CA Access Control Premium Edition

Implementation Guide

r12.0 SP1

Third Edition

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 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
Between braces ({})	Set of mandatory operands

Format	Meaning
Choices separated by pipe (|).	Separates alternative operands (choose one). For example, the following means *either* a user name *or* a group name: {*username*|*groupname*}
...	Indicates that the preceding item or group of items can be repeated
<u>Underline</u>	Default values
A backslash at end of line preceded by a space (\\)	Sometimes a command does not fit on a single line in this guide. In these cases, a space followed by a backslash (\\) at the end of a line indicates that the command continues on the following line. **Note:** Avoid copying the backslash character and omit the line break. These are not part of the actual command syntax.

Example: Command Notation Conventions

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

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

In this example:

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

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/support.

Documentation Changes

The following documentation updates have been made since the r12.0 release of this documentation:

Third Edition

The third edition of this documentation was released with CA Access Control r12.0 SP1 CR1.

- Installation Notes (see page 43)—Updated topic provides installation considerations for CA Access Control 64-bit binaries on a Linux x86 64-bit computer.
- Uninstall Silently (see page 125)—Updated topic provides the new command to silently uninstall CA Access Control from a Windows endpoint.
- When to Restore a DH (see page 232)—Updated topic adds information about the DH_Writer.
- How to Recover from a Disaster (see page 234)—Updated topic adds an optional step to the disaster recovery process.
- Back Up the DMS Using sepmd (see page 235)—Updated topic adds a recommendation to truncate the updates.dat file before you back up the DMS.
- Back Up the DMS Using selang (see page 236)—Updated topic adds a recommendation to truncate the updates.dat file before you back up the DMS.
- Restore the Production DMS (see page 237)—Updated topic corrects the parameters that you use in the dmsmgr -restore function.
- Restore the Disaster Recovery DMS (see page 238)—Updated topic corrects the parameters that you use in the dmsmgr -restore function.
- Restore a DH (see page 239)—Updated topic adds information about the DH_Writer.

Second Edition

The second edition of the documentation was released to coincide with the GA announcement of r12.0 SP1.

- Coexistence with Other Products (see page 110)—New topic describes coexistence issues you should consider before you install CA Access Control on a Windows endpoint.
- Integrating with CA Enterprise Log Manager (see page 201)—New chapter describes how you integrate CA Enterprise Log Manager with CA Access Control.
- Migrating PMDs to an Advanced Policy Management Environment (see page 241)—New chapter describes how you migrate your Policy Models to an advanced policy management environment.

First Edition

The first edition of this documentation was released on the CA Access Control r12.0 SP1 media.

- Installing and Customizing a UNIX Endpoint (see page 41)—Changes to this chapter include:
  - Native Installations (see page 47)—Updated existing package customization script and procedure topics in this section with syntax and steps for reviewing and accepting the license agreement. These changes apply to RPM, Solaris, HP-UX, and AIX native packages. Additional changes in this section:
    - Install RPM Packages (see page 49)—Updated existing topic with a new example that illustrates how you upgrade from r8 SP1.
    - Customize the RPM Packages (see page 52)—Updated existing topic with steps for customizing the package for an upgrade from r8 SP1.
    - customize_eac_rpm Command (see page 53)—Updated existing topic with syntax for upgrading from r8 SP1, and for setting the temporary installation directory.
    - customize_eac_pkg Command (see page 59)—Updated existing topic with syntax for setting the temporary installation directory.
  - install_base Command (see page 76)—Updated existing topic with corrected information for command options and with an explanation of how you specify the Shared Secret that secures SSL communication between the Report Agent and the Report Server in a silent installation.
  - How the install_base Script Works (see page 81)—Updated existing topic with r12.0 SP1 changes.

  - Trace Filter File (see page 91)—Updated existing topic to explain that the file is no longer used to filter out audit records generated by user traces.
  - Install on a Solaris Branded Zone (see page 101)—New topic describes the procedure for installing on a Solaris branded zone.
- Installing and Customizing a Windows Endpoint (see page 105)—Changes to this chapter include:
  - Installation Worksheets (see page 112)—Updated existing section with r12.0 SP1 installation changes.
  - Uninstall Silently (see page 125)—Updated existing topic with r12.0 SP1 instructions for a silent uninstall.
  - setup Command (see page 125)—Updated existing topic with options that were missing in the previous release of the documentation and with new r12.0 SP1 options.
- Installing Endpoint Management (see page 137)—Changes to this chapter include:
  - Install CA Access Control Endpoint Management Using a Graphical Interface (see page 139)—Updated existing topic with the information you need to supply during installation.
  - Install CA Access Control Endpoint Management Using a Console (see page 141)—New topic describes the procedure for using the new console installation.
  - Uninstall CA Access Control Endpoint Management on Windows (see page 142)—New topic describes how you uninstall CA Access Control Endpoint Management on Windows.
  - Uninstall CA Access Control Endpoint Management on Solaris (see page 143)—New topic describes how you uninstall CA Access Control Endpoint Management on Solaris.
- Installing Enterprise Management (see page 147)—Changes to this chapter include:
  - Install CA Access Control Enterprise Management Using a Graphical Interface (see page 159)—Updated existing topic with the information you need to supply during installation.
  - Install CA Access Control Enterprise Management Using a Console (see page 162)—New topic describes the procedure for using the new console installation.

- Uninstall CA Access Control Enterprise Management on Windows (see page 165)—New topic describes how you uninstall CA Access Control Enterprise Management on Windows.
- Uninstall CA Access Control Enterprise Management on Solaris (see page 166)—New topic describes how you uninstall CA Access Control Enterprise Management on Solaris.

- Installing Enterprise Reporting (see page 171)—Changes to this chapter include:
  - How to Set Up Reporting Service Server Components (see page 173)—Changed title and updated existing topic to better explain how you set up the reporting service server components.
  - Install and Configure an RDBMS as a Central Database (see page 174)—New topics describes the procedure for installing an RDBMS as your central database.
  - How to Set Up the Report Server Computer (see page 176)—New topic describes how you set up the Report Server. This section also has new topics that describe upgrades and graphical and console installations and uninstallations of the Report Server.
  - How to Set Up the Report Portal Computer (see page 183)—New topic describes how you set up the Report Server.
  - Report Package Deployment (see page 189)—New topic describes Report Package deployment. This section also has new topics that describe Report Package deployment procedures for Windows, Solaris, and an r12.0-supplied Report Portal.
  - Received "Null page" Error in InfoView (see page 196)—Updated existing topic with the instructions you need to restart BusinessObjects services.
  - Configure an Endpoint for Reporting (see page 199)—Updated existing topic with an example that illustrates the procedure.
- Installing a Disaster Recovery Deployment (see page 219)—New chapter describes how you install a disaster recovery deployment for advanced policy management components.

Contents

Chapter 5: Installing Endpoint Management 137

Chapter 6: Installing Enterprise Management 147

Chapter 7: Installing Enterprise Reporting 171

Chapter 10: Migrating PMDs to an Advanced Policy Management Environment 241

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

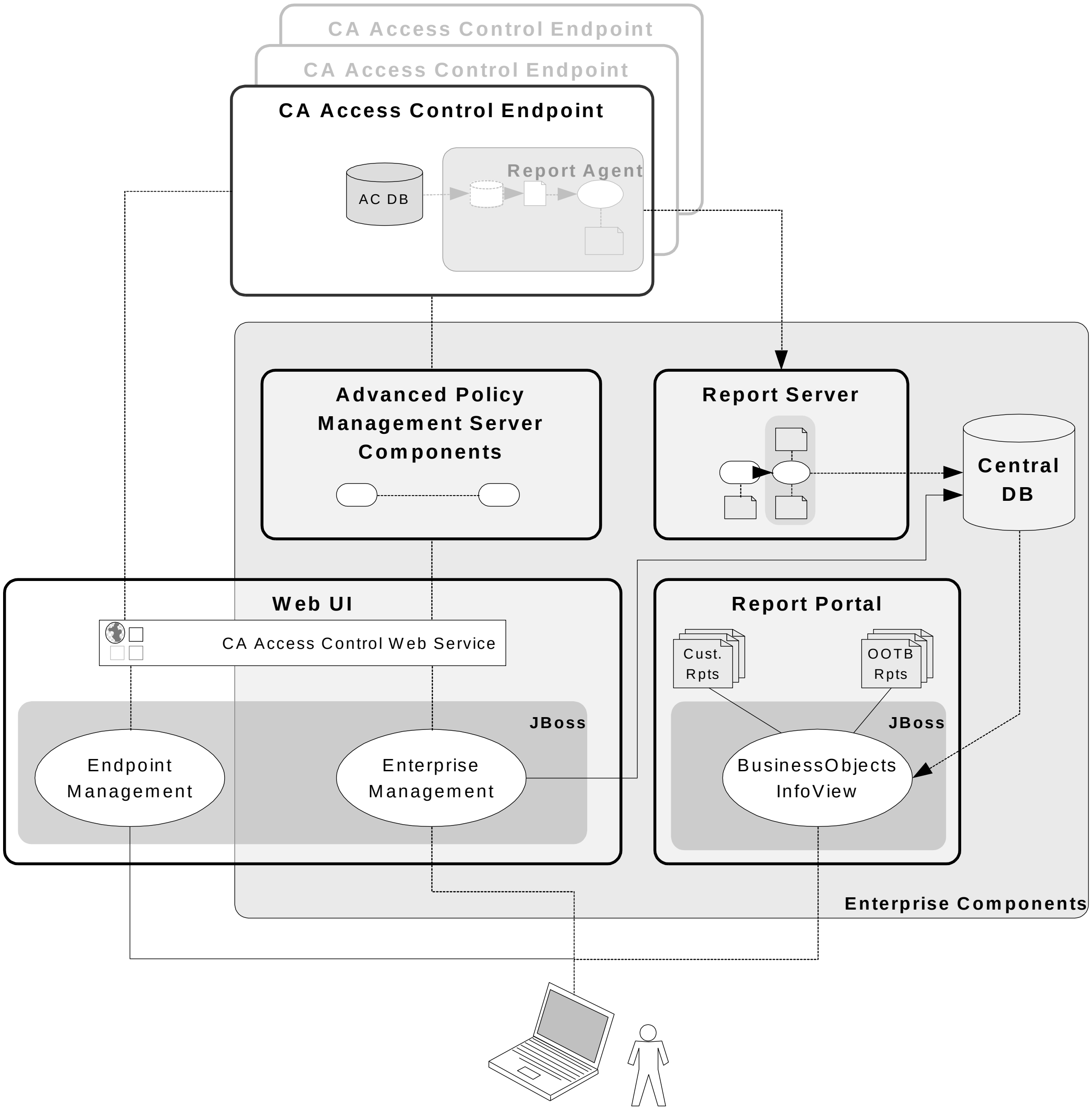
Before you install CA Access Control, you should decide what features of the software you want to use. You can use:

- 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.
- 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.
- 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.

- 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:



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.

For instance, a regular user responsible for printing can be given the ability to bring the spooler service up and down.

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. The tasks of administration can be given to other users, whose accounts are not automatically known.

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 modify the password settings of other users. A password manager cannot change other settings of users. This type of user is not found in the native OS.

Group password managers

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

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 is 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 29)

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
- Whom to define as system administrators, group administrators, password managers, and group password managers

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 Windows 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.

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 manage the password functions of the members of the group.

Security Policies and Groups

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

- What groups to create
- 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 global 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 by security level checking, assign a security level to the resource's record.

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

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.

To allow a user access to resources protected by security category checking, assign one or more security categories to the user's record.

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.

securityLevel

Specifies the security level. Specify an integer between 1 and 255.

For example, to define the security label Managers to contain the security categories Sales and Accounts and a security level of 95, enter the following command:

```
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.
  - 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 26).

  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 the only 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 and universal access (_default) rules let you define approach and switch protection policy at any time.

Accessors

An *accessor*, sometimes called an account, 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 name
- A person who is a member of a group that has access authority
- A production process that is associated with a certain user name

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, by specifying a standard set of user properties for a group or by specifying similar access privileges and restrictions.

You can define new users and groups and modify existing users and groups through CA Access Control Endpoint Management.

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:

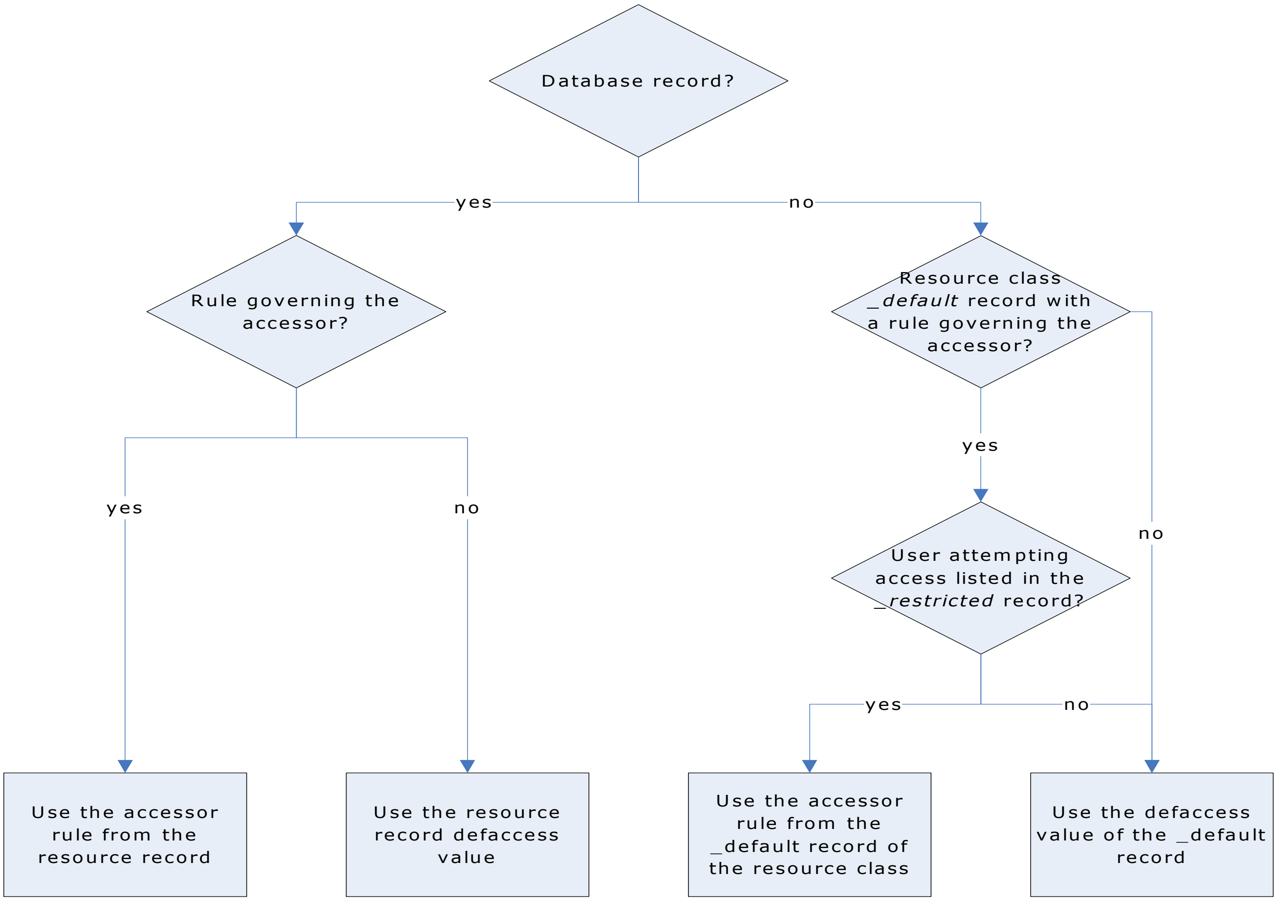
- An access control list (a specific list of the accessors authorized to access the resource and the exact access they can have), also called an ACL
- A negative access control list (a specific list of the accessors for which access should be denied), also called NACL
- A default access for the resource, 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 27).


Database record?
yes
no
Rule governing the accessor?
Resource class _*default* record with a rule governing the accessor?
yes
no
yes
User attempting access listed in the _*restricted* record?
no
yes
no
Use the accessor rule from the resource record
Use the resource record defaccess value
Use the accessor rule from the _default record of the resource class
Use the defaccess value of the _default record

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

Chapter 3: 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 120sp1_CR1_LINUX.tar.Z or 120sp1_CR1_LINUX_RPM.tar.Z installation packages, or later versions of these 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 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: audit-libs, compat-libstdc++, glibc, libgcc, libICE, libSM, libXext, libXp, libXt, ncurses, pam
  - RHEL 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 120_sp1_CR1_LINUX_X64.tar.Z or 120sp1_CR1_LINUX_X64_RPM.tar.Z 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.

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 43)

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
```

Install RPM Packages

To manage the CA Access Control installation with all your other software installations, install the CA Access Control RPM packages. The actual command you need to 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 below.

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.

Note: The following procedure installs CA Access Control with the default settings. Alternatively, you may want to customize the CA Access Control package before installing it.

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, you need to specify the same custom directory for the CAWIN package.

3. (Optional) Customize the *CAeAC* package (see page 52).

