accounts to comply with your organization's security and password policies.

Note: You may need to use more than one method to change the password on all components that the service account interacts with. If the password is a clear text password, use the pwdtools utility to encrypt it before you change the password in the login-config.xml file.

To change the password in the login-config.xml file

1. Stop the JBoss Application Server.
2. Navigate to the following directory, where *JBoss_home* is the directory in which you installed JBoss:

   JBoss_home/server/default/conf
3. Open the login-config.xml file in a text-based editor.
4. Change the RDBMS_service_user password:
   a. Locate each instance of the name of the RDBMS_service_user account in the file.

      There are six instances in the file. You name this account when you create a user to prepare the database for CA ControlMinder Enterprise Management.

   b. Change the password in the parameter that is immediately after each instance of the name.

      The parameter is enclosed by the <module-option name="password"> and </module-option> tags.

   The RDBMS_service_user password is changed.

5. Change the reportserver password:
   a. Locate the following parameter in the file:

      ```
      <module-option name="userName">reportserver</module-option>
      ```

   b. Change the password in the parameter that is immediately after this parameter.

      The parameter is enclosed by the <module-option name="password"> and </module-option> tags.

   The reportserver password is changed.
6. Save and close the file.

Example: Change the RDBMS_service_user Password in the login-config.xml File

This snippet of the login-config.xml file shows you one instance of the changed RDMBS_service_user password. The user is named caidb01. The password has been encrypted and is }>8:Jt^+%INK&i^v:

```
<application-policy name="imobjectstoredb">
        <authentication>
                <login-module
code="com.netegrity.jboss.datasource.PasswordEncryptedLogin"
                flag="required">
                        <module-option name="userName">caidb01</module-option>
                        <module-option
name="password">{AES}:}>8:Jt^+%INK&i^v==</module-option>
                        <module-option name="managedConnectionFactoryName">

        jboss.jca:name=jdbc/objectstore,service=NoTxCM</module-option>
                </login-module>
        </authentication>
</application-policy>
```

Example: Change the reportserver Password in the login-config.xml File

This snippet of the login-config.xml file shows you the changed reportserver password. The password has been encrypted and is }>8:Jt^+%INK&i^v:

```
<application-policy name="JmsXATibcoRealm">
       <authentication>
          <login-module
code="com.netegrity.jboss.datasource.PasswordEncryptedLogin" flag="required">
             <module-option name="userName">reportserver</module-option>
            <module-option
name="password">{AES}:}>8:Jt^+%INK&i^v==</module-option>
                 <module-option name="managedConnectionFactoryName">
                 jboss.jca:service=TxCM,name=TibcoJmsXA</module-option>
          </login-module>
       </authentication>
    </application-policy>
```

More information:

Change the reportserver Password (see page 488)
Change the RDBMS_service_user Password (see page 486)

Change the User Directory Password in the CA IdentityMinder Management Console

You change the user directory password in the CA IdentityMinder Management Console when you change the ADS_LDAP_bind_user password. You may need to regularly change the password for this account to comply with your organization's security and password policies.

Note: You may need to use more than one method to change the password on all components that the service account interacts with.

To change the user directory password in the CA IdentityMinder Management Console

1. Encrypt the clear text password (see page 508).
2. Open the CA IdentityMinder Management Console (see page 88).
3. Click Directories.

   The Directories page appears.
4. Click ac-dir.

   The Directory Properties page appears.

5. Click Export.

   The ac-dir.xml file is exported.

6. Open the exported file in a text-based editor.

7. Find the following parameter:

   ```
   <Credentials user=
   ```

8. Enter the encrypted password in the following field, which is after the <credentials> parameter:

   ```
   {PBES}=
   ```

9. Save and close the file.

10. In the CA IdentityMinder Management Console, from the Directory Properties page, click Update.

    The Update Directory window appears.

11. Type the path and file name of the XML file that you edited, or browse for the file, then click Finish.

    Status information is displayed in the Directory Configuration Output field.

12. Click Continue, and restart the environment.

    You have changed the user directory password in the CA IdentityMinder Management Console.

Example: Change the User Directory Password

This snippet of the exported ac-dir.xml file shows you the changed user directory password. The user is named Administrator. The password has been encrypted and is }>8:Jt^+%INK&i^v:

```
<Credentials user="CN=Administrator,cn=Users,DC=unixauthdemo,DC=co,DC=il">
{PBES}:}>8:Jt^+%INK&i^v==</Credentials>
```

More information:

Enable the CA IdentityMinder Management Console (see page 87)
Open the CA IdentityMinder Management Console (see page 88)
Change the ADS_LDAP_bind_user Password (see page 495)