CA Access Control Premium Edition

Implementation Guide

r12.5 SP2

Second Edition

Third-Party Notices

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

CA Product References

This document references the following CA products:

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

Documentation Conventions

The CA Access Control documentation uses the following conventions:

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

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

Format	Meaning
Italic	Information that you must supply
Between square brackets ([])	Optional operands

Format	Meaning
Between braces ({})	Set of mandatory operands
Choices separated by pipe (|).	Separates alternative operands (choose one). For example, the following means *either* a user name *or* a group name: {*username*|*groupname*}
...	Indicates that the preceding item or group of items can be repeated
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 Access Control documentation uses the following file location conventions:

- *ACInstallDir*—The default CA Access Control installation directory.
  - Windows—C:\Program Files\CA\AccessControl
  - UNIX—/opt/CA/AccessControl
- *ACSharedDir*—A default directory used by both UNAB and CA Access Control for UNIX.
  - UNIX—opt/CA/AccessControlShared
- *ACServerInstallDir*—The default CA Access Control Enterprise Management installation directory.
  - Windows—C:\Program Files\CA\AccessControlServer
  - UNIX—/opt/CA/AccessControlServer
- *DistServerInstallDir*—The default Distribution Server installation directory.
  - Windows—C:\Program Files\CA\DistributionServer
  - UNIX—/opt/CA/DistributionServer
- *JBoss_HOME*—The default JBoss installation directory.
  - Windows—C:\jboss-4.2.3.GA
  - UNIX—/opt/jboss-4.2.3.GA

Contact CA

Contact Technical Support

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

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

Provide Feedback

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

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

Documentation Changes

Second Edition

The second edition of the documentation was released in the CA Bookshelf format, a HTML interface that provides access to the documentation from the CA Access Control product page on CA Support.

The following topics were updated in this edition:

- Deploy the Report Package on the Report Portal (see page 249)—Updated topic updates the values of the <networklayer> and <rdms> XML properties, and provides information about MS SQL Server 2008 support.
- Deploy the Report Package on a Report Portal That You Installed with CA Access Control r12.0 (see page 253)—Updated topic provides information about MS SQL Server 2008 support.

First Edition

The first edition of the documentation was released with r12.5 SP2.

The following documentation updates have been made since the r12.5 SP1 release of this documentation:

- Enterprise Deployment Architecture (see page 26)—Updated diagram with PUPM and UNAB endpoints.
- How to Install the Enterprise Management Server Components (see page 51)—Updated topic provides a new, optional step to change the CA Access Control Web Service URL.
- How to Configure the Central Database to Use Microsoft SQL Server 2008 (see page 58)—New topic provides additional steps to configure the central database to use Microsoft SQL Server 2008.
- SSL Communication for JBoss (see page 70)—Updated topic corrects several parameters in the process to configure SSL communication for JBoss.
- Change the CA Access Control Web Service URL (see page 76)—New topic explains how to change the CA Access Control Web Service URL.
- Configure Email Notification Settings (see page 81)—Updated topic provides additional steps to configure PUPM email notification settings.
- Modify the Microsoft SQL Server Database Connectivity Settings (see page 83)—Updated topic corrects the files that you modify to change the database connectivity settings.

- Installation Considerations for Linux s390 Endpoints (see page 129)—New section explains additional considerations for Linux s390 and s390x UNAB and CA Access Control endpoints.
- Installing and Configuring CA Access Control for High Availability (see page 197)—New chapter explains the concepts and procedures that help you install CA Access Control in a high availability deployment.
- Active Directory Site Support (see page 263)—New topic explains how UNAB implements Active Directory site support.
- Installation Considerations for 64-bit Hosts (see page 264)—New topic explains additional installation considerations for 64-bit UNAB endpoints.
- UNAB Installation Parameters File—Customize UNAB Installation (see page 267)—Updated topic corrects several parameters in the installation parameters file.
- Register a UNIX Host in Active Directory (see page 299)—Updated topic provides additional information about how to register a UNIX host in Active Directory.
- How to Implement Full Integration Mode (see page 304)—New section explains the concepts and procedures that help you migrate UNIX users and groups to Active Directory.
- Configure the Servers to Use an Identical Encryption Key (see page 209)—New topic explains an important step that you must complete to set up CA Access Control in a disaster recovery environment.
- How to Upgrade from r12.0 SP1 (see page 379)—Updated topic provides additional information about how to upgrade from r12.0 SP1.
- Upgrade the Enterprise Management Server (see page 381)—Updated topic provides additional information about how to upgrade from r12.0 SP1 to the Enterprise Management Server.
- Encrypt Passwords in AES Encryption Method (see page 382)—New topic explains an important step that you must complete to upgrade from r12.0 SP1.
- Encrypt a Clear Text Password (see page 435)—Updated topic updates the syntax that the pwdtools utility uses.

Contents

Chapter 1: Introduction

This section contains the following topics:

About this Guide

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

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

Chapter 2: Planning Your Implementation

This section contains the following topics:

Planning for a Security System

The primary goal of any security system is to protect an organization's information assets. To effectively implement security, you must be aware of the threats that exist at your site. You must then determine how to implement CA Access Control so that it best protects your site from these threats.

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

- Block unauthorized users from accessing the system
- Block authorized users from accessing items to which they should not have access

CA Access Control provides tools to protect your system in both ways. CA Access Control also provides auditing tools that let you trace users' activities to track attempted misuse of the computer system.

Once you have determined the goals of the security project based on the threats to your site, you can write a security policy statement and put together an implementation team. The implementation team should set priorities that can help determine what data, applications, and users must be secured.

Getting Management Commitment

A management decision to install CA Access Control is not enough to guarantee adequate security at your site. For the security project to succeed, management must be actively involved. Management must decide on security policy, procedures, and resources to be allocated to the security function, and accountability of users of the computer system. Without such management support, security procedures fall into misuse and become more of an administrative chore than a viable protection scheme. In fact, such a situation could breed a false sense of security that could lead to serious security exposures.

The security administrator should work with management to prepare a clear, inclusive security policy statement. This statement should include the following:

- Corporate policy regarding full-time employees, part-time employees, contract employees, and consultants
- Corporate policy concerning outside users of the system
- Behavior expected from all users of the system
- Physical protection considerations
- Security requirements of user departments
- Auditing requirements

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

Preparing an Implementation Plan

While defining the implementation plan, check repeatedly that the plan's goals come from the security policy. The new security controls should be phased-in gradually to provide users a period of adjustment.

Define a pilot group of users as a prototype for implementing CA Access Control. During the test phase, CA Access Control protects business data, jobs, and users in the pilot group. Test all CA Access Control 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.

In addition to deciding what to protect, the implementation team needs to consider how to phase-in the new security controls with minimum disruption of current work patterns. As you plan implementation, you should consider a period of only auditing access, and not restricting access, for various resources and classes. The resulting audit records show which users tend to require access to the resources.

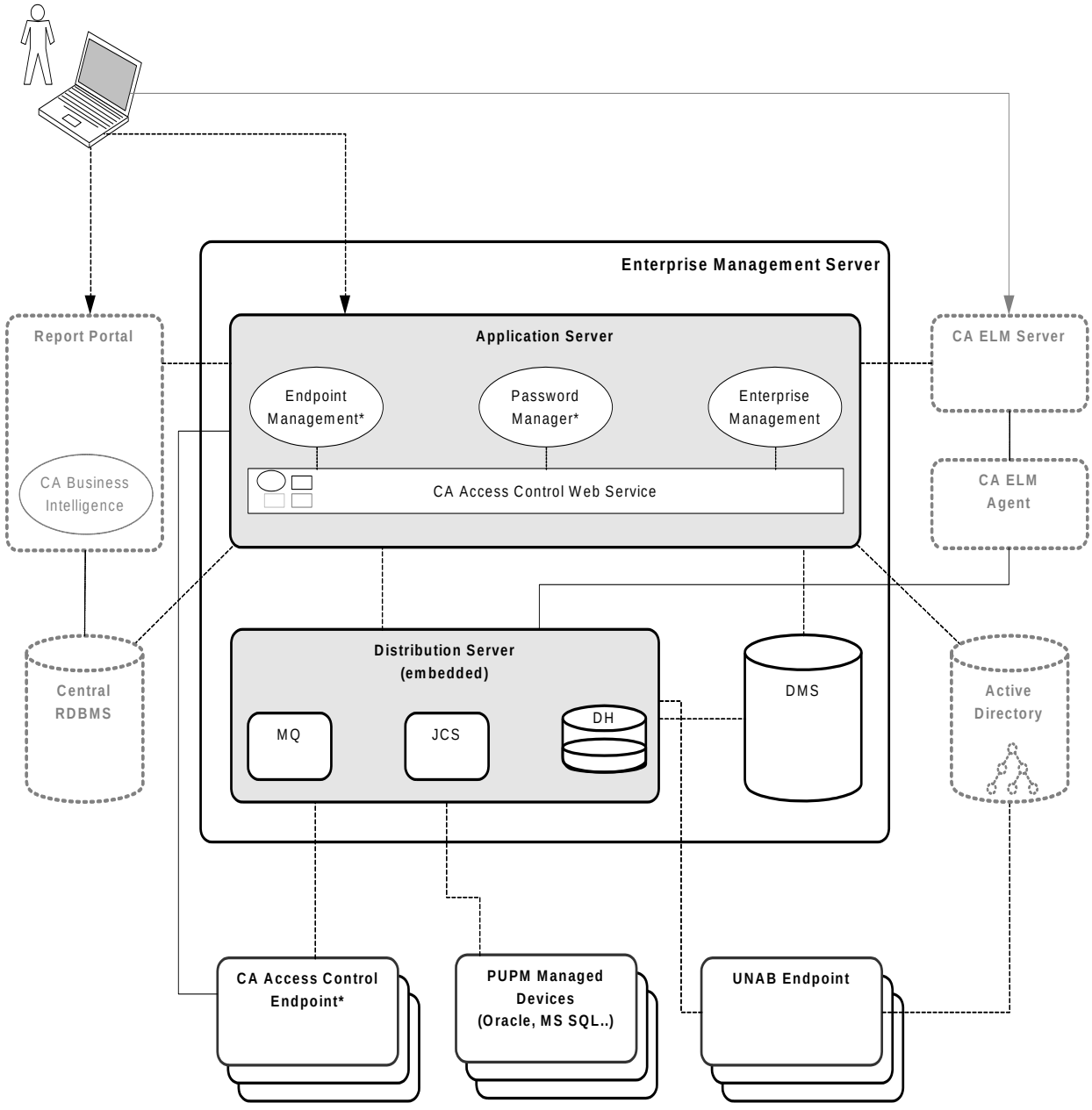
Deciding How to Protect

Before you install CA Access Control, you should decide what features of the software you want to use. You can use:

- CA Access Control to implement native security. In this case, you can use CA Access Control Endpoint Management to implement the security features that are already familiar to you.
- Advanced policy management to deploy multiple-rule policies (script files) you create to your enterprise. Using this policy-based method, you can create version-controlled policies, assign and unassign policies to host groups in your enterprise, directly deploy and remove deployed policies (undeploy), and view deployment status and deployment deviation.
- A Policy Model database (PMDB), which enables you to propagate a security database with users, groups, and access rules defined in it to a set of subscribers. The PMDB regularly propagates all the updates it receives to its subscribers. This mechanism greatly eases the administrative burden on system administrators.
- Privileged User Password Management (PUPM), which provides you with 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, which enables you to validate local UNIX users and groups credentials against Active Directory. You use a single repository for all your users, letting them log in to all platforms with the same user name and password.
- CA Access Control to significantly strengthen native security by guarding against more sophisticated attacks. CA Access Control 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

Enterprise Deployment Architecture

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



Note: The CA Access Control components marked with an asterisk (*) are available in both CA Access Control and CA Access Control Premium Edition. All other components are available in CA Access Control Premium Edition only.

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

Endpoints

An enterprise deployment of CA Access Control has two types of endpoints:

- CA Access Control endpoint—An endpoint on which you have installed CA Access Control.

  CA Access Control endpoint can also optionally serve as PUPM endpoints.

- UNAB endpoint—A UNIX endpoint on which you have installed the UNIX Authentication Broker (UNAB).

  UNAB lets users log in to UNIX computers using credentials that are stored in an Active Directory data store. This means you can use a single data store for all your users, letting them log in to all platforms with the same user name and password.

Report Portal

The report portal lets you view CA Access Control reports.

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

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

Central RDBMS

The central RDBMS stores the following:

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

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

CA Enterprise Log Manager Components

You can send CA Access Control audit events from each of the endpoints to CA Enterprise Log Manager for collection and reporting. The following components support CA Enterprise Log Manager integration with CA Access Control:

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

Note: For more information about CA Enterprise Log Manager components, see the CA Enterprise Log Manager documentation.

Active Directory

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

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

How to Implement CA Access Control

Before you implement CA Access Control 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 Access Control:

- Use a 'top-to-bottom' approach in the implementation process. Begin by installing CA Access Control Enterprise Management and then install the CA Access Control endpoints.
- Before you begin the implementation, verify that the computers you are using meet the required specifications and that all prerequisite software is installed.

  Note: For more information about the required hardware and software specifications, see the *Release Notes*.

To implement CA Access Control, do the following:

1. Review the CA Access Control components, their functionality, and their codependencies with other CA Access Control components. Ensure that you understand what CA Access Control components to install, where to install them, and in what order.
2. Prepare the Enterprise Management Server.
3. Install CA Access Control Enterprise Management on the Enterprise Management Server.
4. Start CA Access Control Enterprise Management.

   This step verifies that you successfully installed CA Access Control Enterprise Management.
5. (Optional) Install another instance of the Distribution Server on a separate server.

   To implement a failover solution for CA Access Control, install the Distribution Server on more than one server.
6. Install the endpoints.

More information:

How to Prepare the Enterprise Management Server (see page 52)
Install CA Access Control Enterprise Management on Windows (see page 61)
Start CA Access Control Enterprise Management (see page 78)
Open CA Access Control Enterprise Management (see page 78)

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 Access Control, 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 Access Control 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 Access Control supports the following types of users:

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 Access Control.

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 Access Control, this is called task delegation.

Administrators

Users who have the highest authority within the native OS and CA Access Control. Administrators can add, delete, and update users and can perform almost all administrative tasks. With CA Access Control, 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 Access Control, and use the secons utility to perform tasks such as manage CA Access Control 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.

Assigning Types

Within CA Access Control, you create a special user by assigning a user one or more authorization attributes. The names of these attributes are ADMIN, AUDITOR, PWMANAGER, OPERATOR, and SERVER at the system level, and GROUP-ADMIN, GROUP-AUDITOR, GROUP-PWMANAGER, and GROUP-OPERATOR at the group level.

More information:

Authorization Attributes (see page 35)

Security Policies and Users

When developing a security policy for your organization, you should decide:

- What users to define
- 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, group 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 Access Control.

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 Access Control, 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 Access Control 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 Access Control. 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).

You add users to the _restricted group the same way you add users to any other group. For example, using selang to join pjones to the _restricted group, enter the following at the prompt:

```
join pjones group(_restricted)
```

For files that are not listed in the database, this command gives pjones only the access (if any) permitted by the _default record of the FILE class.

Note: 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 Access Control define the type of access that is allowed or prohibited to a particular resource. These groups include the following:

- _network

  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 \temp\readonly
  ```

  Then specify the access allowed through the network:

  ```
  authorize FILE \temp\readonly gid(_network) access(read)
  ```

  You can also do this using CA Access Control Endpoint Management.

  Now when accessing \temp\readonly from the network, users can read the file only if they have explicit permission to access the file in other ways.

- _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 Access Control 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.

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.

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 Guide*.

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 Guide*.

B1 Security Features

The Trusted Computer System Evaluation Criteria (TCSEC) is a USA government standard for computer security. It is commonly referred to as the Orange book. Level B1 of the standard provides mandatory protection security through labeled security.

CA Access Control includes the following B1 "Orange Book" features:

- Security levels
- Security categories
- Security labels

You can manage B1 security features using *selang* or CA Access Control Endpoint Management.

Security Levels

When security level checking is enabled, CA Access Control performs security level checking in addition to its other authorization checking. A security level is a positive integer between 1 and 255 that can be assigned to users and resources. When a user requests access to a resource that has a security level assigned to it, CA Access Control compares the security level of the resource with the security level of the user. If the user's security level is equal to or greater than the security level of the resource, CA Access Control continues with other authorization checking; otherwise, the user is denied access to the resource.

If the SECLABEL class is active, CA Access Control uses the security level associated with the security labels of the resource and user; the security level that is explicitly set in the resource and user records is ignored.

To protect a resource with security level checking, assign a security level to the resource's record. The level parameter of the newres or chres command assigns a security level to a resource.

To allow a user access to resources protected by security level checking, assign a security level to the user's record. The level parameter of the newusr or chusr command assigns a security level to a user.

Enable and Disable Security Level Checking

The following setoptions command enables security level checking:

```
setoptions class+ (SECLEVEL)
```

The following setoptions command disables security level checking:

```
setoptions class- (SECLEVEL)
```

Security Categories

When security category checking is enabled, CA Access Control performs security category checking in addition to its other authorization checking. When a user requests access to a resource that has one or more security categories assigned to it, CA Access Control compares the list of security categories in the resource record with the category list in the user record. If every category assigned to the resource appears in the user's category list, CA Access Control continues with other authorization checking; otherwise, the user is denied access to the resource.

If the SECLABEL class is active, CA Access Control uses the list of security categories associated with the security labels of the resource and user; the lists of categories in the user and resource records are ignored.

To protect a resource by security category checking, assign one or more security categories to the resource's record. The category parameter of the newres or chres command assigns security categories to a resource.

To allow a user access to resources protected by security category checking, assign one or more security categories to the user's record. The category parameter of the newusr or chusr command assigns security categories to a user.

Enable and Disable Security Category Checking

The following setoptions command enables security category checking:

```
setoptions class+ (CATEGORY)
```

The following setoptions command disables security category checking:

```
setoptions class- (CATEGORY)
```

Define Security Categories

A security category is defined by defining a resource in the CATEGORY class. The following selang command newres defines a security category:

```
newres CATEGORY name
```

where *name* is the name of the security category.

For example, to define the security category Sales, enter the following command:

```
newres CATEGORY Sales
```

To define the security categories Sales and Accounts, enter the following command:

```
newres CATEGORY (Sales,Accounts)
```

List Security Categories

To display a list of all the security categories defined in the database, use the find command as follows:

```
find class(CATEGORY)
```

Delete Security Categories

You can delete a security category by removing its record from the CATEGORY class. The following rmres command removes a security category:

```
rmres CATEGORY name
```

where *name* is the name of the security category.

For example, to remove the security category Sales, enter the following command:

```
rmres CATEGORY Sales
```

Security Labels

A security label represents an association between a particular security level and zero or more security categories.

When security label checking is enabled, CA Access Control performs security label checking in addition to its other authorization checking. When a user requests access to a resource that has a security label assigned to it, CA Access Control compares the list of security categories specified in the resource record's security label with the list of security categories specified in the user record's security label. If every category assigned to the resource's security label appears in the user's security label, CA Access Control continues with the security level check; otherwise, the user is denied access to the resource.

CA Access Control then compares the security level specified in the resource record's security label with the security level specified in the user record's security label. If the security level assigned in the user's security label is equal to or greater than the security level assigned in the resource's security label, CA Access Control continues with other authorization checking; otherwise, the user is denied access to the resource.

When security label checking is enabled, the security categories and security level specified in the user and resource records are ignored; only the security level and categories specified in the security label definitions are used.

To protect a resource by security label checking, you assign a security label to the resource's record.

To allow a user access to resources protected by security label checking, assign a security label to the user's record.

Enable and Disable Security Label Checking

The following setoptions command enables security label checking:

```
setoptions class+ (SECLABEL)
```

The following setoptions command disables security label checking:

```
setoptions class- (SECLABEL)
```

Define Security Labels

You can define a security label by defining a resource in the SECLABEL class. The following newres command defines a security label:

```
newres SECLABEL name \
category(securityCategories) \
level(securityLevel)
```

where:

name

Specifies the name of the security label.

securityCategories

Specifies the list of security categories. If more than one security category is specified, separate the security category names with a space or a comma.

Note: You must define the security categories in the CATEGORY class before you define a security label.

securityLevel

Specifies the security level. Specify an integer from 1 through 255.

Example: Define a Security Label

The following example defines a security label named Managers that contains the security categories Sales and Accounts and has a security level of 95:

```
newres SECLABEL Manager category(Sales,Accounts) level(95)
```

List Security Labels

To display a list of all the security labels that are defined in the database, use the find command as follows:

```
find class(SECLABEL)
```

Delete Security Labels

You can delete a security label by removing its record from the SECLABEL class. The following rmres command removes a security label:

```
rmres SECLABEL name
```

where *name* is the name of the security label.

For example, to remove the security category Managers, enter the following command:

```
rmres SECLABEL Managers
```

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 Access Control 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*.

Educating and Training Staff

Part of the security administrator's job is to tell the system users what they need to know to work without disruption when CA Access Control is installed.

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

- All users defined in the database
  - Users must know 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.
  - If you want to implement checking of the password policy, users may need to be familiar with the Password Manager.
  - Users should be aware of 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.
  - Users may be interested in the sesudo command, which enables user substitution based on predefined access rules with or without password checking.
- Technical support personnel

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

  Note: For more information about database utilities, see dbmgr in the *Reference Guide*.
- Group administrators

  Users who have one of the group authorities, who have a group attribute (such as GROUP-ADMIN), or who own group records need group information (see page 32).

  Note: For more information about groups, see the group selang commands in the *selang Reference Guide*.
- Auditors

  Users with the AUDITOR attribute should be familiar with the auditing tools (CA Access Control 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 Access Control* 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 Access Control API, see the *SDK Guide*.

- Programmers writing authorized applications

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

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

Implementation Tips

This section provides some miscellaneous implementation information to consider once you have installed CA Access Control.

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 Access Control 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.

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 Access Control is accountability. Each action or access attempt is performed on behalf of a user who is held responsible for the request.

CA Access Control 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 Access Control Endpoint Management or through selang commands.

Resource Classes and Access Rules

When installed, CA Access Control immediately begins intercepting system events and checking for users' authority to access resources. Until you tell CA Access Control 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:

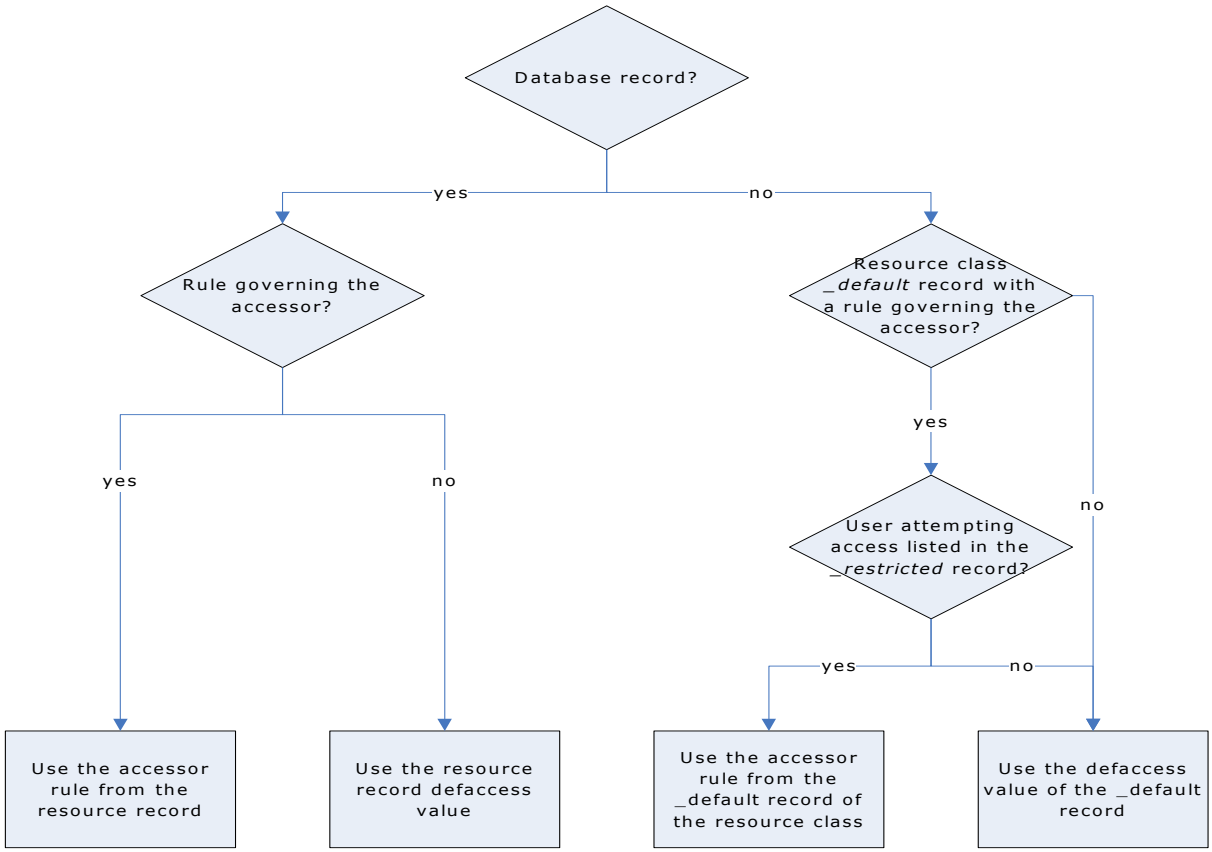
- An access control list (a specific list of the accessors authorized to access the resource and the exact access they can have), also called an ACL
- A negative access control list (a specific list of the accessors for which access should be denied), also called NACL
- A default access for the resource, 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 Access Control 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 Access Control 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 Access Control 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 33).



Note: For more information about resource classes and access rules see the *selang Reference Guide*.

Chapter 3: Installing the Enterprise Management Server

This section contains the following topics:

Environment Architecture

An enterprise installation of CA Access Control lets you centrally manage policies, privileged accounts, and UNAB 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.

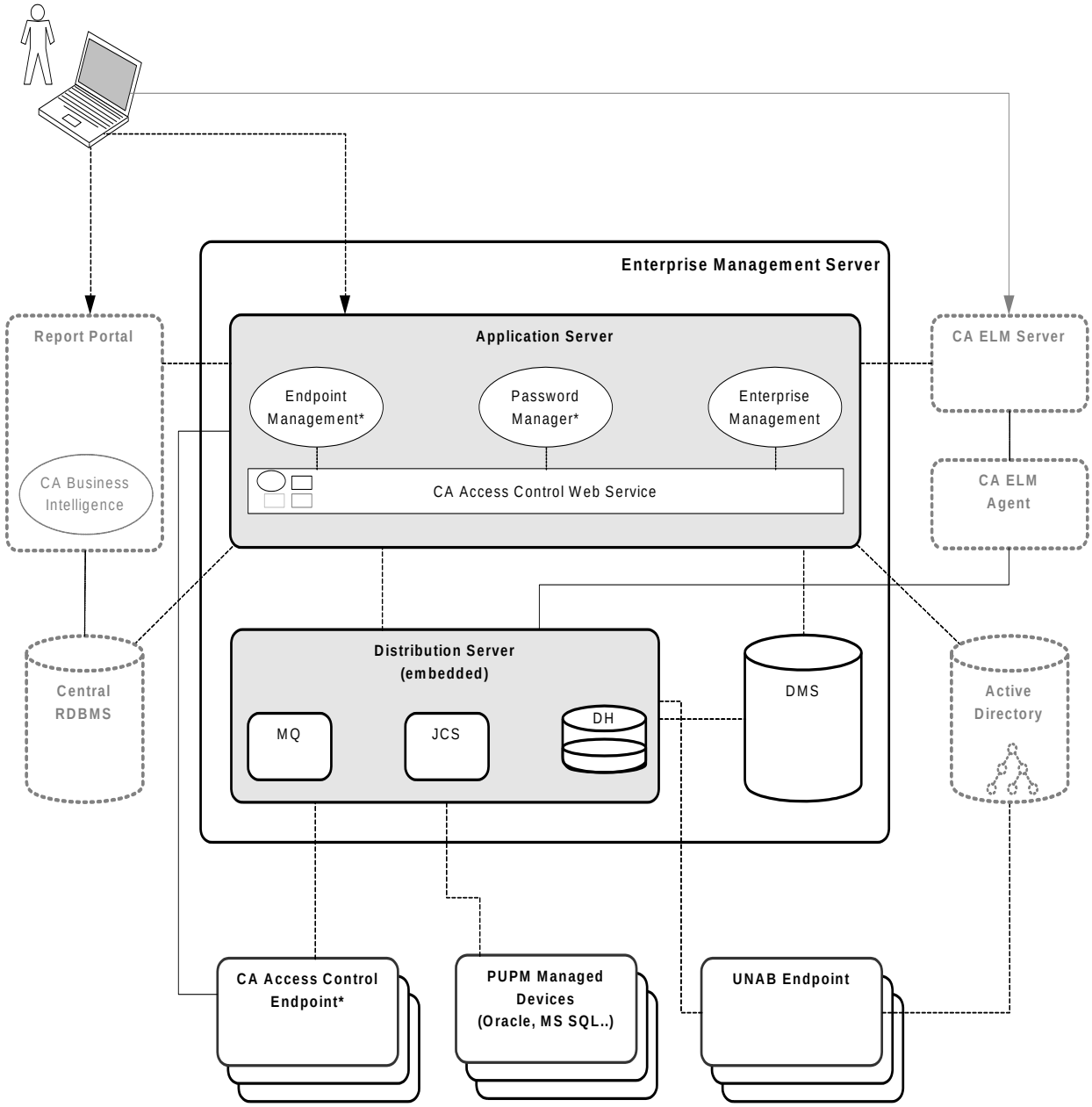
To manage your enterprise installation of CA Access Control, install the Enterprise Management Server on a central computer and configure it for your enterprise. The Enterprise Management Server contains the following components:

- Deployment Map Server (DMS)
- Distribution Server
- Web-based applications

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

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

The following diagram shows the Enterprise Management Server architecture:



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.

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 Access Control reports.

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

  You can configure CA Enterprise Log Manager 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 PUPM endpoints.

Web-based Applications

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

How to Install the Enterprise Management Server Components

The Enterprise Management Server components let you centrally manage your enterprise deployment of CA Access Control. After you install the Enterprise Management Server components, you install the reporting service and the CA Access Control 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 *Release Notes*.

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

1. Prepare the Enterprise Management Server.

   Before you install CA Access Control Enterprise Management, prepare the computer by installing and configuring CA Access Control Enterprise Management prerequisites.

2. Install CA Access Control Enterprise Management.

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

3. (Optional) Configure the Enterprise Management Server for SSL communication, as follows:
   a. Configure JBoss for SSL communications.

      By default, JBoss is not installed with SSL support.

   b. Modify the Message Queue SSL port numbers.

   c. Configure CA Access Control Enterprise Management for SSL communication.

4. (Optional) Set up advanced configuration.

   You use the CA Identity Manager Management Console to perform advanced configuration tasks, such as modifying the properties of the central database to generate custom reports and configuring CA Access Control Enterprise Management to send email notifications when a specific event occurs.

5. (Optional) Change the CA Access Control Web Service URL.

   To increase security, you can change the default CA Access Control Web Service URL.

6. (Optional) Modify the Microsoft SQL Server security settings to Windows Authentication Mode.

   By default, CA Access Control Enterprise Management is installed in SQL Server Authentication Mode.

7. (Optional) Implement enterprise reporting.

   CA Access Control Enterprise Management provides reporting capabilities through a CA Business Intelligence Common Reporting server (CA Access Control Report Portal).

8. (Optional) Integrate with CA Enterprise Log Manager.

   You can now install and configure your endpoints.

More information:

How to Set Up Reporting Service Server Components (see page 243)

How to Prepare the Enterprise Management Server

Before you install CA Access Control Enterprise Management, you need to prepare the server.

Note: When you install CA Access Control Enterprise Management, the installation program also installs CA Access Control Endpoint Management, if it is not already installed. If you have installed CA Access Control Endpoint Management, you do not need to repeat those steps that you have already completed.

To prepare the Enterprise Management Server, do the following:

1. Prepare the central database for Enterprise Management (see page 54).

   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:

   - (Windows) Run the prerequisite installation utility (see page 59).

     CA Access Control provides a utility that installs the Java Development Kit (JDK) and the JBoss application server. If you already have this software installed, 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 Access Control Premium Edition Third Party Components DVDs. For information about supported versions, see the *Release Notes*.

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

     b. Define the JAVA_HOME environment variable and set its value to the JDK installation path.

        For example, on Windows you enter the following command:

        ```
        set JAVA_HOME=C:\j2sdk1.5.0
        ```

        To do the same thing on UNIX, you can enter the following command:

        ```
        export JAVA_HOME=/usr/jdk/j2sdk.1.5.0/
        ```

     c. Install a supported JBoss version.

        We recommend that you run JBoss as a service (daemon on UNIX).

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

   You can now install CA Access Control Enterprise Management on the Enterprise Management Server.

Prepare the Central Database for Enterprise Management

CA Access Control Enterprise Management requires a relational database management system (RDBMS). You must set this up before you install CA Access Control Enterprise Management.

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

- Pre-populate the central database using deployment scripts CA Access Control provides.

  Using this option, you separate between database preparation and CA Access Control Enterprise Management installation. The database administrator can review and control the changes CA Access Control needs to make to the database.

- Let CA Access Control Enterprise Management prepare the central database during installation.

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

To prepare the database for CA Access Control Enterprise Management

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 Access Control Enterprise Management:

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

   - For Oracle, create a new user for the central database.

     This user must have the following permissions and settings:

     - DBA.
     - CONNECT (granting the following system privileges: ALTER SESSION, CREATE CLUSTER, CREATE DATABASE LINK, CREATE SEQUENCE, CREATE SESSION, CREATE SYNONYM, CREATE TABLE, CREATE VIEW)
     - RESOURCE (granting the following system privileges: CREATE CLUSTER, CREATE INDEXTYPE, CREATE OPERATOR, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER, CREATE TYPE)
     - Unlimited quota on the tablespace that hosts the CA Access Control Enterprise Management Server.

- For SQL Server:
  - Create a new case-*insensitive* database.

    The database must have the sort order SQL_Latin1_General_CP1_CI_AS.
  - Create a new user, make the new database the default database of the user, and assign the user the following privileges: DBCREATOR, SYSADMIN

3. (Optional) Pre-populate the central database using the deployment scripts CA Access Control provides.

   a. Customize the deployment scripts before you deploy them (see page 56).

      The deployment scripts define four default user accounts that CA Access Control Enterprise Management uses (superadmin, selfreguser, neteautoadmin, [default user]). You can change the names of these default accounts and their passwords.

      Important! Customize the scripts only if you plan to use the embedded user store. If you use Active Directory, CA Access Control Enterprise Management does not store account information in the central database.

   b. Deploy the deployment scripts (see page 57).

   c. Configure the database user that you will use for CA Access Control Enterprise Management installation.

      - For Oracle, revoke the DBA role and keep the CONNECT and RESOURCE roles for the user you created.
      - For SQL Server, create a new user, selecting the database you created earlier as default, map the user to the database, and set the following permissions: CONNECT.SELECT, INSERT, DELETE, UPDATE, EXECUTE.

Customize the Central Database Deployment Scripts

The deployment scripts define four default user accounts that CA Access Control Enterprise Management uses (superadmin, selfreguser, neteautoadmin, [default user]). You can change the names of these default accounts and their passwords.

Important! Customize the scripts only if you plan to use the embedded user store. If you use Active Directory, CA Access Control Enterprise Management does not store account information in the central database.

To customize the central database deployment scripts

1. Insert the appropriate CA Access Control Premium Edition Server Components DVD for your operating system into your optical disc drive.
2. Copy the deployment script for your RDBMS to a temporary local folder.

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

   - Oracle: /Scheme/ORACLE/AC125_oracle_script.sql
   - SQL Server: /Scheme/MSSQL/AC125_mssql_script.txt
3. Edit the script as follows:

   a. Locate the *Table : TBLUSERS* section.

   b. Edit each line that defines a user to (INSERT INTO tblusers ...) to change the account name and password as required.
4. Save and close the script.

   The customized script can now be deployed.

Example: Customize the CA Access Control RDBMS Deployment Scripts

This example uses code snippets that are common to the Microsoft SQL Server and Oracle Database deployment scripts. In this example, you customize the script to change the default user account superadmin and password to one of your choosing.

The following snippet sets the default CA Access Control Enterprise Management super user if you use the RDBMS as your user store:

```
INSERT INTO tblUsers (ID,loginid, lastname, firstname, password) VALUES (1,'superadmin', 'Admin','Super', 'test')
```

The SQL command creates a user account called *superadmin* (first name *Super*, last name *Admin*) with the password *test*.

In the snippet you edit, you modify the user account to be called sysadmin and assign it with the password *C0mp!ex*.