   Note: You have to customize the package if you are upgrading from an old eTrust Access Control r8 SP1 package.

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, you must 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, CAWIN package, and CA Access Control package (in that order) using the following commands:

```
cd /mnt/AC_DVD/NativePackages/RPMPackages/LINUX
rpm -U ca-lic*rpm ca-cs-cawin*rpm CAeAC*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) using the following commands:

```
cd /mnt/AC_DVD/NativePackages/RPMPackages/LINUX390
rpm -U ca-lic*rpm ca-cs-cawin*rpm
cp -R /mnt/AC_DVD/NativePackages/RPMPackages/LINUX390 /tmp
chmod 777 /tmp/CAeAC*s390.rpm
../customize_eac_rpm -u /opt/CA   -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
rpm -U --prefix /usr/CA 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 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. You must install the license program and CAWIN to the same custom directory.

Customize the RPM Packages

If you want to install CA Access Control with custom settings using RPM packages, you need to customize the package before you install it. You customize the package by extracting the installation parameters file from the package, modifying it as required, and then loading it back into the package.

Note: Follow the steps in the following procedure to customize any of the CA Access Control RPM packages. We recommend that you do not modify the packages manually. Instead, use the customize_eac_rpm script as described.

To customize the RPM packages

1. Copy the package you want to customize from the /NativePackages/RPMPackages/*OS* directory of the CA Access Control Endpoint Components for UNIX DVD 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. (Optional) Enter the following command to set the language of the installation parameters file:

   customize_eac_rpm -r -l *lang* [-d *pkg_location*] *pkg_filename*

3. (Optional) Enter the following command to upgrade from an eTrust Access Control r8 SP1 package:

   customize_eac_rpm -u *install_prefix* [-d *pkg_location*] *pkg_filename*

4. (Optional) Enter the following command to change the default encryption files:

   customize_eac_rpm -s -c *certfile* -k *keyfile* [-d *pkg_location*] *pkg_filename*

5. Enter the following command to get the installation parameters file:

   customize_eac_rpm -g -f *tmp_params* [-d *pkg_location*] *pkg_filename*

6. 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 token (remove the preceding # character) and point it to post-installation script file you want to run.

7. Enter the following command to 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.

More information:

customize_eac_rpm Command—Customize RPM Package (see page 53)

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 -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 CA Access Control 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 customize_eac_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.

-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
```

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 (see page 74), 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. The CA Access Control packages are particularly suited for installing CA Access Control on all zones across your Solaris 10 system.

Important! To uninstall CA Access Control after a package installation, you must use the *pkgrm* command. Do not use uninstall_AC script.

Install Solaris Native Packages

The CA Access Control Solaris native packages let you install CA Access Control on Solaris easily.

Note: The following procedure installs CA Access Control with the default settings. Alternatively, you may want to customize the CA Access Control package before installing it.

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. 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 CA Access Control 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.

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 CA Access Control package (CAeAC) is located.

   Important! The CA Access Control 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 the Solaris Native Packages

If you want to install CA Access Control with custom settings using Solaris native packaging, you need to customize the package before you install it. You customize the script by extracting the installation parameters file from the package, modifying it as required, and then loading it back into the package.

Note: Follow the steps in the following procedure to customize any of the CA Access Control Solaris packages. We recommend that you do not modify the packages manually. Instead, use the customize_eac_pkg script as described.

To customize the Solaris native packages

1. Extract the package you want to customize from the /NativePackages 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 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. (Optional) Copy the customize_eac_pkg script file and the pre.tar file to a temporary location on your file system.

   You only need to have pre.tar file in the same directory as the script file if you want script messages in a language other than English. 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 on the CA Access Control Endpoint Components for UNIX DVD in the same location where the native packages are. You can find the pre.tar file in the /Unix/Access-Control directory of the DVD.

3. (Optional) Enter the following command to set the language of the installation parameters file:

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

4. (Optional) Enter the following command to change the installation directory:

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

5. (Optional) Enter the following command to change the default encryption files:

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

6. Enter the following command to get the installation parameters file:

   customize_eac_pkg -g -f *tmp_params* [-d *pkg_location*] [*pkg_name*]

7. 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 token (remove the preceding # character) and point it to post-installation script file you want to run.

8. Enter the following command to 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.

More information:

customize_eac_pkg Command—Customize Solaris Native Package (see page 59)

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 -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 CA Access Control 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*.

-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 customize_eac_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.

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 to r12.0.

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 tokens in your package configuration file (myadmin) as shown:

   ```
   setuid=nocheck
   action=nocheck
   ```

   Save the file.

3. Run the following command to install CA Access Control silently with the default configuration settings:

   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.

Install HP-UX Native Packages

The CA Access Control Software Distributor-UX (SD-UX) native packages let you install CA Access Control on HP-UX easily.

Note: The following procedure installs CA Access Control with the default settings. Alternatively, you may want to customize the CA Access Control package before installing it.

To install the CA Access Control HP-UX native packages using the command line interface

1. Log in as root.

   To register and install HP-UX native packages you need permissions associated with the root account.

2. Register the 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.

   Note: You can find the SD-UX native packages in the NativePackages directory of the CA Access Control Endpoint Components for UNIX DVD.

3. 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.

Customize the SD-UX Format Packages

If you want to install CA Access Control with custom settings using Software Distributor-UX (SD-UX) format packaging, you need to customize the package before you install it. You customize the script by extracting the installation parameters file from the package, modifying it as required, and then loading it back into the package.

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.

2. (Optional) Copy the customize_eac_depot script file and the pre.tar file to a temporary location on your file system.

   You only need to have pre.tar file in the same directory as the script file if you want script messages in a language other than English. 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 on the CA Access Control Endpoint Components for UNIX DVD in the same location where the native packages are. You can find the pre.tar file in the /Unix/Access-Control directory of the DVD.

3. (Optional) Enter the following command to set the language of the installation parameters file:

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

4. (Optional) Enter the following command to change the installation directory:

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

5. (Optional) Enter the following command to change the default encryption files:

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

6. Enter the following command to get the installation parameters file:

   customize_eac_depot -g -f *tmp_params* [-d *pkg_location*] [*pkg_name*]

7. 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 token (remove the preceding # character) and point it to post-installation script file you want to run.

8. Enter the following command to 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.

More information:

customize_eac_depot Command—Customize an SD-UX Format Package (see page 66)

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 -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 CA Access Control 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*.

-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 customize_eac_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.

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.

Install AIX Native Packages

The CA Access Control AIX native packages let you install CA Access Control on AIX easily.

Note: The following procedure installs CA Access Control with the default settings. Alternatively, you may want to customize the CA Access Control package before installing it.

To install the CA Access Control AIX native packages using the command line interface

1. Log in as root.

   To register and install AIX native packages, you need permissions associated with the root account.

2. (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.

3. 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.

   Note: You can find the AIX 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.

Customize the bff Native Package Files

If you want to install CA Access Control with custom settings using installp format native packaging (bff files), you need to customize the package before you install it. You customize the script by extracting the installation parameters file from the package, modifying it as required, and then loading it back into the package.

To customize the bff native package files

1. Copy the package you want to customize (a bff file) to a temporary location on your file system.

   In the read/write location on the file system, you can customize the package as required.

   Important! 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. (Optional) Copy the customize_eac_bff script file and the pre.tar file to a temporary location on your file system.

   You only need to have pre.tar file in the same directory as the script file if you want script messages in a language other than English. 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 on the CA Access Control Endpoint Components for UNIX DVD in the same location where the native packages are. You can find the pre.tar file in the /Unix/Access-Control directory of the DVD.

3. (Optional) Enter the following command to set the language of the installation parameters file:

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

4. (Optional) Enter the following command to change the installation directory:

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

5. (Optional) Enter the following command to change the default encryption files:

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

6. Enter the following command to get the installation parameters file:

   ```
   customize_eac_bff -g -f tmp_params [-d pkg_location] pkg_name
   ```

7. 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 token (remove the preceding # character) and point it to post-installation script file you want to run.

8. Enter the following command to 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 71)

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! This location should have 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 -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 CA Access Control 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*.

-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 customize_eac_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.

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 so you know how to initiate the installation of this functionality. You may also want to learn first how the install_base script works.

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, MFSD package, and the documentation 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.

-doc

Installs the documentation package that includes user documentation in a PDF and HTML formats.

CA Access Control installs the documentation in the CA Access Control installation directory under a Doc subdirectory. Open the file *ACInstallDir*/Doc/Bookshelf.html in a browser to access the documentation.

-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 the computer with a Policy Model.

This package also installs the advanced policy management server components.

Note: You can also configure advanced policy management (see page 91) after the installation is complete.

-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.

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 Report 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.

-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

If you want to:	Respond with:
	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 Report Server. You must define the Report 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.

- If you install the server package, whether you want to install advanced policy management server components (DMS and DH); and if so:

  - Advanced policy management server components administrator names.
  - Advanced policy management server components administration terminals.

- Whether you want to set up this endpoint for advanced policy management; and if so, the advanced policy management server components' host name to send calculation deviation results to.

  Define the DH 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: If you are also installing server components on this computer, you do not need to supply this information.

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 90) 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 !
   ```

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 92).

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, exportngdb, 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 55).

    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 57).

    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 74).

  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.

Considerations for 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 94) 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.

Messages Appear in Solaris 10 Log File

Valid on Solaris 10

Symptom:

When I stop CA Access Control using "secons -s", CA Access Control messages appear in the "/var/adm/messages" log file on my Solaris 10 computer.

Solution:

These messages are informational only and do not indicate any failure or error. You do not need to do anything. The messages and their interpretation follow:

- "SEOS: Restored tcp wput" "SEOS: Restored strrhead rput"

  These messages indicate that the SEOS_syscall function disabled network hooks.

- "SEOS: Replaced tcp wput" "SEOS: Replaced strrhead rput"

  These messages indicate that the SEOS_syscall function enabled network hooks.

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 4: Installing and Customizing a Windows Endpoint

This chapter guides through the CA Access Control Windows 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 certain preliminary requirements are met and several items of necessary information are available.

Installation Methods

CA Access Control for Windows can be installed by one of three methods from the CA Access Control Endpoint Components for Windows DVD:

- **Product Explorer**—The easiest way to install CA Access Control is to use the Product Explorer. The Product Explorer lets you browse through the CA Access Control features you can install from the product DVD and then select the features you want to install. Use this method to familiarize yourself with the installation options.
- **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.

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.
- CA Access Control should be installed 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, known issues, considerations, and other important information you should read before installing CA Access Control.

- To upgrade, you must have CA Access Control r5.2, or later, installed.

- We recommend that you perform a scaled-down internal testing of the new release before you upgrade your production environment.

- You must reboot the computer when you upgrade CA Access Control for the installation to complete.

  Future patches may not require a reboot.

- 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 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
  ```

- If you already have a version of CA Access Control installed on the computer, you must decide whether you want to continue using the data in your current database or whether you want to delete it and create a new, empty database.

  In order to continue with the installation you must select to reuse your data; CA Access Control will transfer all data into the new database. If you want to create a new, empty database, first uninstall CA Access Control to delete the existing database, and then install CA Access Control again.

  Important! If you choose to delete your current database, you lose all CA Access Control data: users, groups, and resources that you have defined in the database, as well as the access rules that protect the resources.

- 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 XP installation:

```
editres SPECIALPGM ('C:\WINDOWS\system32\DRWTSN32.EXE') pgmtype(DCM)
editres PROGRAM ('C:\WINDOWS\system32\DRWTSN32.EXE') owner(nobody) defacc(a) trust
```

Product Explorer Installations

The CA Access Control Product Explorer lets you browse through the CA Access Control features you can install from the CA Access Control Endpoint Components for Windows DVD. Using the Product Explorer, you can select which component of CA Access Control you want to install on this computer, learn a little about these features, and initiate their installation. You can also view system requirements for installation components, or open the documentation for viewing.

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

To view the installation options and choose which ones meet your needs, you can use the graphical installation program to install CA Access Control. This lets you learn the installation options as you install CA Access Control.

To install CA Access Control using Product Explorer

1. Log on 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.

   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 112).

   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 135).

   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.

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.

   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.

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
Report Agent	Lets you configure the computer to send scheduled snapshots of the database to the Report Server. You can then select to also send audit records to the Report 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.
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.	
Advanced Policy Management Server	Installs the advanced policy management server components (DMS and DH).	Select this feature if this computer should be the advanced policy management server. **Note:** For more information on advanced policy management, see the *Enterprise Administration Guide*.
Advanced Policy	Configures the local computer for	Select this feature for every endpoint

Feature	Description	Recommendation
Management Client	advanced policy management.	you want to be able to deploy policies to (using advanced policy management.
Policy Model	Sets up the Policy Model service. You can then select to install a PMDB parent or a PMDB subscriber.	Select this feature if you want to use PMDBs to propagate selang rules across your enterprise implementation of CA Access Control. **Note:** For more information on the Policy Model service, see the *Endpoint Administration Guide*.

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.	

Information	Description	Recommendation
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 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 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.
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

Information	Description	Recommendation
		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 installation program screens that are concerned with setting inter-component communication encryption guide you through the choices for SSL and certificates.

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.

Screen	Description	Recommendation
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.
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.

Standard Encryption

CA Access Control standard encryption is implemented by a dynamic link library (DLL).

The CA Access Control installation stores all encryption DLLs in the following directory:

ACInstallDir\bin

where *ACInstallDir* is the directory in which you installed CA Access Control.

The DLL files that CA Access Control stores during installation are as follows:

- defenc.dll (default encryption, proprietary)
- aes128enc.dll (128bit AES encryption)
- aes192enc.dll (192bit AES encryption)
- aes256enc.dll (256bit AES encryption)
- desenc.dll (DES encryption)
- tripledesenc.dll (3DES encryption)

The full path of the DLL used for encryption is stored as the following registry value:

HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl\Encryption Package

You can change the key used for the encryption by using the sechkey utility in symmetric mode.

SSL, Authentication, and Certificates

Secure Sockets Layer (SSL), including TLS, provides communications between computer programs. It ensures that communications have the following properties:

- The participants in the communication are the programs, or users, that they purport to be. This is called authentication.
- 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. When a client receives an X509 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 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 a X.509 certificate are as follows:

The 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

The 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 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.

Policy Model Databases

If you chose to install a PMDB parent or a PMDB subscriber, you need to describe the hierarchy context in which they sit. That is, you need to define where in the hierarchy your database is positioned.

The following table explains what information you need to provide and gives recommendations:

Information	Description	Recommendation
Policy Model Parent	Lets you define the name of a PMDB to create, and its position in the hierarchy. You do this by defining one or more subscriber databases to which this PMDB propagates changes to.	You will need to define this PMDB as a parent on each of the subscriber databases.
Policy Model Subscriber Settings	Lets you define the position of the database in the hierarchy. You do this by defining one or more parent PMDBs to which this database subscribes to, and the parent password Policy Model from which password changes are propagated.	You will need to define this database as a subscriber to the parent PMDB. **Note:** Specify _NO_MASTER_ as a parent PMDB to indicate that the local database accepts updates from any PMDB.

Advanced Policy Management Server

If you chose to install an advanced policy management server or configure the local client for advanced policy management, you need to provide information for how to set up this feature.

The following table explains what information you need to provide and gives recommendations:

Information	Description	Recommendation
Advanced Policy Management Server	Lets you configure administrators and administration terminals for the advanced policy management server components.	If the administrators are using CA Access Control Enterprise Management to deploy policies, you only need to define the computer where CA Access Control Enterprise Management is installed. You do not need to define the computer where the administrator opens the browser.
Advanced Policy Management	Lets you define the name of the server where the advanced	Define the host name using the format *dhName@hostName* For example, if you

Information	Description	Recommendation
Client	policy management server components are installed. **Note:** If you are also installing server components on this computer, you do not need to supply this information.	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

If you choose to enable the Report Agent, you need to provide information about the connection to the Report Server.

The following table explains what information you need to provide and gives recommendations:

Information	Description	Recommendation
Specify Report Agent settings	Lets you configure the connection to the Report Server, specify when the Report Agent sends snapshots of the database to the Report Server, and specify to keep time-stamped backups of the audit log file.	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.
Specify SSL communication key	Lets you define a new SSL key to authenticate communication between the Report Server and the Report Agent.	Make sure you use the same key when you install the Report Server.

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 onto 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 on 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. Open a command line and navigate to the following directory in the location where you have your installation media:

   ```
   \architecture
   ```

   architecture

   Defines the architecture abbreviation for your operating system.

   Can be one of **X86**, **X64**, and **IA64**.
3. 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.

Uninstall 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 r12.0 SP1 CR1 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.

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 123) or when performing a silent installation (see page 124).

Note: For more information on the command line syntax, see the Windows Installer SDK documentation.

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. The following are the supported language IDs you can specify and their respective languages:

- 1033 - English
- 1041 - Japanese
- 1042 - Korean
- 2052 - Chinese (simplified)

/v "<*insert_params_here*>"

Defines the parameters to pass to the installation program.

Note: All parameters should 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.

  Note: If you are also installing advanced policy management server components on this computer, you do not need to supply this information.

ADV_POLICY_MNGT_SERVER={1 | 0}

Specifies whether to install advanced policy management server components (1). If you specify this option and set it to 1, you also need to specify:

- **APMS_ADMIN_LIST=\"***admins***\"**

  Defines a comma-separated list of users who can administer the advanced policy management server components' databases.

  Default: User performing the installation

- **APMS_HOSTS_LIST=\"***hosts***\"**

  Defines a comma-separated list of terminal from which administrators can administer the advanced policy management server components' databases.

  Default: Local computer

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*

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.

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)

PMDB_CLIENT={1 | 0}

Specifies whether the local CA Access Control database should be 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 should be 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.

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:

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

  Specifies whether the Audit Routing feature is installed (1).

  Default: 0 (not installed)

- **NEW_KEY=\"***name***\"**

  Defines the SSL key that authenticates communication between the Report Server and the Report Agent. You must also set USE_SECURE_COMM=1.

- **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*

- **REPORT_SERVER_NAME=\"***name***\"**

  Defines the name of the Report Server host for Report Agent configuration (for example, test.company.com).

  Default: *none*

- **REPORT_SERVER_PORT=\"***port***\"**

  Defines the port number of the Report Server for Report Agent configuration.

  Default: *none*

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

  Specifies whether the Report Agent uses secure communication (1).

  Default: 0 (no)

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_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.

- **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.

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

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

- **EXIST_ROOT_PRIVATE=\"***file***\"**

  Defines the fully qualified file name of the root private key file (.key). 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.

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 | \"256bit AES\" | \"192bit AES\" | \"128bit AES\"}**

  Specifies the encryption method to use for communications.

  Default: Default

- **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.

IMPORT_NT_DATA={Y | N}

Specifies whether to support primary user stores. If you specify N, 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).

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"
```

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.

Starting and Stopping CA Access Control

CA Access Control is started whenever you start Windows *if* the startup of the CA Access Control services is automatic.

Stop CA Access Control

You can stop CA Access Control from the command prompt:

1. 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).
2. Stop CA Access Control on the local machine by entering:

   ```
   secons -s
   ```

   Stop CA Access Control on one or more remote machines by entering:

   ```
   secons -s stationNames
   ```

   stationNames

   Defines a list of names of the remote computers separated by spaces.

When CA Access Control stops on the local machine, the following message appears:

```
CA Access Control is now DOWN
```

When you stop CA Access Control on remote machines, CA Access Control reports whether the remote machine shutdown was successful. An attempt is made to shut down each machine on the list, even if the remote machine 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

  These keys are protected so that they can be changed only when CA Access Control is running and by using the selang commands newres or chres (For more information about selang commands, see the *selang Reference Guide*.)

- 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, like Task Delegation and Policy Model, 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 the Windows Services application.

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\Access Control\SplashEnable registry key value from 1 to 0.

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.

Chapter 5: 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 Java Development Kit (JDK) 1.4.2_12 or higher.

   Note: You can find this prerequisite third-party software on the CA Access Control Premium Edition Third Party Components for Solaris and CA Access Control Premium Edition Third Party Components for Windows DVDs.

2. 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:\j2sdk1.4.2_12
   ```

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

   ```
   export JAVA_HOME=/usr/jdk/j2sdk.1.4.2_12/
   ```

3. Install a supported JBoss version.

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

   Note: You can find this prerequisite third-party software on the CA Access Control Premium Edition Third Party Components for Solaris and CA Access Control Premium Edition Third Party Components for Windows DVDs. To install the supplied JBoss version, extract the contents of the JBoss zip file to /opt on Solaris or to your C drive on Windows. For information about supported JBoss versions, see the *Release Notes*.

4. Install CA Access Control.

   Note: Follow the instructions for installing a CA Access Control endpoint.

5. (Windows only) Restart the computer.

6. Stop CA Access Control services (secons -s).

   The server is now ready for CA Access Control Endpoint Management to be installed.

   Important! Make sure that you also manually stop the "CA Access Control Report Server Message Queue" service, which does not stop when you issue the secons -s command. This service exists *only* if you already installed CA Access Control Report Server.

Install CA Access Control Endpoint Management Using a Graphical Interface

The graphical installation uses a wizard to support and guide you when installing CA Access Control Endpoint Management.

To install CA Access Control Endpoint Management using a graphical interface

1. Make sure that you prepare the server correctly (see page 137).
2. Do either of the following:
   - On Windows:
     a. Insert the CA Access Control Premium Edition Server Components for Windows DVD into your optical disc drive.
     b. Open the CA Access Control Product Explorer (ProductExplorerx86.EXE).

        The CA Access Control Product Explorer appears.
     c. Expand the Components folder, select CA Access Control Endpoint Management, then click Install.
   - On UNIX:
     a. Insert the CA Access Control Premium Edition Server Components for Solaris DVD into your optical disc drive.
     b. Connect to the host using an X Window terminal session.
     c. Mount the optical disc drive.
     d. Locate the EndPointMgmt directory, then run install.bin

   The InstallAnywhere wizard starts loading.
3. 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 Using a Console

If you do not want to use the graphical installation because you are installing from a text-only terminal or do not have the required X Server graphics software that the InstallAnywhere wizard requires, you can use the console installation to install CA Access Control Endpoint Management.

To install CA Access Control Endpoint Management using a console

1. Make sure that you prepare the server correctly (see page 137).
2. Do either of the following:
   - On Windows:
     a. Insert the CA Access Control Premium Edition Server Components for Windows DVD into your optical disc drive.
     b. Open a command line and navigate to the EndPointMgmt directory on the optical disc drive.
     c. Enter the following command:

        ```
        install_EM_r12_SP1.exe -i console
        ```
   - On UNIX:
     a. Insert the CA Access Control Premium Edition Server Components for Solaris DVD into your optical disc drive.
     b. Connect to the host using an X Window terminal session.
     c. Mount the optical disc drive.
     d. Open a terminal window and navigate to the EndPointMgmt directory on the optical disc drive.
     e. Enter the following command:

        ```
        install_EM_r12_SP1.bin -i console
        ```

   The InstallAnywhere console appears after a few moments.
3. 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 non-English supported 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 uninstll 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_CA Access Control Endpoint
   Management/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 wizard or console.

   Note: The uninstall loads using the same method you used to install. That is, if you installed using a console the uninstall is also performed in a console. Otherwise, the uninstall loads a wizard.
3. Follow the prompts to uninstall CA Access Control Endpoint Management.

   The uninstll 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) Start the following additional services, which do not load when you issue the seosd -start command:

   - CA Access Control Web Service
   - CA Access Control Report Server Message Queue (if present)

3. Start JBoss Application Server by doing either of the following:

   - On Windows, click Start, Programs, CA, Access Control, CA Access Control Endpoint Management, Start JBoss.
   - On UNIX, enter /*JBOSS_DIR*/bin/run.sh

   You can now 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://appserver123:8080/acem
```

The URL suggests that CA Access Control Endpoint Management is installed on a host named appserver123 and uses the default JBoss port 8080.

Chapter 6: Installing Enterprise Management

This section contains the following topics:

Environment Architecture

CA Access Control lets you manage policies across your enterprise using advanced policy management features. To manage these features easily, CA Access Control offers a web-based interface called CA Access Control Enterprise Management.

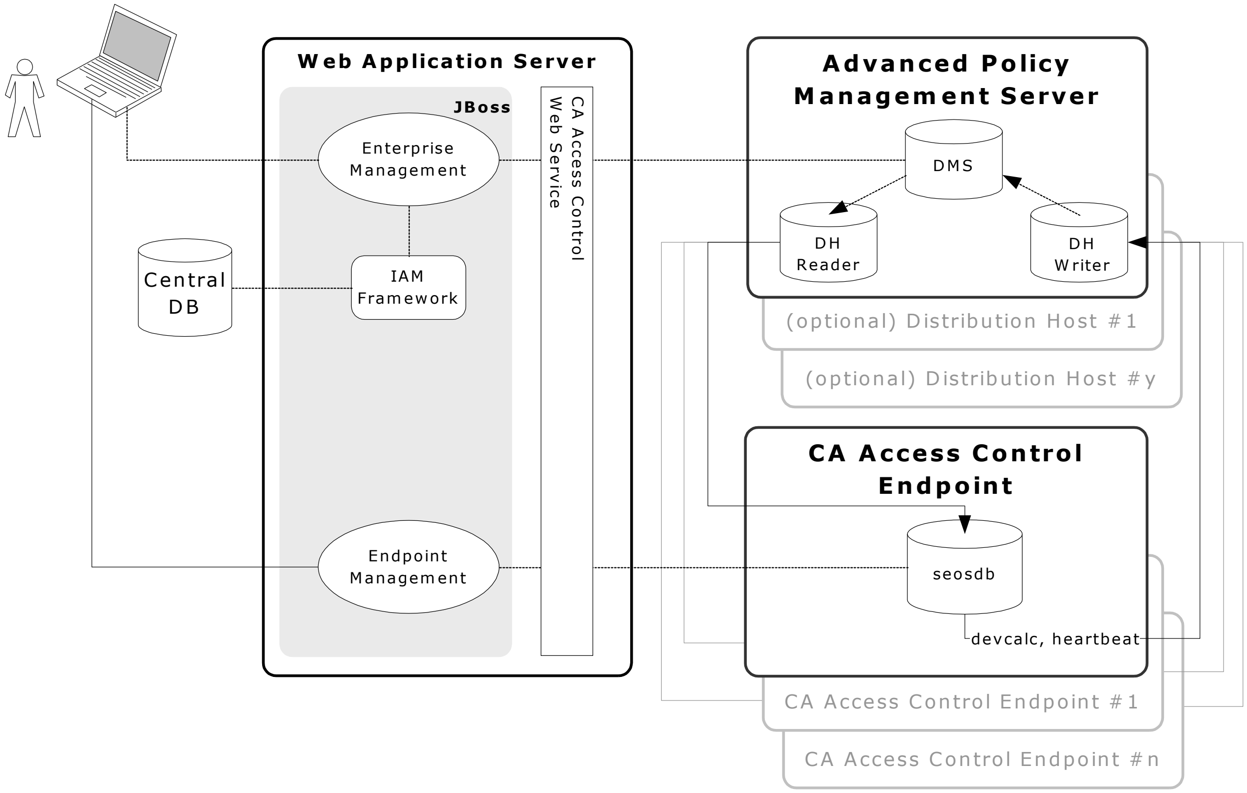
To use advanced policy management, you need to install and configure on a central computer that is designated for this purpose, the advanced policy management server components:

- Deployment Map Server (DMS) (see page 149)
- Distribution Host (DH) (see page 149)

Also, you need to configure each CA Access Control endpoint for advanced policy management.

Finally, to simplify policy management, you can install the CA Access Control Enterprise Management web-interface.

The following diagram shows the implementation architecture of advanced policy management:


Web Application Server
JBoss
Enterprise Management
IAM Framework
Endpoint Management
CA Access Control Web Service
Central DB
Advanced Policy Management Server
DMS
DH Reader
DH Writer
(optional) Distribution Host #1
(optional) Distribution Host #y
CA Access Control Endpoint
seosdb
devcalc, heartbeat
CA Access Control Endpoint #1
CA Access Control Endpoint #n

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 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 DMS. However, you can also install multiple DH nodes so that each manages a section of your enterprise for load balancing.

How to Prepare the Enterprise Management Server

CA Access Control offers a web-based interface for managing your enterprise. CA Access Control Enterprise Management lets you manage advanced policy management and includes a World View. 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 for you, if it is not already installed. If you already 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 database for Enterprise Management (see page 151).
2. Install Java Development Kit (JDK) 1.4.2_12 or higher.

   Note: You can find this prerequisite third-party software on the CA Access Control Premium Edition Third Party Components for Solaris and CA Access Control Premium Edition Third Party Components for Windows DVDs.

3. 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:\j2sdk1.4.2_12
   ```

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

   ```
   export JAVA_HOME=/usr/jdk/j2sdk.1.4.2_12/
   ```

4. Install a supported JBoss version.

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

   Note: You can find this prerequisite third-party software on the CA Access Control Premium Edition Third Party Components for Solaris and CA Access Control Premium Edition Third Party Components for Windows DVDs. To install the supplied JBoss version, extract the contents of the JBoss zip file to /opt on Solaris or to your C drive on Windows. For information about supported JBoss versions, see the *Release Notes*.

5. Install CA Access Control.

   Note: Follow the instructions for installing a CA Access Control endpoint. On Windows, you should also restart the computer.

   Important! When you install CA Access Control as part of this installation, select to install a advanced policy management server components. If you do not want to install advanced policy management server components on the same computer as CA Access Control Enterprise Management, you can install these on a separate computer.

6. Configure a proxy user for CA Access Control Enterprise Management (see page 153).
7. Stop CA Access Control services.

   Important! Make sure that you also manually stop the "CA Access Control Web Service" and "CA Access Control Report Server Message Queue" services, which do not stop when you issue the secons -s command. These services exist *only* if you already installed CA Access Control Endpoint Management and CA Access Control Report Server respectively.

   The server is now ready for CA Access Control Enterprise Management to be installed.

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.

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:

   - Make sure the database can be accessed locally and from a remote client.
   - For Oracle:
     - Create a new administrative user for the central database.

       This user should have permissions to create tables and modify data.
     - Configure the database with at least 200 processes.
   - For SQL Server:
     - Create a new case-*insensitive* database.
     - Create a new user, make the new database their default database, and give them DB_owner privileges.

Example: Install and Configure Oracle Database XE

Important! For simplicity, this procedure describes the installation of Oracle Database XE, which is *not* officially supported for production systems. If you are planning to use the product in production, you should have a database administrator install a fully supported RDBMS.

The following steps illustrate how you configure Oracle for remote clients and create a new administrative user to use with CA Access Control Enterprise Management:

1. When you install Oracle Database XE, provide the SYS and SYSTEM database accounts' password.

   Oracle Database XE is installed.

2. Launch Oracle Database Home Page.

   - On Windows, click Start, Oracle Database 10g Express Edition, Go To Database Home Page

     Note: To do this during installation, select the check box on the final page of the installation wizard.

   - On UNIX, open a browser and enter the following URL:
     http://127.0.0.1:8080/apex

     Note: This URL assumes you installed Oracle Database XE using the default port.

   The Database Login page appears.

3. Log in using the user name *system* and the password you set when you installed Oracle Database XE.

   The Home page appears.

4. Click the down arrow next to the Administration icon and select Manage HTTP Access.

   The Manage HTTP Access page appears.

5. Make sure that the Available from local server and remote clients option is selected, then click Apply Changes.

6. Click the down arrow next to the Administration icon and select Database Users, Create User.

   The Create Database User page appears.

7. Complete the dialog as follows:

   - Type a username and password (make sure you record these credentials)
   - Keep the default Roles selected (CONNECT and RESOURCE but not DBA).
   - Select all of the options for Direct Grant System Privileges.

   Click Create.

   The new administrative user is created and you can use it to connect to the database.

8. Set the maximum number of permitted job queue processes:

   a. Start the SQL Command Line.

   b. Connect as sysdba:

   ```
   connect / as sysdba
   ```

   c. Check how many processes are configured:

   ```
   show parameter processes
   ```

   d. Increase the value to at least 200, if necessary:

   ```
   alter system set processes=200 scope=spfile;
   ```

   e. Stop and restart the database.

   ```
   shutdown immediate
   startup
   ```

Configure a Proxy User for Enterprise Management

CA Access Control Enterprise Management uses a proxy user for advanced policy management actions it performs. The proxy user needs to have the required administrative rights to the DMS CA Access Control Enterprise Management operates in, and be authorized to perform these actions from the terminal where CA Access Control Enterprise Management is installed. We recommend that you create a dedicated proxy user and not use the default administrative user to perform CA Access Control Enterprise Management actions on behalf of the logged in user.

Note: DMS audit records will show that the defined proxy user executed database commands on behalf of the user who is logged in to CA Access Control Enterprise Management.

To configure a proxy user for Enterprise Management

1. On the DMS computer, open a selang window.
2. Connect to the DMS database, as follows:

   ```
   host dmsName@DMShostName
   ```

   dmsName

   Defines the name of the DMS database.

   Note: When you install advanced policy management server components as part of an endpoint installation, or when you use dmsmgr -auto to create the server components, CA Access Control uses DMS__ as the default name for the DMS database.

   DMShostName

   Defines the name of the host computer where the DMS is installed.

3. Create the proxy user and give them administrative and auditor rights to the database, as follows:

   ```
   eu dmsProxy admin auditor
   ```

   dmsProxy

   Defines the name of the proxy user you want to create.

4. Authorize the proxy user to access the DMS from the computer where CA Access Control Enterprise Management is installed, as follows:

   ```
   er TERMINAL (WShostName) owner(nobody)
   authorize TERMINAL (WShostName) uid(dmsProxy) access(a)
   ```

   WShostName

   Defines the name of the computer where CA Access Control Enterprise Management (and the CA Access Control Web Service) is installed.

5. Connect back to the CA Access Control database on the DMS computer, as follows:

   ```
   host DMShostName
   ```

6. Create the proxy user in the native environment and define their password, as follows:

   ```
   env native
   eu dmsProxy password(proxyPassword)
   ```

   proxyPassword

   Defines the password for the proxy user you create.

   Important! Make sure you choose a password that complies with the native operating system password policy for this computer. You should regularly replace the proxy user’s password and then update the DMS connection details for CA Access Control Enterprise Management with the new password.

Example: Configure a Proxy User for CA Access Control Enterprise Management

The following example shows you how you can define user dmsproxy as a proxy user for CA Access Control Enterprise Management. The example assumes the following:

- You installed advanced policy management server components as part of the regular CA Access Control endpoint installation on dmscentral.org.com
- You are installing CA Access Control Enterprise Management on appserver.org.com

To configure the proxy user for CA Access Control Enterprise Management, open a selang window and enter the following commands:

```
host DMS__@dmscentral.org.com
eu dmsproxy admin auditor
er TERMINAL (appserver.org.com) owner(nobody)
authorize TERMINAL (appserver.org.com) uid(dmsproxy) access(a)
host dmscentral.org.com
env native
eu dmsproxy password(C0mp!exPass)
```

How to Set Up Advanced Policy-based Management

CA Access Control uses advanced policy management components to manage the deployment of policies on each computer in your enterprise. By installing and configuring the appropriate components on each computer, you enable policy-based management.

To enable advanced policy-based management, do the following:

1. Install the advanced policy management server components (a DMS and a DH) on a central computer.

   Advanced policy management server components can be installed during CA Access Control installation or by using the dmsmgr utility.

2. Configure advanced policy management functionality on each CA Access Control computer in your enterprise.

   You can configure your endpoint during installation or by using the dmsmgr utility. This configures the endpoint for fetching deployment information from the DH and for sending policy deviation status to the DMS through the DH.

3. (Optional) Configure CA Access Control Enterprise Management to connect to the DMS you want to manage.

   This lets you manage your policies using CA Access Control Enterprise Management.

   Note: You need to install CA Access Control Enterprise Management before you can configure it to connect to a DMS.

Install Advanced Policy Management Server Components

To take advantage of advanced policy management features you must first install the advanced policy management server components.

Note: When you install CA Access Control, you can choose to install advanced policy management server components as part of that installation. For more information, refer to the endpoint installation instructions for your operating system. This procedure shows you how to add these server components to an existing installation of CA Access Control.

To install advanced policy management server components, open a command window and enter the following command:

```
dmsmgr -create -auto
```

This command creates a DMS and a DH with default names (DMS__, DH__, and DH__WRITER). It also creates you as the administrator of these databases. You can find the dmsmgr utility in the *ACInstallDir*/bin directory.

Note: For more information, see the dmsmgr -create command in the *Reference Guide*.

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: When you install CA Access Control, you can choose to install advanced policy management server components as part of that installation. For more information, refer to the endpoint installation instructions for your operating system. This procedure shows you how to configure an existing installation of CA Access Control for advanced policy management.

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*.

Install CA Access Control Enterprise Management Using a Graphical Interface

The graphical installation uses a wizard to support and guide you when installing CA Access Control Enterprise Management.

To install CA Access Control Enterprise Management using a graphical interface

1. Shut down JBoss Application Server if it is running.
2. Stop CA Access Control services.

   Important! Make sure that you also manually stop the "CA Access Control Web Service" and "CA Access Control Report Server Message Queue" services, which do not stop when you issue the secons -s command. These services exist *only* if you already installed CA Access Control Endpoint Management and CA Access Control Report Server respectively.

3. Do either of the following:
   - On Windows:
     a. Insert the CA Access Control Premium Edition Server Components for Windows DVD into your optical disc drive.
     b. Open the CA Access Control Product Explorer (ProductExplorerx86.EXE).

        The CA Access Control Product Explorer appears.

     c. Expand the Components folder, select CA Access Control Enterprise Management, then click Install.
   - On UNIX:
     a. Insert the CA Access Control Premium Edition Server Components for Solaris DVD into your optical disc drive.
     b. Connect to the host using an X Window terminal session.
     c. Mount the optical disc drive.
     d. Locate the EnterpriseMgmt directory, then run install.bin

   The InstallAnywhere wizard starts loading.

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

   Java Development Kit (JDK)

   Defines the location of an existing JDK.

   Select the JDK you specified for the JAVA_HOME environment variable.

   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, C:\jboss-4.0.5.GA on Windows or /opt/jboss-4.0.5.GA on Solaris.

   – Define the URL, which is the IP address or host name of the computer you are installing on.

   – Define the port JBoss uses.

   – Define the port JBoss uses for secure communications (HTTPS).

   Database Information

   Defines the connection details to the RDBMS:

   – **Database Type**—Specifies a supported RDBMS.

   – **Database Host Name**—Defines the name of the host where you have the RDBMS installed.

   – **Database Port**—Defines the port used by the RDBMS you specified. The installation program provides the default port for your RDBMS.

   – **Database Service Name**—Defines the name that identifies your RDBMS on the system. For example, for Oracle Database 10g this is *orcl* by default.

   – **Database Name**—Defines the name of the database you created on your RDBMS.

   – **Database User Name**—Defines the name of the user that you created when you prepared the RDBMS.

   – **Database User Password**—Defines the password of the administrative user you created.

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

Administrator Password

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.

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 but you still need to configure CA Access Control Enterprise Management for your enterprise.

More information:

How to Prepare the Enterprise Management Server (see page 149)
Configure the Connection to the DMS (see page 168)

Install CA Access Control Enterprise Management Using a Console

If you do not want to use the graphical installation because you are installing from a text-only terminal or do not have the required X Server graphics software that the InstallAnywhere wizard requires, you can use the console installation to install CA Access Control Enterprise Management.

To install CA Access Control Enterprise Management using a graphical interface

1. Shut down JBoss Application Server if it is running.
2. Stop CA Access Control services.

   Important! Make sure that you also manually stop the "CA Access Control Web Service" and "CA Access Control Report Server Message Queue" services, which do not stop when you issue the secons -s command. These services exist *only* if you already installed CA Access Control Endpoint Management and CA Access Control Report Server respectively.

3. Do either of the following:
   - On Windows:
     a. Insert the CA Access Control Premium Edition Server Components for Windows DVD into your optical disc drive.
     b. Open a command line and navigate to the EnterpriseMgmt directory on the optical disc drive.
     c. Enter the following command:

        ```
        install_EntM_r12_SP1.exe -i console
        ```

   - On UNIX:
     a. Insert the CA Access Control Premium Edition Server Components for Solaris DVD into your optical disc drive.
     b. Connect to the host using an X Window terminal session.
     c. Mount the optical disc drive.
     d. Open a terminal window and navigate to the EnterpriseMgmt directory on the optical disc drive.
     e. Enter the following command:

        ```
        install_EntM_r12_SP1.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.

   Select the JDK you specified for the JAVA_HOME environment variable.

   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, C:\jboss-4.0.5.GA on Windows or /opt/jboss-4.0.5.GA on Solaris.

   – Define the URL, which is the IP address or host name of the computer you are installing on.

   – Define the port JBoss uses.

   – Define the port JBoss uses for secure communications (HTTPS).

   Database Information

   Defines the connection details to the RDBMS:

   – **Database Type**—Specifies a supported RDBMS.

   – **Database Host Name**—Defines the name of the host where you have the RDBMS installed.

   – **Database Port**—Defines the port used by the RDBMS you specified. The installation program provides the default port for your RDBMS.

   – **Database Service Name**—Defines the name that identifies your RDBMS on the system. For example, for Oracle Database 10g this is *orcl* by default.

   – **Database Name**—Defines the name of the database you created on your RDBMS.

   – **Database User Name**—Defines the name of the user that you created when you prepared the RDBMS.

   – **Database User Password**—Defines the password of the administrative user you created.

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

Administrator Password

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.

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 but you still need to configure CA Access Control Enterprise Management for your enterprise.

More information:

How to Prepare the Enterprise Management Server (see page 149)
Configure the Connection to the DMS (see page 168)

Uninstall CA Access Control Enterprise 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 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's instructions to uninstall CA Access Control Enterprise Management.

   The uninstll 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_CA Access Control Enterprise Management/Uninstall_CA_Access_Control_Enterprise_Management"
   ```

   ACPMInstallDir

   Defines the installation directory of CA Access Control Endpoint Management. By default this path is:

   ```
   /opt/CA/AccessControlServer/EnterpriseManagement/
   ```

   InstallAnywhere loads the uninstall wizard or console.

   Note: The uninstall loads using the same method you used to install. That is, if you installed using a console the uninstall is also performed in a console. Otherwise, the uninstall loads a wizard.
3. Follow the prompts to uninstall CA Access Control Enterprise Management.

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

Start CA Access Control Enterprise Management

Once you install 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 start CA Access Control Enterprise Management

1. Start CA Access Control services.

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

2. (Windows only) Start the following additional services, which do not load when you issue the seosd -start command:

   - CA Access Control Web Service
   - CA Access Control Report Server Message Queue (if present)

3. Do one of the following:

   - On Windows, click Start, Programs, CA, Access Control, Start Task Engine.

     Important! If you set JBoss to start as a Windows service, make sure you start it using run_idm.bat instead of run.bat.

   - On UNIX, enter /*JBOSS_DIR*/bin/run_idm.sh

   This starts JBoss Application Server.

   Note: The first time JBoss Application Server loads should take some time.

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 the following URL, for your host:

   http://*enterprise_host*:*port*/iam/ac

2. Use the *superadmin* credentials you provided during installation 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://appserver123:8080/iam/ac
```

The URL suggests that CA Access Control Enterprise Management is installed on a host named appserver123 and uses the default JBoss port 8080.

Configure the Connection to the DMS

Once you install and start CA Access Control Enterprise Management, when you first log in to CA Access Control Enterprise Management you need to configure it for your environment by configuring the connection to the Deployment Map Server (DMS). You must install and start the DMS before you configure the connection from CA Access Control Enterprise Management to the DMS.

To configure CA Access Control Enterprise Management for your environment

1. Use the *superadmin* credentials you provided during installation to log in.

   CA Access Control Enterprise Management displays the following confirmation under the Welcome message:

   ```
   Confirmation   No DMS connections are defined in the system.
   ```

2. Click the System tab, then click Create Connection in the Connection Management subtab.

   The Create Connection page appears.

3. Complete the fields in the dialog and click Submit. The following fields are not self-explanatory:

   Connection Name

   Defines the name you want to use for this connection.

   Connection Type

   Indicates the type of connection you are creating.

   Description

   (Optional) Defines a description for this connection.

Host Name

Defines the name of the DMS you want CA Access Control Enterprise Management to work against.

Format: *dmsName@hostName*

For example, to use the default DMS that installs when you install advanced policy management server components on host host1.comp.com type: DMS__@host1.comp.com.

User ID

Defines the name of a user with administrative rights to the DMS.

We recommend that you use a dedicated proxy user you create and not use the default administrative user to perform CA Access Control Enterprise Management actions on behalf of the logged in user.

Note: DMS audit records will show that the defined proxy user executed database commands on behalf of the user who is logged in to CA Access Control Enterprise Management.

Password

Defines the password of the user with administrative rights to the DMS.

Default Connection

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

CA Access Control Enterprise Management uses the information you specified to try to log in to the DMS. If the information is correct, the connection is set and you can now use CA Access Control Enterprise Management to manage your enterprise deployment of CA Access Control. If the information is incorrect and CA Access Control Enterprise Management cannot log in to the DMS, an error message appears with the reason the connection could not be established.

4. Log out and then log back into CA Access Control Enterprise Management.

   The CA Access Control Enterprise Management home page appears and you are connected to the DMS you defined.

Chapter 7: Installing Enterprise Reporting

This section contains the following topics:

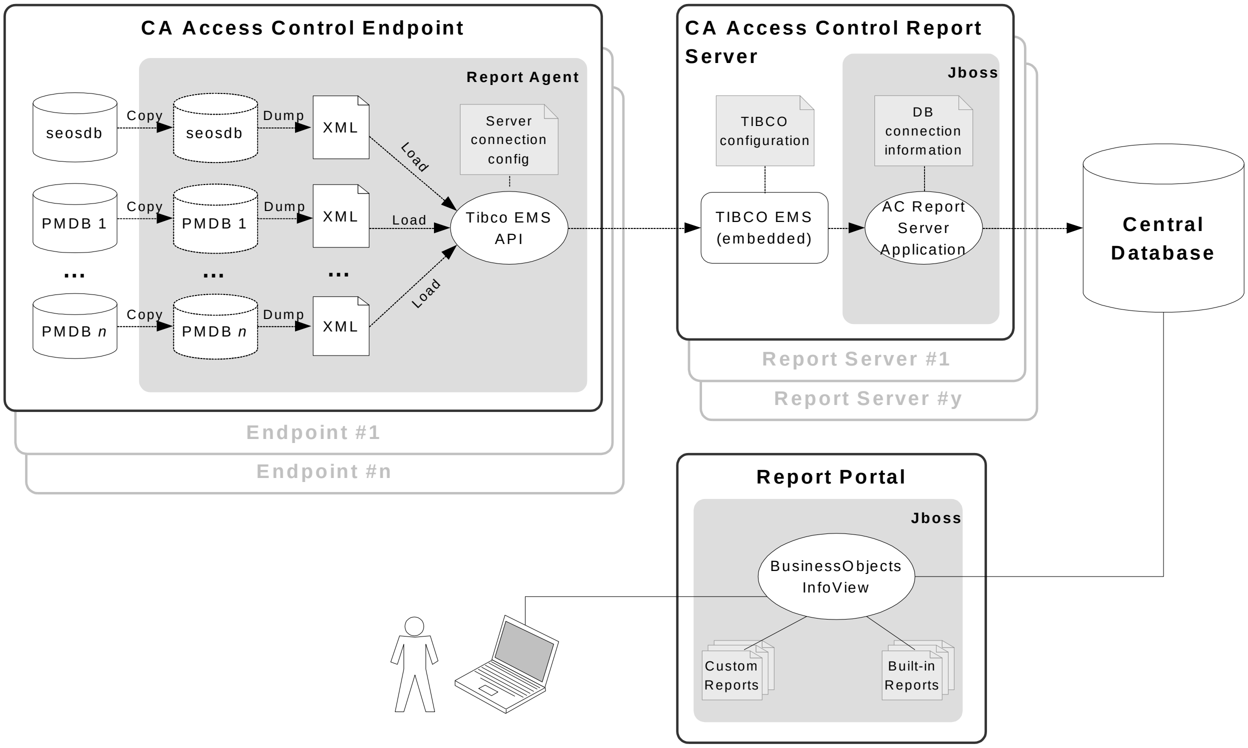
Reporting Service Architecture

CA Access Control reporting service provides a server-based platform for CA Access Control enterprise reporting. You can use this 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, containing 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 Report Server for processing.
- In a simple enterprise model, one Report Server is used to process all endpoint data and send it to the central database for storage. You can also replicate Report Server components to design for fault tolerance and faster processing in large enterprise environments.
- The central database (an RDBMS) is used to store 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 to create reports that contain data from all your CA Access Control endpoints, you first need to install and configure the CA Access Control reporting service server components. You can configure the central database, Report Server, and Report Portal on the same computer or on separate computers. Once you have the server components installed, you need to configure the Report Agent on each endpoint.

Note: Report Agent installation and configuration is part of the CA Access Control endpoint installation and is not covered in this procedure.

To set up the Reporting Service Server Components, follow these steps:

1. Install and configure an RDBMS as the central database.
2. Set up the Report Server computer and install CA Access Control Report Server.
3. Set up the Report Portal computer and install 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.
4. Deploy or upgrade the CA Access Control report package.

   The reporting service server components are set up and the standard CA Access Control reports are available in BusinessObjects InfoView.

   You can now configure the Report Agents on your endpoints to send data to the Report Server.

Note: For operating systems support and detailed information about the supported applications and versions, see the *Release Notes*.

Install and Configure an RDBMS as a Central Database

Before you set up your Report Server or Report Portal, you need to install and configure an RDBMS (relational database management system) as your central database. The central database stores your endpoint data for reporting purposes.

Note: You do not need to install the central database on either the Report Server or Report Portal computer but you need only one instance between both and all computers should be able to communicate over the network.

To install and configure an RDBMS as a central database

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 reporting service:

   - Make sure the database can be accessed locally and from a remote client.
   - For Oracle, create a new administrative user for the central database.

     This user should have permissions to create tables and modify data.
   - For SQL Server:
     - Create a new case-sensitive database.
     - Create a new user, make the new database their default database, and give them DB_owner privileges.

Example: Install and Configure Oracle Database XE

Important! For simplicity, this procedure describes the installation of Oracle Database XE, which is *not* officially supported for production systems. If you are planning to use the product in production, you should have a database administrator install a fully supported RDBMS.

The following steps illustrate how you configure Oracle for remote clients and create a new administrative user to use with CA Access Control reporting service:

1. When you install Oracle Database XE, provide the SYS and SYSTEM database accounts' password.

   Oracle Database XE is installed.

2. Launch Oracle Database Home Page.

   - On Windows, click Start, Oracle Database 10g Express Edition, Go To Database Home Page

     Note: To do this during installation, select the check box on the final page of the installation wizard.

   - On UNIX, open a browser and enter the following URL:
     http://127.0.0.1:8080/apex

     Note: This URL assumes you installed Oracle Database XE using the default port.

   The Database Login page appears.

3. Log in using the user name *system* and the password you set when you installed Oracle Database XE.

   The Home page appears.

4. Click the down arrow next to the Administration icon and select Manage HTTP Access.

   The Manage HTTP Access page appears.

5. Make sure that the Available from local server and remote clients option is selected, then click Apply Changes.

6. Click the down arrow next to the Administration icon and select Database Users, Create User.

   The Create Database User page appears.

7. Complete the dialog as follows:

   - Type a username and password (make sure you record these credentials)
   - Keep the default Roles selected (CONNECT and RESOURCE but not DBA).
   - Select all of the options for Direct Grant System Privileges.

   Click Create.

   The new administrative user is created and you can use it to connect to the database.

How to Set Up the Report Server Computer

To process all of your endpoint data and send it to the central database for storage, you need to set up the Report Server. To do this, you first install the prerequisite software and then install CA Access Control Report Server.

To set up the Report Server, do the following:

1. If you do not already have one, set up the central database.

2. Install a supported JDK version and restart the computer if required by the installation program.

   Note: You can find the prerequisite third-party software on the CA Access Control Premium Edition Third Party Components for Solaris and CA Access Control Premium Edition Third Party Components for Windows DVDs. For a list of supported software and versions, see the *Release Notes*.

3. 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:\j2sdk1.4.2_12
   ```

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

   ```
   export JAVA_HOME=/usr/jdk/j2sdk.1.4.2_12/
   ```

4. Make sure the PATH environment variable includes the JDK installation path.

   To test this, open a command prompt window and enter **java**. If the Java usage screen appears, this is set correctly.