```
INSERT INTO tblUsers (ID,loginid, lastname, firstname, password) VALUES (1,'sysadmin', 'Admin','System',
'C0mp!ex')
```

Central Database Script Deployment Examples

Once you complete customizing the deployment script, you can deploy it to your database. Deploying the script populates the central database and prepares it for CA Access Control Enterprise Management installation. You deploy the script using the native database tools.

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

This example shows you how to deploy the CA Access Control 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\AC126_oracle_script.sql
   ```

   Oracle deploys the script to the database.

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

This example shows you how to deploy the CA Access Control 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 Access Control Microsoft SQL Server deployment script, and click Open.

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

6. Click Execute to deploy the script.

   Microsoft SQL Server deploys the script to the database.

How to Upgrade an Existing Central Database to Microsoft SQL Server 2008

If the CA Access Control Enterprise Management central database is configured on Microsoft SQL Server 2005 and you want to upgrade to Microsoft SQL Server 2008, you need to configure the Enterprise Management Server to work with the new server.

Complete the following process to configure the central database for Microsoft SQL Server 2008:

1. Stop all CA Access Control services on the Enterprise Management Server.
2. Stop JBoss. 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.
3. Upgrade to Microsoft SQL Server 2008.
4. Download the Microsoft SQL Server JDBC Driver 2.0 from the Microsoft website.
5. Extract the file to a temporary directory on the Enterprise Management Server.

6. Do *one* of the following:
   - Locate the sqljdbc.jar file, if you are using JDK version 1.5.
   - Locate the sqljdbc4.jar file and rename it sqljdbc.jar, if you are using JDK version 1.6 or higher.
7. Copy the file into the following directory on the Enterprise Management Server:

   JBoss_HOME/server/default/lib

   Note: Overwrite the existing file in this directory.
8. Start the Microsoft SQL Server 2008 services.
9. Start JBoss.
10. Start CA Access Control Enterprise Management.

Run the Prerequisite Software Installation Utility

Valid on Windows

CA Access Control 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 Access Control Premium Edition 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 Access Control Enterprise Management.
- Installs JBoss as a service.
- Lets you launch the CA Access Control Enterprise Management installation with prerequisite software settings preconfigured.

If you already have this software installed, you can skip this procedure. If you do not have this software installed, 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 Access Control Enterprise Management to resolve any open ports issues.

To run the prerequisite software installation utility

1. Insert the CA Access Control Premium Edition 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 may take some time.

5. Do *one* of the following:

   - If you want to start the CA Access Control Enterprise Management installation process after the prerequisite software installs, when prompted, insert the CA Access Control Premium Edition Server Components DVD for your operating system into your optical disc drive and select Done. Close the Product Explorer window if it appears.

     The CA Access Control Enterprise Management InstallAnywhere wizard opens.

   - If you do not want to start the CA Access Control 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.

Solaris ISO Image Mounting Example

The installation packages for the various CA Access Control components are provided as ISO files. You mount the ISO files to install the CA Access Control components. The following examples demonstrate how to mount and unmount an ISO image on a Solaris computer.

Example: Mount an ISO Image on Solaris

This example creates a mount point, executes the lofiadm utility so that the loopback file driver (lofi) treats the ISO image as a block device, and mounts the ISO image. The mount point is named ac125_server and the ISO image is named CA_AC_PREMIUM_SERVER_12_5_SOL.iso:

```
mkdir /ac125_server
/usr/sbin/lofiadm -a /u01/CAAC/CA_AC_PREMIUM_SERVER_12_5_SOL.iso /dev/lofi/1
/usr/sbin/mount -F hsfs -o ro /dev/lofi/1 /ac125_server
```

Example: Mount an ISO Image on Solaris in a Single Command

This example creates a mount point, executes the lofiadm utility so that the loopback file driver (lofi) treats the ISO image as a block device, and mounts the ISO image in a single command. The mount point is named ac125_server and the ISO image is named CA_AC_PREMIUM_SERVER_12_5_SOL.iso:

```
/usr/sbin/mount -F hsfs -o ro `/usr/sbin/lofiadm -a /u01/CAAC/CA_AC_PREMIUM_SERVER_12_5_SOL.iso`
/ac125_server
```

Example: Unmount an ISO Image on Solaris

This example unmounts the mount point and disassociates the ISO image from lofi:

```
umount /ac125_server
/usr/sbin/lofiadm -d /u01/CAAC/CA_AC_PREMIUM_SERVER_12_5_SOL.iso
```

Install CA Access Control Enterprise Management on Windows

Valid on Windows

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

We recommend that you use the Prerequisite Kit installer to initiate the CA Access Control Enterprise Management installation. This installer installs the prerequisite third-party software and then starts the CA Access Control Enterprise Management installation.

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

To install CA Access Control Enterprise Management on Windows

1. Stop JBoss Application Server if it is running.
2. Stop CA Access Control services if you are installing CA Access Control Enterprise Management on a computer that already has CA Access Control installed.
3. Insert the CA Access Control Premium Edition Server Components DVD for Windows into your optical disc drive.
4. Expand the Components folder in the Product Explorer, select CA Access Control Enterprise Management, then click Install.

   Note: If you have autorun enabled, the Product Explorer automatically appears. If the Product Explorer does not appear, navigate to the optical disc drive directory and double-click the ProductExplorerx86.EXE file.

   The InstallAnywhere installation program starts.

5. Complete the wizard as required. The following installation inputs are not self-explanatory:

   Java Development Kit (JDK)

   Defines the location of an existing JDK.

   Note: If you launch the CA Access Control Enterprise Management installation immediately after you use the CA Access Control Premium Edition 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 Access Control Enterprise Management installation immediately after you use the CA Access Control Premium Edition 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

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

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 on your RDBMS.
- **Username**—Defines the name of the user that you created when you prepared the RDBMS.
- **Password**—Defines the password of the administrative user you created.

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

User Store Type

Defines the user store type CA Access Control Enterprise Management uses.

If you select Embedded User Store, CA Access Control Enterprise Management stores user information in the RDBMS. If you select Active Directory, you must specify the connection information details.

Note: To deploy login authorization policies to UNAB, you must select Active Directory as the user store. If you select Active Directory as the user store, you cannot create or delete users and groups in CA Access Control 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 name of the host where you installed Active Directory.
- **Port**—Defines the port used by Active Directory, for example, 389.
- **Search Root**—Defines the search root, for example, ou=DomainName, DC=com
- **User DN**—Defines the Active Directory administrator account name. Use this user account to manage CA Access Control Enterprise Management. For example: CN=Administrator, cn=Users, DC=DomainName, DC=Com
- **Password**—Defines the Active Directory administrator password.

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 full DNS name of the superuser account.

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

Note: In this step you assign the superadmin account to an existing Active Directory user. The superadmin account is assigned the System Manager admin role in CA Access Control 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 Access Control Enterprise Management administrator. Make a note of the password so you can log in to CA Access Control 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 Access Control Enterprise Management. For more information about the System Manager admin role, see the *Enterprise Administration Guide*.

CA Access Control Enterprise Management is installed after you complete the wizard. You must reboot the computer to complete the CA Access Control Enterprise Management installation.

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

   The computer reboots. You now need to configure CA Access Control Enterprise Management for your enterprise.

More information:

How to Prepare the Enterprise Management Server (see page 52)

Install CA Access Control Enterprise Management on Solaris

Valid on Solaris

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

You must use console installation to install CA Access Control Enterprise Management on a Solaris computer.

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

To install CA Access Control Enterprise Management on Solaris

1. Shut down JBoss Application Server if it is running.
2. Stop CA Access Control services if you are installing CA Access Control Enterprise Management on a computer that already has CA Access Control installed.

3. Do the following:
   a. Insert the CA Access Control Premium Edition Server Components for Solaris DVD into your optical disc drive.
   b. Mount the optical disc drive.
   c. Open a terminal window and navigate to the following directory on the optical disc drive:

      /EnterpriseMgmt/Disk1/InstData/NoVM

   d. Enter the following command:

      ```
      ./install_EntM_r125.bin -i console
      ```

   The InstallAnywhere console appears after a few moments.
4. Complete the prompts as required. The following installation inputs are not self-explanatory:

   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.

   Communication Password

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

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 on your RDBMS.
- **Username**—Defines the name of the user that you created when you prepared the RDBMS.
- **Password**—Defines the password of the administrative user you created.

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

User Store Type

Defines the user store type CA Access Control Enterprise Management uses.

If you select Embedded User Store, CA Access Control Enterprise Management stores user information in the RDBMS. If you select Active Directory, you must specify the connection information details.

Note: To deploy login authorization policies to UNAB, you must select Active Directory as the user store. If you select Active Directory as the user store, you cannot create or delete users and groups in CA Access Control 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 name of the host where you installed Active Directory.
- **Port**—Defines the port used by Active Directory, for example, 389.
- **Search Root**—Defines the search root, for example, ou=DomainName, DC=com
- **User DN**—Defines the Active Directory administrator account name. Use this user account to manage CA Access Control Enterprise Management. For example: CN=Administrator, cn=Users, DC=DomainName, DC=Com
- **Password**—Defines the Active Directory administrator password.

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 full DNS name of the superuser account.

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

Note: In this step you assign the superadmin account to an existing Active Directory user. The superadmin account is assigned the System Manager admin role in CA Access Control 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 Access Control Enterprise Management administrator. Make a note of the password so you can log in to CA Access Control 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 Access Control 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 Access Control Enterprise Management is installed. You must reboot the computer to complete the installation.

6. Press Enter.

   The installer closes.

7. Reboot the computer.

   The computer reboots. You now need to configure CA Access Control Enterprise Management for your enterprise.

Enterprise Management Server SSL Communication

By default, the Enterprise Management Server components do not use SSL for communication. You need to set the following components to communicate using SSL:

- JBoss Application Server.

  By default, JBoss is not installed with SSL support.

- Message Queue.

  By default, the Message Queue uses non-SSL ports.

- CA Access Control Enterprise Management.

SSL Communication for JBoss

By default, JBoss is not installed with SSL support. This means that all communication between CA Access Control Enterprise Management and JBoss is not encrypted. You can configure JBoss to use SSL for secure communication.

Note: For more information about how to configure SSL for JBoss, refer to the JBoss product documentation.

Example: Configure 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.

To configure JBoss for SSL communication

1. Stop JBoss if it is running.
2. Open a command prompt window, then navigate to the following directory:

   JBossInstallDir\server\default\deploy\IdentityMinder.ear\custom\ppm\truststore
3. Enter the following command:

   keytool -genkey -alias entm -keystore ssl.keystore -keyalg RSA

   -genkey

   Specifies that the command should generate a key pair (public and private keys).

   -alias

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

   -keystore

   Specifies the keystore name to add the certificate to.

   -keyalg

   Specifies the algorithm to use to generate the key pair.

   The keytool utility starts.
4. Enter the password *secret*.
5. Complete the prompts as required and press enter to verify the parameters you entered.

   The certificate is added to the keystore.
6. Locate the file named server.xml in the following directory and open it for editing:

   JBossInstallDir\server\default\deploy\jboss-web.deployer

7. 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 Access Control Enterprise Management installation process.

8. Uncomment the "<!--" above the <Connector port> tag.

   You can now edit this tag.

9. Add the following properties to the <Connector port> tag:

   keystoreFile="${jboss.server.home.dir}/conf/ssl.keystore" keystorePass="*newPassword*"

   keystoreFile

   Specifies the full pathname of the keystore file.

   keystorePass

   Specifies the keystore password.

   The <Connector port> tag should now appear as follows:

```
<Connector port="18443" protocol="HTTP/1.1" SSLEnabled="true"
     maxThreads="150" scheme="https" secure="true"
     clientAuth="false" sslProtocol="TLS"
keystoreFile="${jboss.server.home.dir}/server/default/deploy/IdentityMinder.ear/custom/ppm/truststore/ssl.keystore""keystorePass="secret" />
```

10. Save and close the server.xml file.
11. Start and open CA Access Control Enterprise Management.

    Note: After you complete this procedure, you can select to connect to JBoss, and CA Access Control Enterprise Management, in either SSL or non-SSL modes.

More information:

Configure Email Notification Settings (see page 81)

Message Queue Server SSL Port Numbers

When you install CA Access Control 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 Access Control 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 Access Control services or daemons before you modify the Message Queue Server settings.

1. In the CA Access Control 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 Access Control services.

    The Message Queue Server SSL port numbers are now modified as required.

How You Configure CA Access Control Enterprise Management for SSL Communication

By default, CA Access Control Enterprise Management is not installed with SSL support. Therefore, communication between CA Access Control Enterprise Management and Active Directory is not encrypted. You can configure CA Access Control Enterprise Management to use SSL when working with Active Directory. To configure CA Access Control Enterprise Management to use SSL, do the following:

1. Obtain the Active Directory certificate in a DER, CRT or CERT format.
2. Add the Active Directory certificate to the keystore.
3. Configure CA Access Control Enterprise Management to use SSL communication.

More information:

Adding the Active Directory Certificate to the Keystore (see page 74)
Configure CA Access Control Enterprise Management for SSL Communication (see page 75)

Adding the Active Directory Certificate to the Keystore

Before you can configure CA Access Control Enterprise Management to use SSL communication, add the Active Directory certificate to the keystore.

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

Example: Adding the Active Directory Certificate to the Keystore

Important! This example shows you how to configure CA Access Control 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 either *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. On CA Access Control Enterprise Management, open a command prompt window and navigate to the following directory:

   jboss_directory\server\default\deploy\IdentityMinder.ear\custom\ppm\truststore
3. Enter the following command:

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

   A password prompt appears.

   -import

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

   -alias

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

   -file

   Specifies the full pathname of the Active Directory certificate file.

4. Enter the password *secret*.
5. Navigate to the JBoss bin directory. By default this directory is found in:

   jboss_directory/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\IdentityMinder.ear\custom\ppm\truststore\ssl.keystore

7. Save the file and start JBoss.

More information:

Configure CA Access Control Enterprise Management for SSL Communication (see page 75)

Configure CA Access Control Enterprise Management for SSL Communication

After you add the Active Directory certificate to the keystore, you can configure CA Access Control Enterprise Management to work with SSL communication.

Note: To configure CA Access Control Enterprise Management for SSL connection you must enable the CA Identity Manager Management Console. For more information about the CA Identity Manager Management Console, see the *CA Identity Manager Management Console online help*.

To configure CA Access Control Enterprise Management for SSL communication

1. In the CA Identity Manager 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 Identity Manager 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 Access Control Enterprise Management can now communicate with Active Directory using SSL.

More information:

Enable the CA Identity Manager Management Console (see page 80)
Open the CA Identity Manager Management Console (see page 80)
Adding the Active Directory Certificate to the Keystore (see page 74)

Change the CA Access Control Web Service URL

You use the CA Access Control Web Service to access CA Access Control Enterprise Management and CA Access Control Endpoint Management. The CA Access Control 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 Access Control 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 rather than a public hostname or IP address 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.

To change the CA Access Control Web Service URL

1. Stop JBoss and CA Access Control 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.
   - (UNIX) 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.
   - (UNIX) 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. For example:

   webservice.url=http://127.0.0.1:5248
6. Save and close the file.
7. Restart CA Access Control services, including the CA Access Control Web Service.

   CA Access Control services are started.
8. Restart JBoss.

   The CA Access Control Web Service URL is changed.

Start CA Access Control Enterprise Management

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

To start CA Access Control Enterprise Management

1. Verify that CA Access Control services are started.

   CA Access Control Enterprise Management requires that CA Access Control is running.

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

   - (Windows) Click Start, Programs, CA, Access Control, 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.
   - (UNIX) Enter **./***JBOSS_DIR***/bin/run.sh -b 0.0.0.0**

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

Open CA Access Control Enterprise Management

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

To open CA Access Control 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 Access Control Enterprise Management home page appears.

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

Example: Open CA Access Control Enterprise Management

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

http://appserver123:18080/iam/ac

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

Example: Open CA Access Control Enterprise Management Using SSL

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

https://appserver123:18443/iam/ac

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

Advanced Configuration

You use the CA Identity Manager Management Console to perform advanced configuration tasks, such as modifying the properties of the reporting database to generate custom reports and configuring CA Access Control Enterprise Management to send email notifications when a specific event occurs.

The CA Identity Manager 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 Identity Manager Management Console Online Help*, which you can access from the application.

More information:

Enable the CA Identity Manager Management Console (see page 80)
Open the CA Identity Manager Management Console (see page 80)
Configure Email Notification Settings (see page 81)

Enable the CA Identity Manager Management Console

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

To enable the CA Identity Manager 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:

   JBossInstallDir/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 Identity Manager Management Console is enabled.

Open the CA Identity Manager Management Console

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

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

http://*enterprise_host*:*port*/idmmanage

The CA Identity Manager Management Console opens.

Example: Open the CA Identity Manager Management Console

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

http://appserver123:18080/idmmanage

In this example, the CA Identity Manager Management Console is installed on a host named appserver123 and uses the default CA Access Control Enterprise Management port 18080.

Configure Email Notification Settings

When you open the CA Identity Manager 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 PUPM events.

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

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

To configure email notification settings

1. 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. By default, the file is located in the following directory:

   jboss_dir/server/default/deploy
3. Locate the following entry in the file:

   <property name="mail.smtp.host" value="HOSTNAME"/>
4. Change the HOSTNAME value with the outgoing email server host name. For example:

   myMailServer.myDomain.com

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

   a. Open the corresponding email template. For example, to configure email notifications that let recipients know that a privileged account password request was approved, open the CreatePrivilegedAccountExceptionEvent.tmpl file in the following directory:

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

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

   b. Modify the template host name and port from 'localhost:8080" to the Enterprise Management Server host name and port, for example, *computer.com:18080*

   c. Save and close the file.

6. Start JBoss.

7. In the CA Identity Manager Management Console, click Environments, the environment that you want to configure, Advanced Settings, E-mail.

   The E-mail Properties window appears.

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

   Events e-mail Enabled

   Enables email notifications for CA Access Control Enterprise Management events, including PUPM events.

   Tasks e-mail Enabled

   Enables email notifications for CA Access Control Enterprise Management tasks.

   Note: CA Access Control Enterprise Management does not provide email templates for tasks. We recommend that you do not enable email notifications for tasks.

   Template Directory

   Specifies the location of the email templates that CA Access Control Enterprise Management uses to create the email messages.

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

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

9. Specify the events for which email notifications are sent.

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

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

      - BreakGlassCheckOutAccountEvent
      - CheckOutAccountPasswordEvent
      - CreatePrivilegedAccountExceptionEvent

   b. Click Delete.

      All but the three PUPM events are deleted. You have configured CA Access Control Enterprise Management to send email notifications for these three PUPM events.

10. Click Save.

    The email notification properties are saved.

11. Click Restart.

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

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

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 2.0 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

1. If you have not already do so, download and extract the SQL Server JDBC 2.0 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 sqljdbc.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 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:
   - 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 at after the DatabaseName= parameter:

    ;integratedSecurity=true
11. From each file, delete the <security-domain> tag.
12. Save the files and restart JBoss.

    CA Access Control 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. This tag is removed because 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>
```

Uninstall CA Access Control Enterprise Management on Windows

Valid on Windows

To uninstall CA Access Control 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 Access Control 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 Access Control Enterprise Management.
4. Click Change/Remove.

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

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

Uninstall CA Access Control Enterprise Management on Solaris

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

To uninstall CA Access Control Enterprise Management on Solaris

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 Access Control Enterprise Management. By default this path is:

   /opt/CA/AccessControlServer/

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

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

Remove Additional Components from the Enterprise Management Server

To completely uninstall CA Access Control 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 Access Control 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 Access Control.
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 Identity Manager – Connector Server.
   b. Terminate the jcs.exe process.
   c. Delete the CA Identity Manager – 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 Access Control Enterprise Management components are now removed from the computer.

More information:

Uninstallation Methods (see page 120)

Chapter 4: Installing and Customizing a Windows Endpoint

This section contains the following topics:

Before You Begin

Before you can install CA Access Control, you must make sure certain preliminary requirements are met and several items of necessary information are available.

Installation Methods

You can install CA Access Control for Windows from the CA Access Control Endpoint Components for Windows DVD using the following methods:

- **Product Explorer**—The easiest way to install CA Access Control is to use the Product Explorer. The Product Explorer is a graphical installation program that lets you select between different architecture installations of CA Access Control 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 Access Control, 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 Access Control with Unicenter Software Delivery.

New Installations

When installing a new instance of CA Access Control, 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 Access Control.
- The Windows Administrator or a member of the Administrators group must install CA Access Control.
- Install CA Access Control in a unique directory, different from any other product installation directory.
- You must have Microsoft Internet Explorer 6.x or 7.x installed.

- CA Access Control 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 Licensing

  All CA enterprise products and their options require a license file, CA.OLF, for each computer within a network where CA software runs. When you purchase CA Access Control, 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 Access Control line) to the CA_license directory (for example, C:\Program Files\CA\SharedComponents\CA_LIC).

Upgrades and Reinstallations

When upgrading CA Access Control, note the following:

- Read the *Release Notes*.

  This document contains information about supported platforms, CA Access Control versions you can upgrade from, known issues, considerations, and other important information you should read before installing CA Access Control.

- 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 Access Control for the installation to complete. Future patches may not require a reboot.

  Note: For information about which releases of CA Access Control 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 Access Control 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 Access Control registry settings are stored in the following location:

  HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl
- Full auditing is enabled by default when you upgrade CA Access Control.

  Important! Depending on the rules you have in the database, the number of audit events that CA Access Control 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*.

CA Unicenter Integration

When you integrate CA Access Control and Unicenter Security components, consider the following:

- Once you run the Unicenter Integration and Migration Installation process successfully, you should verify that Unicenter TNG login intercepts are disabled.

  We do not recommend running Unicenter TNG login intercepts after running the Unicenter Integration and Migration Installation process.

- Unicenter TNG Data Scoping rules (rules that target Unicenter TNG asset types with a -DT suffix) are ignored during the migration process.

  These rules are not supported by the CA Access Control Migration process.

- Unicenter Security rules that have been implemented against any of the following Unicenter Security asset types are obsolete because Unicenter Security is no longer used: CA-USER, CA-ACCESS, CA-USERGROUP, CA-ASSETGROUP, CA-ASSETTYPE, and CA-UPSNODE.

  Rules that target any of these asset types, or any of their derivatives, are ignored during the migration process.

- If you upgrade Unicenter TNG or apply Unicenter TNG fixes after running the Unicenter Integration process, then you must ensure sure that the CAUSECR.DLL under the %CAIGLBL000%\BIN directory has not been replaced and is the same as the CAUSECR.DLL.EAC file in the CA Access Control installation path bin directory.

- If CA Access Control is uninstalled, the CA_ROUTER_CAUSECU Unicenter Security option is reset to one, the SETLOCAL CAIACTSECSV Unicenter Security option is reset to yes, and CAUSECR.DLL file in the %CAIGLBL000%\BIN directory is replaced by the Unicenter default. You may need to customize these options after the uninstall process.

Coexistence with Other Products

When installing CA Access Control, consider the issue of CA Access Control coexistence with other programs on the computer.

CA Access Control runs in an environment alongside other programs, for example, CA Antivirus. This can lead to collisions between CA Access Control and the programs running on the local computer. To this end, the coexistence utility (eACoexist.exe) runs during CA Access Control 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 Access Control supports. If a program CA Access Control detects is trusted, CA Access Control registers the program by creating a SPECIALPGM rule. This SPECIALPGM rule determines the access to this program and makes sure that CA Access Control 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 Access Control. 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 Access Control Product Explorer lets you select between different architecture installations of CA Access Control 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 Access Control Endpoint Components for Windows DVD into your optical disc drive.

Install Using Product Explorer

The CA Access Control Product Explorer lets you select between different architecture installations of CA Access Control 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 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.

   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 Access Control with and click OK.

   The CA Access Control installation program starts loading and, after a short while, the Introduction screen appears.

   Note: If the installation program detects an existing installation of CA Access Control, you are prompted to select whether you want to upgrade CA Access Control.
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 Access Control, refer to the installation worksheets (see page 96).

   The installation program installs CA Access Control. 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 Access Control was installed properly (see page 117).

   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 Access Control 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 Access Control 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 Access Control 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 Access Control SDK, and API samples.	Select this feature if you want to develop in-house CA Access Control-secured applications.
Stack Overflow Protection (STOP)	Enables the CA Access Control 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 Access Control and migrate Unicenter NSM data. CA Access Control 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*.
PUPM Agent	The PUPM Agent configures the local computer for Privileged User Password Management (PUPM), so that you can discover and manage privileged accounts and applications on the computer.	Select this feature for every endpoint that has privileged accounts that you want to use PUPM to manage. **Note:** For more information about PUPM, 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 Enterprise Log Manager 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 Access Control database.	
Administration terminals	Lets you define computers from which administrators can administer the CA Access Control database.	If the administrators are using CA Access Control Endpoint Management to administer CA Access Control, you only need to define the computer where CA Access Control 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 Access Control to add to host names.	You must enter at least one domain name that CA Access Control 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 Access Control database.	We recommend that you set CA Access Control 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 Access Control 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 Access Control with Unicenter TNG	Lets you set CA Access Control 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 Access Control should send the audit data.
Integrate CA Access Control with Unicenter Calendars	Lets you set support of integration of Users and Access permissions with Unicenter NSM calendars.	Configure CA Access Control 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 Access Control.	If you do not select this option, the Unicenter Security to CA Access Control migration is not performed and user names in CA Access Control 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 399)
SSL, Authentication, and Certificates (see page 403)

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.* For example, if you installed the advanced policy management server components on a host named host123.comp.com, you should use the following: DH__@host123.comp.com **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.
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 Access Control 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 PUPM 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 PUPM 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 PUPM 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.
Communication	Lets you define a new key to	Make sure that you use the same key when you

Information	Description	Recommendation
Key	authenticate communication between the Distribution Server and the Report Agent, and the Distribution Server and the PUPM Agent.	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 Access Control.

Set Custom Defaults for the Installation Program

To set the CA Access Control 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 Access Control Endpoint Components for Windows DVD into your optical disc drive.

   The CA Access Control 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 Access Control.

Install Silently

To install CA Access Control without interactive feedback, you can install CA Access Control silently using the command line.

To install CA Access Control 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 Access Control Endpoint Components for Windows DVD into your optical disc drive.

   The CA Access Control 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 Access Control can be found at the bottom of the license agreement available when running the installation program.

setup Command—Install CA Access Control for Windows

Use the setup command to install CA Access Control for Windows with preset custom defaults (see page 103) or when performing a silent installation (see page 104).

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 Access Control installation language.

Note: For more information about the CA Access Control 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.

/norestart

Specifies not to restart the computer after the installation is complete.

/qn

Specifies a silent installation, in conjunction with the */s* option.

Important! You must 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 Access Control database.

Default: User performing the installation.

ADV_POLICY_MNGT_CLIENT={1 | 0}

Configures the local computer for advanced policy management (1).

Default: 0

If you specify this option and set it to 1, you also need to specify:

- **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 Access Control. The actual *keyword* you need to use can be 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 PUPM Agent and Report Agent communicate with (for example, test.company.com).

Default: *none*

DIST_SERVER_PORT=\"*port*\"

Defines the port number that the PUPM Agent and Report Agent use for communication with the Distribution Server.

Default: 7243

DOMAIN_LIST=\"*domains*\"

Defines a space-separated list of your networks' DNS domain names for CA Access Control 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 Access Control database (CA Access Control 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 Access Control 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 automatically 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 Access Control 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 PUPM Agent and Report Agent.

PMDB_CLIENT={1 | 0}

Specifies whether the local CA Access Control database is subscribed to a parent Policy Model database.

Default: 0 (no)

If you specify this option and set it to 1, you also need to specify:

- **PMDB_PARENTS_STR=\"***parents***\"**

  Defines a comma-separated list of parent Policy Model databases the local CA Access Control 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, you also need to specify:

- **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_AGENT={1 | 0}

Specifies whether the PUPM Agent is installed (1).

Default: 0 (not installed)

If you specify this option and set it to 1, you also need to 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, you also need to 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, you also need to specify:

- **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 will be sent.

  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. You must also set SUPPORT_TNG_CALENDAR=1.

  Default: 10

- **UNICENTER_MIGRATION={1 | 0}**

  Specifies if Unicenter security data is migrated to CA Access Control (1).

  Default: 1 (migrated)

USE_SECURE_COMM={1 | 0}

Specifies whether the PUPM Agent and the Report Agent use secure communication (1).

Default: 1 (yes)

If you specify this option and set it to 1, you also need to 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, you also need to specify:

- **CERT_OPTION={1 | 2}**

  Specifies which certification option to use.

  Values: 1—Generate CA Access Control certificate; **2**—Use an existing installed certificate.

  Default: 1

- **GENERATE_OPTION={1 | 2}**

  Specifies how to generate the CA Access Control certificate. You must also 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 Access Control certificate. You must also set CERT_OPTION=1.

- **GEN_ROOT_CERT=\"***file***\"**

  Defines the fully qualified file name of the root certificate file (.pem). You must also 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). You must also set CERT_OPTION=1 and GENERATE_OPTION=2.

- **ROOT_PRIV_KEY_PWD=\"***password***\"**

  Defines the password for the root private key. You must also set CERT_OPTION=1 and GENERATE_OPTION=2.

- **EXIST_ROOT_CERT=\"***file***\"**

  Defines the fully qualified file name of the root certificate file (.pem). You must also set CERT_OPTION=2.

- **EXIST_SERVER_CERT=\"***file***\"**

  Defines the fully qualified file name of the server certificate file (.pem). You must also set CERT_OPTION=2.

- **EXIST_PRIVATE_KEY=\"***file***\"**

  Defines the fully qualified file name of the server private key file (.key). You must also set CERT_OPTION=2.

- **EXIST_PRIV_KEY_PWD=\"***password***\"**

  Defines the password for the server private key. You must also 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, you also need to specify:

- **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 choose to change the default encryption key. You must 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 Access Control installation, then opens the graphical installation program.