5. Install a supported application server.

   We recommend that you run the application server as a service (daemon on UNIX).

   Note: You can find the prerequisite third-party software on the CA Access Control Premium Edition Third Party Components for Solaris and CA Access Control Premium Edition Third Party Components for Windows DVDs. For a list of supported software and versions, see the *Release Notes*. To install the supplied JBoss version, extract the contents of the JBoss zip file to /opt on Solaris or to your C drive on Windows.

6. Install CA Access Control Report Server.

   You now have your Report Server computer set up.

Report Server Upgrades

The Report Server installation supports upgrade from r12.0. When you upgrade, the installation prompts you for the information that is necessary for the upgrade process only. For example, passwords to access the message bus and the central database.

During upgrade, the installation:

- Replace all Report Server archive file (acrptsrv.ear) contents, except for the configuration files.
- Upgrades the database schema if it is not current.
- Adds a new audit queue to the Report Server for endpoint audit data if it does not already exist.

Install CA Access Control Report Server Using a Graphical Interface

The graphical installation uses a wizard to support and guide you when installing CA Access Control Report Server.

To install CA Access Control Report Server using a graphical interface

1. Make sure you set up the Report Server computer correctly.
2. Do either of the following:
   - On Windows:
     a. Insert the CA Access Control Premium Edition Server Components for Windows DVD into your optical disc drive.
     b. Open the CA Access Control Product Explorer (ProductExplorerx86.EXE).

        The CA Access Control Product Explorer appears.
     c. Expand the Components folder, select CA Access Control Report Server, then click Install.

        The InstallAnywhere wizard starts loading.
   - On UNIX:
     a. Insert the CA Access Control Premium Edition Server Components for Solaris DVD into your optical disc drive.
     b. Connect to the host using an X Window terminal session.
     c. Mount the optical disc drive.
     d. Locate the ReportServer directory, then run install.bin

        The InstallAnywhere wizard starts loading.

   Note: You need a localized operating system to install in any of the non-English supported languages.
3. Complete the wizard. The following wizard pages are not self-explanatory:

   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, C:\jboss-4.0.5.GA on Windows or /opt/jboss-4.0.5.GA on Solaris.

   – Define the name of the JBoss server configuration set where you want CA Access Control Report Server installed.

   InstallAnywhere tests to see whether the directory *JBoss Folder*/server/*Configuration Name* exists before it lets you continue.

Report Server Security Settings

Specifies whether to use SSL to secure the communications between the CA Access Control Report Server and Report Agents.

If you select this option, you also need to define the following SSL settings:

- Path to the server certificate file
- The server certificate password
- The password (shared secret) that is used to authenticate Report Agents

Report Server Settings

Defines the port the Report Server uses to accept CA Access Control database snapshots from the Report Agent.

Keep the default.

Database Server Settings

Defines configuration settings for the reporting service central database. These are:

- Name, port, and SID of the RDBMS server
- The user name and password.

  This must be the same user ID and password you created when you configured the RDBMS.

The installation verifies that it can connect to the database.

Once the installation completes, the Report Server is up and running, ready to receive and process incoming data.

Install CA Access Control Report Server Using a Console

If you do not want to use the graphical installation because you are installing from a text-only terminal or do not have the required X Server graphics software that the InstallAnywhere wizard requires, you can use the console installation to install CA Access Control Report Server.

To install CA Access Control Report Server using a console

1. Make sure you set up the Report Server computer correctly.
2. Do either of the following:
   - On Windows:
     a. Insert the CA Access Control Premium Edition Server Components for Windows DVD into your optical disc drive.
     b. Open a command line and navigate to the ReportServer directory on the optical disc drive.
     c. Enter the following command:

        ```
        install_RS_r12_SP1.exe -i console
        ```
   - On UNIX:
     a. Insert the CA Access Control Premium Edition Server Components for Solaris DVD into your optical disc drive.
     b. Connect to the host using a terminal session.
     c. Mount the optical disc drive.
     d. Open a terminal window and navigate to the ReportServer directory on the optical disc drive.
     e. Enter the following command:

        ```
        install_RS_r12_SP1.bin -i console
        ```

   The InstallAnywhere console appears after a few moments.
3. Complete the prompts as required. The following prompts 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 non-English supported languages.

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, C:\jboss-4.0.5.GA on Windows or /opt/jboss-4.0.5.GA on Solaris.

- Define the name of the JBoss server configuration set where you want CA Access Control Report Server installed.

InstallAnywhere tests to see whether the directory *JBoss Folder*/server/*Configuration Name* exists before it lets you continue.

Report Server Security Settings

Specifies whether to use SSL to secure the communications between the CA Access Control Report Server and Report Agents.

If you select this option, you also need to define the following SSL settings:

- Path to the server certificate file
- The server certificate password
- The password (shared secret) that is used to authenticate Report Agents

Report Server Settings

Defines the port the Report Server uses to accept CA Access Control database snapshots from the Report Agent.

Keep the default.

Database Server Settings

Defines configuration settings for the reporting service central database. These are:

- Name, port, and SID of the RDBMS server
- The user name and password.

  This must be the same user ID and password you created when you configured the RDBMS.

The installation verifies that it can connect to the database.

Once the installation completes, the Report Server is up and running, ready to receive and process incoming data.

Uninstall CA Access Control Report Server 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 Report Server 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 Report Server.
4. Click Change/Remove.

   The Uninstall CA Access Control Report Server wizard appears.
5. Follow the wizard's instructions to uninstall CA Access Control Report Server.

   The uninstll completes and removes CA Access Control Report Server from your computer.
6. Click Done to close the wizard.

Uninstall CA Access Control Report Server on Solaris

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

To uninstall CA Access Control Report Server 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:

   ```
   "/ACRSnstallDir/_uninst/Uninstall_CA_Access_Control_Report_Server"
   ```

   ACRSInstallDir

   Defines the installation directory of CA Access Control Report Server. By default this path is:

   ```
   /opt/CA/AccessControlServer/ReportServer/
   ```

   InstallAnywhere loads the uninstall wizard or console.

   Note: The uninstall loads using the same method you used to install. That is, if you installed using a console the uninstall is also performed in a console. Otherwise, the uninstall loads a wizard.

3. Follow the prompts to uninstall CA Access Control Report Server.

   The uninstll completes and removes CA Access Control Report Server from your computer.

How to Set Up the Report Portal Computer

The Report Portal lets you access the endpoint data that the Report Server stores in the central database to produce built-in reports, or to interrogate the data and produce custom reports. To do this, it uses CA Business Intelligence.

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

To set up the Report Portal, do the following:

1. If you have not already done so, set up the central database and Report Server.
2. (Solaris only) Prepare your operating system for CA Business Intelligence installation.

3. Install CA Business Intelligence for your operating system.

   You can find the CA Business Intelligence installation files on the CA Access Control Premium Edition Server Components DVD for your operating system.

   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.

4. (Optional) Configure CA Business Intelligence for large deployments.

Example: Install CA Business Intelligence on Windows

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

1. If you do not already have one, set up the central database.
2. Install a supported JDK version and restart the computer if required by the installation program.

   Note: You can find the prerequisite third-party software on the CA Access Control Premium Edition Third Party Components for Solaris and CA Access Control Premium Edition Third Party Components for Windows DVDs. For a list of supported software and versions, see the *Release Notes*.

3. 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:\j2sdk1.4.2_12
   ```

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

   ```
   export JAVA_HOME=/usr/jdk/j2sdk.1.4.2_12/
   ```

4. Make sure the PATH environment variable includes the JDK installation path.

   To test this, open a command prompt window and enter **java**. If the Java usage screen appears, this is set correctly.

5. Insert the CA Access Control Premium Edition Server Components for Windows DVD into your optical disc drive.
6. Navigate to the \ReportPortal\Disk1\InstData\VM folder and double-click install.exe.

   The CA Business Intelligence installation wizard begins.

7. 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 non-English supported languages.
License Agreement	Select I accept the terms of the License Agreement and click Next.
Installation Type	Select Typical and click Next3
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
Enable Auditing	Click Next to accept the defaults.
Audit Database Settings	Enter the following information, then click Next: ■ **User Name:** cadbusr ■ **Password:** C0nf1dent1al ■ **Database Name:** MySQL1
Review Settings	Review the settings and click Install to complete the installation.

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

Prepare Solaris for CA Business Intelligence Installation

Before you can install CA Business Intelligence on Solaris, you must prepare the computer for this installation. This involves creating a non-root user for the CA Business Intelligence installation and to make sure that the Oracle RDBMS is exposed to the installation of CA Business Intelligence.

To prepare Solaris for CA Business Intelligence installation

1. Logged in as *root*, create a non-root user.

   For example:

   ```
   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.

   Note: The CA Business Intelligence installation requires a non-root use. In the preceding example, we created a user named *bouser* that belongs to the group *other*.

2. Log in as the non-root user you created.

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

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

   A non-empty output verifies 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, ensure these 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
   ```

4. Ensure 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, add 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
   ```

5. Ensure 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
   ```

6. Ensure that Oracle connectivity is valid, using the TNS Ping utility as follows:

   ```
   $ORACLE_HOME/bin/tnsping XE
   ```

   The output from TNS Ping should look as follows:

   ```
   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 = XE)))
   OK (30 msec)
   ```

   You can now install CA Business Intelligence on Solaris.

Configure BusinessObjects for Large Deployments

So you can run CA Access Control reports on large deployments, you need to change the BusinessObjects default configuration. By default, the maximum number of concurrent connections that the BusinessObjects page server can create is set to 20,000. You also need to set 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. 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. If not already there, append the following text 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 link to 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.

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 a Windows Report Portal

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 Windows when no previous version of the same package is already deployed.

To deploy the report package on a Windows Report Portal

1. If you have not already done so, set up the central database, Report Server, and Report Portal.
2. Insert the CA Access Control Premium Edition Server Components for Windows DVD into your optical disc drive and navigate to the \ReportPortal folder.
3. Extract the contents of biconfig.zip into *System_Drive*:\BO folder.

4. Copy the following files from the optical disc drive into *System_Drive*:\BO folder as well:

   ■ \ReportPortal\AC_BIAR_Config

   ■ \ReportPackage\AC_BIAR_File

   AC_BIAR_Config

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

   For example, for Oracle Database 10g this is import_biar_config.xml while for SQL Server 2005 it is import_biar_config_mssql_2005.xml.

   AC_BIAR_File

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

   Note: The biar-file 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 *System_Drive*:\BO\AC_BIAR_Config file as required.

   For example, for Oracle Database 10g, edit the file as follows:

```
<biar-file name="System_Drive:/BO/AC_BIAR_File">
    <networklayer>Oracle OCI</networklayer>
    <rdms>Oracle 10</rdms>
    <username>adminUserName</username>
    <password>adminUserPass</password>
    <datasource>Oracle_TNS_Name</datasource>
    <server></server>
</biar-file>
```

   For SQL Server 2005, edit the file as follows:

```
<biar-file name="System_Drive:/BO/AC_BIAR_FILE">
    <networklayer>OLE DB</networklayer>
    <rdms>MS SQL Server 2005</rdms>
    <username>adminUserName</username>
    <password>adminPassword</password>
    <datasource>SQL_databaseName</datasource>
    <server>localhost</server>
</biar-file>
```

   biar-file name

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

   networklayer

   Defines the network layer supported by your RDBMS.

username

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

password

Defines the password of the RDBMS administrative user you created.

datasource

Defines the name of the Transparent Network Substrate (TNS) of the Oracle database or the database you created in SQL Server 2005.

server

Defines the name of the SQL Server 2005 server. Leave this empty for Oracle Database 10g.

6. Open a command prompt and run the following command:

   System_Drive:\BO\biconfig.bat -h <*host_name*> -u <*user_name*> -p <*password*> -f <*config_xml*>

   For example:

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

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

Example: Sample Import Configuration File

The following code snippet is an example of how you can edit the import configuration file (import_biar_config.xml) for Oracle Database XE:

```
<?xml version="1.0"?>
<biconfig version="1.0">
 <step priority="1">
  <add>
   <biar-file name="c:/BO/accesscontrolr12.0.102.biar">
    <networklayer>Oracle OCI</networklayer>
    <rdms>Oracle 10</rdms>
    <username>ciadb01</username>
    <password>P@ssw0rd</password>
    <datasource>XE</datasource>
    <server></server>
   </biar-file>
  </add>
 </step>
</biconfig>
```

Deploy the Report Package on a Solaris Report Portal

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 Solaris when no previous version of the same package is already deployed.

To deploy the report package on a Solaris Report Portal

1. If you have not already done so, set up the central database, Report Server, and Report Portal.
2. Insert the CA Access Control Premium Edition Server Components for Solaris DVD into your optical disc drive and navigate to the /ReportPortal directory.
3. Extract the contents of biconfig.zip into a temporary directory.
4. Copy the following files from the optical disc drive into the same temporary directory:
   - /ReportPortal/import_biar_config.xml
   - /ReportPackage/*AC_BIAR_File*

   AC_BIAR_File

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

   Note: The biar-file property of the import configuration file (import_biar_config.xml) points to this file and is set by default to the name of the English version for Oracle Database.
5. Edit your copy of the import_biar_config.xml file as follows:

```
<biar-file name="/temp_dir/AC_BIAR_File">
    <networklayer>Oracle OCI</networklayer>
    <rdms>Oracle 10</rdms>
    <username>Oracle_adminUserName</username>
    <password>Oracle_adminUserPass</password>
    <datasource>Oracle_TNS_Name</datasource>
    <server></server>
</biar-file>
```

   AC_BIAR_File

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

   Oracle_adminUserName

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

Oracle_adminUserPass

Defines the password of the Oracle administrative user you created.

Oracle_TNS_Name

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

6. 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 <config_xml>
   ```

   For example:

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

   The script file imports the CA Access Control reports into InfoView and can take a few minutes to complete.

Deploy the Report Package on a Report Portal That You Installed with 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 for Windows that you installed with CA Access Control r12.0.

To deploy the report package on a Report Portal that you installed with r12.0

1. Create a temporary folder for the installation files:
   - On Windows, create a BO folder under the root of C drive.
   - On Solaris, create the directory /work/bo
2. Insert the CA Access Control Premium Edition r12.0 SP1 Server Components DVD for your platform into the optical disc drive and navigate to the /ReportPortal directory.
3. Copy /ReportPackage/*AC_BIAR_File* from the optical disc drive into temporary installation folder you created.

   AC_BIAR_File

   Defines the name of the CA Access Control reports file (.biar) for your language and 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 (~2 GB) from the DVD to the C:\BO folder you created.

   - On Solaris, extract the data from the /ReportPortal/bo_install.tar.gz file, that is on CA Access Control Premium Edition Server Components DVD, into the /work/bo folder you created.

6. Edit your copy of the *BO_Files*/biek-sdk/biekInstall.properties file as follows:

```
BIEK_CONNECT_LAYER=Oracle OCI
BIEK_CONNECT_DB=Oracle 10
BIEK_CONNECT_USER=Oracle_adminUserName
BIEK_CONNECT_PASSWORD=Oracle_adminUserPass
BIEK_CONNECT_SOURCE=Oracle_TNS_Name
BIEK_BO_USER=InfoView_adminUserName
BIEK_BO_PASSWORD=InfoView_adminUserPass
BIEK_BIAR_FILE=AC_BIAR_File
```

   Oracle_adminUserName

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

   Oracle_adminUserPass

   Defines the password of the Oracle administrative user you created.

   Oracle_hostName

   Defines the host name of the Oracle server.

   Oracle_TNS_Name

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

   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

Defines the full pathname to the CA Access Control reports file (.biar).

7. Do one of the following:

   - On Windows, launch the batch file *BO_Files*/biek-sdk/importBiarFile.bat
   - On UNIX, run the *BO_Files*/biek-sdk/importBiarFile.sh script file.