```
setup.exe /s /v"INSTALLDIR="C:\CA\AC" /L*v %SystemRoot%\eACInstall.log"
```

Examples: Use the setup Command to Specify Encryption Settings

The following examples install CA Access Control in silent mode with various encryption settings. In each example, the command also installs CA Access Control, 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 Access Control 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 Access Control 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 399)

Unicenter Software Delivery Installation

To install CA Access Control from Unicenter Software Delivery, follow these steps:

Note: The CA Access Control Endpoint Components for Windows DVD contains a directory named REGINFO. This directory contains several files needed to install CA Access Control using Unicenter Software Delivery.

1. To export the CA Access Control Unicenter Software Delivery package, insert the CA Access Control Endpoint Components for Windows DVD into your optical disc drive.
2. Launch the Unicenter Software Delivery explorer.
3. Register the Unicenter Software Delivery package for CA Access Control by choosing the root directory of the CA Access Control installation.
4. Unseal the CA Access Control package.
5. In the procedures for Start Services, Stop Services, Uninstall, and Upgrade replace the parameters <admin> and <password> with the credentials of the CA Access Control ADMIN user.

   Note: These credentials are used to shut down CA Access Control during these processes. The user you enter should be able to log on to client computers with these credentials.
6. Seal the package.

Upgrade a Windows Endpoint

When you upgrade an endpoint, the CA Access Control installation program upgrades the core CA Access Control functionality and any features that are already installed on the endpoint. You can choose to install new features after you upgrade the core CA Access Control functionality.

Note: You may have to reboot the computer to complete the upgrade. For information about which releases of CA Access Control 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 Access Control on the computer.

   A dialog appears asking if you want to perform an upgrade of CA Access Control.

5. Click Yes.

   The CA Access Control 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 Access Control. 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 Access Control features, as follows:

   a. Click Start, Control Panel, Add or Remove Programs.

   b. Scroll through the program list and select CA Access Control, and click Change.

      The CA Access Control 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 96). You may need to reboot your computer for the installation to complete.

Starting and Stopping CA Access Control

By default, CA Access Control services start automatically whenever you start Windows.

Stop CA Access Control

You use the secons utility to stop CA Access Control on local and remote computers. You do not require any specific Windows privileges to stop CA Access Control, but you must have the ADMIN or OPERATOR attribute in CA Access Control.

Note: You cannot stop CA Access Control while it is running from Windows Services Manager. You must use the secons utility to stop CA Access Control before you modify a CA Access Control service in Windows Services Manager.

To stop CA Access Control

1. Open a command prompt window and navigate to the directory containing the CA Access Control binaries.

   By default, the CA Access Control 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 Access Control services on the defined, space-separated, remote hosts. If you do not specify any hosts, CA Access Control 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 Access Control on a local computer, the following message appears:

   CA Access Control is now DOWN

   When you stop CA Access Control on remote hosts, CA Access Control 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 Access Control Manually

Typically, you start CA Access Control by starting Windows.

If you stopped CA Access Control, you can also restart it manually by issuing commands from the command prompt.

To start CA Access Control 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 Access Control binaries (by default, C:\Program Files\CA\AccessControl\bin on your system directory).
3. Start CA Access Control by entering:

   ```
   seosd -start
   ```

Checking Your Installation

If you have installed CA Access Control successfully, you will notice the following changes:

- A new key is added to the Windows registry:

  HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl

  While CA Access Control is running, the CA Access Control keys and sub-keys are protected and you can modify the keys only through CA Access Control Endpoint Management or by using selang commands. However, you do not need to use CA Access Control Endpoint Management or selang commands to read the keys and values.

- When you restart your computer, several new CA Access Control 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 Access Control services begins with "CA Access Control". 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 Access Control, every time a user logs in interactively (GINA) and CA Access Control services are running, a protection screen appears, telling the user that this computer is protected by CA Access Control.

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 Access Control for advanced policy management. If you specified this information when you installed CA Access Control 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 Access Control 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 Access Control, 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 Access Control.

3. Click Change.

   The CA Access Control installation wizard appears.

4. Follow the wizard prompts to modify the CA Access Control installation so that you enable the Report Agent feature.

Note: After you enable the Report Agent, you can modify CA Access Control configuration settings to change performance-related settings. For more information on Report Agent configuration settings, see the *Reference Guide*.

Customizing CA Access Control for Cluster Environments

To use CA Access Control in a cluster environment, you must install CA Access Control 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 Access Control can detect that it is running in a cluster environment. If CA Access Control 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 Access Control rules if NODE1 or NODE2 are contacted using outside network IP addresses.

In addition, network interception acts as defined by CA Access Control 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 Access Control from a Windows endpoint:

- Regular uninstallation—This method uses a graphical interface to uninstall CA Access Control and provides interactive feedback.
- Uninstall silently—This method uses the command line to uninstall CA Access Control without interactive feedback.

Uninstall CA Access Control

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 Access Control

1. (Optional) Shut down CA Access Control (see page 116).

   Note: If you do not do this manually, the installation program shuts CA Access Control 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 Access Control from the installed programs list and click Add/Remove.

5. In the message box confirming that you want to remove CA Access Control, click Yes.

6. When uninstall is complete, click OK.

7. Reboot the computer to remove all CA Access Control components.

Uninstall CA Access Control Silently

To uninstall CA Access Control without interactive feedback, you can uninstall CA Access Control 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 Access Control 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 Access Control 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 Access Control down for you.

Chapter 5: Installing and Customizing a UNIX Endpoint

This chapter guides through the CA Access Control UNIX endpoint installation process. When you have finished installing CA Access Control following the instructions in this chapter, your system should contain a copy of the CA Access Control endpoint software and an elementary CA Access Control database. The chapter then explains how to start CA Access Control 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 Access Control, 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 Access Control on any one of the supported UNIX operating systems.

Note: For more information, check the *Release Notes*.

Administration Terminals

You can administer CA Access Control policy from a central place using CA Access Control Endpoint Management and CA Access Control 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 Access Control database.

By default, CA Access Control 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 Access Control management), and let enterprise user *my_uid* log in to the computer and use CA Access Control management tools (selang, CA Access Control Endpoint Management, and so on).

Note: If the administrators are using CA Access Control Endpoint Management to administer CA Access Control, you only need to define the computer where CA Access Control Endpoint Management is installed. You do not need to define the computer where the administrator opens the browser.

Installation Notes

When installing CA Access Control (whether for the first time or as part of an upgrade), 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 Access Control.

- 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, but not vice versa. As commands in earlier versions are supported in later versions, earlier PMDBs can propagate to CA Access Control 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 be 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 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 Access Control 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, you need to 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 Access Control 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 Access Control 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 Unicenter support team for a compatibility patch. You must install this compatibility patch before installing CA Access Control on the host.

- If you want 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 Access Control.

  The setup script for CCI Standalone (CCISA) uses ksh which is not installed by default on Linux.

- To install CA Access Control 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 Access Control binaries on Linux x86 64-bit systems. If you are upgrading, these packages maintain compatibility with the previous 32-bit CA Access Control installation. Before you install CA Access Control, you must make sure 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 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 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 Access Control 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 before installing or upgrading CA Access Control 64-bit binaries on Linux x86 64-bit:

  - The 64-bit installation package does not support CA Access Control GUI utilities, such as selock and selogo.
  - If the install_base script can access both the 32-bit and 64-bit tar files, then by default the install_base script uses the 32-bit tar file. 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.
  - 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 Access Control installation from a 32-bit installation, you must set the -force_install flag prior to installation. The installation will fail if you do not set this flag.
  - To fully uninstall cawin after uninstalling CA Access Control, use rpm -e --allmatches to ensure that the uninstall process removes both 32-bit and 64-bit versions of cawin.

- To install CA Access Control on Linux s390x 64-bit, 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, libICE.so.6, liblaus.so.1 (SLES 8, RHEL 3), libaudit.so.0 (RHEL 4, RHEL 5), libm.so.6, libnsl.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 is a list of relevant RPM packages that 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 install CA Access Control on Linux and Linux-IA64 platforms using the -all option, mfsd is not installed.
- Before you install CA Access Control 32-bit binaries on a 32-bit or 64-bit Linux computer, you must make sure 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 Access Control.

Installation Considerations for Linux s390 Endpoints

To use Message Queue functionality on CA Access Control Linux s390 endpoints and to remotely manage UNAB Linux s390 endpoints, you must install J2SE version 5.0 or later on the endpoint. Message Queue functionality lets you send report and audit data from CA Access Control endpoints to the Report Portal and CA Enterprise Log Manager, respectively. Remote management lets you use CA Access Control Enterprise Management to manage UNAB endpoints.

You can install J2SE before or after you install CA Access Control or UNAB on the endpoint. If you install J2SE after you install CA Access Control or UNAB, you must also configure the Java location on the endpoint.

How the Installation Interacts with Java

Valid on Linux s390 and Linux s390x

To use Message Queue functionality on CA Access Control Linux s390 endpoints and to remotely manage UNAB Linux s390 endpoints, you must install a supported Java version on the endpoint.

When you install CA Access Control or UNAB on a Linux s390 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 Access Control installation parameters file, customized packages for native installations, and user input from interactive CA Access Control installations.

   b. The JAVA_HOME environment variable.

   c. 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 the Endpoint

Valid on Linux s390 and Linux s390x

To use Message Queue functionality on CA Access Control Linux s390 endpoints 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 Access Control or UNAB, you must perform additional configuration steps.

To configure the Java location on the endpoint

1. Stop CA Access Control 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 Access Control and UNAB.

   The Java location is configured.

Native Installations

CA Access Control offers native package formats for installing and managing CA Access Control natively on supported operating systems. Native packages let you manage your CA Access Control installation using native package management tools.

Native Packages

CA Access Control 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 Access Control components. Native packages are located in the NativePackages directory of the CA Access Control Endpoint Components for UNIX DVD.

The following are the packages and their descriptions:

ca-lic

(Linux only) Installs the CA license program which is a prerequisite for all other packages.

Note: Only available in RPM format for Linux.

ca-cs-cawin

(Linux only) Installs the CAWIN shared component which must be installed before installing any CA Access Control package.

Note: Only available in RPM format for Linux.

CAeAC

Installs the core CA Access Control components. This is the main CA Access Control installation package and combines the server, client, documentation, TNG integration, API, and mfsd packages which are traditionally packaged separately.

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 Access Control using native packaging, note the following additional considerations:

- To install the CA Access Control RPM package you must have the following installed first:
  - License program package ca-lic-01.0080 or higher
  - CAWIN package ca-cs-cawin-11.0.6 or higher
- To build a custom CA Access Control RPM native installation package (customize_eac_rpm), you must have the rpmbuild utility on your computer.

- To build a custom CA Access Control 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 Access Control package.

  Use the CA Access Control 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.

More information:

Installation Notes (see page 125)

How to Specify That CA Access Control Uses a Password-Protected Root Certificate

When you install CA Access Control, you can configure it to use a third-party password-protected root certificate.

After you install CA Access Control, you use the root certificate to create CA Access Control server certificates. The server certificates encrypt and authenticate communication between CA Access Control components.

To configure CA Access Control to use a third-party password-protected root certificate, you must perform some additional steps when you use native packages to install CA Access Control, 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 Access Control, do the following:

   a. Create a CA Access Control server certificate from the root certificate, as follows, where *ACInstallDir* is the directory in which you installed CA Access Control:

      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 Access Control 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 Access Control components.

      use_ssl

      Specify this value to enable SSL encryption only. This value lets the computer communicate with only the CA Access Control components that use SSL encryption.

   d. Start CA Access Control.

      CA Access Control starts and uses the CA Access Control server certificate to encrypt and authenticate communication.

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

How to Specify That CA Access Control Uses a Third-Party Password-Protected Server Certificate

You can use third-party password-protected server certificates to encrypt and authenticate communication between CA Access Control components.

To configure CA Access Control to use third-party password-protected server certificates, you must perform some additional steps when you use native packages to install CA Access Control, 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 Access Control, do the following:
   a. Store the password for the for the private key on the computer, as follows, where *ACInstallDir* is the directory in which you installed CA Access Control:

      ACInstallDir/bin/sechkey -g -subpwd *password*

      -subpwd *password*

      Specifies the password for the private key of the server certificate.

   b. Verify that CA Access Control 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 Access Control components.

      use_ssl

      Specify this value to enable SSL encryption only. This value lets the computer communicate with only the CA Access Control components that use SSL encryption.

   d. Start CA Access Control.

      CA Access Control 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. It is intended for use on UNIX platforms.

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 Access Control provides. This lets you manage your CA Access Control 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 Access Control 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 Access Control 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 Access Control RPM Package

Before you can install CA Access Control using a native package, you must customize the CA Access Control 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 Access Control package.

You can find the RPM packages for each of the supported Linux operating systems in the NativePackages/RPMPackages directory of the CA Access Control Endpoint Components for UNIX DVD.

To customize the CA Access Control RPM package

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 Access Control 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 Access Control package to specify that you accept the license agreement:

   customize_eac_rpm -w *keyword* [-d *pkg_location*] *pkg_filename*

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 Access Control 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 Access Control RPM package that you can find on the CA Access Control 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 Access Control.

More information:

customize_eac_rpm Command—Customize RPM Package (see page 140)

Install CA Access Control RPM Packages

To manage the CA Access Control installation with all your other software installations, install the customized CA Access Control 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 Access Control RPM packages

1. Use the rpm command to install the ca-lic package.

   The license program installs.

2. Use the rpm command to install the ca-cs-cawin RPM package.

   CAWIN installs.

   Note: If you installed the license program to a custom directory, specify the same custom directory for the CAWIN package.

3. Customize the CAeAC package (see page 135).

   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.

4. Use the rpm command to install the CAeAC package.

   CA Access Control installs.

   Important! If you are upgrading an existing CA Access Control package, unload SEOS syscall before you try to install the new package. Otherwise, the installation fails.

Example: Install or Upgrade CA Access Control on Red Hat Linux

The following example shows how you can install the CA Access Control package that you can find on the CA Access Control 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 Access Control or an upgrade of a currently installed CA Access Control RPM package (without needing to remove the installed package first). To do this, you install the license program package and the CAWIN package (in that order), and then customize the CA Access Control 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 Access Control package that you can find on the CA Access Control 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 Access Control 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 Access Control and the Prerequisites to a Custom Directory

The following example shows how you can install the default CA Access Control and the prerequisite packages that you can find on the CA Access Control 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
rpm -U --prefix /usr/CA/shared ca-cs-cawin*ia64.rpm
cp -R CAeAC*ia64.rpm /tmp
cp ../pre.tar /tmp
chmod 777 /tmp/CAeAC*s390.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 Access Control 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. You must install the license program and CAWIN to the same custom directory.

More information:

Additional Considerations for Native Installations (see page 131)
Customize the CA Access Control RPM Package (see page 135)
customize_eac_rpm Command—Customize RPM Package (see page 140)

customize_eac_rpm Command—Customize RPM Package

The customize_eac_rpm command runs the CA Access Control RPM package customization script.

You should consider the following when using this command:

- The script works on the CA Access Control RPM packages only.

  Note: The script is not intended for use with the CAWIN and license program packages.

- 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 Access Control 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.

-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 RPM Packages

To uninstall a CA Access Control RPM package installation, you need to uninstall the CA Access Control packages in the reverse order of their installation.

To uninstall RPM packages

1. Uninstall the main CA Access Control package.

   rpm -e *CAeACPackage_name*

2. Uninstall the CAWIN package.

   rpm -e *ca-cs-cawinPackage_name*

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 Access Control provides. This lets you manage your CA Access Control installation with all your other software installations performed using Solaris native packaging.

Important! To uninstall CA Access Control 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 Access Control using a native package, you must customize the CA Access Control 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 Access Control package.

You can find the Solaris native package for each of the supported Solaris operating systems in the NativePackages directory of the CA Access Control 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, 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 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 Access Control 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 Access Control 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 Access Control 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 Access Control Solaris package that you can find on the CA Access Control 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 Access Control.

More information:

customize_eac_pkg Command—Customize Solaris Native Package (see page 148)

Install Solaris Native Packages

To manage the CA Access Control installation with all your other software installations, install the customized CA Access Control Solaris native package. The CA Access Control Solaris native packages let you install CA Access Control 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 Access Control 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 Access Control, using the pkgadd -a option. However, this file is not specific to CA Access Control.

      Important! You must perform this step to upgrade an existing Solaris package installation from an older CA Access Control 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 Access Control 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 143).

   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 Access Control 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 Access Control Endpoint Components for UNIX DVD.

CA Access Control is now fully installed but not started.

More information:

Additional Considerations for Native Installations (see page 131)
Install Solaris Native Packages on Selected Zones (see page 147)
Customize the Solaris Native Packages (see page 143)
customize_eac_pkg Command—Customize Solaris Native Package (see page 148)
convert_eac_pkg—Configure Solaris Native Installation (see page 150)

Install Solaris Native Packages on Selected Zones

You can use Solaris native packaging to install CA Access Control to selected zones. However, you must also install CA Access Control on the global zone.

Note: We recommend that you use Solaris native packaging to install CA Access Control to *all* zones.

To install CA Access Control to selected zones

Important! Make sure you use the same CA Access Control version in all zones.

1. From the global zone, issue the command to install CA Access Control.

   pkgadd -G -d *pkg_location* CAeAC

   pkg_location

   Defines the directory where the customized CA Access Control 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 Access Control only to the global zone.

2. In the global zone, enter the SEOS_load command to load the CA Access Control kernel module.

   Note: The CA Access Control kernel loads but CA Access Control does not intercept events in the global zone.

3. On each of the non-global zones where you want to install CA Access Control:

   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 Access Control (using the package you copied in the previous step) on the non-global zone you are working from.

   You can now start CA Access Control on the internal zone.

Note: You must uninstall from all non-global zones before you remove CA Access Control from the global zone.

customize_eac_pkg Command—Customize Solaris Native Package

The customize_eac_pkg command runs the CA Access Control Solaris native package customization script.

You should consider the following when using this command:

- The script works on any of the available CA Access Control 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 Access Control package you want to customize. If you do not specify a package, the script defaults to the main CA Access Control 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.

-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.

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 Access Control 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 Access Control, using the pkgadd -a option. However, this file is not specific to CA Access Control.

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 Access Control r8 SP1. You need to convert these before you upgrade.

You can convert information for an installed CA Access Control 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 Access Control 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 you how can 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 Access Control 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 Access Control 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 Access Control 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 Access Control provides. This lets you manage your CA Access Control installation with all your other software installations performed using the SD-UX.

Important! To uninstall CA Access Control 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 Access Control using a native package, you must customize the CA Access Control 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 Access Control 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 Access Control 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 Solaris 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 Access Control 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 Access Control 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 Access Control 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 Access Control SD-UX package that you can find on the CA Access Control 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 Access Control.

More information:

customize_eac_depot Command—Customize an SD-UX Format Package (see page 155)

Install HP-UX Native Packages

To manage the CA Access Control installation with all your other software installations, install the customized CA Access Control SD-UX format package. The CA Access Control SD-UX format packages let you install CA Access Control 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 Access Control 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 152).

   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 Access Control package (CAeAC) is located.

4. Install the CA Access Control package using the following command:

   swinstall -s *pkg_location* CAeAC

   SD-UX starts installing the CAeAC package from the *pkg_location* directory.

   CA Access Control is now fully installed but not started.

More information:

Additional Considerations for Native Installations (see page 131)
Customize the SD-UX Format Packages (see page 152)

customize_eac_depot Command—Customize an SD-UX Format Package

The customize_eac_depot command runs the CA Access Control 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 Access Control 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 Access Control package you want to customize. If you do not specify a package, the script defaults to the main CA Access Control 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 Access Control HP-UX package installation, you need to uninstall the CA Access Control packages in the reverse order of their installation.

To uninstall CA Access Control packages uninstall the main CA Access Control 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 Access Control provides. This lets you manage your CA Access Control 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 Access Control provides the AIX native package format (installp) only.

Important! To uninstall CA Access Control 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 Access Control using a native package, you must customize the CA Access Control 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 Access Control package.

You can find the installp format native packaging (bff files) for each of the supported AIX operating systems in the NativePackages directory of the CA Access Control Endpoint Components for UNIX DVD.

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_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 Access Control 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.

3. Display the license agreement:

   customize_eac_bff -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 Access Control package to specify that you accept the license agreement:

   customize_eac_bff -w *keyword* [-d *pkg_location*] *pkg_name*

6. (Optional) Set the language of the installation parameters file:

   customize_eac_bff -r -l *lang* [-d *pkg_location*] *pkg_name*

7. (Optional) Change the installation directory:

   customize_eac_bff -i *install_loc* [-d *pkg_location*] *pkg_name*

8. (Optional) Change the default encryption files:

   customize_eac_bff -s -c *certfile* -k *keyfile* [-d *pkg_location*] *pkg_name*

9. Get the installation parameters file:

   customize_eac_bff -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_bff -s -f *tmp_params* [-d *pkg_location*] *pkg_name*

    You can now use the package to install CA Access Control with the customized defaults.

More information:

customize_eac_bff Command—Customize a bff Native Package File (see page 161)

Install AIX Native Packages

To manage the CA Access Control installation with all your other software installations, install the customized CA Access Control AIX native package. The CA Access Control AIX native packages (bff files) let you install CA Access Control 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.

To install the CA Access Control 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 CAeAC package (see page 158).

   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 Access Control 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 Access Control 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.

   AIX starts installing the CAeAC package from the *pkg_location* directory.

   CA Access Control is now fully installed but not started.

More information:

Customize the bff Native Package Files (see page 158)
Additional Considerations for Native Installations (see page 131)

customize_eac_bff Command—Customize a bff Native Package File

The customize_eac_bff command runs the CA Access Control native package customization script for bff native package files.

The script works on any of the available CA Access Control 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]
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*

pkg_name

The name of the CA Access Control 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.

-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 Access Control AIX package installation, you need to uninstall the CA Access Control packages in the reverse order of their installation.

To uninstall CA Access Control packages uninstall the main CA Access Control package:

```
installp -u CAeAC
```

Regular Script Installations

CA Access Control offers the install_base script for installing CA Access Control 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 Access Control installation media:

- **install_base**—A script that installs CA Access Control from the tar file.
- ***_opSystemVersion_ACVersion*.tar.Z**—A compressed tar file containing all the CA Access Control files. For example, if you are installing CA Access Control 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 Access Control Endpoint Components for UNIX DVD.

Install Using install_base Script

You can install CA Access Control 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 166) 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 172).

To install CA Access Control

1. If you already have CA Access Control 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 Access Control, you need to have root permissions.

3. Mount the optical disc drive with the CA Access Control 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 Access Control 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 Access Control features. During the installation you are asked to answer questions related to installing the client and server packages of CA Access Control.

```
/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 Access Control 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 Access Control 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 Access Control 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 Access Control, 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 Access Control packages you can install:

-all

Installs all CA Access Control 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 Access Control 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 Access Control 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 Access Control 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 Access Control 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 Access Control 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 Access Control 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 Access Control 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 Access Control. 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 Access Control to the default path (/opt/CA/AccessControl).

CA Access Control creates a link to seos.ini in the /etc directory when you install CA Access Control to a non-default directory. This lets CA Access Control "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 Access Control).

-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*

-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 Access Control 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 Access Control *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 Access Control database and builds the seos.ini file. The database files are placed in the *ACInstallDir*/seosdb directory (*ACInstallDir* is the CA Access Control 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 Access Control 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 Access Control.
- Whether you want CA Access Control 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 Access Control 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 Access Control lets you specify how you want to provide the subject certificate and root certificate.

  Depending on your choices, CA Access Control 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 Access Control 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 Access Control from a remote host.
- Whether you want to enable the Report Agent, and if so, whether you want to enable CA Enterprise Log Manager.

  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 Enterprise Log Manager, you can also specify to keep time-stamped backups of the audit log file.
- Whether you want to enable the PUPM Agent.

  The PUPM Agent configures the local computer for PUPM, 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 PUPM 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 Access Control for your environment.

To configure post-installation settings

1. Append the *ACInstallDir*/bin directory to your path

   By default, the installation directory is /opt/CA/AccessControl
2. Check the seos.ini (see page 182) file tokens to make sure that the settings meet your requirements.

   If necessary, modify the settings.
3. To give yourself access to the CA Access Control man pages, add the directory *ACInstallDir*/man to your MANPATH.

   For example, if you are using csh, for the sake of your current session, enter the command:

   ```
   setenv MANPATH $MANPATH:/opt/CA/AccessControl/man
   ```

   For the sake of future sessions, add a similar line to your .login, .profile, or .cshrc file.

Start CA Access Control

Assuming you are working in an X Windows environment, invoke CA Access Control, 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 Access Control 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 Access Control 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 Access Control is writing the trace messages, to see whether CA Access Control intercepts the execution of the who command and reports on it. CA Access Control 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 Access Control reacts to them.

   The database does not yet contain any rules for blocking access attempts. Nevertheless, CA Access Control monitors the system so that you can see how the system behaves with CA Access Control installed and running, and which events CA Access Control intercepts.
6. Shut down the seosd daemon, by entering the following command:

   ```
   secons -s
   ```

   The following message displays on the screen:

   ```
   CA Access Control 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 Access Control for advanced policy management. If you specified this information when you installed CA Access Control 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 Access Control 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 Access Control, 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 Access Control 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 Access Control

Implementing full-scale security using CA Access Control 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 Access Control; they would get access based solely on resource _default settings. At a bank, however, you would probably define every user to CA Access Control and set access lists for every resource to allow specific users access to specific resources. Thus, for the same number of users, implementing CA Access Control 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 Access Control 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 Access Control 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 Access Control 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 Access Control 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 Access Control 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 Access Control 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 Access Control automatically includes the user "nobody" in the database.

```
newres PROGRAM _default defaccess(none) \
owner(nobody) audit(all)
```

CA Access Control 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 Access Control 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 Access Control reads at initialization time. By default, CA Access Control places the initialization files in the directory containing the file seos.ini, which is the installation directory for CA Access Control.

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 Access Control 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 Access Control is running:

newres FILE *ACInstallDir*/seos.ini owner(*authUser*) defacc(read)

ACInstallDir is the installation directory for CA Access Control, 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 Access Control 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 Access Control 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 184).

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 Access Control is not loaded. However, on some operating systems (for example, AIX) these utilities do not work when CA Access Control is not loaded. For these operating systems, CA Access Control 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 Access Control is not loaded.

Note: You only need to follow this procedure if the sesu utility does not run when CA Access Control 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 Access Control 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 Access Control is not loaded.

Note: You only need to follow this procedure if the sepass utility does not run when CA Access Control 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 Access Control 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 Access Control has a maintenance mode, also known as silent mode, for protection when the CA Access Control daemons are down for maintenance. In this mode, CA Access Control denies events while these daemons are down.

When CA Access Control is running, it intercepts security sensitive events and checks whether the event is allowed. Without activating maintenance mode, all events are permitted when CA Access Control services are down. With active maintenance mode, events are denied when CA Access Control 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 Access Control 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 Access Control 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 Access Control 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 Access Control 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 Access Control authorization daemon setuid to the root user so that you can start CA Access Control in maintenance mode. To make this change enter the following command:
   chmod 6111 seosd

4. Start CA Access Control daemons with seload command.

   Note: If the maintenance mode user is not root, start CA Access Control daemons with seosd command.

Installing Unicenter Security Integration Tools

Use one of two types of Unicenter Security integration installations for UNIX environments.

Full Integration

The full integration installation is useful for CA Access Control installations with Unicenter Security in use. The integration imports data from Unicenter Security to CA Access Control, so CA Access Control becomes the security system used on that host or group of hosts.

Minimal Integration

The minimal integration installation is useful for CA Access Control installations without Unicenter Security or for installations that include Unicenter Security, but it is not in use.

To Install with Full Integration of Unicenter Security

Important! To run the migration, you must log on as root; you cannot run the su (substitute user) command to change to root after you install CA Access Control.

For *full* integration of Unicenter Security and CA Access Control, do the following:

1. Install CA Access Control without populating the CA Access Control database.

   To avoid populating the database, accept the default of No when the following prompt appears on the screen:

   Import users, groups and hosts now? [y/N] :

2. Run the uni_migrate_master.sh script on the master node.

   Note: The master node is the machine that hosts the Unicenter Security database.

3. Run the uni_migrate_node.sh script on each satellite node (that is, every Unicenter Security-controlled machine).

4. Run the uni_migrate_node.sh script on the master node.

   The master node is the last machine to disable Unicenter Security after all the other nodes have been integrated.

5. Manually edit the $CAIGLBL0000/secopts file to set the value for the SSF_SCOPE_DATA and SSF_SCOPE_KEYWORD keywords to **NO**.

The installation scripts perform the following tasks:

- Execute a shell script, defclass.sh, to define user-defined security asset types as CA Access Control classes in the CA Access Control database.
- Run a program, migopts, to read and translate the current Unicenter Security environment to a similar CA Access Control environment.
- Run a program, exporttngdb, to read and translate current Unicenter Security database objects to CA Access Control database objects.
- Stop and disable the Unicenter Security daemons.

For *minimal* integration of Unicenter Security and CA Access Control, complete the following steps:

1. Run the uni_migrate_node.sh script on all nodes.
2. Manually edit the $CAIGLBL0000/secopts file to set the value for the SSF_SCOPE_DATA and SSF_SCOPE_KEYWORD keywords to **NO**.

Installation Notes

- We do not recommend running Unicenter TNG login intercepts after running the Unicenter Integration and Migration Installation. When the Unicenter Integration and Migration Installation has completed successfully, Unicenter TNG login intercepts are disabled.
- Unicenter TNG Data Scoping and Keyword Scoping rules (rules that target Unicenter TNG asset types with a -DT or -KW suffix) are not supported by the CA Access Control Migration process. Rules of this type are ignored during the migration process.
- Unicenter Security rules that have been implemented against any of the following Unicenter Security asset types are obsolete because Unicenter Security is no longer in use: CA-USER, CA-ACCESS, CA-USERGROUP, CA-ASSETGROUP, CA-ASSETTYPE, and CA-UPSNODE. Rules that target any of these asset types, or any of their derivatives, are ignored during the migration process.

  The -e (-edit) option available for uni_migrate_node.sh and uni_migrate_master.sh allows you to see and edit the rule entering the CA Access Control database.
- If you want full or minimal Unicenter TNG integration, then you must install the Unicenter Integration and Migration package with the -uni option to the install_base script. The Unicenter Integration and Migration Installation installs the Unicenter Integration and Migration scripts and binary files in the *ACInstallDir*/tng directory.
- Do not use selang -c during migration if you are listing more than one command. Instead, use selang -f input_file_name.

Solaris 10 Zones Implementation

Solaris 10 provides virtualized OS services which look like different Solaris instances, called *zones*. All Solaris 10 systems contain a master zone, called the *global zone*. Non-global zones run alongside it, and you can configure, monitor, and control them from the global zone.

You can protect each zone (or selected zones) in your environment using CA Access Control. This lets you define different rules and policies for each zone, and therefore defining different access restrictions for each zone.

Installing CA Access Control on Solaris 10 zones is no different to a regular installation, and you can do it by either one of the following methods:

- Install CA Access Control using Solaris native packaging

  CA Access Control is designed to be installed and uninstalled using Solaris native packaging tools (pkgadd and pkgrm).

  If you install using the Solaris native package installation, you can either:

  – Install CA Access Control on all zones (see page 142).

    The easiest and recommended way of installing CA Access Control on Solaris 10 is to either install on the global zone, *or* on *all* zones, including non-active zones and any zones that are created in the future.

  – Install CA Access Control on selected zones (see page 147).

    While we do not recommend this, you can use Solaris native packaging tools to install CA Access Control on selected zones. However, for CA Access Control to work in any non-global zone, you must also install CA Access Control in the global zone.

  If you installed using Solaris native packaging, use the native packaging to uninstall CA Access Control from all zones.

- Install CA Access Control in each zone using the install_base script (see page 164).

  The install_base script installs CA Access Control in the zone you are executing the script in.

  For CA Access Control to work in any non-global zone, you must also install CA Access Control in the global zone.

  If you installed CA Access Control using the install_base script, you can uninstall it from individual non-global zones. However, the CA Access Control kernel can be uninstalled only from the global zone *and* only after CA Access Control has been stopped in all zones.

  Important! If you uninstall CA Access Control from the global zone using install_base before you uninstall from all zones, users may be locked out of the zones. We recommend you use Solaris native packaging to install and uninstall CA Access Control on Solaris zones.

Zone Protection

CA Access Control 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 Access Control 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 Access Control 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.

New Zone Setup

If you install CA Access Control using Solaris native packaging on all zones, CA Access Control also automatically installs on any zones you create after the original installation. However, while the post-installation CA Access Control 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 Access Control 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.

Install on a Solaris Branded Zone

Solaris limitations mean that pkgadd does not support propagation of applications installed in the Solaris 10 global zone into branded zones. Also, CA Access Control must use an ioctl instead of a syscall to communicate with the kernel module.

To install on a Solaris branded zone

1. Install CA Access Control in the Solaris global zone using pkgadd.
2. Install CA Access Control in the Solaris branded zone using pkgadd.

   Note: The installation parameter file also lets you do this automatically when you install on the global zone.
3. In the branded zone, verify that the seos.ini entry SEOS_use_ioctl is set to 1 and fix if needed.

   This confirms that CA Access Control is configured to use ioctl.
4. In the global zone, verify that the seos.ini entry SEOS_use_ioctl is set to 1.

   This confirms that CA Access Control is configured to use ioctl.

   The installation is complete and you can now start CA Access Control in the branded zone.

   Important! If SEOS_use_ioctl is set to 0, you need to modify CA Access Control 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 Access Control in Solaris branded zones, you must use an ioctl instead of a syscall to communicate with the kernel module.

To modify CA Access Control to use ioctl for communication

1. Stop CA Access Control in the global zone and all non-global zones.

   Stop the last zone with secons -sk to disable event interception and prepare the kernel module for unloading.

2. Unload the CA Access Control kernel module in the global zone (SEOS_load -u).

   Note: The SEOS_load -u command ensures that CA Access Control is not running on any non-global zone before unloading it.

3. In each zone where CA Access Control is installed (global, non-global, and branded zones), set the seos.ini entry SEOS_use_ioctl = 1 (by default, this is set to 0).

4. Load the kernel module in the global zone (SEOS_load).

   This installs a pseudo device to let CA Access Control 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, identified as requiring a reboot, where CA Access Control is installed.

Starting and Stopping CA Access Control in a Zone

Starting and stopping CA Access Control in Solaris 10 zones is generally done in the same way you would normally start and stop CA Access Control on any Solaris computer.

The following exceptions apply to starting CA Access Control in zones:

- You can load the CA Access Control kernel module (SEOS_load) from the global zone only.
- You must load the CA Access Control kernel module in the global zone before you can start CA Access Control in any non-global zone.

  Once the CA Access Control kernel module is loaded in the global zone, you can then start and stop CA Access Control in any non-global zone and in any order.

The following exceptions apply to stopping CA Access Control in zones:

- You cannot unload the CA Access Control kernel module when one or more zones has maintenance mode (see page 186) enabled.
- You can stop CA Access Control in all zones in any order by issuing the *secons -s* command in each zone.
- You can stop CA Access Control 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 Access Control across all zones.
- You should stop the last zone with the *secons -sk* to disable event interception and prepare the CA Access Control kernel module for unloading.
- You can unload the CA Access Control kernel module (SEOS_load -u) from the global zone only.

  Note: The SEOS_load -u command ensures that CA Access Control is not running on any non-global zone before unloading it.

Start CA Access Control in A Non-global Zone

You can start CA Access Control from any non-global zone just as you would normally, but you must first load the CA Access Control kernel module in the global zone.

To start CA Access Control in a non-global zone

1. In the global zone, enter the SEOS_load command to load the CA Access Control kernel module.

   The CA Access Control kernel loads and you can now start CA Access Control in any zone.

   Note: The CA Access Control kernel loads but CA Access Control does not intercept events in the global zone.
2. In the non-global zone, enter the seload command to start CA Access Control in that zone.

   The non-global zone is protected by CA Access Control.

   Note: You can also start CA Access Control in the non-global zone remotely. For more information, see the seload command in the *Reference Guide*.

zlogin Utility Protection

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 Access Control comes with a predefined LOGINAPPL resource for protecting the zlogin utility.

Start CA Access Control Automatically

After you have tested CA Access Control and experimented with its features, you are ready to implement CA Access Control 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.

Chapter 6: Installing and Configuring CA Access Control for High Availability

This section contains the following topics:

High Availability

The high availability strategy CA Access Control Enterprise Management uses is called mirrored sites. *Mirrored* sites are fully redundant facilities with full, real-time information mirroring and are identical to the primary site in all technical aspects. The data is processed and stored at the primary and mirrored sites simultaneously.

Mirrored sites employ an active-passive deployment for failover and load balancing. 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 to use 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 Access Control 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.

Components of a High Availability Environment

You need the following to deploy CA Access Control in a high availability environment.

- Primary server:
  - Enterprise Management Server
- Secondary server:
  - Enterprise Management Server
- User repository
- Shared storage solution:
  - Policy and reporting database
  - CA Business Intelligence
  - 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 have been written to durable, persistent storage.

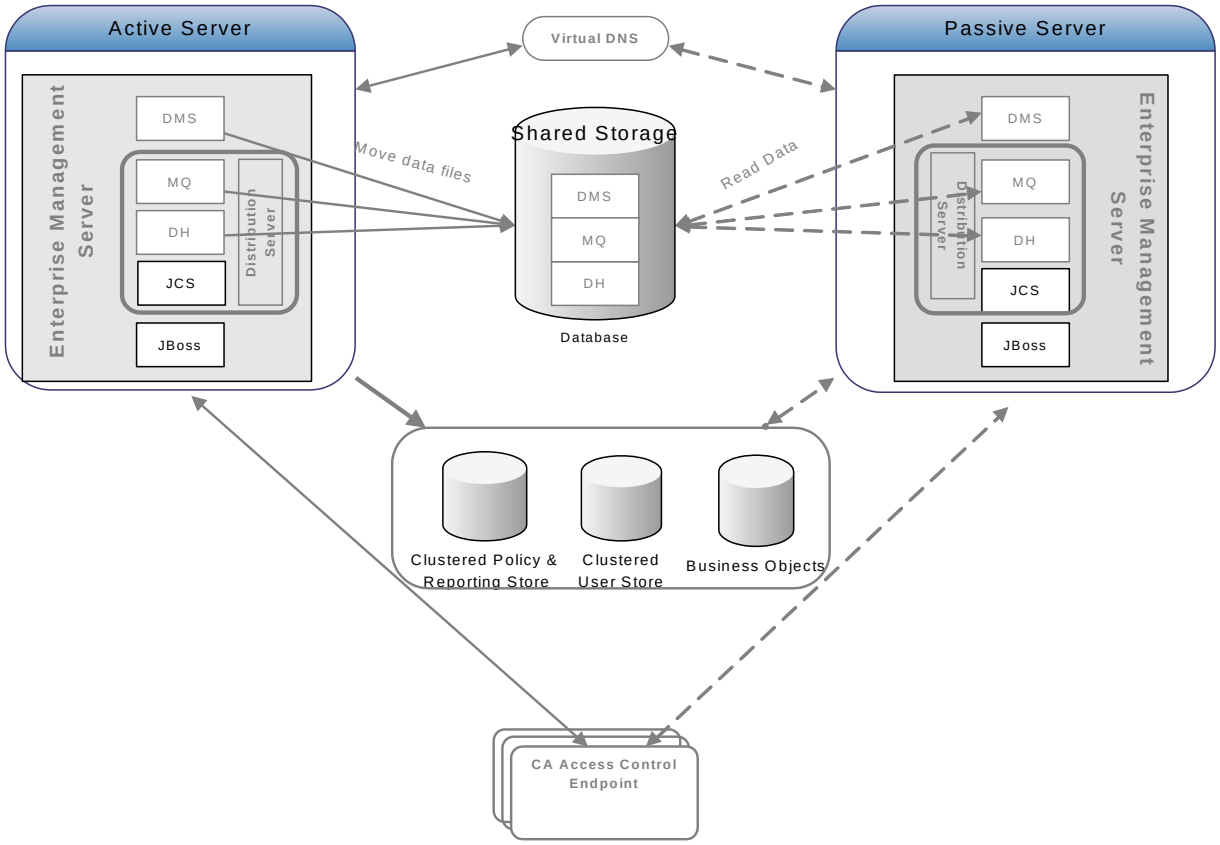
The following are examples of the software based shared storage solutions:

- Dual-Port SCSI device
- Storage Area Network (SAN)

Dual-Port SCSI and SAN solutions comply with the write order and synchronous write persistence requirments.

High Availability Implementation Architecture

The following diagram shows how you implement CA Access Control in a high availability environment:

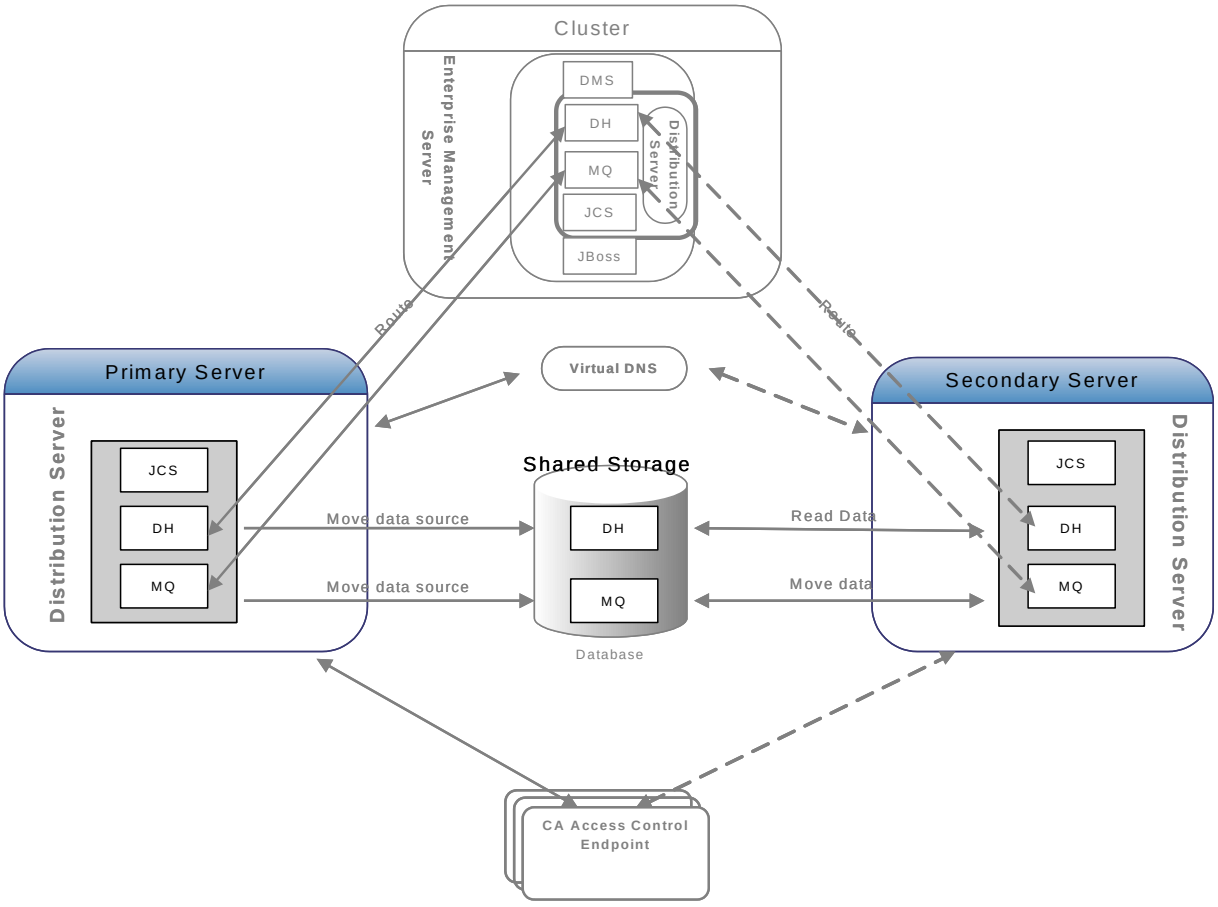


As illustrated in the preceding diagram, a high availability implementation has the following:

- A primary Enterprise Management Server and at least one secondary Enterprise Management Server
- A clustered installation of a policy and reporting store, user store and CA Business Intelligence
- A shared storage that holds the DH, DMS and Message Queue data files and is accessible by both the primary and secondary CA Access Control Enterprise Management servers
- A virtual DNS or similar routing software
- CA Access Control endpoints able to work with both the primary and secondary Enterprise Management Servers

Distribution Servers in a High Availability Environment Architecture

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 DH and Message Queue data files and that is accessible by both the primary and secondary Distribution Servers.
- A virtual DNS or a similar routing software.
- CA Access Control endpoints able to work against both the primary and secondary Distribution Servers

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 Access Control 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 Access Control 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 ot the application are logged out. To continue using the application, the users must log in to CA Access Control Enterprise Management again.

Distribution Servers for High Availability

The Distribution Server handles all communication between the CA Access Control Enterprise Management Server and the endpoints. According to the amount of CA Access Control endpoints that you plan to deploy, you may need to install additional Distribution Servers.

We recommend that you use virtual DNS names that are controlled by the clustering software solution to enable a seamless transition from between the Distribution Servers in case of failure.

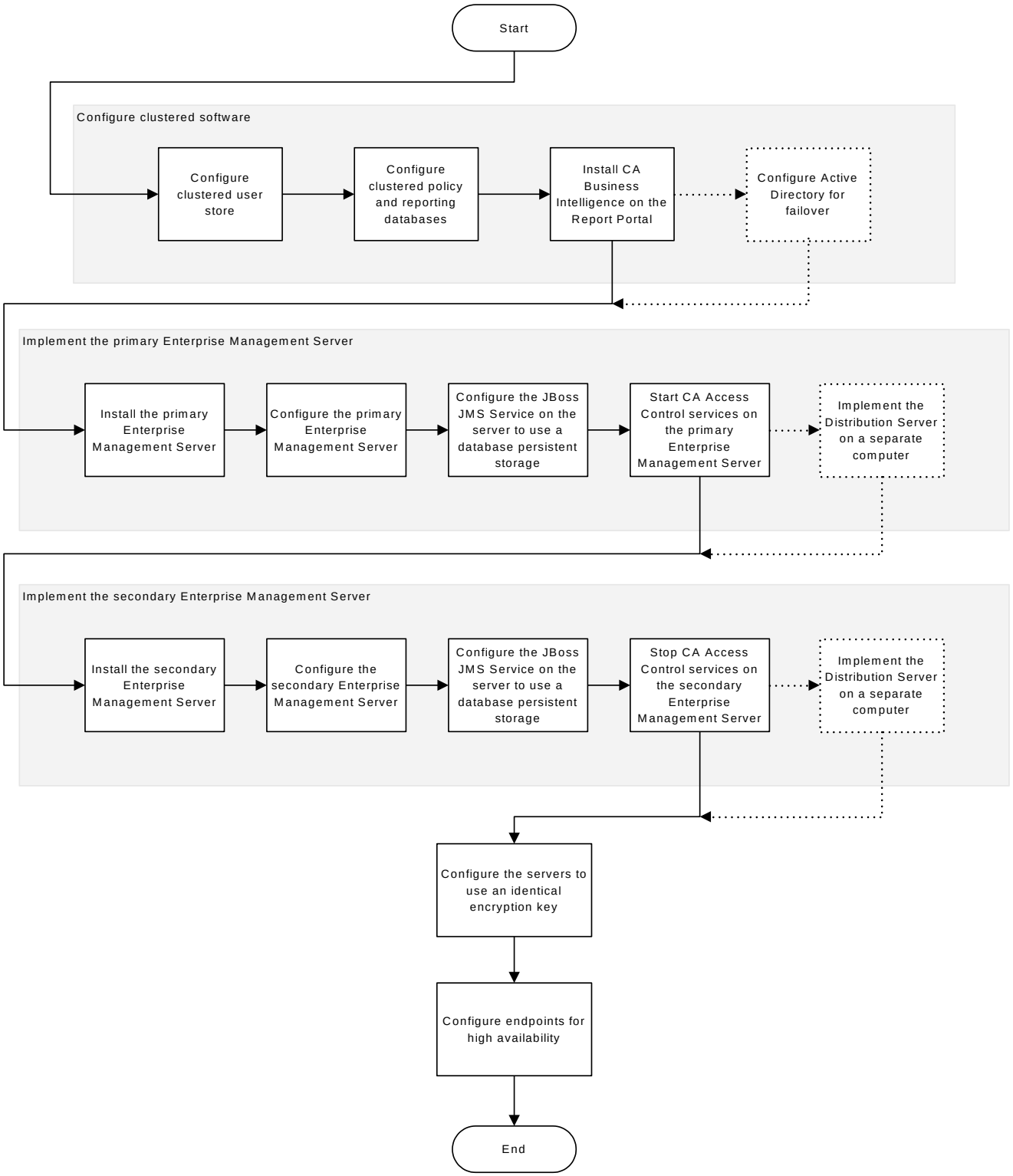
Note: You can have multiple Distribution Servers installed and configured to work with only one Enterprise Management Server.

How to Configure CA Access Control Enterprise Management for High Availability

To correctly configure the high availability environment, 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 clustered user store
Configure clustered policy and reporting databases
Install CA Business Intelligence on the Report Portal
Configure Active Directory for failover
Implement the primary Enterprise Management Server
Install the primary Enterprise Management Server
Configure the primary Enterprise Management Server
Configure the JBoss JMS Service on the server to use a database persistent storage
Start CA Access Control services on the primary Enterprise Management Server
Implement the Distribution Server on a separate computer
Implement the secondary Enterprise Management Server
Install the secondary Enterprise Management Server
Configure the secondary Enterprise Management Server
Configure the JBoss JMS Service on the server to use a database persistent storage
Stop CA Access Control services on the secondary Enterprise Management Server
Implement the Distribution Server on a separate computer
Configure the servers to use an identical encryption key
Configure endpoints for high availability
End

More information:

How to Set Up Reporting Service Server Components (see page 243)
How to Install the Enterprise Management Server Components (see page 51)

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.

To configure the primary Enterprise Management server

1. If you did not do so, install CA Access Control Enterprise Management on the primary server.

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

2. Stop all CA Access Control services.

3. 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

      The DMS and DH are on the shared storage.

   d. Set the *_pmd directory_* 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.

4. Configure the Message Queue to use the shared storage as follows:
   a. Copy the Message Queue data store folder to the shared storage. These files are located in the following directory:

      ACServerInstallDir/MessageQueue/tibco/ems/bin/datastore

   b. Open the tibemsd.conf file for editing. This file is located by default in the following directory:

      EACServerInstallDir/MessageQueue/tibco/ems/bin

   c. 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.

   d. Save and close the file.

   e. Open the queues.conf file for editing.

   f. Append a comma and add the word "**failsafe**" at the end of every queue definition line, then save and close the file.
5. Start all CA Access Control 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,failsafe
queue/audit secure,failsafe
ac_endpoint_to_server secure,failsafe
ac_server_to_endpoint secure,failsafe
```

Configure the Secondary Enterprise Management Server

The secondary Enterprise Management Server handles endpoint requests in an event of failure to the primary server.

To configure the secondary Enterprise Management Server

1. If you have not already done so, install the Enterprise Management Server on the secondary server (see page 61).

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

2. Stop all CA Access Control services.

3. Set the *_pmd directory_* 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.

4. 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/ems/bin

      ACServerInstallDir

      Defines the name of the directory where the Enterprise Management Server is installed.

   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.

   c. Save and close the file.

   d. Open the queues.conf file for editing.

   e. Append a comma and add the word "**failsafe**" at the end of every queue definition line, then save and close the file.

5. Verify that the CA Access Control services are not running

   You have configured the secondary Enterprise Management Server.

Configure the JBoss JMS Service to Use a Database Persistent Storage

The JBoss JMS (Java Message Service) uses a local file to persist its messages. If the primary Enterprise Management Server fails, the messages that are stored in the local file are not replicated to the secondary Enterprise Management Server. To help ensure persistency, configure the JBoss JMS service on the primary and secondary Enterprise Management Servers to use the shared storage. You must complete this procedure on both the primary and secondary Enterprise Management Servers, starting with the primary server.

Important! Specify identical user account settings and persistent storage settings on both the primary and secondary Enterprise Management Servers.

To configure the JBoss JMS to use a database persistent storage

1. Stop JBoss if it is running.
2. Navigate to the following directory, where *JBoss_HOME* specifies the name of the directory where JBoss is installed:

   JBoss_HOME/server/default/deploy/jms
3. Delete the file hsqldb-jdbc2-service.xml.
4. Navigate to the following directory:

   JBoss_HOME/docs/examples/jms
5. Locate *one* of the following files:
   - (Oracle) oracle-jdbc2-service.xml.
   - (SQL Server) mssql-jdbc2-service.xml.
6. Copy the file to the deploy directory, located in the following location:

   JBoss_HOME/server/default/deploy
7. In the deploy directory duplicate the file objectstore-ds.xml and save it under the name: jmsstore-ds.xml.
8. Open the jmsstore-ds.xml file for editing and locate the following tag:

   <jndi-name>jdbc/objectstore</jndi-name>
9. Replace the default value with *one* of the following:
   - (MSSQL) MSSQLDB
   - (Oracle) OracleDS

   For example:

   <jndi-name>OracleDS/objectstore</jndi-name>

10. Locate and add a comment marks (<!--) and (-- >) to the <security-domain> tag. For example:

    <!--security-domain>imobjectstoredb</security-name-->

11. Locate and uncomment the following tag:

    <!—Replacing clear text password with Security Domain settings -- >
    <user-name>DB_USER</user-name>
    <password>DB_PASSWORD</password>

12. Replace the DB_USER and DB_PASSWORD fields with a user name and password of a user that is assigned administrative privileges.

13. Start the JBoss service.

    The JBoss application server starts.

    The JBoss JMS now stores messages on the relational database. Messages are accessible to both the primary and secondary Enterprise Management Servers.

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.

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 on 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 435).

   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}:/lxnvWwAEcYhSmOu3YT3ow==</module-option>
                        <module-option
name="managedConnectionFactoryName">jboss.jca:name=jdbc/objectstore,service=NoTxCM</module-option>
                </login-module>
        </authentication>
</application-policy>
```

Configure Endpoints for High Availability

After you installed and configured the primary and secondary Enterprise Management Servers, you set up the CA Access Control endpoints to work in a high availability environment.

To configure endpoints for high availability

1. Install CA Access Control with the Advanced Policy Management Client feature enabled on the endpoint (see page 95).

   The CA Access Control 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. From a command prompt window, connect to the DMS computer.

   ```
   host dms__@computer.com
   ```

   A message appears informing of a successful connection.

2. 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.

3. 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\communicatio
     n
     ```

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.

To configure Active Directory for failover

1. Enable the CA Identity Manager Management Console (see page 80).

   You use the CA Identity Manager Management Console to configure the list of Domain Controllers in the environment.

2. Open the CA Identity Manager Management Console (see page 80)

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="primaryDir.com:389 secondaryDir.com:389" failover/>
   ```

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.

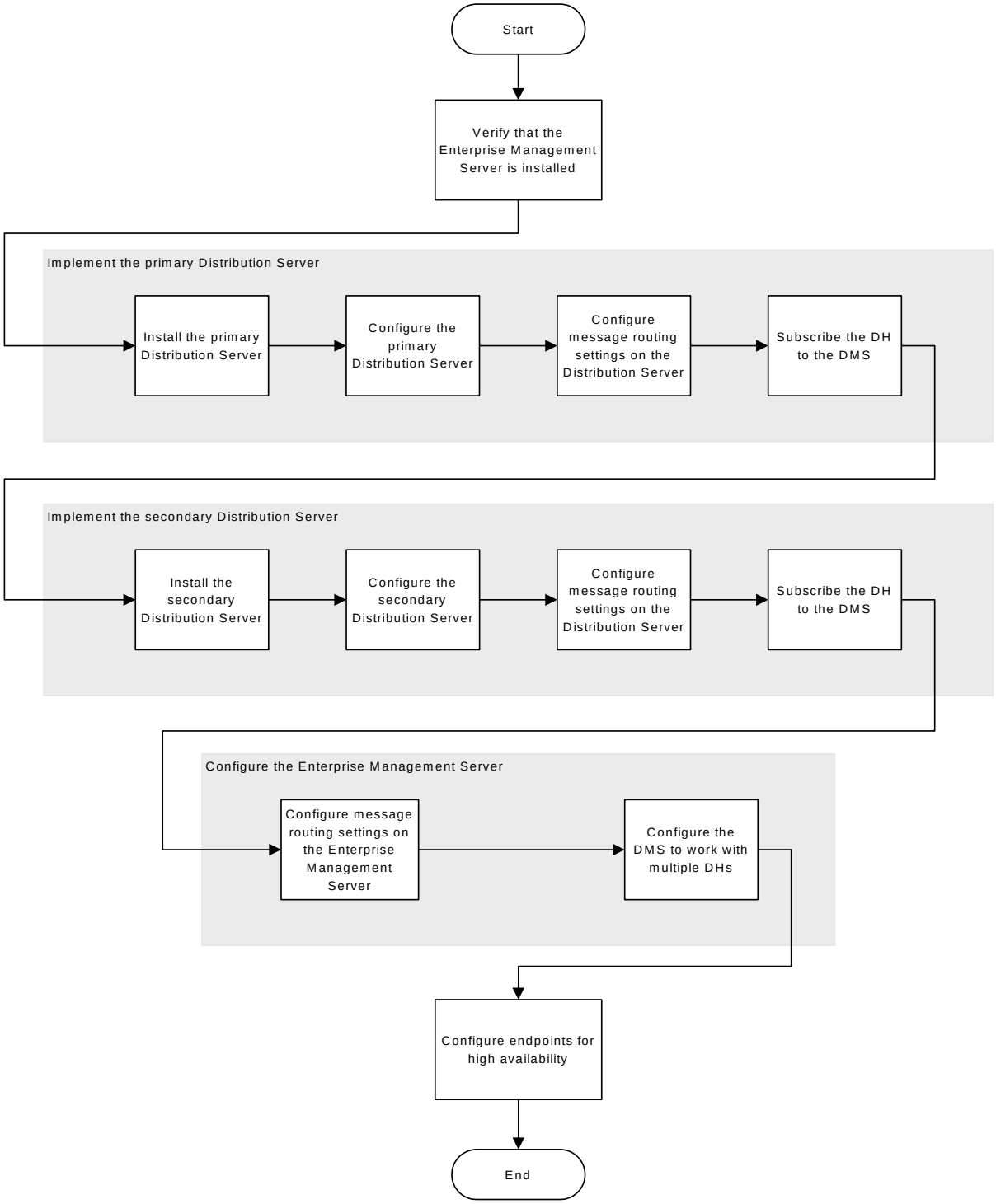
9. Click Continue, and restart the environment.

   The Enterprise Management Server can now work with the primary and secondary Domain Controllers.

How You Configure the Distribution Servers for High Availability

To correctly configure multiple Distribution Servers in a high availability environment, you must 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 against one Enterprise Management Server.


Start
Verify that the Enterprise Management Server is installed
Implement the primary Distribution Server
Install the primary Distribution Server
Configure the primary Distribution Server
Configure message routing settings on the Distribution Server
Subscribe the DH to the DMS
Implement the secondary Distribution Server
Install the secondary Distribution Server
Configure the secondary Distribution Server
Configure message routing settings on the Distribution Server
Subscribe the DH to the DMS
Configure the Enterprise Management Server
Configure message routing settings on the Enterprise Management Server
Configure the DMS to work with multiple DHs
Configure endpoints for high availability
End

More information:

How to Install the Enterprise Management Server Components (see page 51)
Install the Distribution Server (see page 352)
How to Configure Message Routing Settings (see page 364)
Subscribe a DH to a DMS (see page 385)
Configure Endpoints for High Availability (see page 211)

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.

To configure the primary distribution server

1. Stop the JCS, CA Access Control and Message Queue Server services.
2. 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. Set the *_pmd_directory_* 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.

3. Configure the Message Queue to use the shared storage, as follows:
   a. Copy the Message Queue data store files to the shared storage.These files are located in the following directory:

      DistServerInstallDir/MessageQueue/tibco/ems/bin/datastore

   b. Open the tibemsd.conf file for editing. This file is located in the following directory:

      DistServerInstallDir/MessageQueue/tibco/ems/bin

   c. 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.
   d. Save and close the file.
   e. Open the queues.conf file for editing.
   f. Append a comma and add the word "**failsafe**" to the end of every queue definition line, then save the file.
4. Start the CA Access Control 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,failsafe
queue/audit secure,failsafe
ac_endpoint_to_server secure,failsafe
ac_server_to_endpoint secure,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.

To configure the secondary distribution server

1. Stop the JCS, CA Access Control and Message Queue Server services.
2. Configure the Distribution Host to use the shared storage, as follows:
   a. Set the *_pmd_directory_* 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.
3. 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/ems/bin

      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 "**failsafe**" at the end of every queue definition line, then save the file.
4. Verify that the CA Access Control services on the secondary server are stopped.

Configure the DMS to Work with Multiple DHs

Configuring the DMS on the Enterprise Management Server to work with multiple DHs is a step in the process to set up Distribution Servers for high availability.

To configure the DMS to work with multiple DHs

1. Log into CA Access Control 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 secondary and primary Distribution Hosts can now share the DMS computer.

Chapter 7: Integrating with CA Enterprise Log Manager

This section contains the following topics:

About CA Enterprise Log Manager

CA Enterprise Log Manager focuses on IT compliance and assurance. It lets you collect, normalize, aggregate, and report on IT activity, and generate alerts requiring action when possible compliance violations occur. You can collect data from disparate security and non-security devices.

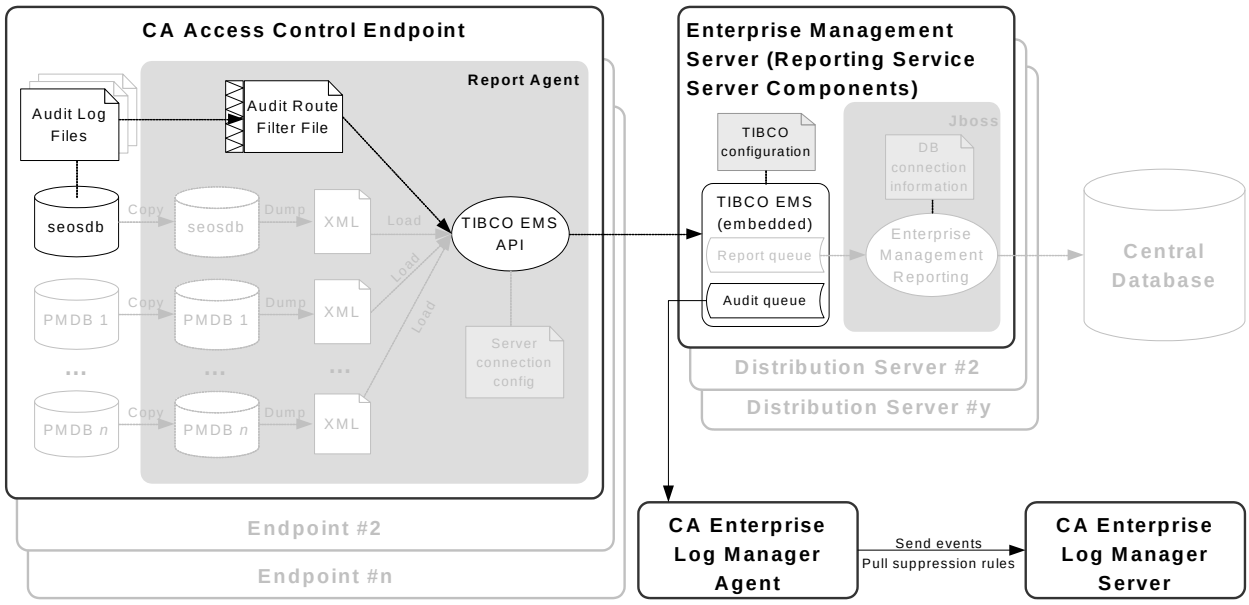
CA Enterprise Log Manager Integration Architecture

Integration with CA Enterprise Log Manager lets you send CA Access Control audit events from each of your endpoints for collection and reporting by CA Enterprise Log Manager.

You can configure CA Access Control to send audit events from the audit file on the local endpoint to a remote audit queue on the Distribution Server. You can then configure a CA Enterprise Log Manager connector to connect with the audit queue and pull events (messages) from it. CA Enterprise Log Manager processes these events and sends them to the CA Enterprise Log Manager server.

The CA Access Control installation supports CA Enterprise Log Manager integration.

The following diagram shows the architecture of CA Enterprise Log Manager integration components:



The preceding diagram illustrates the following:

- Each endpoint, containing a CA Access Control database (seosdb), has the Report Agent component installed.
- The Report Agent collects audit data from the endpoint and sends them to the Distribution Server.
- The Distribution Server accumulates the audit data in an audit queue.
- A CA Enterprise Log Manager agent collects events from the audit queue and sends it to the CA Enterprise Log Manager server for processing.

Note: CA Enterprise Log Manager integration relies on reporting service components. As such, your architecture includes other reporting service components and features that are not used for CA Enterprise Log Manager integration. These components and features are dimmed in the diagram.

Note: CA Access Control Enterprise Management installs the Distribution Server on the Enterprise Management Server by default. For high availability purposes, you can install the Distribution Server on a separate computer.

More information:

Reporting Service Architecture (see page 241)

CA Enterprise Log Manager Integration Components

CA Enterprise Log Manager integration uses the following CA Access Control components. These components are part of the CA Access Control enterprise reporting service:

- A *Report Agent* is a Windows service or a UNIX daemon that runs on each CA Access Control or UNAB endpoint and sends information to queues on a configured Message Queue that resides on the Distribution Server. For CA Enterprise Log Manager integration, the Report Agent collects endpoint audit messages from the audit log files on a scheduled basis, and sends these events to the audit queue on a configured Distribution Server.
- A *Message Queue* is a component of the Distribution Server that is configured for receiving endpoint information that Report Agents send. For reporting, the Message Queue forwards endpoint database snapshots to the central database using the CA Access Control Web Service. For redundancy and failover, you can have multiple Distribution Servers collecting and forwarding the information.

Note: CA Access Control Enterprise Management installs the Distribution Server on the Enterprise Management Server by default.

CA Enterprise Log Manager integration also uses the following CA Enterprise Log Manager components:

- A *CA Enterprise Log Manager agent* is a generic service configured with connectors, each of which collects raw events from a single event source and then sends the events to a CA Enterprise Log Manager server for processing. For CA Access Control audit data, the agent deploys the CA Access Control connector.
- A *CA Access Control connector* is an out-of-the-box CA Enterprise Log Manager integration for a CA Access Control audit event source. The connector enables raw event collection from a CA Access Control Distribution Server and the rule-based transmission of converted events to an event log store, where they are inserted into the hot database.
- A *collection server* is a CA Enterprise Log Manager server that refines incoming event logs, insert them into the hot database, compresses the hot database when it reaches the configured size into a warm database, and auto-archives the warm database to the related management server on the configured schedule.

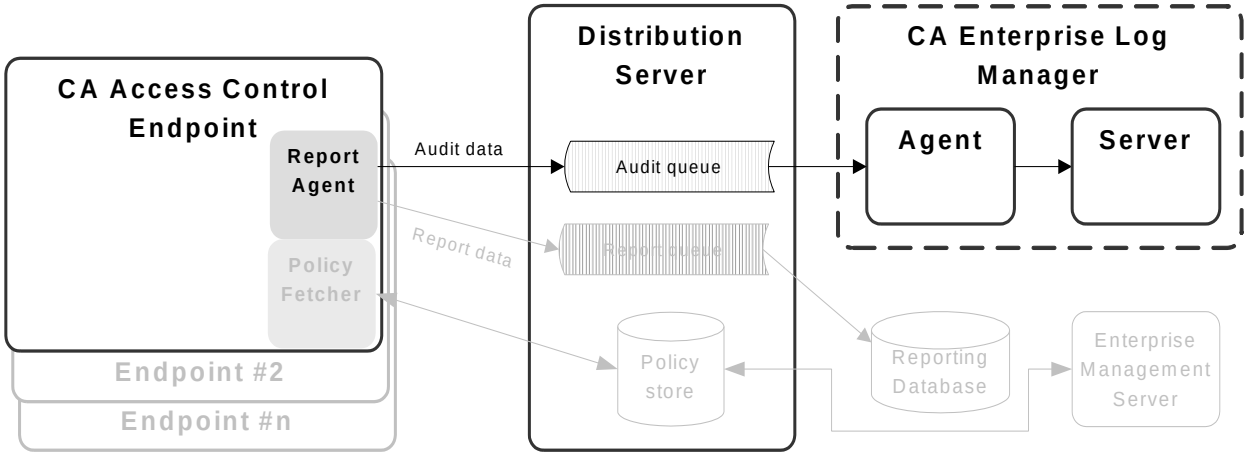
Note: For more information about CA Enterprise Log Manager components, see the CA Enterprise Log Manager documentation.

More information:

Reporting Service Architecture (see page 241)

How Audit Data Flows from CA Access Control to CA Enterprise Log Manager

To understand how CA Access Control integrates with CA Enterprise Log Manager, and what to consider when configuring this integration, first consider the flow of audit data between CA Access Control and CA Enterprise Log Manager. The following illustration describes how CA Access Control routes audit events to a messaging queue on a Distribution Server, where the CA Access Control connector of the CA Enterprise Log Manager agent pulls, maps, transforms, and then sends the events to the CA Enterprise Log Manager server:



1. The Report Agent collects audit events from the local endpoint audit files, applies any filtering policies, and places the events on a audit queue located on the Distribution Server.
2. A CA Enterprise Log Manager connector, deployed by the CA Enterprise Log Manager agent, connects with the audit queue and pulls events (messages) from it.
3. The CA Enterprise Log Manager connector and agent maps the events to the Common Event Grammar (CEG) using data mapping and parsing files, and then applies suppression and summarization rules before routing the events to the CA Enterprise Log Manager server.
4. The CA Enterprise Log Manager server receives the events and may apply additional suppression and summarization rules before the events are stored.