   The file imports the CA Access Control reports and into InfoView and can take a few minutes to complete.

Open InfoView for Working with Reports

You access CA Access Control reports using BusinessObjects InfoView. The following procedure describes how you access the reporting interface (BusinessObjects InfoView).

To open InfoView for working with reports

1. Launch InfoView in *one* of the following ways:

   - On the computer where BusinessObjects InfoView is installed, select Start, Programs, BusinessObjects XI Release 2, BusinessObjects Enterprise, BusinessObjects Enterprise Java InfoView.
   - From a browser on any computer, navigate to the following URL:

     http://*ACRPTGUI_host*:*ACRPTGUI_port*/businessobjects/enterprise115

     ACRPTGUI_host—The name or IP address of the computer where the InfoView is installed (Report Portal).

     ACRPTGUI_port—The port number used to access InfoView, by default, 9085.

   The InfoView Log On page appears.

2. Enter the credentials you set up when you installed InfoView, and click Log On.

   The InfoView Home page appears.

Note: For more information about using BusinessObjects InfoView, see the *BusinessObjects Enterprise XI Release 2 InfoView User's Guide*.

Received "Null page" Error in InfoView

Symptom:

When I try to access the CA Access Control reports I get the following error in InfoView:

```
Null page: Unable to create page from report source
```

Solution:

On Windows, the CA Access Control universe may not be defined or installed properly. Test the connection for the CA Access Control universe and edit it if it is not working or replace it if it is.

On Solaris, log in as bouser and edit $CASHCOMP/CommonReporting/bobje/setup/env.sh to append the following LIBRARYPATH and then restart BusinessObjects services:

```
$MWHOME/lib-sunos5_optimized
cd $CASHCOMP/CommonReporting/bobje
./stopservers
./startservers
```

Test the CA Access Control Universe Connection

The CA Access Control Universe is provided by CA to simplify the creation of reports from the CA Access Control reporting service central database.

Note: For more information about the CA Access Control Universe, see the *Enterprise Administration Guide*.

If after you install the standard CA Access Control reports you experience issues with the reporting service connection, you should test and modify the connection as required.

To test the CA Access Control Universe Connection

1. Select Start, Programs, Business Objects XI Release 2, BusinessObjects Enterprise, Designer.

   The User Identification dialog appears, letting you log in to BusinessObjects Designer.

2. Enter your credentials and click OK.

   The welcome screen of the Quick Design wizard appears.

3. Clear the Run this Wizard at Startup check box, and click Cancel

   An empty Designer session opens. The user name and repository name appear in the title bar.

4. Click File, Import, browse to the directory that contains the CA Access Control Universe, select the CA Access Control universe, then click OK.

   The CA Access Control Universe imports successfully and opens in the current Designer window.

   Note: The CA Access Control Universe is stored under CA Universe\CA Access Control in the directory designated as the default universe file store.

5. Click Tools, Connections

   The Wizard Connection dialog appears.

6. Select the Access_Control1 connection that you want to test, then click Test.

   A message confirms that the connection is responding. If the connection is not responding you receive an error message.

7. If you received an error, click Edit to modify connection settings:

   - Database Middleware Selection—Oracle\Oracle 10\Oracle Client
   - Type—Secured
   - Name—Access_Control1
   - User name—*Oracle_adminUserName*
   - Password—*Oracle_adminUserPass*
   - Service—Oracle_TNS_Name

   Repeat step 6 as required to test the connection.

Replace the CA Access Control Universe

The CA Access Control Universe is provided by CA to simplify the creation of reports from the CA Access Control reporting service central database.

Note: For more information about the CA Access Control Universe, see the *Enterprise Administration Guide*.

If you tested the connection for the CA Access Control universe and it was fine, but you are still experiencing issues with the reporting service connection, you should replace the connection.

To replace the CA Access Control Universe Connection

1. Select Start, Programs, Business Objects XI Release 2, BusinessObjects Enterprise, Designer.

   The User Identification dialog appears, letting you log in to BusinessObjects Designer.

2. Enter your credentials and click OK.

   The welcome screen of the Quick Design wizard appears.

3. Clear the Run this Wizard at Startup check box, and click Cancel

   An empty Designer session opens. The user name and repository name appear in the title bar.

4. Click File, Import, browse to the directory that contains the CA Access Control Universe, select the CA Access Control universe, then click OK.

   The CA Access Control Universe imports successfully and opens in the current Designer window.

   Note: The CA Access Control Universe is stored under CA Universe\CA Access Control in the directory designated as the default universe file store.

5. Click Tools, Connections

   The Wizard Connection dialog appears.

6. Select the Access_Control1 connection that you want to replace, then click Remove.

   A warning appears, asking you to confirm that you want to remove the connection.

7. Click Add and follow the wizard to define a new connection with the following settings:

   - Database Middleware Selection—Oracle\Oracle 10\Oracle Client
   - Type—Secured
   - Name—Access_Control1

- User name—*Oracle_adminUserName*
- Password—*Oracle_adminUserPass*
- Service—Oracle_TNS_Name

Make sure you test the connection.

8. Click File, Export, and export the universe to the CA Access Control universe.

   A message confirming that the universe was successfully exported appears.

Configure an Endpoint for Reporting

Once you have your Report Server installed and configured, you can configure your endpoints for sending data to the Report 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 an endpoint for reporting on Windows

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.

To configure an endpoint for reporting on UNIX

1. Run ACInstallDir/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 Report 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)
```

Chapter 8: 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.

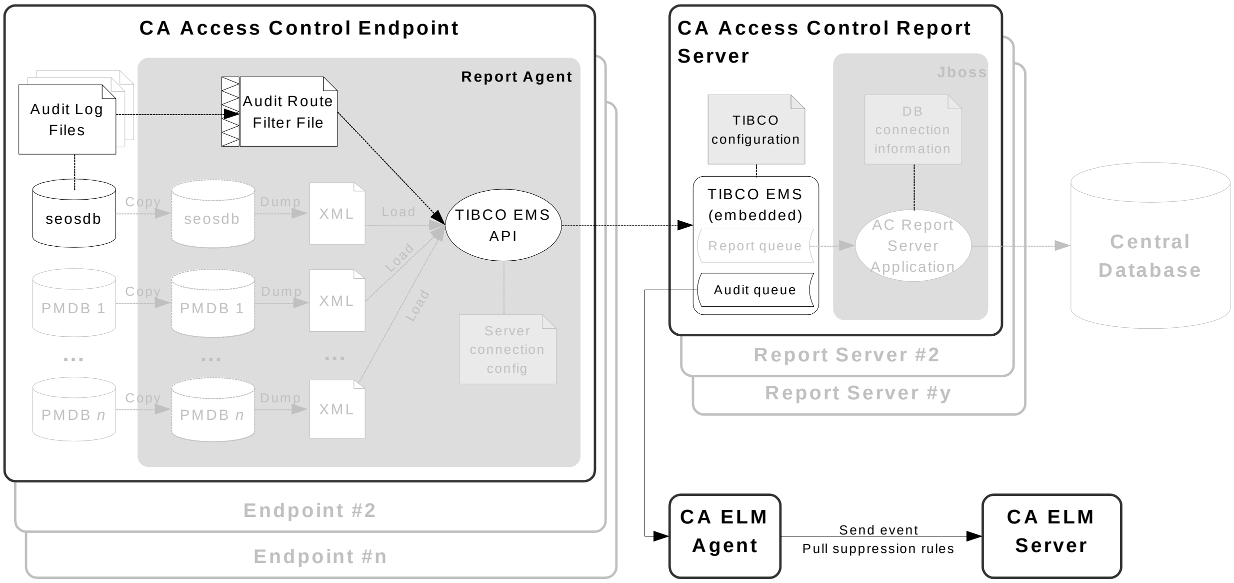
CA Enterprise Log Manager Integration Architecture

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 local endpoint's audit file to a remote audit queue on the Report 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 it to the Report Server.
- The Report 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 (Report Agent and Report Server). 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 grayed-out in the diagram.

More information:

Reporting Service Architecture (see page 171)

CA Enterprise Log Manager Integration Components

CA Enterprise Log Manager integration uses the following CA Access Control components:

- A *Report Agent* is a Windows service or a UNIX daemon that runs on each CA Access Control endpoint and sends information to message queues on a configured Report 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 Report Server.
- A *Report Server* is a server with message queues configured for receiving endpoint information that Report Agents send. For redundancy and failover, you can have multiple Report Servers collecting the information.

Note: These components are part of the CA Access Control reporting service.

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 Report Server and 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 dedicated to refining incoming event logs, inserting them into the hot database, compressing the hot database when it reaches the configured size into a warm database, and auto-archiving the warm database to the related management server on the configured schedule.

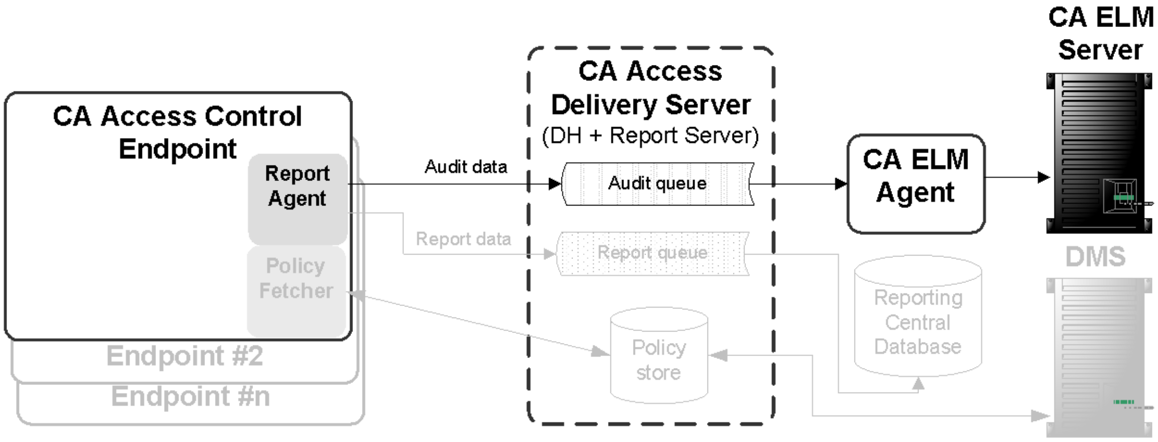
Note: For more information about CA Enterprise Log Manager components, see the CA Enterprise Log Manager documentation.

More information:

Reporting Service Architecture (see page 171)

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 you need to consider when configuring this integration, you first need to 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 Report 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's audit files, applies any filtering policies, and places the events on a remote audit queue located on the Report 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/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 on how CA Enterprise Log Manager works, see the CA Enterprise Log Manager documentation.

How to Set Up Report Server for CA Enterprise Log Manager

To use CA Enterprise Log Manager to create reports that contain audit data from all your CA Access Control endpoints, you first need to install and configure the Report Server component of the CA Access Control reporting service.

To set up Report Server for CA Enterprise Log Manager, follow these steps:

1. Install and configure an RDBMS as the central database (see page 174).
2. Set up the Report Server computer and install CA Access Control Report Server (see page 176).

Note: For operating systems support and detailed information about the supported applications and versions, see the *Release Notes*.

Once you have the Report Server installed, you need to set up CA Enterprise Log Manager for CA Access Control and configure the Report Agent on each endpoint.

More information:

How to Set Up CA Enterprise Log Manager for CA Access Control (see page 206)
Configure the Endpoint for CA Enterprise Log Manager Integration (see page 215)

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

Once you set up the CA Access Control Report Server for CA Enterprise Log Manager, you need to set up CA Enterprise Log Manager for CA Access Control. In particular, you need to install a CA Enterprise Log Manager agent on or near the CA Access Control Report Server and create a CA Enterprise Log Manager connector so that CA Enterprise Log Manager can access the CA Access Control event source.

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 Report Server.

   The agent must be accessible to the Report 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 trying to install it. For more information on installing the agent, see the *CA Enterprise Log Manager Agent Installation Guide*.

3. Create a new connector for the agent.

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

   Note: This section's topics describe settings that are required for CA Access Control event collection. For more information on how to create a connector, see the *CA Enterprise Log Manager Administration Guide* and the *Online Help*.

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 (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.

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

Integration

Specifies the integration you want to use as a template.

Select AccessControl_R12SP1_TIBCO_Connector

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.

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 or Access Control. When you create rules, select the values for Event Category, Event Class, and Event Action as needed to identify events.

Note: For information on other optional settings that may 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 on other optional settings that may 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 TIBCO server in the following format:

Protocol://server IP or name:Port number

For example, when installing the CA Access Control Report Server you specify if you want to communicate using SSL. Based on your response, specify one of the following:

- If you did not select SSL, specify the following value:

  tcp://AC*ReportServer*:7222

- If you selected SSL, specify the following value:

  ssl://AC*ReportServer*:7243

These port values are the default ports that the Report Server uses. If you specified a different value when you installed the Report Server, you must use that port value.

TIBCO User

Specifies the user name for TIBCO server authentication.

For example, when installing the CA Access Control Report Server you specify if you want to communicate using SSL. Based on your response, specify one of the following:

- If you did not select SSL, you did not enter a user name. Leave this field empty.

  The Report Server uses anonymous authentication.

- If you selected SSL, specify the user name you defined during the CA Access Control Report Server Installation.

TIBCO Password

Specifies the password for TIBCO server authentication.

For example, when installing the CA Access Control Report Server you specify if you want to communicate using SSL. Based on your response, specify one of the following:

- If you did not select SSL, you did not enter a password. Leave this field empty.

  The Report Server uses anonymous authentication.

- If you selected SSL, specify the password you defined during the CA Access Control Report Server Installation.

Event Log Name

Specifies the log name for the event source.

Accept the default, "eTrust Access Control".

PollInterval

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

SourceName

Specifies the identifier for the TIBCO queue.

Accept the default, "queue_audit".

TIBCO Queue

Specifies the name of the TIBCO 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 TIBCO queue messages.

Adjust this value to keep up with events and if you know you have sufficient CPU on the CA Enterprise Log Manager agent system.

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

Types of Events Mapped

Assuming CA Access Control performs no event filtering, the following types of events are mapped for this connector:

Identity Management

- Account creation
- Account deletion
- Account modification
- Account password change
- Group creation
- Group deletion
- Group modification
- Group membership addition
- Group membership removal

Configuration Management

- Configuration change
- Policy creation
- Policy deletion
- Policy modification
- Policy activation

Network Security

- Connection attempt

Operational Security

- Process create
- Process delete
- Process modify
- Process start
- Process stop

Resource Access

- Resource access
- Resource creation

- Resource deletion
- Resource modification

System Access

- Login attempt

SIM Operations

- Alert escalation

Log Name

The log name for CA Access Control is eTrust Access Control. You can use the log name when setting filter conditions for generating custom reports.

How the Report Agent Collects and Routes Audit Events to the Report Server

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 Report Server. You can affect performance by tuning the Report Agent settings.

Note: The Report Agent is part of the CA Access Control 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 if you enable audit collection (audit_enabled configuration setting):

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

  The Report Agent reads the number of audit records you defined in the audit_read_chunk configuration setting and then waits for the duration you defined in the audit_sleep configuration setting before reading the audit files again. It reads previously unread records in the active audit log *and* all of 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 Report Server messaging queue 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 since 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 needs to read 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 Report Server handles big 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 this amount of records to the Report Server. Assuming 30 events per second, if we want the Report Agent to send audit records at approximately one minute intervals (60 seconds), we need to set 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 make sure the Report Agent still regularly sends audit records to the Report Server, we set a maximum interval of five minutes between sending audit records, as follows:

```
audit_timeout=300
```

Filter Events from CA Enterprise Log Manager

You can use a filter file to define which records CA Access Control should *not* send to the Report Server if you do not want to send to CA Enterprise Log Manager all of the audit records that CA Access Control writes to the log file.

Note: Filtered audit events are written to the local audit file but CA Access Control does not send them to the message queue on the Report Server. To filter out audit messages from the local audit file, modify filter rules in the file defined by the AuditFiltersFile configuration setting in the logmgr section (by default, audit.cfg).

To filter events from CA Enterprise Log Manager, create an audit filtering policy and assign the policy to the endpoints where you want it to be effective.

Note: Alternatively, you can directly edit the audit routing filter file on the endpoint. 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 Report Server.

Secure Communications using SSL

When you install the Report Server you can choose to either secure the communication between the Report Server and Report Agent by using SSL or choose to not secure the communication. Whichever option you choose, you must specify the same option when you install the Report Agent on the endpoint.

For example, if you choose to use SSL to encrypt the communications between the Report Agent and the Report Server (the default), then you must provide authentication information when you install the Report Server such as:

- The port to be used
- The administrative password to access the message bus console
- The password for the certificate
- The password required for the Report Agents to communicate with the Report 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 Report 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.

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, 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 the Endpoint for CA Enterprise Log Manager Integration

Once you have your Report Server installed and configured, you can configure your endpoints for sending audit data to the Report 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 endpoint for CA Enterprise Log Manager integration on Windows

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 and the Audit Routing sub-feature.

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

To configure an endpoint for CA Enterprise Log Manager integration on UNIX

1. Run ACInstallDir/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 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 Report 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 Report Server (see page 211). For more information on 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.

You can find CA Access Control events in the following queries, reports, and action alerts:

- **Q**—query
- **R**—report
- **AA**—action alert

Type	Title
AA	Excessive Session Activity in an Hour
AA	Ten Failed Resource Access by Session in an Hour
Q, R	Resource Access Sessions By Action
Q	Resource Access Sessions By Host
Q	Resource Access Sessions By Performer
Q	Resource Access Sessions by Action Summary
R	Resource Access Sessions by Business Critical Hosts
Q	Resource Access Sessions by Business Critical Hosts By Action
Q	Resource Access Sessions by Business Critical Hosts By Performer
Q	Resource Access Sessions by Business Critical Hosts By Result
Q	Resource Access Sessions by Business Critical Hosts Detail
Q	Resource Access Sessions by Business Critical Hosts Summary
Q	Resource Access Sessions by Business Critical Hosts Trend
Q, R	Resource Access Sessions by Host
Q	Resource Access Sessions by Host Summary
Q, R	Resource Access Sessions by Performer
Q	Resource Access Sessions by Performer Summary
Q, R	Resource Access Sessions by Resource Name
Q	Resource Access Sessions by Resource Name Summary
Q	Resource Access Sessions By Result

Type	Title
Q	Resource Access Sessions Detail
Q	Resource Access Sessions Trend
Q	Session Tracking By Account
Q	Session Tracking By Action
Q, R	Session Tracking by Host
Q	Session Tracking by Host Summary
Q	Session Tracking By Performer
Q	Session Tracking Detail
Q	Session Tracking Trend

Additionally, the following queries are available under the Investigation tag:

Type	Title
Q	Excessive Session Activity in an Hour
Q	Investigate By Destination Object Class
Q	Investigate Hourly Trend
Q	Investigate Session By Category
Q	Resource Access Sessions By Host

Chapter 9: 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.

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.
- Each endpoint does not have to be re-subscribed to the restored DHs after you have recovered from a disaster.

The following CA Access Control components are not backed up or restored during the disaster recovery process. You must back up these components separately:

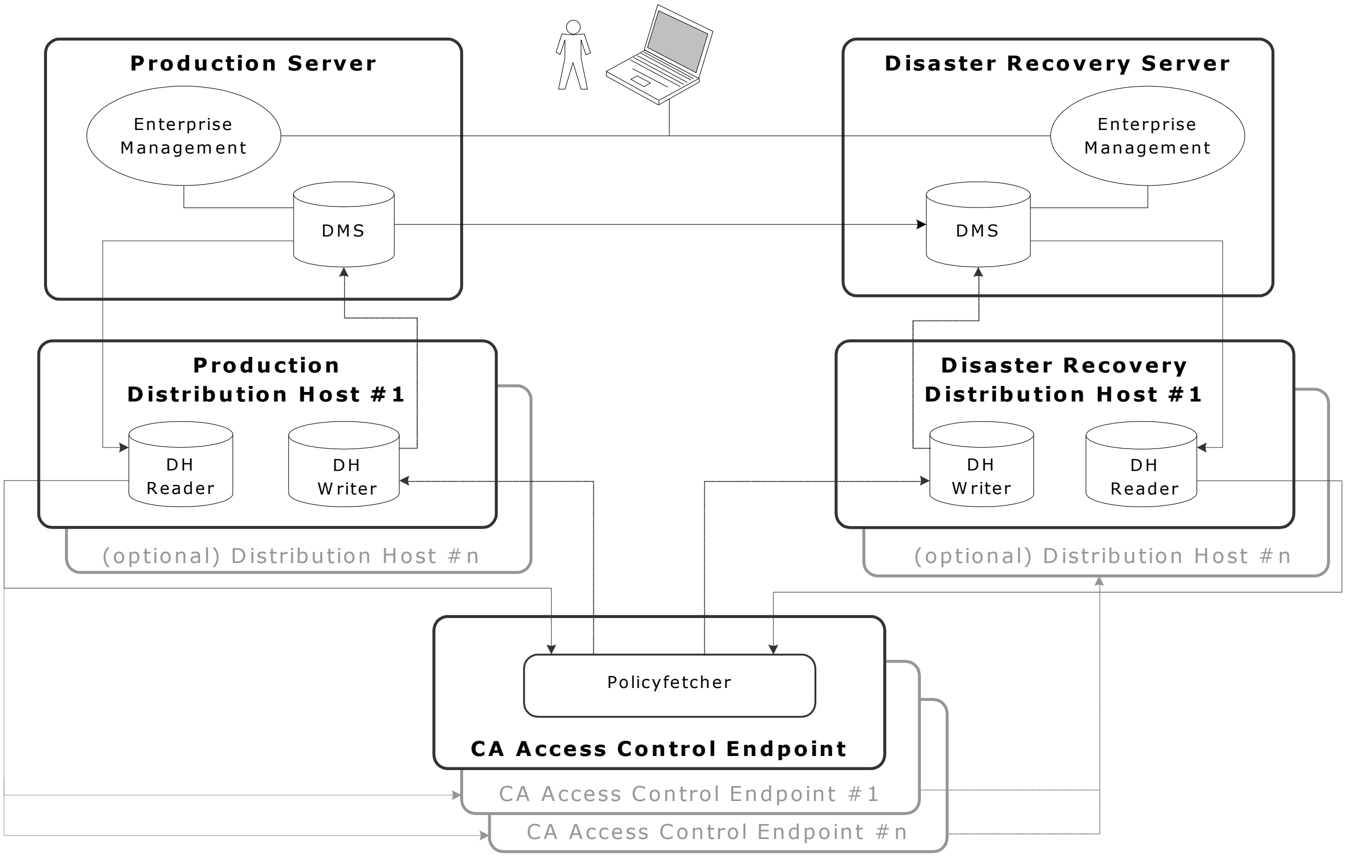
- password policy models
- PMDBs
- CA Access Control Endpoint Management
- CA Access Control Enterprise Management
- data on the endpoints
- CA Access Control audit files

Note: CA Access Control audit files are not saved when the DMS is backed up, however the DMS audit file is saved when the DMS is backed up.

Disaster Recovery Architecture

The following diagram shows how you can deploy CA Access Control in a disaster recovery configuration.

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.


Production Server
Enterprise Management
DMS
Disaster Recovery Server
Enterprise Management
DMS
Production Distribution Host #1
DH Reader
DH Writer
(optional) Distribution Host #n
Disaster Recovery Distribution Host #1
DH Writer
DH Reader
(optional) Distribution Host #n
Policyfetcher
CA Access Control Endpoint
CA Access Control Endpoint #1
CA Access Control Endpoint #n

Components for Disaster Recovery

You need the following components to deploy CA Access Control in a disaster recovery configuration:

- For the production environment:
  - One DMS server
  - One installation of CA Access Control Enterprise Management
  - One or more DHs

    Note: We recommend that you do not install the DMS and DH on the same host. Installing the DMS and DH on separate hosts increases the scalability of the deployment.
- For the disaster recovery environment:
  - One DMS server
  - One installation of CA Access Control Enterprise Management
  - One or more DHs

    Note: We recommend that you do not install the DMS and DH on the same host. Installing the DMS and DH on separate hosts increases the scalability of the deployment.
- For the enterprise:
  - One or more endpoints, each with Advanced Policy Management Client components installed
  - (Optional) CA Access Control Enterprise Management web interface

    Note: The enterprise components work with both the production and disaster recovery environments.

You should also 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 r12.0 SP1 from backup files of a DMS using CA Access Control r12.0.
- You should store the backup DMS files in a safe location, preferably protected by CA Access Control access rules.
- If you wish, you can install a single instance of CA Access Control Enterprise Management, and configure a connection from this installation to both the production DMS and the disaster recovery DMS. However, to make it easier to upgrade to future versions of CA Access Control, we recommend that you install CA Access Control Enterprise Management on both the production DMS and the disaster recovery DMS servers.

How a Disaster Recovery Deployment Works

A disaster recovery deployment creates a duplicate of your production DMS database, ensures 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 works:

1. You configure the endpoints to work against a list of production and disaster recovery DHs.
2. At the specified time, the endpoint tries to connect to a DH in the production environment.
    a. The endpoint tries to connect to the first production DH in its list. If it does not connect, it tries to connect to that DH for a specified number of attempts. *One* of the following happens:
        - The endpoint connects to the production DH. The process ends at this step.
        - The endpoint does not connect to the production DH. The process goes to the next step.

        Note: The number of times the endpoint attempts to connect to the DH is defined in the max_dh_command_retry configuration setting in the policyfetcher section.

    b. The endpoint tries to connect to the second production DH in its list, then the third, and so on (for the same defined number of times, if required). One of the following happens:
        - The endpoint connects to a production DH. The process ends at this step.
        - The endpoint does not connect to any production DH, and the cycle ends. The process goes to the next step.
3. The endpoint repeats Step 2 for a specified number of cycles. *One* of the following happens:
    - The endpoint connects to a production DH. The process ends at this step.
    - The endpoint does not connect to a production DH. The process goes to the next step.

    Note: The number of cycles for which the endpoint attempts to connect to a DH is defined in the max_dh_retry_cycles configuration setting in the policyfetcher section.

4. The endpoint tries to connect to the first disaster recovery DH in its list. If it does not connect to this DH, it tries to connect to the second disaster recovery DH in its list, then the third, and so on, until the endpoint connects to a disaster recovery DH.

   Note: If an endpoint cannot connect to a production or disaster recovery DH, 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 recover DH, the endpoint continually tries to connect to a production DH. *One* of the following happens:

   - The endpoint connects to a production DH, and returns to the production environment.
   - The endpoint does not connect a production DH. 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 ensure that you correctly subscribe the disaster recovery components to each other, you must set up 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.

Important! You cannot restore a DMS from backup files that use another platform, operating system, or version of CA Access Control. Ensure that the production and disaster recovery environments are deployed on identical platforms, operating systems, and versions of CA Access Control.

The following process describes how to install a disaster recovery deployment:

1. Set up the production DMS (see page 225).
2. Set up a production DH (see page 226).
3. Set up the disaster recovery DMS (see page 227).
4. Set up a disaster recovery DH (see page 228).
5. Set up an endpoint (see page 230).

Note: This process installs the DMS and DH on separate hosts.

Set Up the Production DMS

The production 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 ensures the subscriptions are correctly configured later in the installation process.

To set up the production DMS

1. Install CA Access Control endpoint functionality on the production DMS server.

   Important! Do not select the Advanced Policy Management Server feature when you install the endpoint. If you select this feature, CA Access Control installs a DMS and a DH on the same host, and you cannot correctly subscribe the DH to the DMS later in the installation process.

2. Run the following command on the production DMS:

   ```
   dmsmgr -create -dms name [-admin user[,user...]]\
   [-desktop host[,host...]]
   ```

   -dms *name*

   Creates a DMS with the *name* specified on the local host.

   -admin *user*[,*user...*]

   (Optional) Defines internal users as administrators of the created DMS.

   -desktop *host*[,*host...*]

   (Optional) Defines a list of computers that have TERMINAL access rights to the computer with the created DMS.

   Note: Whether specified or not, the terminal running the utility is always granted administration rights for the created DMS.

   The production DMS is created with no subscribers.

3. Install CA Access Control Enterprise Management on the production DMS server.

4. Configure the connection from CA Access Control Enterprise Management to the production DMS.

   You can now manage the production DMS through the CA Access Control Enterprise Management web interface.

Set Up a Production DH

A production 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.

We recommend you install each production DH on a separate host to the production DMS. Complete the following procedure for each production DH that you want to set up.

To set up a production DH

1. Install CA Access Control endpoint functionality on the production DH host.

   Important! Do not select the Advanced Policy Management Server feature when you install the endpoint. If you select this feature, CA Access Control installs a DMS and a DH on the same host, and you cannot correctly subscribe the DH to the DMS later in the installation process.

2. Run the following command on the production DH:

   ```
   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.

3. Move to the production DMS.

4. Run the following command on the production DMS:

   ```
   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*.

   The DH is subscribed to and synchronized with the production DMS.

5. Repeat Steps 1-4 for each production DH.

Set Up the Disaster Recovery DMS

The disaster recovery DMS deploys and manages your enterprise policies in the event of a catastrophic system failure. Because the disaster recovery DMS is a subscriber of the production DMS, its database contains the same information about policy versions, policy scripts, and endpoint deployment status as the production DMS. You must set up the production DMS before you set up the disaster recovery DMS.

To set up the disaster recovery DMS

1. Install CA Access Control endpoint functionality on the disaster recovery DMS server.

   Important! Do not select the Advanced Policy Management Server feature when you install the endpoint. If you select this feature, CA Access Control installs a DMS and a DH on the same host, and you cannot correctly subscribe the DH to the DMS later in the installation process.

2. Run the following command on the disaster recovery DMS:

   ```
   dmsmgr -create -dms name [-admin user[,user...]] [-desktop host[,host...]]
   ```

   -dms *name*

   Creates a DMS with the *name* specified on the local host.

   -admin *user*[,*user*...]

   (Optional) Defines internal users as administrators of the created DMS.

   -desktop *host*[,*host*...]

   (Optional) Defines a list of computers that have TERMINAL access rights to the computer with the created DMS.

   Note: Whether specified or not, the terminal running the utility is always granted administration rights for the created DMS.

   The disaster recovery DMS is created with no subscribers.

3. Install CA Access Control Enterprise Management on the disaster recovery DMS server.
4. Configure the connection from CA Access Control Enterprise Management to the disaster recovery DMS.

   You can now manage the disaster recovery DMS through the CA Access Control Enterprise Management web interface.
5. Move to the production DMS.
6. Run the following command on the production DMS:

   ```
   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 DMS is subscribed to and synchronized with the production DMS.

Set Up a Disaster Recovery DH

A disaster recovery DH distributes policy deployments made on the disaster recovery DMS to the endpoints, and sends deployment status updates from the endpoints to the disaster recovery DMS, in the event of a catastrophic system failure.

We recommend you set up each disaster recovery DH on a separate computer to the disaster recovery DMS. Complete the following procedure for each disaster recovery DH that you want to set up.

To set up a disaster recovery DH

1. Install CA Access Control endpoint functionality on the disaster recovery DH host.

   Important! Do not select the Advanced Policy Management Server feature when you install the endpoint. If you select this feature, CA Access Control installs a DMS and a DH on the same host, and you cannot correctly subscribe the DH to the DMS later in the installation process.

2. Run the following command on the disaster recovery DH:

   ```
   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.

3. Move to the disaster recovery DMS.

4. Run the following command on the disaster recovery DMS:

   ```
   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*.

   The DH is subscribed to and synchronized with the disaster recovery DMS.

5. Repeat Steps 1-4 for each disaster recovery DH.

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.

To set up an endpoint

1. Install CA Access Control endpoint functionality, with the Advanced Policy Management Client Components enabled, on the endpoint host.

   Note: You must provide the Advanced Policy Management Server Component machine name as part of the installation process. Enter the names of the production DHs in the following format: *prDH_name@hostname*[, *prDH_name@hostname*..]

   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. Run the following command:

   ```
   so dh_dr+(drDH_name[, drDH_name...])
   ```

   drDH_name

   Defines the names of the disaster recovery DH. Specify the disaster recovery DHs in the following format: *drDH_name@hostname*.

   The endpoint is subscribed to the disaster recovery DHs.

   Note: You can also subscribe an endpoint to a disaster recovery DH by creating a policy with the above selang command and deploying it to the endpoint. For more information about creating and deploying policies, see the *Enterprise Administration Guide*.

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 new 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.

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
- the 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:

- A catastrophic production system failure has occurred.
- The production DMS database is corrupt.
- You need to set up a new production DMS on a different host.

The following scenarios describe when to restore a disaster recovery DMS:

- The disaster recovery DMS is not in sync with the production DMS.
- The disaster recovery DMS database is corrupt.
- 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:

- A catastrophic production system failure has occurred.
- The DH database is corrupt.
- The DH is out of sync with its DMS.
- 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 DMS and the production DHs.
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.

   Note: You can back up the DMS using either of the following methods:

   - local backup (see page 235)
   - remote backup (see page 236)
5. Restore the production DMS (see page 237) from the disaster recovery DMS backup files.
6. Start CA Access Control on the production DMS.
7. Back up the production DMS.

   Note: You can back up the DMS using either of the following methods:

   - local backup (see page 235)
   - remote backup (see page 236)
8. Restore each production DH (see page 239) from the production DMS backup files.
9. Start CA Access Control on each production DH.
10. Move all administrative work to the production DMS, that is, start CA Access Control Enterprise Management and the policydeploy utility on the production DMS.

11. (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 238) from the production DMS backup files.

    b. Back up the disaster recovery DMS.

       Note: You can back up the DMS using either of the following methods:

       - the sepmd utility (see page 235)
       - selang commands (see page 236)

    c. Restore each disaster recovery DH (see page 239) from the disaster recovery DMS backup file.

Back Up the DMS Using sempd

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

When you back up the DMS, you 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 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, run 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, run 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.

Restore a DH

When you restore a DH, dmsmgr copies data from the DMS backup files into the DH Reader directory. 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.

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.