Note: For more information about how CA Enterprise Log Manager works, see the CA Enterprise Log Manager documentation.

How to Set Up CA Enterprise Log Manager for CA Access Control

To use CA Enterprise Log Manager to create reports that contain audit data from all your CA Access Control endpoints, first implement enterprise reporting. You must implement enterprise reporting before you integrate with CA Enterprise Log Manager because implementing enterprise reporting enabled the Report Agents on your endpoints. Once you have enterprise reporting implemented, set up CA Enterprise Log Manager for CA Access Control.

To set up CA Enterprise Log Manager for CA Access Control, follow these steps:

1. Install the CA Enterprise Log Manager server.

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

2. Install the CA Enterprise Log Manager agent on or near the Distribution Server.

   The agent must be accessible to the Distribution Server and communicate with it through a specified port. It must also be accessible to the CA Enterprise Log Manager server.

   Note: Verify the operating system support for the CA Enterprise Log Manager agent before you install it. For more information about installing the agent, see the *CA Enterprise Log Manager Agent Installation Guide*.

3. Install CA Access Control Enterprise Management.

   Note: For more information, see the *Implementation Guide*.

4. Create a connector for the agent.

   Once you have the CA Enterprise Log Manager agent installed and communicating with the CA Enterprise Log Manager server, create a connector and configure it so that it can access the CA Access Control event source (the audit queue on the Distribution Server).

   Note: The following topics describe settings that are required for CA Access Control event collection, including the connector details and connector configuration requirements that you must configure for the integration to succeed. For more information about how to create a connector, see the *CA Enterprise Log Manager Administration Guide* and the *Online Help*.

5. Create a connection to CA Enterprise Log Manager from CA Access Control Enterprise Management.

6. (Optional) Configure an audit collector.

7. Configure CA Access Control endpoints for audit collection.

More information:

Enterprise Reporting Capabilities (see page 241)
How to Set Up Reporting Service Server Components (see page 243)

Connector Details

Once you install the CA Enterprise Log Manager agent on a computer, that computer appears in the CA Enterprise Log Manager server management interface (for example, to view a computer in the Default Agent Group click Administration, Log Collection, Agent Explorer, Default Agent Group, *computer_name*). You must now create a connector. This topic describes the settings that you *must* configure on the Connector Details page of the Connector Creation wizard.

Integration

Specifies the integration you want to use as a template.

Select the appropriate CA Access Control integration.

Example: AccessControl_R12SP5_TIBCO

You can optionally change the name of the connector and add a description. You can then apply suppression rules to events handled by the connector.

Note: For information about other optional settings that let you customize your event collection, see the *CA Enterprise Log Manager Administration Guide* and the *Online Help.*

Suppression and Summarization Rules

Once you create the connector and specify the connector details, you can optionally apply suppression rules on the Apply Suppression Rules page of the Connector Creation wizard.

The name of the Ideal Model for the suppression and summarization rules for CA Access Control is Host IDS/IPS. When you create rules, select the values for Event Category, Event Class, and Event Action as needed to identify events.

Note: For information about other optional settings that let you customize your event collection, see the *CA Enterprise Log Manager Administration Guide* and the *Online Help.* For more information on field identification or individual values, see the Common Event Grammar Reference in the *CA Enterprise Log Manager Online Help*.

Connector Configuration Requirements

Once you create the connector and specify the connector details, you can configure the connector. This topic describes the settings that you *must* configure on the Connector Configuration page of the Connector Creation wizard to begin event collection.

Note: For information about other optional settings that let you customize your event collection, see the *CA Enterprise Log Manager Administration Guide* and the *Online Help.*

TIBCO Server

Specifies the host name or IP address of the Message Queue (TIBCO server) in the following format:

Protocol://server IP or name:Port number

The Message Queue is installed on CA Access Control Enterprise Management.

- Define the following value:

  ssl://ACentmserver:7243

The port values and communication method are the default ports that CA Access Control Enterprise Management uses. If you configured different values after installing CA Access Control Enterprise Management, use that port and communication method values.

TIBCO User

Specifies the user name for Message Queue authentication. CA Access Control defines a default user named "reportserver".

TIBCO Password

Specifies the password for Message Queue authentication. Enter the password that you defined in the "Communication Password" dialog when you installed CA Access Control Enterprise Management.

Event Log Name

Specifies the log name for the event source.

Accept the default, "CA Access Control".

PollInterval

Specifies the number of seconds the agent waits before polling for events when the Message Queue has become unavailable or disconnected.

SourceName

Specifies the identifier for the Message Queue queue.

Accept the default, "queue_audit".

TIBCO Queue

Specifies the name of the Message Queue queue from which the log sensor is to read messages (events).

Accept the default, "queue/audit".

Number of Collection threads

Specifies the number of threads the log sensor spawns to read Message Queue messages.

You should consider the number of events in the Message Queue queue and the CPU of the CA Enterprise Log Manager agent system when you adjust this value.

Limits: The minimum value is 1. The maximum number of threads that the log sensor can spawn is 20.

How Configuration Settings Affect the Report Agent

For CA Enterprise Log Manager integration, the Report Agent collects endpoint audit messages from the audit log files on a scheduled basis, and routes these events to the audit queue on a configured Distribution Server. You can affect performance by tuning the Report Agent settings.

Note: The Report Agent is part of the CA Access Control enterprise reporting service and is also responsible for sending database snapshots for endpoint reporting purposes. This process describes only those actions that the Report Agent takes for audit event routing to CA Enterprise Log Manager.

The Report Agent does the following when you enabled audit collection (set the audit_enabled configuration settings to 1):

- Collects new audit records by reading records from the endpoint audit files and committing them to memory.

  The Report Agent reads the number of audit records that you defined in the audit_read_chunk configuration setting and then waits for the duration that you defined in the audit_sleep configuration setting before reading the audit files again. The Report Agent reads previously unread records in the active audit log *and* all the backup audit files. It then commits to memory those records that pass the audit filter as defined in the audit filter file (audit_filter configuration setting).

- Sends a group of audit records it has in memory to the Distribution Server Message Queue that you defined in the audit_queue configuration setting.

  The Report Agent sends audit records when *one* of the following applies:

  – The number of records in memory reaches the number defined by the audit_send_chunk configuration setting.

  – The amount of time that has passed because the last audit records were sent equals the interval defined by the audit_timeout configuration setting.

Example: Default Report Agent Settings for Audit Collection and Routing

This example illustrates how we set the default Report Agent configuration settings, what environment these are set for, and how they affect performance.

We expect an average environment to have 30 events per second (EPS). Therefore, the Report Agent reads 30 events for every second that passes. To reduce the impact on other running applications (CPU use and context switches) we chose to have the Report Agent read 300 events every 10 seconds, as follows:

```
audit_sleep=10
audit_read_chunk=300
```

The message bus CA Access Control uses to transport messages between the Report Agent and the Distribution Server handles large packets that are sent at long intervals better than it handles small packets at short intervals. The following configuration setting specifies that when the number of audit records the Report Agent collects reaches the defined number, the Report Agent sends the records to the Distribution Server. Assuming 30 events per second, if we want the Report Agent to send audit records at approximately one-minute intervals (60 seconds), we et the Report Agent as follows:

```
audit_send_chunk=1800
```

However, at night, or at other times when there are less than 30 events per second, there are less than 1800 events per minute. To verify that the Report Agent still regularly sends audit records to the Distribution Server, we set a maximum interval of 5 minutes between sending audit records, as follows:

```
audit_timeout=300
```

Filter Events from CA Enterprise Log Manager

You can use a filter file to prevent CA Access Control from sending every audit record in the log file to CA Enterprise Log Manager. The filter file specifies the audit records that are not sent to CA Enterprise Log Manager.

Note: This filter file prevents CA Access Control from sending the specified audit events to the Distribution Server, but does not stop CA Access Control from writing the audit events to the local files. To filter out audit events from the local audit file, modifyfilter rules in the file defined be the AuditFiltersFile configuration setting in the logmgr section (by default, audit.cgf).

To filter events from CA Enterprise Log Manager, edit the audit filter file on the endpoint. If you want to apply the same filtering rules to more than one endpoint, we recommend that you create an audit filtering policy and assign the policy to the endpoints where you want it to be effective.

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

Example: Audit Filter Policy

This example shows you what an audit filtering policy looks like:

```
env config
er config auditrouteflt.cfg line+("FILE;*;*;R;P")
```

This policy writes the following line to the auditrouteflt.cfg file:

```
FILE;*;*;R;P
```

This line filters audit records that record a permitted attempt by any accessor to access any file resource for reading. CA Access Control will not send these audit records to the Distribution Server.

Secure Communications using SSL

When you install CA Access Control Enterprise Management you can select to either secure the communication between the Distribution Server and Report Agent by using SSL or select not to secure the communication. Whichever option you select, specify the same option when you install the Report Agent on the endpoint.

For example, if you use SSL to encrypt the communications between the Report Agent and the Distribution Server (the default), then you must provide authentication information when you install CA Access Control Enterprise Management, such as the password required for the Report Agents to communicate with the Distribution Server.

This is the password you provide when you configure the CA Access Control Report Agent on the endpoint and in the CA Enterprise Log Manager agent Connector Configuration page.

You must provide the same information when you install the Report Agent. Only Report Agents that can provide the correct certificate and password information can write events to the audit queue on the Distribution Server and thus be retrieved by CA Enterprise Log Manager.

Audit Log Files Backup for CA Enterprise Log Manager Integration

To collect audit data, the Report Agent reads the CA Access Control audit log files according to its configuration settings. The Report Agent reads a configured number of audit records from the audit log files at configured intervals. In a default legacy installation, or when you do not enable audit log routing during installation, CA Access Control keeps a single size-triggered audit log backup file. Every time the audit log reaches the configured maximum size, it creates a backup file, overwriting the existing audit log backup file. As a result, it is possible that the backup file will be overwritten before the Report Agent read all of its records.

We strongly recommend that you set CA Access Control to keep time-stamped backups of your audit log file. This way, CA Access Control does not overwrite the backup audit log files until it reaches a configured maximum of audit log files it should keep. This is the default setting when you enable the audit log routing sub-feature during installation on the endpoint.

Example: Audit Log Backup Settings

This example illustrates how the recommended configuration settings affect CA Enterprise Log Manager integration. When you enable the audit log routing sub-feature during installation on an endpoint, CA Access Control sets the following logmgr section configuration settings:

```
BackUp_Date=yes
audit_max_files=50
```

In this case, CA Access Control timestamps each backup copy of the audit log file and keeps a maximum of 50 backup files. This provides plenty of opportunity for the Report Agent to read all of the audit records from the files and for you to copy the backup files for safe keeping if required.

Important! If you set audit_max_files to 0, CA Access Control does not delete backup files and will keep accumulating the files. If you want to manage the backup files through an external procedure, remember that CA Access Control protects these files by default.

Configure an Existing Windows Endpoint for CA Enterprise Log Manager Integration

Once you have CA Access Control Enterprise Management installed and configured, you can configure your endpoints for sending audit data to the Distribution Server by enabling and configuring the Report Agent.

Note: When you install CA Access Control, it lets you configure the endpoint for collecting and sending audit data. This procedure illustrates how you configure an existing endpoint for sending audit data if you did not configure this option at install time.

To configure an existing Windows endpoint for CA Enterprise Log Manager integration

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 Access Control.

3. Click Change.

   The CA Access Control installation wizard appears.

   Follow the wizard prompts to modify the CA Access Control installation so that you enable the Report Agent feature and the Audit Routing sub-feature.

   Verify that you also specify to keep time-stamped backups of the audit log file.

Note: After you enable the Report Agent and audit routing, you can modify CA Access Control configuration settings to change performance-related settings. Before you do this, you should understand how the Report Agent collects audit events and routes them to the Distribution Server (see page 228). For more information about Report Agent configuration settings, see the *Reference Guide*.

Configure an Existing UNIX Endpoint for CA Enterprise Log Manager Integration

Once you have CA Access Control Enterprise Management installed and configured, you can configure your endpoints for sending audit data to the Distribution Server by enabling and configuring the Report Agent.

Note: When you install CA Access Control, it lets you configure the endpoint for collecting and sending audit data. This procedure illustrates how you configure an existing endpoint for sending audit data if you did not configure this option at install time.

To configure an existing UNIX endpoint for CA Enterprise Log Manager integration

1. Run *ACSharedDir*/lbin/report_agent.sh:

   report_agent config -server *hostname* [-proto {ssl|tcp}] [-port *port_number* [-rqueue *queue_name*] -audit -bak

   If you omit any configuration options, the default setting is used.

   Note: For more information about 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 and audit routing, you can modify CA Access Control configuration settings to change performance-related settings. Before you do this, you should understand how the Report Agent collects audit events and routes them to the Distribution Server (see page 228). For more information about Report Agent configuration settings, see the *Reference Guide*.

Example: Configure a UNIX Endpoint for CA Enterprise Log Manager Integration 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)
```

Queries and Reports for CA Access Control Events

The queries, reports, and action alerts for CA Access Control are grouped under the Server Resource Protection tags in the CA Enterprise Log Manager interface.

Note: For information, visit the CA Enterprise Log Manager Product page at http://ca.com/support and click the CA Enterprise Log Manager - Reports - Complete List link.

How to Enable CA Enterprise Log Manager Reports in CA Access Control

Before you can view CA Enterprise Log Manager reports in CA Access Control Enterprise Management, you must enable CA Enterprise Log Manager reporting in CA Access Control Enterprise Management, export and add the CA Enterprise Log Manager certificate and configure the connection to CA Enterprise Log Manager from CA Access Control Enterprise Management.

1. Enable CA Enterprise Log Manager reporting by configuring advanced settings (see page 79).
2. Export and add the CA Enterprise Log Manager trusted certificate to the keystore (see page 235).
3. Configure the connection to CA Enterprise Log Manager (see page 236).
4. (Optional) Configure an audit collector (see page 238).

   Configure an audit collector if you want to send PUPM audit events to CA Enterprise Log Manager.

Add the CA Enterprise Log Manager Trusted Certificate to the Keystore

CA Enterprise Log Manager reports are authenticated using trusted certificates. The certificate verifies that the information displayed in the reports originated from a trusted CA Enterprise Log Manager source, which verifies the authenticity of the data.

To view CA Enterprise Log Manager reports in CA Access Control Enterprise Management, you first export the certificate and add than it to the keystore.

To add the CA Enterprise Log Manager trusted certificate to the keystore

1. Enter the URL of the CA Enterprise Log Manager server in a web browser in the format: https://*host*:*port*

   A security alert dialog appears.

2. Click View Certificate.

   The Certificate dialog appears.

3. Click Details, Copy to File.

   The Certificate Export Wizard appears.

4. Complete the wizard using the following instructions:

   - **Export File Format**—Select Base-64 encoded X.509 (.CER).
   - **File to Export**—Define the full pathname of the exported certificate file.

     For example, C:\certificates\computer.base64.cer

   A message appears indicating that the export completed successfully.

5. Import the certificate to the keystore. For example:

   ```
   C:\jdk1.5.0\jre\lib\security>c:\jdk1.5.0\bin\keytool.exe -import -file computer.base64.cer -keystore
   C:\jboss-4.2.3.GA\server\default\deploy\IdentityMinder.ear\custom\ppm\truststore\ssl.keystore
   ```

6. Enter the keystore password. The default password is 'secret'.
7. Click Yes to trust the certificate.

   The certificate is added to the keystore.

Configure the Connection to CA Enterprise Log Manager

CA Access Control Enterprise Management communicates with CA Enterprise Log Manager to display reports with CA Access Control related information. To display these reports you need to configure the connection to CA Enterprise Log Manager.

To configure the connection to CA Enterprise Log Manager

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

   The Manage CA Enterprise Log Manager Connection task appears in the list of available tasks.
2. Click Manage CA Enterprise Log Manager Connection .

   The Manage CA Enterprise Log Manager Connection: *PrimaryCALMServer* task page appears.
3. Complete the fields in the dialog. The following fields are not self-explanatory:

   Connection name

   Identifies the name of the CA Enterprise Log Manager connection.

   Description

   (Optional) Defines a description for this connection.

   Host Name

   Defines the name of the CA Enterprise Log Manager host you want CA Access Control Enterprise Management to work against.

   Example: host1.comp.com

   Port #

   Defines the port that the CA Enterprise Log Manager host uses for communication.

   Default: 5250

Certificate Authority Signed SSL certificate

Specifies whether the connection to CA Enterprise Log Manager uses an SSL certificate signed by a certificate authority.

Certificate name

Defines the name of the certificate.

Password

Defines the certificate password.

4. Click Submit.

   CA Access Control Enterprise Management saves the CA Enterprise Log Manager connection settings.

Example: Obtain the CA Enterprise Log Manager Certificate Information

The following example shows you how to obtain the CA Enterprise Log Manager certificate information that you need to provide when creating and managing the CA Enterprise Log Manager connection settings in CA Access Control Enterprise Management.

1. Enter the CA Enterprise Log Manager URL in a web browser using the following format:

   https://*host*:*port*/spin/calmapi/products.csp

   Example: https://localhost:5250/spin/calmapi/products.csp

2. Enter a valid user name and password to log in to CA Enterprise Log Manager.

3. Select the Register option to register a certificate with CA Enterprise Log Manager.

   The New Product Registration screen appears.

4. Enter the certificate name and password and select Register.

   A message appears informing you that the certificate registered successfully.

Configure an Audit Collector

CA Access Control Enterprise Management collects audit events, including PUPM audit events, and stores them in the central database. You can configure CA Access Control Enterprise Management to send the audit events to CA Enterprise Log Manager.

To configure an audit collector

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

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

   The Create Audit Collector: Audit Collector Search Screen appears.
3. (Optional) Create a copy of an existing audit collector, as follows:
   a. Select Create a copy of an object of type ELM Sender.
   b. Select an attribute for the search, type in the filter value, and click Search.

      A list of ELM Senders that match the filter criteria appear.
   c. Select the object you want to use as a basis for the new audit collector.
4. Click OK.

   The Create Audit Collector task page appears. If you created the audit collector from an existing object, the dialog fields are pre-populated with the values from the existing object.
5. Complete the fields in the dialog. The following fields are not self-explanatory:

   Job Enable

   Specifies whether the audit collector is enabled.

   Name

   Defines the name of the audit collector.

   Queue Jndi

   Defines the name of the Message Queue that CA Access Control Enterprise Management sends audit event messages to.

   Example: *queue/audit*

Sleep

Defines the interval, in minutes, between database queries.

Default: 1

Time Out

Defines the collector time out period, in minutes, for sending the audit event messages to the messages queue.

Default: 10

Note: Once the timeout period has passed, the collector sends the messages although the number of messages in the queue did not reach the level defined in the Msg Block Size field.

Msg Block Size

Defines the maximum number of messages to accumulate in the database before sending the messages to the queue.

Default. 100

6. Click Submit.

   CA Access Control Enterprise Management creates the audit collector.

Chapter 8: Implementing Enterprise Reporting

This section contains the following topics:

Enterprise Reporting Capabilities

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

CA Access Control enterprise reporting, once set up, works independently to collect data from each endpoint and report it continually to a central server 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.

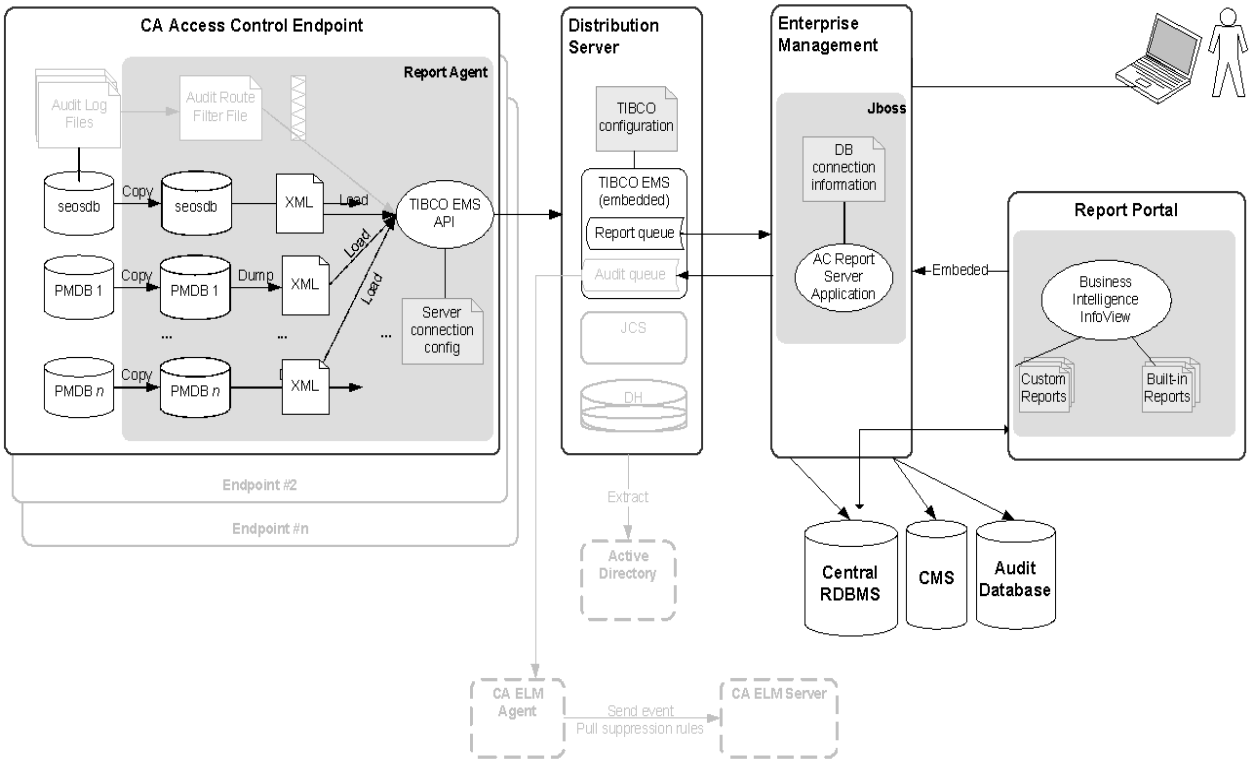
Reporting Service Architecture

The CA Access Control reporting service provides a server-based platform for CA Access Control enterprise reporting. You can use this platform to create reports that contain data from all your CA Access Control 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 Access Control 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 Access Control 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 Access Control 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 Access Control 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 CA Access Control Enterprise Management.
2. Set up the Report Portal computer (CA Business Intelligence).

   Important! If you use Oracle Database 11g, install the BusinessObjects XI Release 2.1 SP5 patch that is available on the CA Access Control Premium Edition Report Portal (Disc 2) DVD under the \boeXIR2_SP5 directory.
3. Deploy the CA Access Control 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 Access Control 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 118)
Configure a UNIX Endpoint for Reporting (see page 177)
Configure UNAB for Reporting (see page 302)

How to Set Up the Report Portal Computer

The Report Portal lets you access the endpoint data that CA Access Control 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.

Important! If you use Oracle Database 11g, install the BusinessObjects XI Release 2.1 SP5 patch that is available on the CA Access Control Premium Edition Report Portal (Disc 2) DVD under the \boeXIR2_SP5 directory.

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 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.
3. (Solaris) If the Report Portal computer is a Solaris computer, prepare the Solaris computer for CA Business Intelligence installation (see page 246).
4. 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 Access Control Enterprise Management generates will remain in a pending or recurring status.
5. Install CA Business Intelligence for your operating system.

   You can find the CA Business Intelligence installation files on the CA Access Control Premium Edition Report Portal optical discs.

   Note: For detailed installation information, see the *CA Business Intelligence Installation Guide*, which is available from the CA Access Control Premium Edition bookshelf.

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

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 Access Control Premium Edition Report Portal 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
Destination Location	Click Next to accept the default.
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 Access Control Premium Edition 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) contains the report data that is used to generate and display the reports.
Enable Auditing	Click Next to accept the defaults.

Information	Action
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.

Note: The CA Business Intelligence Central Management Server (CMS) contains the report data that is used to generate and display the reports. The central database 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*.

More information:

Prepare the Central Database for Enterprise Management (see page 54)

Prepare Solaris for CA Business Intelligence Installation

Before you can install CA Business Intelligence on Solaris, you must prepare the computer for the installation. When you prepare the computer, you create a non-root user for the CA Business Intelligence installation and verify that the Oracle RDBMS is exposed to the installation of CA Business Intelligence.

To prepare Solaris for CA Business Intelligence installation

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. Log in as the non-root user you created.

4. 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
   ```

5. 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
   ```

6. 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

7. 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.ora
   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 Solaris.

Report Package Deployment

The report package is a .BIAR file, which deploys the CA Access Control 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 Access Control reports, you first 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. Insert the appropriate CA Access Control Premium Edition Server Components DVD for your operating system into your optical disc drive and navigate to the \ReportPackages folder.

3. Extract the contents of the biconfig.zip file into a temporary directory.

4. 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 Access Control 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 Access Control 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, and is set by default to the name of the English version for your RDBMS.

5. 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 Access Control reports file (.biar). The reports file is the file that you copied in the previous step.

   <networklayer>

   Defines the network layer supported by your RDBMS.

   Values (Windows): OLE DB, Oracle OCI, ODBC

   Values (UNIX): Oracle OCI

   <rdms>

   Defines the type of RDBMS used for CA Access Control reporting.

   Values (Oracle OCI): Oracle 10 or Oracle 11

   Values (ODBC): Generic ODBC datasource

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

   Note: If you use MS SQL Server 2008, specify MS SQL 2005 for this property. 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 Access Control for reporting and not the CA Business Intelligence CMS.

   <server>

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

6. Do one of the following:

   - (Windows) 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_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_mssql_2005.xml

   The batch file imports the CA Access Control reports into InfoView. The import may 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>host01</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 UNIX Endpoint for Reporting (see page 177)
Configure a Windows Endpoint for Reporting (see page 118)

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

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

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

To deploy the report package on a Report Portal that you installed with CA Access Control r12.0

1. Insert the appropriate CA Access Control Premium Edition r12.5 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 Solaris, 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 Access Control 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 Access Control Premium Edition 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. Do either of the following:

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

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

7. 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 Access Control reports file (.biar). This is the file you copied earlier.

8. Do one of the following:
   - On Windows, launch the *BO_Files*/biek-sdk/importBiarFile.bat batch file.
   - On UNIX, run the *BO_Files*/biek-sdk/importBiarFile.sh script file.

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

Configure BusinessObjects for Large Deployments

To run CA Access Control 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, Crystal Configuration Manager.

      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 11.5/Crystal Reports/Database

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

To configure the connection to CA Business Intelligence

1. Enable the CA Identity Manager Management Console (see page 80).
2. Open the CA Identity Manager Management Console (see page 80).
3. Click Environments, ac-env, Advanced Settings, Reports.

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

   Note: For more information, see the *CA Identity Manager 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 CA Access Control r12.
5. Click Save.

   The CA Business Intelligence settings are saved.

Create a Snapshot Definition

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

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

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 Access Control Enterprise Management to capture a snapshot each day, report data is collected weekly from the endpoints but daily from PUPM and the user store, and out-of-date endpoint data appears in the reports.

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

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

To create a snapshot definition

1. In CA Access Control 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 Access Control Enterprise Management enables the snapshot definition.

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

Keep Last

Specifies the number of successful snapshots stored in the central database. CA Access Control 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 Access Control 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 Access Control and UNAB endpoints.

   CA Access Control 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*.

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 266).
2. Customize the UNAB installation package (see page 267).

   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 once and use it to install UNAB in your enterprise.

3. Configure UNAB to work with CA Access Control Enterprise Management (see page 271).

   Use the CA Access Control Enterprise Management server user interface to manage the UNAB endpoints.

4. Install the UNAB package on the UNIX hosts.

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

5. (Optional) Check for system compliance (see page 299).

   The uxpreinstall utility verifies that the system is compatible with the UNAB requirements.

6. Register the UNIX host with Active Directory (see page 299).

7. Start UNAB (see page 303).

   This step starts the UNAB daemon (uxauthd).

8. Create login authorization policies in CA Access Control 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 303).

   Activating UNAB lets enterprise users log in to UNIX hosts.

10. (Optional) Implement UNAB in full integration mode (see page 304).

    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

Installation Considerations for Linux s390 Endpoints

To use Message Queue functionality on CA Access Control Linux s390 endpoints and to remotely manage UNAB Linux s390 endpoints, you must install J2SE version 5.0 or later on the endpoint. Message Queue functionality lets you send report and audit data from CA Access Control endpoints to the Report Portal and CA Enterprise Log Manager, respectively. Remote management lets you use CA Access Control Enterprise Management to manage UNAB endpoints.

You can install J2SE before or after you install CA Access Control or UNAB on the endpoint. If you install J2SE after you install CA Access Control or UNAB, you must also configure the Java location on the endpoint.

How the Installation Interacts with Java

Valid on Linux s390 and Linux s390x

To use Message Queue functionality on CA Access Control Linux s390 endpoints and to remotely manage UNAB Linux s390 endpoints, you must install a supported Java version on the endpoint.

When you install CA Access Control or UNAB on a Linux s390 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 Access Control installation parameters file, customized packages for native installations, and user input from interactive CA Access Control installations.

   b. The JAVA_HOME environment variable.

   c. 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 the Endpoint

Valid on Linux s390 and Linux s390x

To use Message Queue functionality on CA Access Control Linux s390 endpoints 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 Access Control or UNAB, you must perform additional configuration steps.

To configure the Java location on the endpoint

1. Stop CA Access Control 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 Access Control and UNAB.

   The Java location is configured.

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 nslookup command with the IP address of the UNIX computer from both the UNIX computer and the Active Directory computer.

Example: Verify that the Name of a UNIX Computer Resolves Correctly

This example shows you the result of a forward and reverse nslookup command for a computer named computer.com on both a Windows, Active Directory server and UNIX computer:

```
Server:        computer.com
Address:       123.456.789.1
123.456.789.1.in-addr.arpa    name = computername.com
```

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 Access Control 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 Enterprise Log Manager.

Note: If you set the value to yes, set CA Access Control 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

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.

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

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 Access Control Enterprise Management

You can use CA Access Control 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 Access Control Enterprise Management to manage UNAB endpoints, you register UNAB with CA Access Control 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 Access Control 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

   DISTRIBUTION_SHARED_SECRET

   Specify the shared secret that the ReportAgent uses for authentication purposes with the Distribution Server.

   Limits: any valid string.

   Default: none
4. Set the installation parameters in the customized package.
5. Install UNAB using the customized package.

   After the installation is complete, use CA Access Control Enterprise Management to manage UNAB endpoints.

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 Access Control provides for UNAB to manage your UNAB installation with all your other software installations performed using RPM.

More information:

Customize the UNAB Package (see page 272)
customize_uxauth_rpm Command—Customize UNAB RPM Package (see page 273)
Install UNAB (see page 275)
Verify That the Installation Completed Successfully (see page 276)
Upgrade UNAB (see page 276)
Uninstall UNAB (see page 277)

Customize the UNAB 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. Copy the package you want to customize from the /UNAB directory of the CA Access Control 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.

2. (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*

3. Enter the following command to display the license agreement:

   customize_uxauth_rpm -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. Enter the following command:

   customize_uxauth_rpm -w *keyword* [-d *pkg_location*] [*pkg_name*]

   This command specifies that you accept the license agreement.

6. (Optional) Enter the following command:

   customize_uxauth_rpm -s -c *certfile* -k *keyfile* [-d *pkg_location*] [*pkg_name*]

   This command changes the default encryption files.

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 267).

   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.

customize_uxauth_rpm Command—Customize 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 *command* [-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 -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.

-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 *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.

Install UNAB

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.

To install UNAB

1. Log in to the UNIX computer as a superuser.
2. Locate the UNAB installation program on the installation CD and copy the program to a temporary directory.

   For example:

   mnt/AC_DVD/UNAB/*CDPATH*/uxauth-1-0.10.i386.rpm
3. Use the rpm command to install the UNAB package.

   The installation process begins.

   A message informs you that the installation process completed successfully.
4. Review the installation log file, uxauth-rpm.log, for information about the installation process.

   You can find the log file in the UNAB installation directory.

   By default the UNAB is installed in the following location:

   /opt/CA/uxauth/

Example: Install UNAB on Red Hat Linux

The following example shows you how to install the UNAB package on a Red Hat Linux x86 ES 4.0 computer.

In the example, the installation package is found on the installation media (is mounted to /mnt/UNIX/auth_DVD).

```
cd /mnt/UNIX/auth_DVD/CDPATH
rpm -i unab.rpm
```

Verify That the Installation Completed Successfully

After you finish installing the UNAB, you should verify that the installation completed successfully.

To verify that the installation completed successfully enter the following command:

```
rpm -q uxauth
```

unab

Defines the name of the UNAB native package.

If you successfully installed UNAB, a message informs you that the package is installed.

Upgrade UNAB

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.

To upgrade UNAB

1. Log in to the UNIX computer as a superuser.
2. Locate the UNAB installation program on the installation CD.

   For example:

   mnt/AC_DVD/UNAB/*CDPATH*/unab.rpm
3. Use the rpm command to upgrade UNAB.

   A message informs you that the process completed successfully.

Example: Upgrade UNAB on Red Hat Linux

The following example shows you how to upgrade the currently installed version of UNAB on a Red Hat Linux x86 ES 4.0 computer.

In the example, the installation package is found on the installation media (mounted to /mnt/UNIX/auth_DVD).

```
cd /mnt/UNIX/auth_DVD/CDPATH

rpm -u unab.rpm -verbose
```

Uninstall UNAB

To uninstall UNAB you need to remove the package from the UNIX computer where you installed it.

To uninstall UNAB, enter the following command as a superuser:

rpm -e *unab*

unab

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.

More information:

Customize the UNAB Solaris Native Packages (see page 278)
customize_uxauth_pkg Command—Customize Solaris Native Package (see page 279)
Install UNAB Solaris Native Packages (see page 282)
Install UNAB Solaris Native Packages on Selected Zones (see page 283)
Upgrade UNAB on Solaris (see page 284)
Uninstall UNAB Solaris Native Package (see page 285)

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 Access Control 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. (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.

4. Enter the following command:

   customize_uxauth_pkg -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_pkg -w *keyword* [-d *pkg_location*] [*pkg_name*]

   This command specifies that you accept the license agreement.

7. (Optional) Enter the following command:

   customize_uxauth_pkg -i *install_loc* [-d *pkg_location*] [*pkg_name*]

   This command changes the installation directory.

8. (Optional) Enter the following command to change the default encryption files:

   customize_uxauth_pkg -s -c *certfile* -k *keyfile* [-d *pkg_location*] [*pkg_name*]

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 267)

    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 -l *install_loc* [-d *pkg_location*] [*pkg_name*]
customize_uxauth_pkg -s {-f *tmp_params* | -c *certfile* | -k *keyfile*} [-d *pkg_location*] [*pkg_name*]
customize_uxauth_pkg -g [-f *tmp_params*] [-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.

-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.

-k *keyfile*

Defines the full pathname of the root private key file.

-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.

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 Access Control 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 packages in the reverse order of their installation.

To uninstall CA Access Control packages uninstall the main UNAB package, enter the following command:

pkgrm *UNAB*

unab

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.

More information:

Customize the UNAB SD-UX Format Packages (see page 286)
customize_uxauth_depot Command—Customize an SD-UX Format Package (see page 288)
Install UNAB HP-UX Native Packages (see page 289)
Uninstall HP-UX Packages (see page 290)

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 Access Control 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:

   customize_uxauth_depot -a [-d *pkg_location*] *pkg_name*

   This command displays the license agreement.

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. Enter the following command:

   customize_uxauth_depot -w *keyword* [-d *pkg_location*] [*pkg_name*]

   This command specifies that you accept the license agreement

6. (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

7. (Optional) Enter the following command:

   customize_uxauth_depot -i *install_loc* [-d *pkg_location*] [*pkg_name*]

   This command changes the installation directory.

8. (Optional) Enter the following command:

   customize_uxauth_depot -s -c *certfile* -k *keyfile* [-d *pkg_location*] [*pkg_name*]

   This command changes the default encryption files.

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 267).

    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 155)

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 -l *install_loc* [-d *pkg_location*] [*pkg_name*]
customize_uxauth_depot -s {-f *tmp_params* | -c *certfile* | -k *keyfile*} [-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.

-c *certfile*

Defines the full pathname of the root certificate file.

Note: This option is applicable to the uxauth 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.

-k *keyfile*

Defines the full pathname of the root private key file.

Note: This option is applicable to the uxauth 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.

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 286).

   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 131)
Customize the SD-UX Format Packages (see page 152)

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 Access Control packages uninstall the main UNAB package:

swremove *UNAB*

unab

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.

Important! 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.

More information:

Pluggable Authentication Module (PAM) on AIX (see page 291)
Customize the bff Native Package Files (see page 294)
customize_uxauth_bff Command—Customize a bff Native Package File (see page 295)
Install UNAB AIX Native Package (see page 297)
Uninstall AIX Packages (see page 298)

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.cgf 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 Access Control 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:

   customize_uxauth_bff -a [-d *pkg_location*] *pkg_name*

   This command displays the license agreement.

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. Enter the following command:

   customize_uxauth_bff -w *keyword* [-d *pkg_location*] *pkg_name*

   This command specifies that you accept the license agreement

6. (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:

7. (Optional) Enter the following command:

   customize_uxauth_bff -i *install_loc* [-d *pkg_location*] *pkg_name*

   This command changes the installation directory.

8. (Optional) Enter the following command:

   customize_uxauth_bff -s -c *certfile* -k *keyfile* [-d *pkg_location*] *pkg_name*

   This command changes the default encryption files.

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 267).

    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

The customize_uxauth_bff command runs the UNAB native package customization script for bff native package files.

The script works on any of the available UNAB 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* | -c *certfile* | -k *keyfile*} [-d *pkg_location*] *pkg_name*
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.

-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.

-k *keyfile*

Defines the full pathname of the root private key file.

Note: This option is applicable to the uxauth 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.

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 Access Control Enterprise Management, you must register the UNAB endpoint with CA Access Control 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 294).

   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 131)

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*

unab

Defines the name of the UNAB native package.

Post-Installation Tasks

The following topics describe the post-installation tasks that you need to perform to configure the UNAB endpoint and activate UNAB.

Check for System Compliance

After installing UNAB you can run the uxpreinstall utility to verify that the computer complies with the requirements.

Important! The uxpreinstall utility can inform you of real or potential problems but does not correct them. You cannot use the utility to configure the operating system or UNAB.

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

To check for system compliance, log in to the UNIX computer as a superuser and run the uxpreinstall utility.

The uxpreinstall utility runs and when completed, displays the results of the process.

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
```

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), 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 –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.

UNAB Host Name Limitations

Active Directory imposes NetBIOS-based restrictions on the number of characters in the name of computer objects. As a result, the host name of the UNIX computer (excluding the domain name suffix) must be 15 characters or less. If the host name of the UNIX computer contains more than 15 characters, the registration does not succeed. For example, you cannot register a UNIX computer named engineering-dept-sol2 in Active Directory because the host name contains more than 15 characters. You can register a UNIX computer named eng-dept-sol2.example.com. To display the host name of the UNIX computer, run the hostname command.

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*.

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 Access Control 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, UNAB must be running.

To start UNAB you run the uxauthd daemon.

To start UNAB

1. Log in to the UNIX computer as a superuser.
2. Locate the UNAB directory.
3. Enter the following command:

   ./uxauthd -start

   Note: To start UNAB on Linux 390, use the uxauthd.sh -start command. The uxauthd.sh file is located by default in the bin directory of the UNAB directory.

   The UNAB daemon starts.

   A message informs you that the daemon is running.

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.

Example: Activate UNAB

The following example shows you how you can log in to a UNIX computer using an Active Directory account after you installed and registered UNAB.

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, do the following:

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 Access Control 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 Access Control UNIX Attributes Plug-in

The CA Access Control 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.

You must 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).

To install the CA Access Control UNIX Attributes plug-in

1. Verify that the Microsoft C++ 2005 SP1 Redistributable Package ATL Security Update is installed on the server.

   You can download this update from the Microsoft website.

2. Insert the CA Access Control Endpoint Components for UNIX DVD into an optical disc drive on the server.

3. Browse to the following directory:

   ADTools\UnixADTabExt

4. Open the appropriate directory for your operating system.

5. Copy the file ACUnixAttributesShellExt.dll to the %WINDIR%\system32 directory.

6. Open a command prompt window.

7. Use the regsvr32 utility to install the DLL, as follows:

   regsvr32 %WINDIR%\system32\ACUnixAttributesShellExt.dll

   A message appears confirming that the DLL successfully registered. CA Access Control UNIX Attributes now appears as a new tab for every user account that is defined in Active Directory.

8. (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 Access Control 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. 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

Entry	Default Value	Field Name in Plug-in
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 Access Control UNIX Attributes Plug-in

The CA Access Control UNIX Attributes plug-in lets you manage UNIX attributes for users and groups on Active Directory.

To uninstall the CA Access Control UNIX Attributes plug-in

1. Use the regsvr32 utility to uninstall ACUnixAttributesShellExt.dll.
2. Delete the following registry key:

   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\uxauth
3. Delete the ACUnixAttributesShellExt.dll file from the computer.

   The CA Access Control UNIX Attributes plug-in is uninstalled.

Example: Uninstall ACUnixAttributesShellExt.dll

The following example uninstalls the CA Access Control 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 308)
Migrate UNIX Users and Groups to Active Directory (see page 309)

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 exists in Active Directory and the group UNIX attributes are identical to the attributes of the UNIX host, the group is migrated.
   - If the groups exists 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.

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 Access Control 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.

To configure 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 Access Control UNIX Attributes tab.

   The CA Access Control 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

   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.

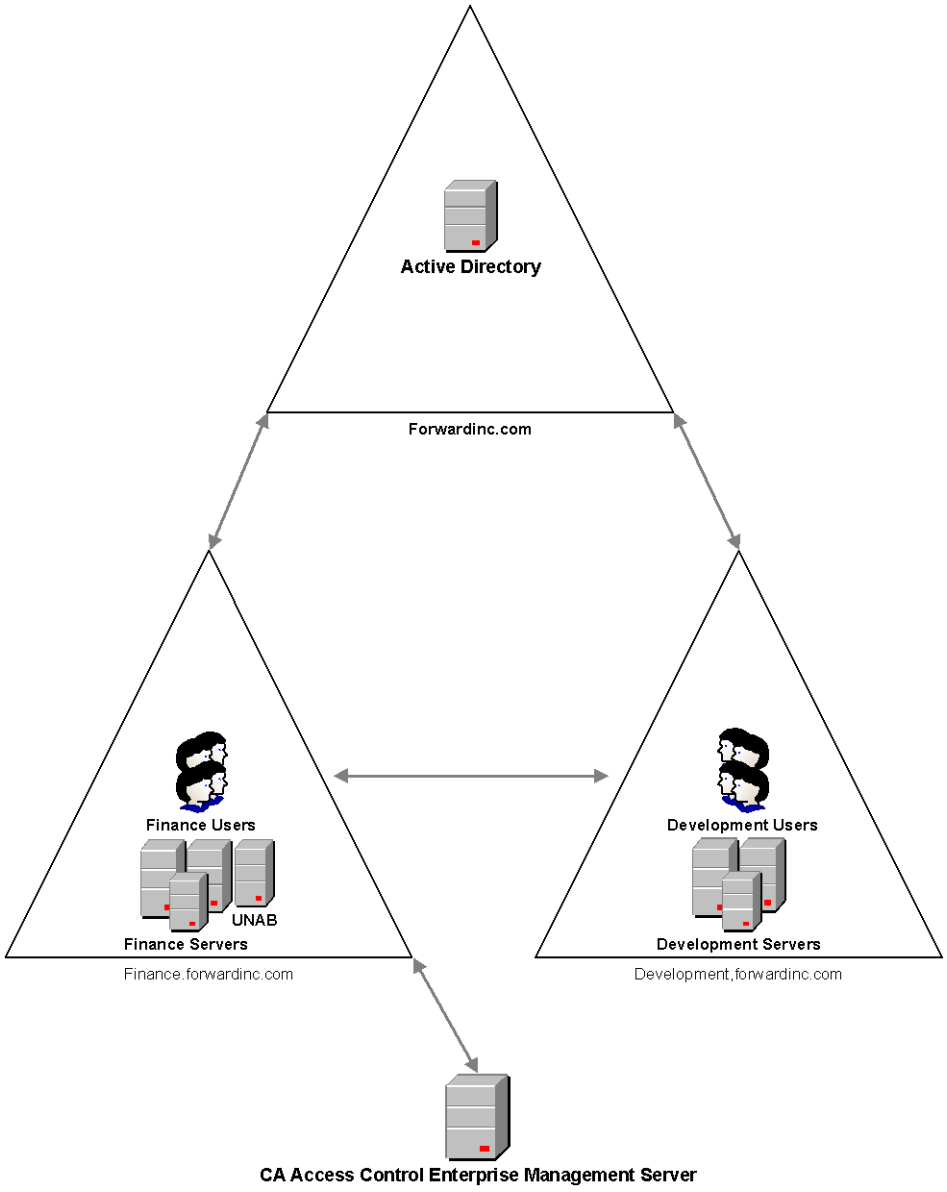
   The user UNIX attributes are configured.

Implementing UNAB in a Trusted Domains Environment

When you configure UNAB during the installation process you specify the parameters of the domain UNAB is a member of. After you install UNAB, register it with Active Directory, and activate UNAB, you can migrate UNIX users from that domain.

If the domain that you specified has a trust relationship with other domains, users from those domains can potentially have access to computers in the domain that UNAB is installed.

This diagram displays a UNAB implementation in a trusted domains environment:



In the 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 potentially access the other domain although the users are not members of that domain.

Consider of the following before you install UNAB in a trusted domains environment:

- The UNAB login policy controls access to computers 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.

Chapter 10: Installing Endpoint Management

This section contains the following topics:

How to Prepare the Endpoint Management Server

Before you install CA Access Control Endpoint Management, you need to prepare the server.

Important! If you intend to install CA Access Control Enterprise Management on the same computer, you do not need to follow these steps. The installation program installs CA Access Control Endpoint Management as part of CA Access Control 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 Access Control Premium Edition 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 Access Control Premium Edition Third Party Components DVDs. For information about supported versions, see the *Release Notes*.

3. Install CA Access Control.

   Note: Follow the instructions for installing a CA Access Control endpoint.

4. (Windows only) Restart the computer.

5. Stop CA Access Control services (secons -s).

   The server is now ready for CA Access Control Endpoint Management to be installed.

Install CA Access Control Endpoint Management on Windows

Valid on Windows

The graphical installation uses a wizard to support and guide you when installing CA Access Control Endpoint Management on a Windows computer.

To install CA Access Control Endpoint Management on Windows

1. Make sure that you prepare the server correctly (see page 315).
2. Insert the CA Access Control Premium Edition Server Components for Windows DVD into your optical disc drive.
3. Open the CA Access Control Product Explorer (ProductExplorerx86.EXE).

   The CA Access Control Product Explorer appears.
4. Expand the Components folder, select CA Access Control 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 Access Control 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 Access Control Endpoint Management on Solaris

You must use console installation to install CA Access Control Endpoint Management on a Solaris computer.

To install CA Access Control Endpoint Management on Solaris

1. Make sure that you prepare the server correctly (see page 315).
2. Insert the CA Access Control Premium Edition Server Components for Solaris 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 Access Control 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 Access Control Endpoint Management on Windows

Be sure you are 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).

To uninstall CA Access Control 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 Access Control Endpoint Management.
4. Click Change/Remove.

   The Uninstall CA Access Control Endpoint Management wizard appears.
5. Follow the wizard's instructions to uninstall CA Access Control Endpoint Management.

   The uninstall completes and removes CA Access Control Endpoint Management from your computer.
6. Click Done to close the wizard.

Uninstall CA Access Control Endpoint Management on Solaris

If you want to remove CA Access Control Endpoint Management from your computer you need to use the uninstall program that CA Access Control Endpoint Management provides.

To uninstall CA Access Control Endpoint Management on Solaris

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 Access Control Endpoint Management. By default this path is:

   /opt/CA/AccessControlServer/EndpointManagement/

   InstallAnywhere loads the uninstall console.
3. Follow the prompts to uninstall CA Access Control Endpoint Management.

   The uninstall completes and removes CA Access Control Endpoint Management from your computer.

Start CA Access Control Endpoint Management

Once you install CA Access Control Endpoint Management you need to start CA Access Control and the web application server.

To start CA Access Control Endpoint Management

1. Start CA Access Control services.

   CA Access Control Endpoint Management requires that CA Access Control be running.

2. (Windows only) Do the following:

   a. Start the following additional services, which do not load when you issue the seosd -start command:

      - CA Access Control Web Service
      - CA Access Control Message Queue (if present)

   b. 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 Access Control Endpoint Management web-based interface.

3. (UNIX only) Enter */JBoss_HOME*/bin/run.sh -b 0.0.0.0

   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 Access Control Endpoint Management web-based interface.

Open CA Access Control Endpoint Management

Once you install and start CA Access Control Endpoint Management you can open the web-based interface from a remote computer using the URL for CA Access Control Endpoint Management.

To open CA Access Control 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 Access Control 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 Access Control 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 Access Control Endpoint Management is installed (using the TERMINAL resource).

   Click Log In.

   CA Access Control Endpoint Management opens on the Dashboard tab.

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

Example: Open CA Access Control Endpoint Management

Enter the following URL into your web browser to open CA Access Control Endpoint Management from any computer on the network:

```
http://appserver123:18080/acem
```

The URL suggests that CA Access Control Endpoint Management is installed on a host named appserver123 and uses the default JBoss port 18080.

Chapter 11: Migrating PMDs to an Advanced Policy Management Environment

This section contains the following topics:

Migration to an Advanced Policy Management Environment

When you migrate from a Policy Model (PMD) environment to an advanced policy management environment, you change the way you deploy rules to your endpoints:

- In a PMD environment, regular rules you define in a central database (PMDB) are automatically propagated to databases in a configured hierarchy.
- In an advanced policy management environment, you assign policies (groups of rules) to one or more host or host groups. You can also undeploy (remove) policies and view deployment status and deployment deviation.

When you migrate from a PMD environment to an advanced policy management environment, you:

- Install additional components
- Create policies from the rules in the PMDB
- Upgrade the endpoints
- Flatten your PMD structure

Advanced policy management does not support hierarchical host groups. If your PMD architecture contains hierarchical PMDBs, you must flatten your PMD hierarchy.

Note: Advanced policy management does not support policies with password management commands. You must use a password PMD to synchronize passwords between endpoints and to distribute password management rules. You cannot migrate a password PMD to the advanced policy management environment. Instead, you apply a filter file to the password PMD so that it only sends password rules to its subscribers.

How the Migration Process Works

Migrating to an advanced policy management environment lets you deploy and undeploy policies, and check the deployment and deviation status of policies. While you use CA Access Control to perform most migration tasks, there are still some tasks you must perform yourself. Understanding how the migration process works helps you troubleshoot any problems that may arise.

The following process gives you an overview of the stages in the migration process:

1. You install the Enterprise Management server components.

   The advanced policy management environment is set up as part of the Enterprise Management installation process.

2. You upgrade the PMD to CA Access Control r12.5 or later.
3. You migrate the endpoints that subscribe to the PMD to the advanced policy management environment.
4. In CA Access Control Enterprise Management, you export the rules in the PMDB to policy files.
5. CA Access Control Enterprise Management creates the following on the DMS:
   - A host group (GHNODE object) that corresponds to the migrated PMDB
   - Hosts (HNODE objects) that correspond to the endpoint subscribers of the PMDB
   - POLICY objects that contain the rules in the policy files

6. In CA Access Control Enterprise Management, you join the hosts to the host group. CA Access Control assigns the POLICY objects to the host group and deploys the POLICY objects to the hosts that correspond to the endpoint subscribers of the PMDB.
7. In CA Access Control Enterprise Management, you do *one* of the following:
   - If the PMD is a password PMD, you apply a filter file to the PMD.
   - If the PMD is not a password PMD, you delete the PMD.

Note: You can also use the policydeploy utility to perform migration tasks.

More information:

How to Migrate to Advanced Policy Management (see page 328)

How Policies Are Created and Assigned

When you migrate from a PMD environment to an advanced policy management environment, you use CA Access Control to create policies from the rules in the PMDB and assign the policies to host groups on the DMS.

The following process explains how CA Access Control creates and assigns policies:

1. CA Access Control exports the rules in the PMDB to a policy file.

   Note: You can specify that CA Access Control only exports rules that modify resources in a particular class.

2. CA Access Control changes each rule that creates a new resource or accessor to a rule that modifies the resource or accessor. For example, CA Access Control changes all newres rules to editres rules.

   This step prevents the deployment errors that result if you deploy a rule that creates a new resource or accessor more than once to the same endpoint.

3. CA Access Control creates a host group (GHNODE object) that corresponds to the PMD on the DMS.

4. For each endpoint subscriber that is listed in the PMDB, CA Access Control checks if a corresponding host (HNODE object) is already created in the DMS.
   - For each subscriber that is listed in the PMDB and that has a corresponding host in the DMS, CA Access Control joins the host to the host group created in Step 3.
   - For each subscriber that is listed in the PMDB and that does not have a corresponding host in the DMS, CA Access Control creates a host that corresponds to the endpoint and joins the host to the host group created in Step 3.

   Note: CA Access Control does not create hosts that correspond to subscriber PMDBs.
5. CA Access Control uses the rules in the exported policy file to create a POLICY object in the DMS.

   Note: CA Access Control does not create an undeploy script for the POLICY object.
6. CA Access Control assigns the POLICY object to the host group that it created in Step 3.

More information:

Migrate a PMDB (see page 330)

How Policies Are Initially Sent to a Migrated Endpoint

When you migrate from a PMD environment to an advanced policy management environment, CA Access Control creates policies from the rules in the PMDB and sends them to the migrated endpoints. Understanding how CA Access Control initially sends the policies to the migrated endpoint may help you troubleshoot any errors that occur during the migration process.

The following process explains how policies are initially sent to a migrated endpoint after you start CA Access Control on the endpoint:

1. CA Access Control starts and invokes policyfetcher, which sends a heartbeat notification to the DMS.
2. The DMS receives the heartbeat notification and checks if a corresponding host (HNODE) object exists on the DMS.

3. *One* of the following happens:
   - If a corresponding host exists on the DMS, and the host is part of the host group that corresponds to the PMD that you migrated:
     a. CA Access Control associates the endpoint and the host.
     b. CA Access Control deploys the policies that are assigned to the host group to the endpoint.
   - If a corresponding host does not exist on the DMS:
     a. CA Access Control creates the host.
     b. When you create and assign policies, CA Access Control joins the host to the host group that corresponds to the PMD that you migrated.
     c. CA Access Control deploys the policies that are assigned to the host group to the endpoint.
4. CA Access Control modifies the Update Time property for each resource listed in the policy to the time the policy was deployed.

   Note: Because CA Access Control changed commands that create objects to commands that modify objects, you should not see any deployment errors for the policy.

Note: For more information about policies and host groups, see the *Enterprise Administration Guide*.

How CA Access Control Applies a Filter File to a Password PMD

Advanced policy management does not support policies with password management commands. Use a password PMD to synchronize passwords between endpoints and to distribute password management rules. When you migrate a password PMD to the advanced policy management environment, you apply a filter file to the password PMD so that it only deploys password rules to its subscribers.

The following process explains how CA Access Control applies a filter file to a password PMD:

1. CA Access Control creates a text file named filter.flt and adds the following lines to it:

```
#-------------------------------------------------------------------
# access    env     class    objects    properties          pass/nopass
#-------------------------------------------------------------------
 *    *     USER     *     OLD_PASSWD;CLR_PASSWD PASS
 *    *     *        *     *                     NOPASS
#-------------------------------------------------------------------
```

2. CA Access Control saves filter.flt in the password PMD directory.
3. CA Access Control adds the full path of filter.flt to the "filter" configuration setting in the following location:
   - (UNIX) The [pmd] section of the pmd.ini file
   - (Windows) The following registry key:

     HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Pmd*PMDB_Name*

How to Migrate to Advanced Policy Management

Migrating to an advanced policy management environment lets you deploy and undeploy policies, and check the deployment and deviation status of policies.

Note: Advanced policy management does not support policies with password management commands. You must use a password PMD to synchronize passwords between endpoints and to distribute password management rules. You cannot migrate a password PMD to the advanced policy management environment.

Before you begin the migration process, verify that:

- All subscribers are available
- The subscribers have received all updates from the PMDB
- No subscribers are synchronized with the PMDB

Important! We strongly recommend that you back up the PMDB before you begin the migration process.

To migrate from a PMD environment to an advanced policy management environment, do the following:

1. Install the Enterprise Management server components (see page 51).

   The advanced policy management environment is set up as part of the Enterprise Management installation process.

2. Upgrade the PMD host to CA Access Control r12.5 or later.

3. Migrate the endpoints (see page 329).

4. Migrate the PMDB (see page 330).

More information:

How the Migration Process Works (see page 324)

Migrate an Endpoint

Migrating the endpoints is the third step in the process to migrate from a PMD environment to an advanced policy management environment. In the preceding steps, you:

- Installed the Enterprise Management server components
- Upgraded the PMD host to CA Access Control r12.5 or later

In this step, you migrate the endpoints that subscribe to the migrated PMDB.

To migrate an endpoint

1. Upgrade the endpoint to CA Access Control r12.0 or later.

2. Run the following commands on the endpoint to configure advanced policy management client components:

   dmsmgr -config -endpoint
   dmsmgr -config -dh *dh_name@host_name*

   The endpoint is upgraded to the advanced policy management environment.

Migrate a PMDB

We recommend that you understand the steps you must perform at each stage of the overall migration process before you migrate a PMDB. Migrating a PMDB is only one step in the process to migrate an enterprise deployment of CA Access Control to an advanced policy management environment.

Migrating a PMDB is the final step in the process to migrate from a PMD environment to an advanced policy management environment. In the preceding steps, you:

- Installed the Enterprise Management Server
- Upgraded the PMD host to CA Access Control r12.5 or later
- Migrated an endpoint (upgraded the endpoint to CA Access Control r12.0 or later and configured advanced policy management client components)

In this step, you use CA Access Control Enterprise Management to create a policy from the rules in the PMDB, create a host group for the migrated PMDB, and join the hosts that correspond to the PMDB subscribers to this host group. You can also choose to assign the new policy to the host group.

Important! Each time you click the Next button, CA Access Control Enterprise Management completes an action in the DMS or in the PMDB. It may be difficult to undo the result of these actions.

To migrate a PMDB

1. In CA Access Control Enterprise Management, click the Policy Management tab, click the Policy sub-tab, expand the Policy tree, and click PMDB Migrate.

   The PMDB Host Login page appears.

2. Type a user name and password that is authorized to access the PMDB and the name of the PMDB that you want to migrate, and click Log In.

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

   The PMDB Migrate Process page appears at the General task stage.

3. Complete the following fields, and click Next:

   Name

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

   Description

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

Policy Classes

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

Export dependent classes

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

The Policy Script task stage appears.

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

   CA Access Control Enterprise Management creates a policy from the rules. The Host Group task stage appears.

5. Complete the dialog and click Next, as follows:

   Host Group

   Specifies the name of the host group to add the hosts to. You can specify an existing host group or create a new host group.

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

   Assign Policy

   (Optional) Specifies to assign the policy to the host group.

   Assigned Hosts

   Specifies the hosts to add to the host group.

   Note: By default, this table contains all subscribers of the migrated PMDB that you have authority to access. You can add and remove hosts from the Assigned Hosts list; however, you cannot add a host to the host group if you do not have authority to access the host.

   CA Access Control Enterprise Management adds the hosts to the hosts group and, if specified, assigns the policy to the host group. The PMD Options task stage appears.

6. Select any of the following options that you want to apply to the migrated PMDB:

   Unsubscribe the hosts that you specified in step 3 (Host Group step)

   Specifies to unsubscribe the endpoints that you selected in the previous task stage from the migrated PMDB.

   Unsubscribe all of the PMDB subscribers

   Specifies to unsubscribe all subscribers from the migrated PMDB.

Delete the PMD

Specifies to delete the migrated PMDB.

Important! Do not delete the PMDB if you use it to propagate user password commands.

Add PMD filter file

Specifies to add a filter file to the migrated PMDB so that the PMDB only propagates user password commands to its subscribers. If you select this option, the migrated PMDB becomes a password PMDB.

7. Click Next.

   CA Access Control performs the actions that you specified. The Migration Actions Summary task stage appears and the migration process is complete.

More information:

How Policies Are Created and Assigned (see page 325)

Class Dependency

When you export the rules for specified classes from a PMDB, you can choose to also export the rules for dependent classes. If you specify that CA Access Control should export dependent classes, CA Access Control exports the following:

- If you export rules that modify resources in a particular class, and the class has a corresponding resource group, CA Access Control also exports the rules that modify resources in that resource group.

  For example, if you specify to export FILE class rules, CA Access Control exports the rules that modify resources in the FILE and GFILE classes.

- If you export rules that modify resources in a particular resource group, CA Access Control also exports the rules that modify the member resource of the resource group.

  For example, if you specify to export GFILE class rules, CA Access Control exports the rules that modify resources in the GFILE and FILE classes.

- If you export rules that modify resources in a particular class and that class has a PACL, CA Access Control also exports the rules that modify resources in the PROGRAM class.

- If you export rules that modify resources in a particular class and that class has a CALACL, CA Access Control also exports the rules that modify resources in the CALENDAR class.
- If you export rules that modify resources in a particular class, and one of the resources in that class is a member of a CONTAINER resource group, CA Access Control exports the rules that modify resources in the CONTAINER class and the rules that modify the resources that are members of each CONTAINER resource group.

  For example, if you specify to export CONTAINER class rules, and the CONTAINER object holds FILE objects, CA Access Control exports the rules that modify resources in the CONTAINER and FILE classes.

Duplicate HNODEs Appear In DMS

Symptom:

After I migrated a PMD to an advanced policy management environment, two HNODEs that represent the same endpoint are created in the DMS.

Solution:

The fully qualified host name of the endpoint is not the same on the DMS and on the endpoint. To fix this problem, delete one of the HNODE objects in the DMS.

Note: For more information about HNODE objects and the DMS, see the *Enterprise Administration Guide*.

Migrate Hierarchical PMDBs

Advanced policy management does not support hierarchical host groups. If your PMD architecture contains hierarchical PMDBs, you must flatten your PMD hierarchy during the migration process.

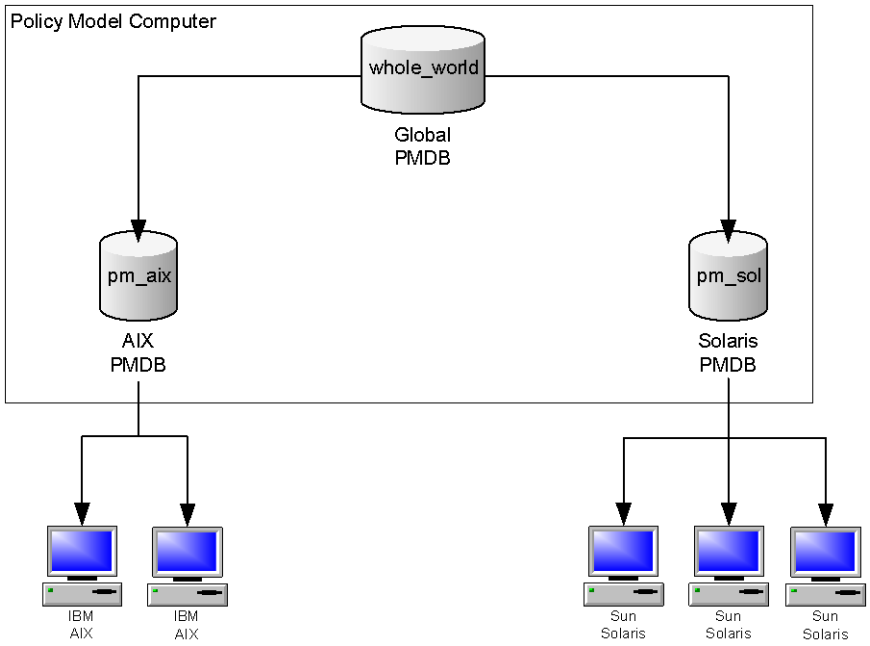
When you flatten the PMD hierarchy, you migrate each PMDB separately. During the migration CA Access Control creates a host group for each PMDB in the hierarchical environment and adds each endpoint to all the host groups that correspond to the PMDBs to which it was subscribed.

To migrate hierarchical PMDBs

1. Migrate the master PMDB.
2. Migrate each subscriber PMDB.

Example: Migrate Hierarchical PMDBs

The following diagram shows an example of a PMD environment with hierarchical PMDBs.



In this example, the PMDBs pm_aix and pm_solaris are subscribers of the PMDB whole_world. All IBM AIX endpoints are subscribers of pm_aix. All Sun Solaris endpoints are subscribers of pm_sol. Effectively, all endpoints are subscribers of whole_world.

When you migrate this PMD environment to an advanced policy management environment, you do the following:

1. Migrate the whole_world PMDB.

   CA Access Control creates the whole_world host group. All endpoints are members of this host group.

2. Migrate the subscriber PMDBs:

   - Migrate the pm_aix PMDB.

     CA Access Control creates the pm_aix host group. IBM AIX endpoints are members of this host group.

   - Migrate the pm_sol PMDB.

     CA Access Control creates the pm_sol host group. Sun Solaris endpoints are members of this host group.

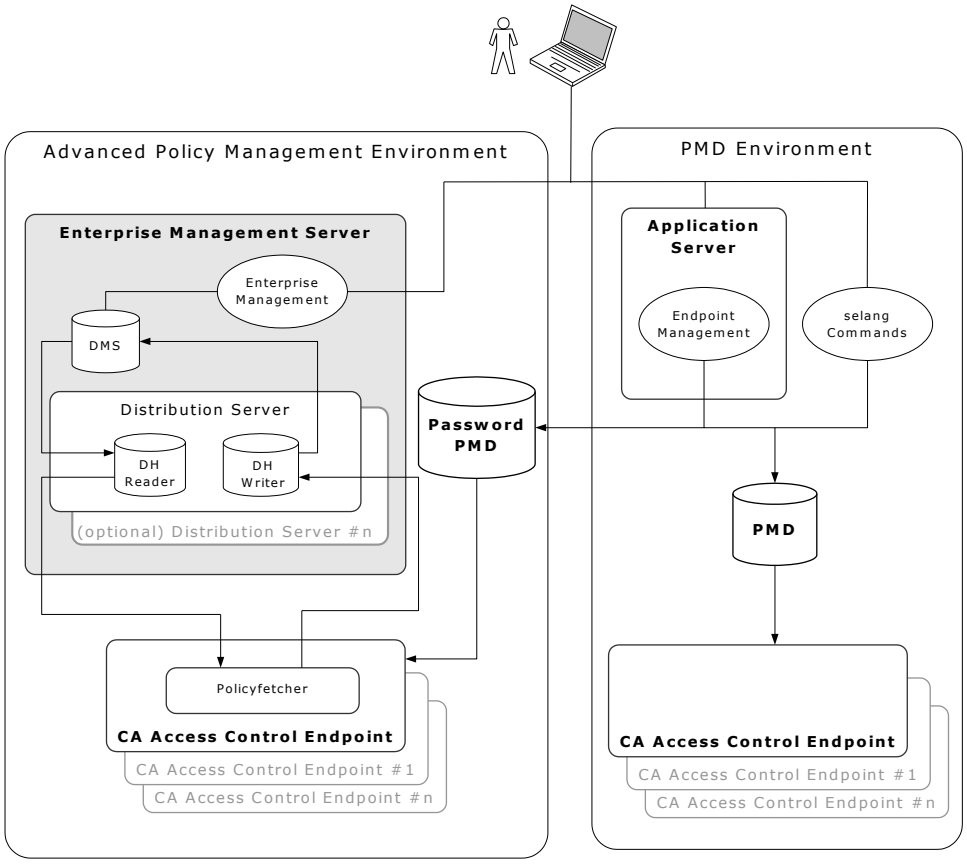
Note: In a PMD environment, if you apply a filter file to the pm_aix PMDB, the filter file may prevent the rules that you deploy from the whole_world PMDB from reaching the IBM AIX endpoints. In an advanced policy management environment, the IBM AIX endpoints are members of the whole_world host group. All the rules that you deploy to the whole_world host group are deployed to all the endpoints without filtering. You should be aware of this changed behavior when you deploy rules in an advanced policy management environment.

Mixed Policy Management Environments

A mixed policy management environment is a CA Access Control deployment in which some endpoints subscribe to a PMD and some endpoints are defined in an advanced policy management environment.

The following diagram shows an example of a CA Access Control deployment with a mixed policy management environment.

Note: Although it is not shown in this diagram, an endpoint can subscribe to a PMD and also be defined in an advanced policy management environment. For example, you can deploy policies to an endpoint in an advanced policy management environment, and also propagate selang rules from a PMD to the same endpoint.



Update Endpoints in a Mixed Policy Management Environment

When you update endpoints in a mixed policy management environment, you update the endpoints in each environment separately.

Note: Endpoints cannot accept rules that modify classes that were introduced in a later CA Access Control version. For example, an r8 endpoint can only accept rules that change r8 functionality, even though you deploy the rules from an r12.5 PMD or DMS.

To update endpoints in a mixed policy management environment

1. Create a script file with the selang deployment commands you want to deploy to the endpoints.
2. In CA Access Control Enterprise Management, do the following:
   a. Store the policy version on the DMS.
   b. Assign the stored policy version to the host groups you want to update.

   CA Access Control deploys the policy to the endpoints in the host group.
3. Update the PMDB with the selang commands in the script file.

   The PMDB propagates the commands to its endpoints.

Note: For more information about how to store and assign policy versions, see the *Enterprise Administration Guide*. For more information about how to update the PMDB, see the *Endpoint Administration Guide* for your OS.

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.

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 Access Control components separately.

More information:

Disaster Recovery in CA Access Control

A disaster recovery deployment makes it easier to restore your advanced policy management components in the event of a catastrophic system failure. If the 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.

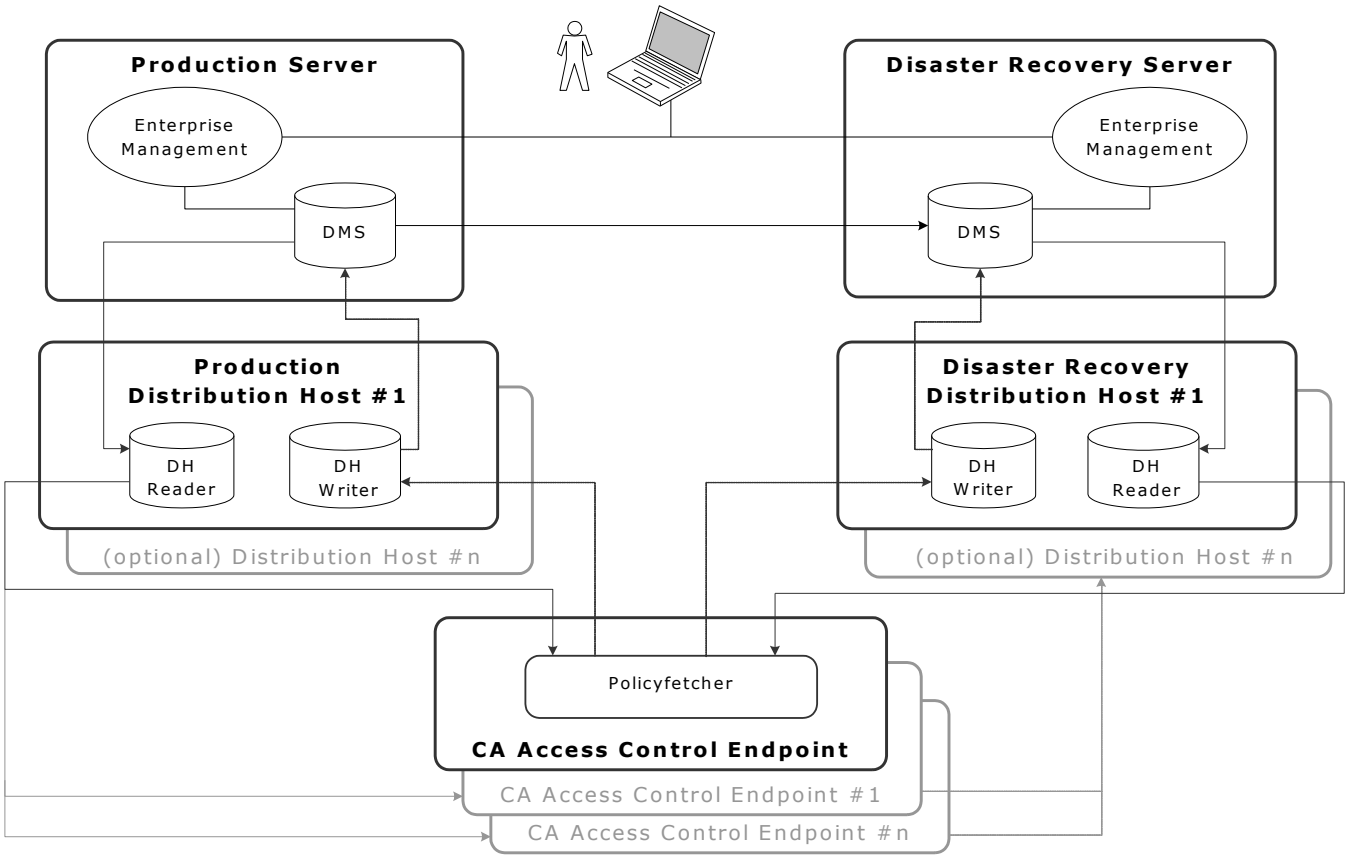
The following CA Access Control components are not backed up or restored during the disaster recovery process. Back up these components separately:

- Password policy models
- PMDBs
- RDBMSs
- CA Access Control Endpoint Management
- CA Access Control Enterprise Management
- data on the endpoints
- CA Access Control audit files
- Reports
- UNAB policies
- Message Queue

Note: The DMS audit file is saved when the DMS is backed up.

Disaster Recovery Architecture

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



Components for Disaster Recovery

You need the following components to deploy CA Access Control in a disaster recovery configuration:

- For the production environment:
  - One installation of CA Access Control Enterprise Management
  - Central database (RDBMS)
  - On or more installation of the Distribution Server.
- For the disaster recovery environment:
  - One installation of CA Access Control Enterprise Management
  - 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 Access Control. For example, you cannot restore a DMS using CA Access Control r12.5 from backup files of a DMS using CA Access Control r12.0SP1.
- You should store the backup DMS files in a safe location, preferably protected by CA Access Control access rules.
- You can setup clustering or other failover solution on your RDBMS.

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.

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 Access Control components separately.

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 CA Access Control Enterprise Management 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 is defined in the 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 cycles for which the endpoint attempts to connect to a Distribution Server is defined in the max_dh_retry_cycles 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 section, 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 must 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 advanced policy management components in the event of a catastrophic system failure. You may need to back up other CA Access Control 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 Access Control. Verify that the production and disaster recovery environments are deployed on identical platforms, operating systems, and versions of CA Access Control.

Note: This process installs the DMS and DH on separate hosts.

The following process describes how to install a disaster recovery deployment:

1. Set up the central database (RDBMS)
2. Set up the production CA Access Control Enterprise Management (see page 345).
3. Set up the disaster recovery CA Access Control Enterprise Management (see page 345).
4. Configure the servers to use an identical encryption key (see page 209).
5. Set up the production Distribution Server (see page 346).
6. Set up the disaster recovery Distribution Server (see page 348).
7. Set up an endpoint (see page 351).

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 Access Control Enterprise Management

The production CA Access Control Enterprise Management 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, you must 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 CA Access Control Enterprise Management

1. Install the production CA Access Control Enterprise Management (see page 47).
2. If you want to disable the local DH and use the DH on the Distribution Server, run the following command on the production CA Access Control Enterprise Management to configure the DMS:

   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.

Set up the Disaster Recovery CA Access Control Enterprise Management

The disaster recovery CA Access Control Enterprise Management deploys and manages your enterprise policies in the event of a catastrophic system failure. Because the disaster recovery CA Access Control Enterprise Management is a subscriber of the production CA Access Control Enterprise Management, its database contains the same information about policy versions, policy scripts, and endpoint deployment status as the production CA Access Control Enterprise Management.

Note: You must set up the production CA Access Control Enterprise Management before you set up the disaster recovery CA Access Control Enterprise Management.

To set up the disaster recovery CA Access Control Enterprise Management

1. Install CA Access Control Enterprise Management on the disaster recovery server (see page 47).

2. If you wish to disable the local DH and use the DH on the Distribution Server, you must run the following command on the disaster recovery CA Access Control Enterprise Management:

   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.

3. Move to the production CA Access Control Enterprise Management.
4. Run the following command on the production CA Access Control Enterprise Management:

   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 CA Access Control Enterprise Management is subscribed to and synchronized with the production CA Access Control Enterprise Management.

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 352) 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 (see page 364).
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 352) 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 (see page 364).

5. Repeat Steps 1-4 for each disaster recovery Distribution Server.

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.

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 on 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 435).
   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}:/lxnvWwAEcYhSmOu3YT3ow==</module-option>
                        <module-option
name="managedConnectionFactoryName">jboss.jca:name=jdbc/objectstore,service=NoTxCM</module-option>
                </login-module>
        </authentication>
</application-policy>
```

Set Up an Endpoint

Once you install the advanced policy management components in the production and disaster recovery environments, 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: 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 Access Control endpoint functionality, with the Advanced Policy Management Client Components enabled, on the endpoint host.

   CA Access Control 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*.

Install the Distribution Server

The Distribution Server handles communication between the application server and the endpoints. The Distribution Server is installed by default on the Enterprise Management Server. For failover purposes, you can install more than one Distribution Server in your enterprise.

When you configure CA Access Control to work in a disaster recovery environment, you install a minimum of two 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 Access Control Premium Edition 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 Access Control 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_r125.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 password for the Message Queue server administrator.

   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 Access Control Enterprise Management with privileged account management capabilities.

   The CA Access Control 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 346)
Set Up the Disaster Recovery Distribution Server (see page 348)

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 Access Control components separately.

More information:

Data That Can Be Restored (see page 354)
When to Restore a DMS (see page 354)
When to Restore a DH (see page 355)
How a DMS Is Restored (see page 355)
How a DH Is Restored (see page 356)

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 Access Control 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 Access Control on the production CA Access Control Enterprise Management and the production Distribution Servers.
2. Stop all administrative work against the disaster recovery DMS, that is, stop CA Access Control 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 358)
   - remote backup (see page 359)
5. Restore the production database (RDBMS).
6. Restore the production DMS (see page 361) from the disaster recovery DMS backup files.
7. Start CA Access Control 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 358)
   - remote backup (see page 359)
9. Restore each production DH (see page 360) from the production DMS backup files.
10. Start CA Access Control on each production Distribution Server.
11. Move all administrative work to the production DMS, that is, start CA Access Control Enterprise Management and the policydeploy utility on the production CA Access Control 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 362) 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 358)
        - selang commands (see page 359)
    c. Restore each disaster recovery DH (see page 360) 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 CA Access Control Enterprise Management 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 Access Control 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 Access Control 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.

To restore a DH, run the following command on the DH host:

dmsmgr -restore -dh *name* -source *path* -parent *name*\
[-admin *user*[,*user...*]] [-xadmin *user*[,*user...*]] [-desktop *host*[, *host...*]]

-admin *user*[,*user...*]

(UNIX) Defines internal users as administrators of the restored DMS or DH.

-desktop *host*[, *host...*]

(Optional) Defines a list of computers that have TERMINAL access rights to the computer with the restored DH.

Note: Whether specified or not, the terminal running the utility is always granted administration rights for the restored DH.

-dh *name*

Defines the name of the DH that is restored on the local host.

-parent *name*

Defines the name of the parent DMS the restored DH will subscribe to. Specify the parent DMS in the following format: *DMS_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 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 Configure Message Routing Settings

When working in an environment that consists of a single instance of CA Access Control Enterprise Management and multiple Distribution Servers, you must configure the MQ routing settings on all the Distribution Servers to point to the MQ on the CA Access Control Enterprise Management. This helps ensure that all the messages that the CA Access Control endpoints send are ultimately routed to a single MQ, that is located on the CA Access Control Enterprise Management server.

To route messages from the MQ on every Distribution Server to the CA Access Control Enterprise Management server, do the following:

- On each Distribution Server in your enterprise, do the following:
  - Stop the Message Queue service.
  - Modify the routing to the CA Access Control Enterprise Management Message Queue.
  - Define the parameters of the CA Access Control Enterprise Management Message Queue.
  - Configure the names of the Distribution Server message queues.
  - Specify the location of the CA Access Control Enterprise Management Message Queue.
  - Start the Message Queue service.
- On the CA Access Control Enterprise Management, do the following:
  - Stop the Message Queue service.
  - Modify the routing to the Distribution Server Message Queue.
  - Define the parameters of the Distribution Server Message Queue
  - Configure the names of the CA Access Control Enterprise Management message queues.
  - Specify the location of the CA Access Control Enterprise Management Message Queue
  - Start the Message Queue service.

Note: For information about message routings, refer to the *TIBCO Enterprise Message Server User's Guide*.

More information:

Modify the Message Queue Settings on the Distribution Server (see page 365)
Modify the Message Queue Settings on CA Access Control Enterprise Management (see page 366)
Message Queue Connection Configuration (see page 367)
Configure the Names of the Message Queues on the Distribution Server (see page 372)
Configure the Names of the Message Queues on the CA Access Control Enterprise Management Computer (see page 373)
Message Routing Configuration (see page 373)
How To Synchronize the Message Queue Servers Data Files (see page 375)

Modify the Message Queue Settings on the Distribution Server

By default, every Distribution Server is configured to work with the Message Queue that is running on that server. To route messages to another Message Queue, you must reconfigure the Message Queue settings.

This procedure shows you how to modify the Message Queue settings on the Distribution Server to enable communication with the CA Access Control Enterprise Management Message Queue. Complete this procedure for every Distribution Server in your enterprise.

To modify the Message Queue settings on the Distribution Server

1. Stop the CA Access Control Message Queue service.
2. On the Distribution Server, open the file tibemsd.conf file, located by default in the following directory, where *DistServerInstallDir* is the directory in which you installed the Distribution Server:

   DistServerInstallDir/ACMQ/tibco/ems/bin
3. Enter the Distribution Server short host name in the 'server' parameter.
4. Change the 'routing' parameter value to enabled.
5. Start the CA Access Control Message Queue service.

   You have modified the message queue settings on the Distribution Server.

Note: For information about message routings, see the *TIBCO Enterprise Message Server User's Guide*.

Example: tibemsd.conf file

The example shows you a snippet from the tibemsd.conf file after you modify the routing settings for a Distribution Server named DS_Example:

```
########################
# Server Identification Information.
# server:    unique server name
# password:  password used to login into other routed server
########################
server              = DS_Example
password            =
########################
…
########################
# Routing. Routes configuration is in 'routes.conf'. This enables or
# disables routing functionality for this server.
########################
routing             = enabled
########################
```

Modify the Message Queue Settings on CA Access Control Enterprise Management

This procedure shows you how to modify the Message Queue settings on CA Access Control Enterprise Management to enable communication with the Distribution Server.

To modify the Message Queue settings on CA Access Control Enterprise Management

1. Stop the CA Access Control Message Queue service.
2. On CA Access Control Enterprise Management, open the tibemsd.conf file for editing. This file is located in the following directory by default, where *DistServerInstallDir* is the directory in which you installed the Distribution Server:

   DistServerInstallDir/ACMQ/tibco/ems/bin
3. Enter the CA Access Control Enterprise Management server short host name, not separated by dots, in the 'server' parameter.
4. Change the 'routing' parameter value to enabled.
5. Start the CA Access Control Message Queue service.

   You have modified the message queue settings on CA Access Control Enterprise Management.

Note: For information about message routings, refer to the *TIBCO Enterprise Message Server User's Guide*.

Example: tibemsd.conf file

The example shows you a snippet from the tibemsd.conf file after you modify the routing settings for a CA Access Control Enterprise Management Server named ENTM_Example:

```
########################
# Server Identification Information.
# server:    unique server name
# password:  password used to login into other routed server
########################
server              = ENTM_Example
password            =
########################
…
########################
# Routing. Routes configuration is in 'routes.conf'. This enables or
# disables routing functionality for this server.
########################
routing             = enabled
########################
```

Message Queue Connection Configuration

To route messages from the Message Queue on the Distribution Server to the Enterprise Management Server conversely, you modify the existing Message Queue settings in your enterprise.

Example: Configuring the Message Queue Connection Settings on the Distribution Server

This example shows you how to configure the Message Queue server settings on the Distribution Server. You configure the Message Queue to send messages to the Enterprise Management Server by defining the parameters of the Message Queue that is running on the Enterprise Management Server.

To configure the Message Queue connection settings on the Distribution Server

1. On the Distribution Server, do one of the following:
   - (Windows 2003 Server) Select Start, Programs, TIBCO, TIBCO EMS 4.4.1, Start EMS Administration Tool.
   - (UNIX) Do the following:
     a. Navigate to the following directory, where *DistServerInstallDir* is the directory in which you installed the Distribution Server:

        DistServerInstallDir/MessageQueue/tibco/ems/bin

     b. Run the following command:

        tibemsadmin

        The TIBCO EMS Administration Tool command prompt window opens.
2. Connect to the Message Queue using either of the following:
   - Enter the following command to connect using SSL:

     connect ssl://localhost:7243
   - Enter the following command to connect using TCP:

     connect tcp://localhost:7222

   A login name prompt appears.
3. Enter **admin**.

   A password prompt appears.
4. Enter the password that you provided when you installed the Distribution Server.
5. When prompted, enter a new password for the Message Queue server.
6. Define the Message Queue password.

   set server password=

   Example: set server password=<*C0mp1ex*>

7. Create a user named ENTM-NAME and assign a password to the user.

   create user ENTM-NAME password=*acserver_user-passwd*

   Example: create user EMS-SERVER password=<*acserver_user-passwd*>

   Important! Specify the same name that you defined in the 'server' parameter of the tibemsdf.conf file on the Enterprise Management Server.

8. Do the following:

   a. Enter the following command:

      add member ac_server_users *ENTM_NAME*

      The user you created is added to the ac_server_users group.

   b. Enter the following command:

      add member ac_endpoint_users *ENTM_NAME*

      The user you created is added to the ac_endpoint_users group.

   c. Enter the following command:

      add member report_publishers *ENTM_NAME*

      The user you created is granted permissions to read and publish messages to CA Access Control queues.

9. Restart the Distribution Server.

   The changes you made are applied.

Example: Configure the Message Queue Connection Settings on CA Access Control Enterprise Management

This example shows you how to configure the Message Queue server settings on the Enterprise Management Server. You configure the Message Queue to send messages to the Distribution Server.

In this example the term *DS-NAME* relates to the name of the Distribution Server computer and the term *ENTM-NAME* relates to name of the Enterprise Management Server. When you define the message queue server settings, you replace the name with the server actual names, as defined in the 'server' token in the *tibemsd.conf* file.

To configure the Message Queue connection settings on CA Access Control Enterprise Management

1. On the CA Access Control Enterprise Management computer, do one of the following:
   - (Windows 2003 Server) Select Start, Programs, TIBCO, TIBCO EMS 4.4.1, Start EMS Administration Tool.
   - (UNIX) Do the following:
     a. Navigate to the following directory, where *ACServerInstallDir* is the directory in which you installed CA Access Control Enterprise Management:

     ACServerInstallDir/MessageQueue/tibco/ems/bin

     b. Run the following command:

     tibemsadmin

     The TIBCO EMS Administration Tool command prompt window opens.
2. Connect to the Message Queue using either of the following:
   - Enter the following command to connect using SSL:

     connect ssl://localhost:7243
   - Enter the following command to connect using TCP:

     connect tcp://localhost:7222

   A login name prompt appears.
3. Enter **admin**.

   A password prompt appears.
4. Enter the password that you provided when you installed the Enterprise Management Server.

5. Define the Message Queue password.

   set server password=*entm_server-passwd*

   Example: set server password=<*ENTM_SERVER_NAME-passwd*>

6. For each Distribution Server, create a user named DS-NAME and assign a password to the user.

   create user DS-NAME password=*dist_server_user*

   Example: create user EMS-Server password=<*C0mp1ex*>

   Important! Specify the same name that you defined in the 'server' parameter of the tibemsdf.conf file on the Enterprise Management Server.

7. Do the following:

   a. Enter the following command:

      add member ac_server_users *DS_NAME*

      The user you created is added to the ac_server_users group.

   b. Enter the following command:

      add member ac_endpoint_users *DS_NAME*

      The user you created is added to the ac_endpoint_users group.

   c. Enter the following command.

      add member report_publishers *DS_NAME*

      The user you created is granted permissions to read and publish messages to CA Access Control queues.

8. Restart the Distribution Server for the changes to take effect.

   You have configured the message queue connection settings on CA Access Control Enterprise Management.

   Note: For information about message routings, see the *TIBCO Enterprise Message Server User's Guide*.

Configure the Names of the Message Queues on the Distribution Server

To forward messages from the Distribution Server to CA Access Control Enterprise Management, configure each messages route to forward the messages from the Message Queue on the Distribution Server to the Message Queue on CA Access Control Enterprise Management.

In this procedure you define the message queue settings on the Distribution Server. You modify the message queue settings file to provide the settings of the Message Queue on CA Access Control Enterprise Management.

To configure the names of the Message Queue on the Distribution Server

1. On the Distribution Server, open the file queues.conf. The file is located by default in the following directory, where *DistServerInstallDir* is the directory in which you installed the Distribution Server:

   DistServerInstallDir/ACMQ/tibco/ems/bin

2. Locate the queue named 'queue/snapshots' and add the ENTM-NAME value at the end of the queue name, preceded by a @ sign as follows:

   queue/snapshots@*ENTM-NAME*

   ENTM-NAME

   Defines the short name of the CA Access Control Enterprise Management computer.

   Important! Specify the same name that you defined in the 'server' parameter of the tibemsd.conf file on CA Access Control Enterprise Management.

3. Locate the queue name 'queue/audit' and add the ENTM-NAME value at the end of the queue name, preceded by a @ sign as follows:

   queue/audit@*ENTM-NAME*

4. Locate the queue named 'ac_endpoint_to_server' and add the ENTM-NAME value at the end of the queue name, preceded by a @ sign as follows:

   ac_endpoint_to_server@*ENTM-NAME*

5. Locate the queue named 'ac_server_to_endpoint' and add the ENTM-NAME value at th end of the queue name, preceded by a @ sign as follows:

   ac_server_to_endpoint@*ENTM-NAME*

6. Save and close the file.

Note: For information about message routings, see the *TIBCO Enterprise Message Server User's Guide*.

Configure the Names of the Message Queues on the CA Access Control Enterprise Management Computer

In this procedure you define the message routing settings on CA Access Control Enterprise Management. You configure the Message Queue settings on CA Access Control Enterprise Management to identify this Message Queue as the primary server.

To configure the names of the Message Queues on the CA Access Control Enterprise Management computer

1. On CA Access Control Enterprise Management, open the file queues.conf in an editable form. The file is located by default in the following directory, where *ACServerInstallDir* is the directory in which you installed CA Access Control Enterprise Management:

   ACServerInstallDir/MessageQueue/tibco/ems/bin

2. Locate the queue named 'queue/snapshots' and add the word 'global' after the word 'secure' at the end of the queue name, as follows:

   queue/snapshot secure, global

3. Locate the queue named 'queue/audit' and add the word 'global' after the word 'secure' at the end of the queue name, as follows:

   queue/audit secure, global

4. Locate the queue named 'ac_endpoint_to_server' and add the word 'global' after the word 'secure' at the end of the queue name, as follows:

   ac_endpoint_to_server secure, global

5. Locate the queue named 'ac_server_to_endpoint' and add the word 'global' after the word 'secure' at the end of the queue name, as follows:

   ac_server_to_endpoint secure, global

6. Save and close the file.

Note: For information about message routings, refer to the *TIBCO Enterprise Message Server User's Guide*.

Message Routing Configuration

After you have configured the Message Queue settings and configured the message queue routing settings on the Distribution Server and CA Access Control Enterprise Management, you set up the message routes on the Distribution Server and CA Access Control Enterprise Management.

Example: Set Up Message Routes on the Distribution Server

This example shows you how to set up the message route settings on the Distribution Server. You set up a route between the Distribution Server and CA Access Control Enterprise Management to route messages arriving from CA Access Control endpoints to the Message Queue on CA Access Control Enterprise Management. Complete this procedure on every Distribution Server in your enterprise.

1. On the Distribution Server, open the file routes.conf for editing. The file is located by default in the following directory, where *DistServerInstallDir* is the directory in which you installed the Distribution Server:

   DistServerInstallDir/MessageQueue/tibco/ems/bin

2. Add the following entries:

   ```
   [ENTM-NAME]
   url        = ENTM-URL
   ssl_verify_host = disabled
   ssl_verify_hostname = disabled
   ```

   ENTM-NAME

   Defines the short name of the CA Access Control Enterprise Management computer.

   ENTM_URL

   Defines the CA Access Control Enterprise Management URL.

3. Save the file.
4. Restart the CA Access Control Message Queue service.

Example: Set Up Message Routes on CA Access Control Enterprise Management

This example shows you how to set up the message route settings on CA Access Control Enterprise Management. You set up a route between CA Access Control Enterprise Management and the Distribution Server to send messages from CA Access Control Enterprise Management to the Distribution Server and from there to the endpoints.

1. On CA Access Control Enterprise Management, open the file routes.conf. The file is located by default in the following directory, where *ACServerInstallDir* is the directory in which you installed CA Access Control Enterprise Management:

   ACServerInstallDir/MessageQueue/tibco/ems/bin

2. Add the following entries:

   [DS-NAME]

   url = DS-URL

   ssl_verify_host = disabled

   ssl_verify_hostname = disabled

   DS_NAME

   Defines the short name of the Distribution Server.

   DS_URL

   Defines the Distribution Server URL.

3. Save the file.
4. Restart the CA Access Control Message Queue service.

Note: For information about message routings, refer to the *TIBCO Enterprise Message Server User's Guide*.

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 CA Access Control Enterprise Management Server.
2. Set up message routing settings between the Message Queue Servers on the disaster recovery Distribution Servers and the disaster recovery CA Access Control Enterprise Management Server.
3. Modify the queues.conf file on both the disaster recovery and production Message Queue Servers on the CA Access Control 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 CA Access Control Enterprise Management:

   ACServerInstallDir/MessageQueue/tibco/ems/bin
4. Replicate the production Message Queue Server EMS data files on the CA Access Control Enterprise Management Server to the Message Queue Server on the disaster recovery CA Access Control 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 CA Access Control Enterprise Management:

   ACServerInstallDir/MessageQueue/tibco/ems/bin/datastore

   You have configured the Message Queue Servers EMS data files synchronization settings.

Chapter 13: Upgrading from CA Access Control r12.0 SP1

This section contains the following topics:

Upgrade from CA Access Control r12.0 SP1

This chapter takes you through the steps of upgrading an existing CA Access Control r12.0 SP1 deployment. The upgrade process in the chapter assumes that you installed CA Access Control r12.0 SP1 components on separate computers.

For example, CA Access Control Enterprise Management is installed on one computer, where as the DMS, DH and Report Server are also installed on separate computers.

The upgrade process described in this chapter instructs you how to upgrade each component separately.

Note: You can upgrade from CA Access Control Enterprise Management r12.0 SP1 only.

Before You Begin

Before you begin the process of upgrading the current CA Access Control installation consider the following:

- We recommend that you backup CA Access Control components before starting the upgrade process. We recommend backing up the system files before starting the upgrade process, including all databases.
- CA Access Control Enterprise Management installs the following components: CA Access Control Enterprise Management, CA Access Control, Distribution Server, Enterprise reporting service.
- After upgrading the previous DMS is unavailable. You must upgrade CA Access Control Enterprise Management, DMS and DH before starting the server.
- Specify to use an embedded user store when installing CA Access Control Enterprise Management.

  Important! You cannot use UNAB reports and login authorization policies when you install CA Access Control Enterprise Management on the embedded user store. To generate UNAB reports and configure login authorization policies, you must install Active Directory. If you choose to install Active Directory all records of the existing users and roles will be lost.

How to Upgrade from r12.0 SP1

Before you start upgrading we recommend that you review the steps that you need to complete to upgrade your existing CA Access Control r12.0 SP1 deployment:

1. Upgrade CA Access Control Enterprise Management.
    a. Uninstall CA Access Control Enterprise Management r12.0 SP1, JBoss and JDK
    b. Install JDK 1.5.0 and JBoss 4.2.3 using the Prerequisite Installer
    c. Install CA Access Control Enterprise Management
2. Encrypt the existing passwords in AES.

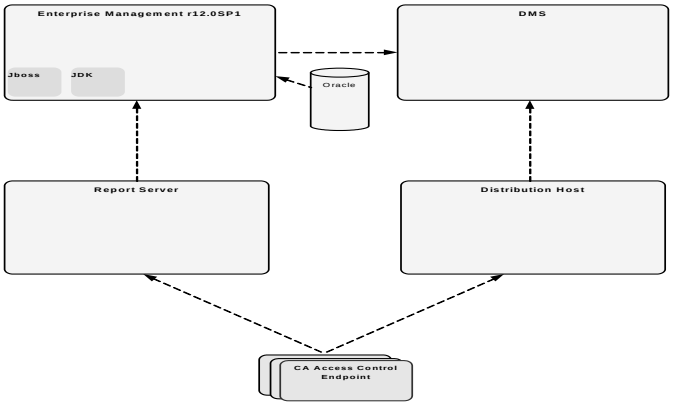
    In CA Access Control Enterprise Management r12.5 SP1, the encryption method was changed from RC2 to AES.
3. Upgrade the DMS computer.

    Note: You do not need to complete this step if the DMS is installed on the same computer as CA Access Control Enterprise Management.
4. Upgrade the DH computer.

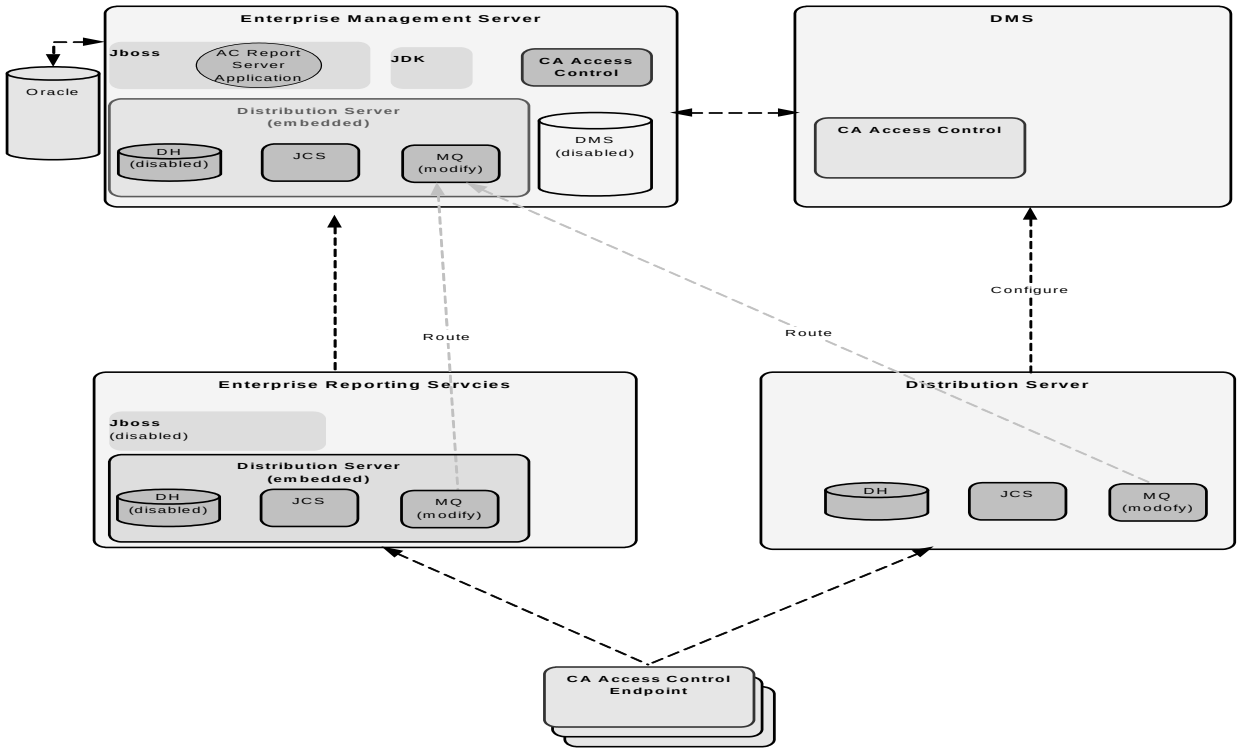
    Note: You must upgrade every DH in your enterprise. You do not need to complete this step if the DH is installed on the same computer as the CA Access Control Enterprise Management.
5. Define Message Queue (MQ) route settings.
6. Migrate the Report Server to Enterprise Reporting Services.
7. Subscribe the DH with the new DMS.
8. (Optional) Install CA Access Control on endpoints.

CA Access Control Upgrade Process

The following diagram displays an example of a CA Access Control r12.0 SP1 deployment architecture before the upgrade:



The following diagram displays an example of a CA Access Control deployment after it was upgraded:



Upgrade the Enterprise Management Server

This procedure shows you the steps you follow for upgrading the Enterprise Management Server and the post installation steps that you need to do.

To upgrade the Enterprise Management Server

1. Uninstall CA Access Control Enterprise Management r12.0 SP1.

   Note: For information about uninstalling CA Access Control Enterprise Management r12.0 SP1, see the *Implementation Guide* for that release.

   Important! On Solaris, search for and remove the /var/.CA_IAM_FW.registry and.com.zerog.registry.xml hidden files if they exist.

2. Uninstall the existing JDK and JBoss.

3. Install prerequisite software (see page 59).

4. Install CA Access Control Enterprise Management (see page 61).

   CA Access Control Enterprise Management also installs the following:

   - Enterprise Management Server
   - CA Access Control
   - Enterprise reporting service
   - Distribution Server

   Important! You must specify an embedded user store when you install CA Access Control Enterprise Management.

5. Update the database schema by running the supplied scripts if the reporting database schema is not identical to the schema on CA Access Control Enterprise Management.

6. (Optional) Configure secure communication for JBoss (see page 70).

7. Disable the DMS and DH on CA Access Control Enterprise Management. Run the following command:

   ```
   dmsmgr -remove -auto
   ```

   Important! Complete this step only if the DMS is installed on a separate computer than CA Access Control Enterprise Management.

   Note: After upgrading the existing DMS is no longer available. Upgrade the DMS after installing the new Enterprise Management Server. For more information about the dmsmgr utility, see the *Reference Guide*.

   The new CA Access Control Enterprise Management Server is installed. You must now upgrade the DMS and Distribution Host before you start CA Access Control Enterprise Management.

Encrypt Passwords in AES Encryption Method

In CA Access Control r12.0 SP1, passwords were encrypted using the RC2 encryption method. In CA Access Control r12.5 SP1,the password encryption method was changed to AES. Therefore, passwords that were encrypted using RC2 encryption method cannot work in newer versions of CA Access Control. To solve this problem, you encrypt the existing passwords in AES after you upgrade from CA Access Control r12.0SP1.

To encrypt passwords in AES encryption method

1. If you have not already done so, install CA Access Control Enterprise Management.
2. Stop all the CA Access Control services.
3. Do the following:
   a. Connect to the Enterprise Management Server database as a user with read and write access privileges.
   b. Run the following query to remove the password CA Access Control Enterprise Management use to connect to the user store:

      ```
      update IM_DIR_CONNECTION set password=null where connection_name='java:/userstore';
      ```
4. Encrypt all the passwords in the database using the pwdtools utility.

   For each entry in the tlbusers table, change the password with the encrypted passwords that you generate.
5. Remove the DMS settings from the connection table. Run the following query:

   ```
   DELETE FROM connection WHERE connection_name='con1';
   ```

   The DMS connection settings are removed from the database.
6. Start CA Access Control Enterprise Management.
7. Configure the DMS connection settings in CA Access Control Enterprise Management.

   Note:For more information about the DMS connection settings, see the *Online Help*.

Example: Encrypt passwords using the pwdtools utility

This example shows you how to encrypt a user password in AES encryption mode using the pwdtools utility and set the encrypted password in the Enterprise Management Server database.

1. Open the pwdtool.bat for editing. The file is located in the following directory, where *ACServerInstallDir* is the directory where the Enterprise Management Server is installed:

   ACServerInstallDir\IAM_Suite\Access_Control\tools\PasswordTool\

2. Enter the JAVA_HOME path in the "::SET JAVA_HOME=<enter valid java home here>" token. For example:

   SET JAVA_HOME=C:\jdk1.5.0

3. From a command-line window, run the following command, where *password* is a clear text password and *JBOSS_Home* is the directory where JBoss is installed:

   pwdtools -FIPS -p <"*password*"> -k
   JBOSS_HOME\server\default\deploy\IdentityMinder.ear\config\com\netegrity\config\keys\FIPSkey.dat

   The encrypted password is displayed. Copy the password to a clipboard.

4. Connect to the Enterprise Management Server as a user with read and write access rights to the database.

5. Run the following query where *encrypted password* is the encrypted password that you previously copied to a clipboard and *username* is the name of the user account:

   update tblusers set password = '<encrypted password>' where loginid='<username>';

   You have set the account password with an encrypted password.

Upgrade the DMS

After installing the new CA Access Control Enterprise Management Server, you must upgrade the existing DMS. You do not need to remove the existing installation of the DMS before upgrading.

Important! Complete this step only if the DMS is installed on a separate computer than CA Access Control Enterprise Management.

To upgrade the DMS, install CA Access Control on the DMS computer (see page 95).

You can now configure CA Access Control Enterprise Management to connect to the DMS.

Upgrade the Distribution Host (DH)

After successfully upgrading the DMS, you must upgrade the Distribution Host (DH). You upgrade the DH by installing the Distribution Server on every computer that is running the Distribution Host. After installing the Distribution Server, you must configure the Message Queue routing settings to establish routes for sending and receiving messages between the Distribution Server and CA Access Control Enterprise Management.

Important! Complete this step only if the DH is installed on a separate computer than CA Access Control Enterprise Management.

To upgrade the distribution host

1. Install the Distribution Server on the DH computer (see page 352).

   The Distribution Server installs the Java Connector Server (JCS), the DH, and the Message Queue.

2. Define the Message Queue routing settings (see page 364) between the Distribution Server and CA Access Control Enterprise Management.

   The Distribution Server is now configured.

Subscribe a DH to a DMS

When you create a new DH, you must subscribe it to the DMS.

If you are upgrading from r12.0 SP1, once you have completed upgrading CA Access Control Enterprise Management components, you cannot continue working with the previous DMS. You must configure the upgraded DH to work with the new DMS before starting CA Access Control Enterprise Management.

Important! If you are upgrading from r12.0 SP1, complete this step only if you installed the Distribution Server on the Report Server computer.

To subscribe a DH to a DMS

1. Open a command prompt window on the Distribution Server.
2. Subscribe the new DMS with the Distribution Host.

   Example: sepmd -s *DH__WRITER DMS__@<entm>*
3. Add the new DMS as the Distribution Host parent.

   Example: sepmd -s *DMS__ DH__@<host_name>*
4. On the Enterprise Management Server, open a command prompt window and create a new subscriber.

   Example: sepmd -n *DH__@<host_name>*

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

Migrate the Report Server to the Enterprise Reporting Services

The Enterprise Reporting services bundle the Report Server functionality into a single enterprise wide reporting service. Due to architectural changes, the Report Server is now a part of CA Access Control Enterprise Management and is no longer an individual component. You migrate the Report Server by installing Distribution Server on the Report Server and reconfiguring the Message Queue settings.

Note: This migration process lets existing endpoints continue using the Message Queue on the Report Server computer. You do not need to reconfigure the ReportAgent settings on the endpoints after you complete this procedure.

Important! Complete this step only if the Report Server is installed on a separate computer than CA Access Control Enterprise Management.

To migrate the Report Server to Enterprise Reporting services

1. Install the Distribution Server on the Report Server computer (see page 352).
2. Disable the JBoss service.
3. Define Message Queue route settings (see page 364) between the Distribution Server and CA Access Control Enterprise Management.

   The Enterprise Reporting services (including the Report Server) are installed. You can now configure the Enterprise Reporting ser (see page 243)ver components.
4. Subscribe the DH on the new DMS (see page 385).

Upgrade CA Access Control Endpoints

After upgrading CA Access Control Enterprise Management, the DMS, the Distribution Host and the Report Server, you can now upgrade the existing CA Access Control r12.0 SP1 endpoints.

To upgrade CA Access Control endpoints install CA Access Control on the endpoints (see page 95).

How to Configure Message Routing Settings

When working in an environment that consists of a single instance of CA Access Control Enterprise Management and multiple Distribution Servers, you must configure the MQ routing settings on all the Distribution Servers to point to the MQ on the CA Access Control Enterprise Management. This helps ensure that all the messages that the CA Access Control endpoints send are ultimately routed to a single MQ, that is located on the CA Access Control Enterprise Management server.

To route messages from the MQ on every Distribution Server to the CA Access Control Enterprise Management server, do the following:

- On each Distribution Server in your enterprise, do the following:
  - Stop the Message Queue service.
  - Modify the routing to the CA Access Control Enterprise Management Message Queue.
  - Define the parameters of the CA Access Control Enterprise Management Message Queue.
  - Configure the names of the Distribution Server message queues.
  - Specify the location of the CA Access Control Enterprise Management Message Queue.
  - Start the Message Queue service.
- On the CA Access Control Enterprise Management, do the following:
  - Stop the Message Queue service.
  - Modify the routing to the Distribution Server Message Queue.
  - Define the parameters of the Distribution Server Message Queue
  - Configure the names of the CA Access Control Enterprise Management message queues.
  - Specify the location of the CA Access Control Enterprise Management Message Queue
  - Start the Message Queue service.

Note: For information about message routings, refer to the *TIBCO Enterprise Message Server User's Guide*.

More information:

Modify the Message Queue Settings on the Distribution Server (see page 388)
Modify the Message Queue Settings on CA Access Control Enterprise Management (see page 389)
Message Queue Connection Configuration (see page 390)
Configure the Names of the Message Queues on the Distribution Server (see page 395)
Configure the Names of the Message Queues on the CA Access Control Enterprise Management Computer (see page 396)
Message Routing Configuration (see page 396)

Modify the Message Queue Settings on the Distribution Server

By default, every Distribution Server is configured to work with the Message Queue that is running on that server. To route messages to another Message Queue, you must reconfigure the Message Queue settings.

This procedure shows you how to modify the Message Queue settings on the Distribution Server to enable communication with the CA Access Control Enterprise Management Message Queue. Complete this procedure for every Distribution Server in your enterprise.

To modify the Message Queue settings on the Distribution Server

1. Stop the CA Access Control Message Queue service.
2. On the Distribution Server, open the file tibemsd.conf file, located by default in the following directory, where *DistServerInstallDir* is the directory in which you installed the Distribution Server:

   DistServerInstallDir/ACMQ/tibco/ems/bin
3. Enter the Distribution Server short host name in the 'server' parameter.
4. Change the 'routing' parameter value to enabled.
5. Start the CA Access Control Message Queue service.

   You have modified the message queue settings on the Distribution Server.

Note: For information about message routings, see the *TIBCO Enterprise Message Server User's Guide*.

Example: tibemsd.conf file

The example shows you a snippet from the tibemsd.conf file after you modify the routing settings for a Distribution Server named DS_Example:

```
########################
# Server Identification Information.
# server:    unique server name
# password:  password used to login into other routed server
########################
server              = DS_Example
password            =
########################
…
########################
# Routing. Routes configuration is in 'routes.conf'. This enables or
# disables routing functionality for this server.
########################
routing             = enabled
########################
```

Modify the Message Queue Settings on CA Access Control Enterprise Management

This procedure shows you how to modify the Message Queue settings on CA Access Control Enterprise Management to enable communication with the Distribution Server.

To modify the Message Queue settings on CA Access Control Enterprise Management

1. Stop the CA Access Control Message Queue service.
2. On CA Access Control Enterprise Management, open the tibemsd.conf file for editing. This file is located in the following directory by default, where *DistServerInstallDir* is the directory in which you installed the Distribution Server:

   DistServerInstallDir/ACMQ/tibco/ems/bin
3. Enter the CA Access Control Enterprise Management server short host name, not separated by dots, in the 'server' parameter.
4. Change the 'routing' parameter value to enabled.
5. Start the CA Access Control Message Queue service.

   You have modified the message queue settings on CA Access Control Enterprise Management.

Note: For information about message routings, refer to the *TIBCO Enterprise Message Server User's Guide*.

Example: tibemsd.conf file

The example shows you a snippet from the tibemsd.conf file after you modify the routing settings for a CA Access Control Enterprise Management Server named ENTM_Example:

```
########################
# Server Identification Information.
# server:    unique server name
# password:  password used to login into other routed server
########################
server              = ENTM_Example
password            =
########################
…
########################
# Routing. Routes configuration is in 'routes.conf'. This enables or
# disables routing functionality for this server.
########################
routing             = enabled
########################
```

Message Queue Connection Configuration

To route messages from the Message Queue on the Distribution Server to the Enterprise Management Server conversely, you modify the existing Message Queue settings in your enterprise.

Example: Configuring the Message Queue Connection Settings on the Distribution Server

This example shows you how to configure the Message Queue server settings on the Distribution Server. You configure the Message Queue to send messages to the Enterprise Management Server by defining the parameters of the Message Queue that is running on the Enterprise Management Server.

To configure the Message Queue connection settings on the Distribution Server

1. On the Distribution Server, do one of the following:
   - (Windows 2003 Server) Select Start, Programs, TIBCO, TIBCO EMS 4.4.1, Start EMS Administration Tool.
   - (UNIX) Do the following:
     a. Navigate to the following directory, where *DistServerInstallDir* is the directory in which you installed the Distribution Server:

        DistServerInstallDir/MessageQueue/tibco/ems/bin

     b. Run the following command:

        tibemsadmin

        The TIBCO EMS Administration Tool command prompt window opens.
2. Connect to the Message Queue using either of the following:
   - Enter the following command to connect using SSL:

     connect ssl://localhost:7243
   - Enter the following command to connect using TCP:

     connect tcp://localhost:7222

   A login name prompt appears.
3. Enter **admin**.

   A password prompt appears.
4. Enter the password that you provided when you installed the Distribution Server.
5. When prompted, enter a new password for the Message Queue server.
6. Define the Message Queue password.

   set server password=

   Example: set server password=<*C0mp1ex*>

7. Create a user named ENTM-NAME and assign a password to the user.

   create user ENTM-NAME password=*acserver_user-passwd*

   Example: create user EMS-SERVER password=<*acserver_user-passwd*>

   Important! Specify the same name that you defined in the 'server' parameter of the tibemsdf.conf file on the Enterprise Management Server.

8. Do the following:

   a. Enter the following command:

      add member ac_server_users *ENTM_NAME*

      The user you created is added to the ac_server_users group.

   b. Enter the following command:

      add member ac_endpoint_users *ENTM_NAME*

      The user you created is added to the ac_endpoint_users group.

   c. Enter the following command:

      add member report_publishers *ENTM_NAME*

      The user you created is granted permissions to read and publish messages to CA Access Control queues.

9. Restart the Distribution Server.

   The changes you made are applied.

Example: Configure the Message Queue Connection Settings on CA Access Control Enterprise Management

This example shows you how to configure the Message Queue server settings on the Enterprise Management Server. You configure the Message Queue to send messages to the Distribution Server.

In this example the term *DS-NAME* relates to the name of the Distribution Server computer and the term *ENTM-NAME* relates to name of the Enterprise Management Server. When you define the message queue server settings, you replace the name with the server actual names, as defined in the 'server' token in the *tibemsd.conf* file.

To configure the Message Queue connection settings on CA Access Control Enterprise Management

1. On the CA Access Control Enterprise Management computer, do one of the following:
   - (Windows 2003 Server) Select Start, Programs, TIBCO, TIBCO EMS 4.4.1, Start EMS Administration Tool.
   - (UNIX) Do the following:
     a. Navigate to the following directory, where *ACServerInstallDir* is the directory in which you installed CA Access Control Enterprise Management:

     ACServerInstallDir/MessageQueue/tibco/ems/bin

     b. Run the following command:

     tibemsadmin

     The TIBCO EMS Administration Tool command prompt window opens.
2. Connect to the Message Queue using either of the following:
   - Enter the following command to connect using SSL:

     connect ssl://localhost:7243
   - Enter the following command to connect using TCP:

     connect tcp://localhost:7222

   A login name prompt appears.
3. Enter **admin**.

   A password prompt appears.
4. Enter the password that you provided when you installed the Enterprise Management Server.

5. Define the Message Queue password.

   set server password=*entm_server-passwd*

   Example: set server password=<*ENTM_SERVER_NAME-passwd*>

6. For each Distribution Server, create a user named DS-NAME and assign a password to the user.

   create user DS-NAME password=*dist_server_user*

   Example: create user EMS-Server password=<*C0mp1ex*>

   Important! Specify the same name that you defined in the 'server' parameter of the tibemsdf.conf file on the Enterprise Management Server.

7. Do the following:

   a. Enter the following command:

      add member ac_server_users *DS_NAME*

      The user you created is added to the ac_server_users group.

   b. Enter the following command:

      add member ac_endpoint_users *DS_NAME*

      The user you created is added to the ac_endpoint_users group.

   c. Enter the following command.

      add member report_publishers *DS_NAME*

      The user you created is granted permissions to read and publish messages to CA Access Control queues.

8. Restart the Distribution Server for the changes to take effect.

   You have configured the message queue connection settings on CA Access Control Enterprise Management.

   Note: For information about message routings, see the *TIBCO Enterprise Message Server User's Guide*.

Configure the Names of the Message Queues on the Distribution Server

To forward messages from the Distribution Server to CA Access Control Enterprise Management, configure each messages route to forward the messages from the Message Queue on the Distribution Server to the Message Queue on CA Access Control Enterprise Management.

In this procedure you define the message queue settings on the Distribution Server. You modify the message queue settings file to provide the settings of the Message Queue on CA Access Control Enterprise Management.

To configure the names of the Message Queue on the Distribution Server

1. On the Distribution Server, open the file queues.conf. The file is located by default in the following directory, where *DistServerInstallDir* is the directory in which you installed the Distribution Server:

   DistServerInstallDir/ACMQ/tibco/ems/bin

2. Locate the queue named 'queue/snapshots' and add the ENTM-NAME value at the end of the queue name, preceded by a @ sign as follows:

   queue/snapshots@*ENTM-NAME*

   ENTM-NAME

   Defines the short name of the CA Access Control Enterprise Management computer.

   Important! Specify the same name that you defined in the 'server' parameter of the tibemsd.conf file on CA Access Control Enterprise Management.

3. Locate the queue name 'queue/audit' and add the ENTM-NAME value at the end of the queue name, preceded by a @ sign as follows:

   queue/audit@*ENTM-NAME*

4. Locate the queue named 'ac_endpoint_to_server' and add the ENTM-NAME value at the end of the queue name, preceded by a @ sign as follows:

   ac_endpoint_to_server@*ENTM-NAME*

5. Locate the queue named 'ac_server_to_endpoint' and add the ENTM-NAME value at th end of the queue name, preceded by a @ sign as follows:

   ac_server_to_endpoint@*ENTM-NAME*

6. Save and close the file.

Note: For information about message routings, see the *TIBCO Enterprise Message Server User's Guide*.

Configure the Names of the Message Queues on the CA Access Control Enterprise Management Computer

In this procedure you define the message routing settings on CA Access Control Enterprise Management. You configure the Message Queue settings on CA Access Control Enterprise Management to identify this Message Queue as the primary server.

To configure the names of the Message Queues on the CA Access Control Enterprise Management computer

1. On CA Access Control Enterprise Management, open the file queues.conf in an editable form. The file is located by default in the following directory, where *ACServerInstallDir* is the directory in which you installed CA Access Control Enterprise Management:

   ACServerInstallDir/MessageQueue/tibco/ems/bin

2. Locate the queue named 'queue/snapshots' and add the word 'global' after the word 'secure' at the end of the queue name, as follows:

   queue/snapshot secure, global

3. Locate the queue named 'queue/audit' and add the word 'global' after the word 'secure' at the end of the queue name, as follows:

   queue/audit secure, global

4. Locate the queue named 'ac_endpoint_to_server' and add the word 'global' after the word 'secure' at the end of the queue name, as follows:

   ac_endpoint_to_server secure, global

5. Locate the queue named 'ac_server_to_endpoint' and add the word 'global' after the word 'secure' at the end of the queue name, as follows:

   ac_server_to_endpoint secure, global

6. Save and close the file.

Note: For information about message routings, refer to the *TIBCO Enterprise Message Server User's Guide*.

Message Routing Configuration

After you have configured the Message Queue settings and configured the message queue routing settings on the Distribution Server and CA Access Control Enterprise Management, you set up the message routes on the Distribution Server and CA Access Control Enterprise Management.

Example: Set Up Message Routes on the Distribution Server

This example shows you how to set up the message route settings on the Distribution Server. You set up a route between the Distribution Server and CA Access Control Enterprise Management to route messages arriving from CA Access Control endpoints to the Message Queue on CA Access Control Enterprise Management. Complete this procedure on every Distribution Server in your enterprise.

1. On the Distribution Server, open the file routes.conf for editing. The file is located by default in the following directory, where *DistServerInstallDir* is the directory in which you installed the Distribution Server:

   DistServerInstallDir/MessageQueue/tibco/ems/bin

2. Add the following entries:

   ```
   [ENTM-NAME]
   url        = ENTM-URL
   ssl_verify_host = disabled
   ssl_verify_hostname = disabled
   ```

   ENTM-NAME

   Defines the short name of the CA Access Control Enterprise Management computer.

   ENTM_URL

   Defines the CA Access Control Enterprise Management URL.

3. Save the file.
4. Restart the CA Access Control Message Queue service.

Example: Set Up Message Routes on CA Access Control Enterprise Management

This example shows you how to set up the message route settings on CA Access Control Enterprise Management. You set up a route between CA Access Control Enterprise Management and the Distribution Server to send messages from CA Access Control Enterprise Management to the Distribution Server and from there to the endpoints.

1. On CA Access Control Enterprise Management, open the file routes.conf. The file is located by default in the following directory, where *ACServerInstallDir* is the directory in which you installed CA Access Control Enterprise Management:

   ACServerInstallDir/MessageQueue/tibco/ems/bin

2. Add the following entries:

   [DS-NAME]

   url = DS-URL

   ssl_verify_host = disabled

   ssl_verify_hostname = disabled

   DS_NAME

   Defines the short name of the Distribution Server.

   DS_URL

   Defines the Distribution Server URL.

3. Save the file.
4. Restart the CA Access Control Message Queue service.

Note: For information about message routings, refer to the *TIBCO Enterprise Message Server User's Guide*.

Appendix A: Changing Communication Encryption Methods

This section contains the following topics:

Communication Encryption

You can use the following methods to encrypt communication between CA Access Control components and to encrypt CA Access Control client/server communication:

- Symmetric encryption
- SSL

Symmetric Encryption

CA Access Control uses encryption libraries to implement symmetric (standard) encryption. You can use the following methods to encrypt communication between CA Access Control components:

- Default (proprietary) encryption
- AES128
- AES192
- AES256
- DES
- 3DES

Note: The encryption method named default is not the default CA Access Control encryption method. The default encryption method is AES256.

When you install CA Access Control, the installer stores the encryption libraries in the following directory, where *ACInstallDir* is the directory in which you installed CA Access Control:

- (Windows) *ACInstallDir*\bin
- (UNIX) *ACInstallDir*/lib

On Windows, CA Access Control 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 401)
Change the Symmetric Encryption Method (see page 402)

How sechkey Configures Symmetric Encyption

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 Access Control 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 Access Control database, including CA Access Control Message Queue passwords and, if CA Access Control 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 Access Control API to create a program that communicates with CA Access Control, the communication for the new program is encrypted with the same key.

Change the Symmetric Encryption Key

Symmetric encryption keys protect communication between CA Access Control 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 Access Control components.

To change the symmetric encryption key

1. Stop CA Access Control.

   If you are changing the encryption settings on a CA Access Control Enterprise Management server, also stop the CA Access Control 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 Access Control.

   If you are changing the encryption settings on a CA Access Control Enterprise Management server, also start the CA Access Control Web Service.

   CA Access Control 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 Access Control 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 Access Control 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 Access Control is operating in FIPS-only mode, you cannot change the symmetric encryption method. CA Access Control 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 Access Control components.

To change the symmetric encryption method

1. Stop CA Access Control.

   If you are changing the encryption settings on a CA Access Control Enterprise Management server, also stop the CA Access Control Web Service.

2. Use the sechkey utility to change the symmetric encryption method.

3. Start CA Access Control.

   If you are changing the encryption settings on a CA Access Control Enterprise Management server, also start the CA Access Control Web Service.

   CA Access Control 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*.

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 Access Control:

- The default CA Access Control root certificate
- A third-party root certificate, including a password-protected certificate

The server certificate encrypts and authenticates CA Access Control client/server communication and communication between CA Access Control components. You can use the following types of server certificate in CA Access Control:

- The default CA Access Control server certificate
- A third-party server certificate, including a password-protected certificate
- A CA Access Control server certificate created from a third-party root certificate

Enable SSL Encryption

You configure encryption settings when you install CA Access Control. 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 Access Control components.

To enable SSL encryption

1. Stop CA Access Control.

   If you are changing the encryption settings on a CA Access Control Enterprise Management Server, also stop the CA Access Control 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 Access Control components.

   Note: If you specify this value, CA Access Control uses SSL encryption each time that it tries to communicate with another CA Access Control component. If SSL fails, it then uses symmetric encryption. This value lets you migrate your CA Access Control 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 Access Control components that use SSL encryption.

   Note: (Windows) If you are working with a third-party program that uses the CA Access Control SDK, the crypto section is located at the CA Access Control 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 407).
   - Use a server certificate you generate from a third-party root certificate (see page 409).

   Note: If you do not configure SSL encryption further, you can use the default CA Access Control X.509 certificates to encrypt and authenticate communication between CA Access Control components. However, we recommend that you change the default certificates instead.

4. Start CA Access Control:
   - If you are changing the encryption settings on a CA Access Control Enterprise Management Server, also start the CA Access Control Web Service.
   - If you are working with a third-party program that uses the CA Access Control SDK, restart the process that uses the CA Access Control 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 Access Control 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 Access Control 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 Access Control 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 Access Control 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 Access Control 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 Access Control 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 Access Control can use the stored password to open the private key:

      sechkey -g -verify

      If CA Access Control 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 Access Control:
   - If you are changing the encryption settings on a CA Access Control Enterprise Management Server, also start the CA Access Control Web Service.
   - If you are working with a third-party program that uses the CA Access Control SDK, restart the process that uses the CA Access Control 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 Access Control components.

You can create a password-protected server certificate; if you do, CA Access Control 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 Access Control 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 Access Control 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 Access Control:

   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 Access Control 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 Access Control 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 Access Control:

   - If you are changing the encryption settings on a CA Access Control Enterprise Management Server, also start the CA Access Control Web Service.
   - If you are working with a third-party program that uses the CA Access Control SDK, restart the process that uses the CA Access Control 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 Access Control 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 Access Control to use a password-protected server certificate; if you do, CA Access Control uses a specified password to protect the private key for the server certificate. CA Access Control stores the password in the crypto.dat file in the *ACInstallDir*/Data/crypto directory, where *ACInstallDir* is the directory in which you installed CA Access Control. The crypto.dat file is hidden, encrypted, read-only, and protected by CA Access Control. If CA Access Control is stopped, only the superuser can access the password.

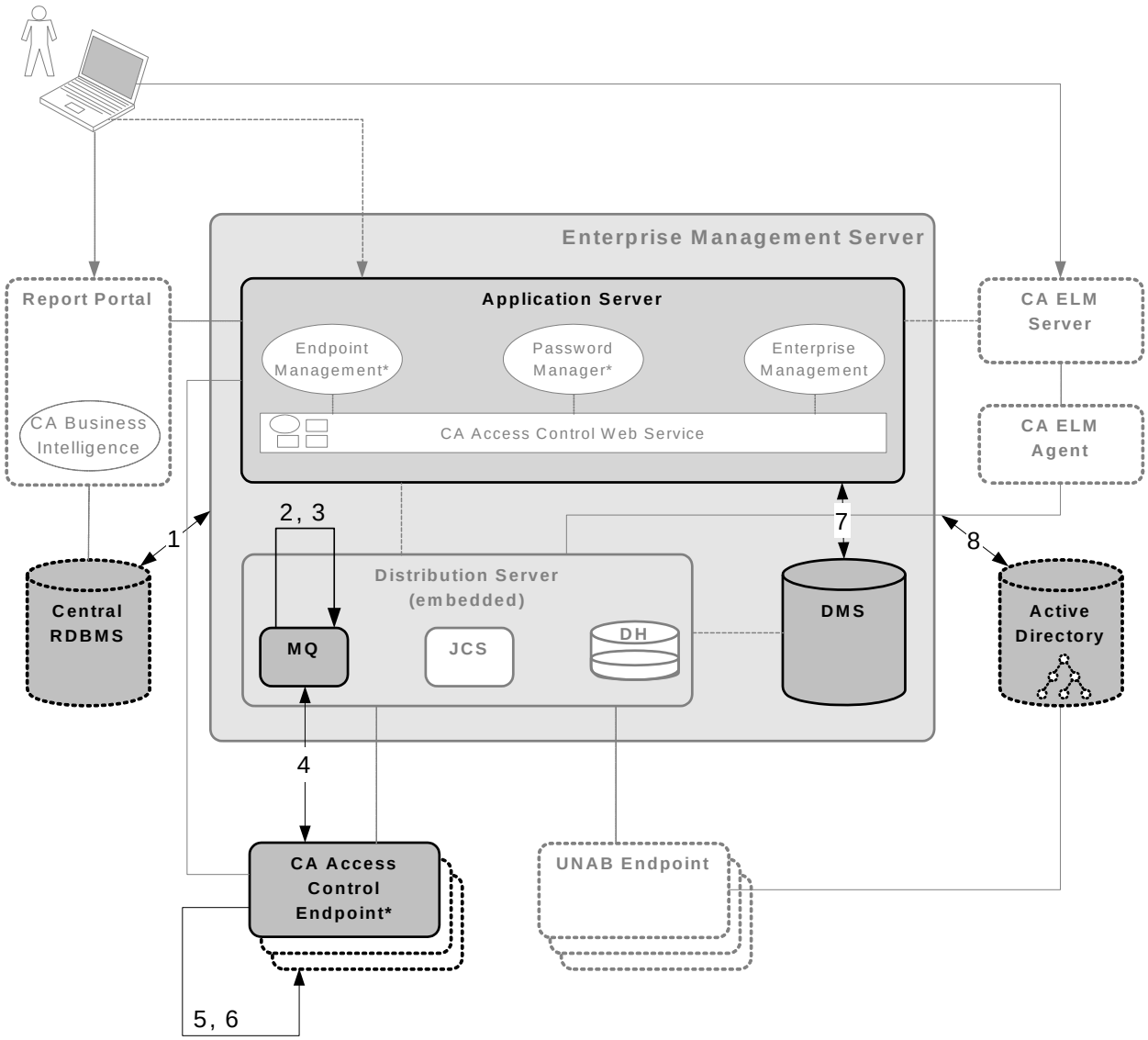
If you create a password-protected server certificate, sechkey does not encrypt the certificate. If you create a server certificate that is not password-protected, sechkey encrypts the certificate using AES256 and the CA Access Control encryption key.

Appendix B: Changing CA Access Control Service Account Settings

This section contains the following topics:

How CA Access Control Service Accounts Interact with CA Access Control Components

The following diagram shows how the service accounts interact with various CA Access Control 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 Access Control 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 Access Control 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 Access Control 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 Access Control Enterprise Management.

Service Account Passwords

In most cases, you set the password for CA Access Control service accounts when you install CA Access Control 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 Access Control 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 Access Control Enterprise Management, and you provide the account name and password, along with other database information, when you install CA Access Control 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 435).

   c. Change the password in the login-config.xml file (see page 437).

   d. Restart JBoss Appplication Server.

   e. Verify that you can log in to CA Access Control 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">}>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 Access Control Enterprise Management and the DMS use the reportserver account to connect to the Message Queue.

CA Access Control Enterprise Management uses the reportserver account to do the following:

- Send reporting data to CA Enterprise Log Manager
- Send UNAB remote migration commands
- Provide privileged account passwords to the PUPM Agent on PUPM endpoints
- Receive reporting data from CA Access Control 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 Access Control 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 433).

   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 435).

   c. Change the password in the properties-service.xml file (see page 436).

   d. Change the password in the login-config.xml file (see page 437).

   e. Restart JBoss Application Server.

   f. Verify that you can log in to CA Access Control 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 432).

   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=}>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">}>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, PUPM 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 Access Control 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 Access Control 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 433).

   The +reportagent password is changed on the Message Queue.

2. Use sechkey to change the password (see page 432) 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 Access Control database (seosdb), and sends a heartbeat to the DH at regular intervals. CA Access Control 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 Access Control 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 Access Control database.

Important! To prevent this user from logging in to the CA Access Control 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 431).

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 Access Control 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 Access Control 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 Access Control database.

Important! To prevent this user from logging in to the CA Access Control 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 431).

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 Access Control 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 431).
2. In CA Access Control 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 Access Control 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> host DMS__@example.com
(DMS__@example.com)
Successfully connected
AC> cu ac_entm_pers password("secret") grace- nonative
(localhost)
Successfully updated USER ac_entm_pers
```

Change the ADS_LDAP_bind_user Password

The ADS_LDAP_bind_user account lets CA Access Control 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 Access Control 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 Access Control 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 Identity Manager Management Console (see page 439).

   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 Access Control 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/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 Access Control 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.TibjmsInitialContextFactory
                        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 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 Access Control Enterprise Management and the DMS use to connect to the Message Queue

  Note: CA Access Control Enterprise Management and the DMS use the reportserver service account to connect to the Message Queue.

More information:

Change the +reportagent Password (see page 419)
Change the reportserver Password (see page 416)

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 Access Control 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.

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 433).

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 Access Control endpoints and CA Access Control Enterprise Management.

To change the Message Queue server certificate

1. Stop the CA Access Control 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 Access Control 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 Access Control 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 Access Control 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 Access Control 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.

Password Change Procedures

The following procedures explain the different ways in which you can change CA Access Control 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 420)
Change the +devcalc Password (see page 421)
Change the ac_entm_pers Password (see page 422)

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 Access Control 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 reportserver Password (see page 416)
Change the +reportagent Password (see page 419)

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 Access Control 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 reportserver Password (see page 416)
Change the +reportagent Password (see page 419)

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 Access Control 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\config\keys\FIPSkey.dat"
```

More information:

Change the RDBMS_service_user Password (see page 414)
Change the reportserver Password (see page 416)

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=}>8:Jt^+%INK&i^v
</attribute>
```

More information:

Change the reportserver Password (see page 416)

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 Access Control 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">}>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">}>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 RDBMS_service_user Password (see page 414)
Change the reportserver Password (see page 416)

Change the User Directory Password in the CA Identity Manager Management Console

You change the user directory password in the CA Identity Manager 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 Identity Manager Management Console

1. Encrypt the clear text password (see page 435).
2. Open the CA Identity Manager Management Console (see page 80).
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 Identity Manager 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 Identity Manager 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 Identity Manager Management Console (see page 80)
Open the CA Identity Manager Management Console (see page 80)
Change the ADS_LDAP_bind_user Password (see page 423)