DH or Disaster Recovery DMS Fails to Resubscribe

Symptom:

When I resubscribe a DH to a DMS, or resubscribe the disaster recovery DMS to the production DMS, the following message appears:

Failed to resubscribe *subscriber* on *dms@host*.
To complete restore operation please manually resubscribe *subscriber@host* on *dms@host* at offset *value*.

Solution:

The message appears when you resubscribe a DH or a disaster recovery DMS to a parent DMS that is not running. You must use the offset value in the message to manually resubscribe the DH to the DMS, or the disaster recovery DMS to the production DMS. Specifying the offset value ensures that the subscriber is only sent commands that were not present in its database when it was restored.

To resubscribe a DH or disaster recovery DMS to its parent DMS, run the following command on the parent DMS host:

```
sepmd -s parent_name child_name@host offset
```

Example: Subscribe a DH to a DMS

The following example subscribes DH__@test.com to DMS__ with an offset of 18028. Run this command on DMS__:

```
sepmd –s DMS__ DH__@test.com 18028
```

Chapter 10: 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
- (optional) flatten your PMD structure

If your PMD architecture contains hierarchical PMDBs, you must flatten your PMD hierarchy because advanced policy management does not support hierarchical host groups. You do not have to upgrade all your endpoints at the same time; if you prefer, you can continue to deploy policies to endpoints in a mixed policy management environment.

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 password PMDs to the advanced policy management environment.

How to Migrate to Advanced Policy Management

Migrating your endpoints 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 password PMDs to the advanced policy management environment.

To migrate from a PMD environment to an advanced policy management environment, do the following:

1. Set up the advanced policy management environment (see page 243).
2. Create policies from the PMDB (see page 245).
3. Assign the policies to the appropriate host groups.
4. Migrate the endpoints (see page 253).

   Note: You do not have to upgrade every endpoint in your enterprise at the same time. Instead, you can work in a mixed policy management environment until you finish upgrading the endpoints.

5. Delete the PMDs you do not use for user password synchronization.

   Important! Before you delete a PMD, ensure you have upgraded each endpoint that subscribes to the PMD. Do *not* delete a PMD that you use for password synchronization.

6. Apply a filter file to password PMDs and user synchronization PMDs that removes everything but user and password commands from the rules that are propagated to subscribers.

Note: For more information about deleting a PMD, see the *selang Reference Guide*. For more information about filter files, see the *Endpoint Administration Guide* for your OS.

Set Up the Advanced Policy Management Environment

Setting up the advanced policy management environment is the first step in the process to migrate from a PMD environment to an advanced policy management environment. When you set up the advanced policy management environment, you install additional components and create policies from the rules in the PMDB.

To set up the advanced policy management environment

1. Prepare the Enterprise Management server (see page 149).

2. Install the advanced policy management server components (see page 157).

   A DMS and a DH are installed.

3. Install (see page 159) and start CA Access Control Enterprise Management (see page 167).

4. Configure the connection to the DMS (see page 168).

5. In CA Access Control Enterprise Management, create a host group for each PMD that you want to migrate.

   Important! Advanced policy management does not support a hierarchical structure. If you have a hierarchical PMD structure, you must flatten it before you create host groups.

   Host groups are created and the advanced policy management environment is set up. For ease of transition, we recommend you give the host group the same name as the PMD.

Note: For more information about host groups and policies, see the *Enterprise Administration Guide*.

More information:

Flatten the PMD Hierarchy (see page 250)

Create Policies from a PMDB

After you set up the advanced policy management environment, the next step in the migration process is to create policies from the selang rules in the PMDBs.

You create a cluster of policies for each PMDB that you migrate. Each policy cluster contains all the selang rules that were stored in a particular PMDB. You then assign all the policies in a policy cluster to a host group. This means all the rules that were stored in the PMDB are now assigned to the corresponding host group.

To create policies from a PMDB

1. Stop CA Access Control on the PMDB.
2. Navigate to the PMDB directory and export the PMDB to a file, using the following command:

   ```
   dbmgr -export -l -f output_file_name
   ```

   The script that consists of the selang commands required to define the PMDB is exported to the file that you specified.
3. Create a policy cluster (see page 246).

   Policies corresponding to the selang rules in the PMDB are created and stored on the DMS.
4. Review the policies in the policy cluster alongside each other:
   a. Locate references to objects that are created in another policy.
   b. Create a dependency between the policy that references the object and the policy that creates the object.

   Policy dependencies are set.
5. Assign the policies to the host group that corresponds to the PMDB.

Note: For more information about policy dependencies, see the *Enterprise Administration Guide*.

Create a Policy Cluster

A *policy cluster* is a group of policies that you create from selang rules that were stored in the same PMDB. When you first create a policy cluster, many of the policies in the policy cluster are quite small. Creating policy clusters makes it easier to migrate from a PMD environment to an advanced policy management environment because it is much easier to correct deployment errors in small policies.

Note: To create and modify enterprise users and groups, we recommend you enable the use of enterprise users and groups, use the ntimport and UxImport utilities, or use a provisioning tool such as CA Identity Manager.

To create a policy cluster

1. Remove the built-in commands from the output file (see page 247).
2. Change each rule that creates a new resource or accessor to a rule that modifies the resource or accessor. For example, change each newres command to an editres command.
3. Move the editres SEOS rules to a policy file, give the policy a meaningful name, and store the policy on the DMS.

   Note: A policy file is a text file that contains selang commands.
4. Move the editres CONFIG rules to a policy file, give the policy a meaningful name, and store the policy on the DMS.

   Important! You must precede each editres CONFIG rule with the env config command to ensure the rule executes in the correct selang environment.
5. Move the editusr rules that refer to an administrative role to a policy file, give the policy a meaningful name, and store the policy on the DMS.

   Note: An administrative role has one or more of the following attributes: ADMIN, AUDITOR, IGNORE-HOLIDAY, LOGICAL, OPERATOR, PWMANAGER, or SERVER.
6. Create policies for protected resources (see page 248).

   The rules for protected resources are moved from the output file to the policy files.
7. Move the rules for runtime resources to a separate policy file, give the policy a meaningful name, and store the policy on the DMS.

   Note: A runtime resource is a resource that does not have an ACL, for example, a resource in the CALENDAR or DICTIONARY classes.
8. Create policies for logical users and groups (see page 249).

   The rules for logical users and groups are moved from the output file to the policy files.

9. Move the remaining commands to a separate policy file, give the file a meaningful name, and store the policy on the DMS.

   Note: We recommend you name the policy *pmd_name*_unclassified.

Remove Built-In Commands from the Output File

When you remove built-in commands from the output file, you remove the commands that the PMD automatically adds to its database when you first create it. Built-in commands are superfluous in policies.

This procedure is the first step in the procedure to create a policy cluster.

To remove built-in commands from the output file

1. Create a temporary PMDB on the same computer as the existing PMDB, using the following selang commands:

   ```
   env pmd
   createpmd temp_pmdname
   ```

   The temporary PMDB is created.

2. Navigate to the temporary PMDB directory and export the database of the temporary PMDB to file, using the following command:

   ```
   dbmgr -export -l -f output_file_name
   ```

   The script that consists of the selang commands required to define the PMDB is exported to the file that you specified.

3. Compare the output files for the temporary PMDB and the existing PMDB.
4. Remove all the commands that are in the temporary PMDB output file from the existing PMDB output file.

   The built-in commands are removed from the existing PMDB output file.

Create Policies for Protected Resources

A protected resource is a resource with an ACL that enforces access restrictions, for example, resources in the FILE, PROGRAM, and TERMINAL classes. The policy you create for the protected resource can be self-contained or dependent on other policies.

This procedure is a step in the procedure to create a policy cluster.

To create policies for protected resources

1. Find all the rules for a protected resource, or for two or more protected resources that should be in the same policy, in the output file.

   For example, the rules for the following FILE resources should be in the same policy:

   - c:\inetpub
   - c:\inetpub\wwwroot

2. Move the rules you found to a policy file, and give the policy a meaningful name.

   Note: A policy file is a text file that contains selang commands.

3. Find all the rules that start with the following command:

   ```
   authorize class_name protected_resource_name
   ```

4. Move the access authority rules you found to the policy file you created earlier.

   The rules that authorize access to the protected resource or resources are moved from the output file to the policy file.

5. Do *one* of the following:

   - Add the rules that create the accessor, program, and calendar restrictions to the policy, and store the policy on the DMS.

     This creates a self-contained policy for the protected resource.

   - Create one or more policies that contain the rules to create the accessor, program, and calendar restrictions for the protected resource. Store these policies and the policy you created earlier on the DMS, and set dependencies between the policies.

     This creates dependent policies for the protected resource.

6. Repeat Steps 1–5 for each protected resource in the output file.

Create Policies for Logical Users

A *logical user* is a user with the LOGICAL attribute applied to their record, or a surrogate who runs a trusted program (SPECIALPGM resource). A logical user cannot log in and is used for internal CA Access Control purposes only. The policy you create for the logical user can be self-contained or dependent on other policies.

This procedure is a step in the procedure to create a policy cluster.

To create policies for logical users

1. Find all the rules for logical users in the output file, move the rules to a policy file, and give the policy a meaningful name.

   Note: A policy file is a text file that contains selang commands.

   The rules are moved from the output file to the policy file.

2. (Optional) If a logical user is a member of a group, do *one* of the following:

   - Add selang rules to the policy that add the user to the group, and store the policy on the DMS.

     This creates a self-contained policy for the logical user.

   - Create a separate policy, and add selang rules to the policy that create the group and that add the logical user to the group. Store this policy and the policy you created earlier on the DMS, and set policy dependencies between the policies.

     This creates dependent policies for the logical user.

Policy Creation for Enterprise Users and Groups

We recommend you do not use policies to create and modify enterprise users and groups. Because enterprise users and groups change frequently, if you create a new policy version each time you need to modify an enterprise user or group you will soon have hundreds of versions of the same policy, which presents maintenance difficulties.

To create and modify enterprise users and groups, we recommend you enable the use of enterprise users and groups, use the ntimport and UxImport utilities, or use a provisioning tool such as CA Identity Manager.

Note: For more information about enterprise user and groups, see the *Endpoint Administration Guide* for your OS. For more information about the ntimport and UxImport utilities, see the *Reference Guide*.

Flatten the PMD Hierarchy

An advanced policy management environment does not support hierarchical host groups. If you have a hierarchical PMD environment, you must flatten your hierarchical PMD architecture before you migrate to an advanced policy management environment.

When you flatten the PMD hierarchy, you create a host group for each PMD and add each endpoint to the host group corresponding to the PMD it was subscribed to in the PMD environment.

To flatten the PMD hierarchy

1. Create a host group for each of your PMDs, and give each host group the same name as its corresponding PMD.
2. Export each PMD database to file, using the following command:

   ```
   dbmgr -export -l -f output_file_name
   ```

   Each PMD database is exported to the file you specified.
3. Compare the output files for the parent and subscriber PMDs.
4. Find the rules that are in both the parent and subscriber PMD output file, and use these rules to create a policy cluster (see page 246).

   Note: You assign the policy cluster to the host group that corresponds to the parent PMD later in the migration process. We recommend that you use the name of the parent PMD in the names of the policies in the policy cluster.

   The rules from the parent PMD database are moved from the output file to a cluster of policy files.
5. Find the rules that are only in a specific subscriber PMD output file, and use these rules to create a policy cluster (see page 246).

   Note: You assign the policy cluster to the host group that corresponds to the subscriber PMD later in the migration process. We recommend that you use the name of the subscriber PMD in the names of the policies in the policy cluster.
6. Repeat Step 5 for each subscriber PMD.

7. Find any rules that are only in the parent PMD, and use these rules to create a policy cluster (see page 246).

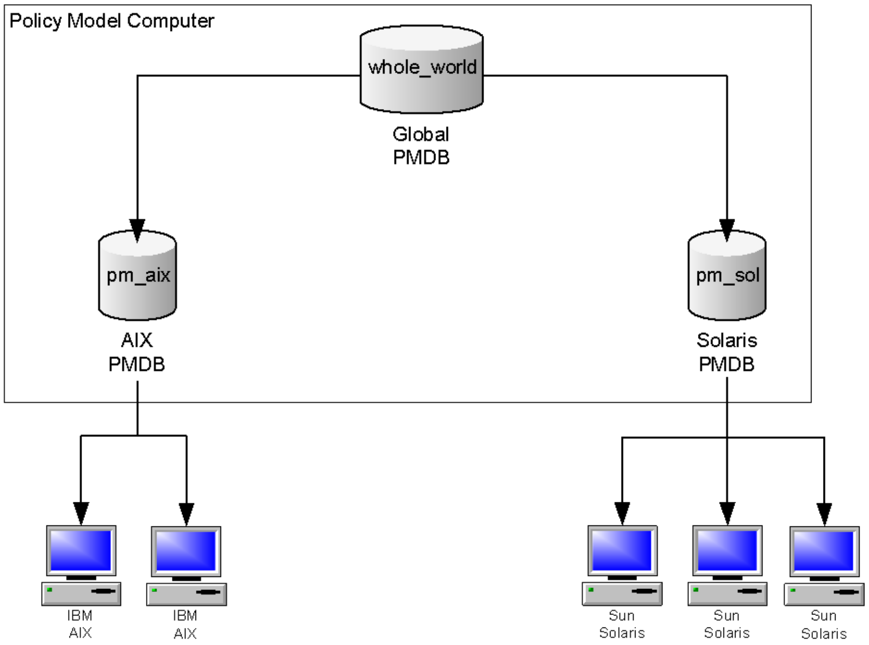
   Note: Because the subscriber PMDs are subscribers of the parent PMD, there may not be any rules in the parent PMD output file that are not in the subscriber PMD output files.

   The rules from the parent PMD database are moved from the output file to the policy cluster.

Note: For more information about host groups, see the *Enterprise Administration Guide*.

Example: Flatten the PMD Hierarchy

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 create the following host groups:

- whole_world—All endpoints are members of this host group
- pm_aix—IBM AIX endpoints are member of this host group
- pm_sol—Sun Solaris endpoints are members of this host group

To migrate this PMD environment to an advanced policy management environment, do the following:

1. In CA Access Control Enterprise Management, create host groups named whole_world, pm_aix, and pm_sol.
2. Export each PMDB to an output file.
3. Compare the output files for the whole_world, pm_aix, and pmd_sol PMDBs.
4. Find the rules that are in all of the whole_world, pm_aix, and pmd_sol output files, and use these rules to create a policy cluster. Use whole_world in the name of each policy in the cluster.

   Note: You assign this policy to the whole_world host group later in the migration process.

5. Find the rules that are only in the pm_aix output file, and use these rules to create a policy cluster. Use pm_aix in the name of each policy in the cluster.

   Note: You assign this policy to the pm_aix host group later in the migration process.

6. Find the rules that are only in the pm_sol output file, and use these rules to create a policy cluster. Use pm_sol in the name of each policy in the cluster.

   Note: You assign this policy to the pm_sol host group later in the migration process.

7. Find the rules that are only in the whole_world output file, and use these rules to create a policy cluster. Use whole_world in the name of each policy in the cluster.

   Note: Because the whole_world PMDB propagates all the commands in its database to its subscribers, and because the pm_aix and pm_sol PMDBs are subscribers of the whole_world PMDB, there may not be any rules that are only in the whole_world output file.

Migrate an Endpoint

After you set up the advanced policy management environment, flatten the PMD hierarchy, and create policies from a PMDB, the next step in the migration process is to migrate the endpoints that subscribe to the PMDB.

When you migrate an endpoint, you add the endpoint to a host group in CA Access Control Enterprise Management. This triggers CA Access Control to send the endpoint the policies that you assigned to the host group earlier in the migration process.

To migrate the endpoints

1. Upgrade the endpoint to CA Access Control r12.0 or later.

   The endpoint is upgraded.

2. Run the following commands on the endpoint:

   ```
   dmsmgr -config -endpoint
   dmsmgr -config -dh dh_name@host_name
   ```

   Advanced policy management client components are configured on the endpoint.

3. Run the following commands on the endpoint:

   a. Connect to the PMDB from the endpoint:

      ```
      host pmdb_name@host_name
      ```

   b. Move to the selang PMD environment:

      ```
      env pmd
      ```

   c. Unsubscribe the endpoint from the PMD:

      ```
      unsubs pmd_name subs(endpoint_name)
      ```

   d. Repeat Steps a–c for each PMD the endpoint subscribes to.

      Important! Do not unsubscribe the endpoint from password PMDs.

   The endpoint is unsubscribed from all PMDs except password PMDs.

4. Start CA Access Control on the endpoint.

   Note: You stop CA Access Control when you upgrade the endpoint.

5. Open CA Access Control Enterprise Management.

6. Add the endpoint to each host group that corresponds to a PMD to which the endpoint was subscribed.

   The endpoint is migrated to the advanced policy management environment.

How Policies are Initially Sent to a Migrated Endpoint

When you migrate from a PMD environment to an advanced policy management environment, you create policies from the rules in the PMDB. 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. The DMS receives the heartbeat notification and creates a corresponding host (HNODE) object on the DMS.
2. After you add the endpoint (HNODE) to the host group (GHNODE) that corresponds to the PMD to which it was subscribed, CA Access Control deploys any policies assigned to the host group to the endpoint.
3. CA Access Control modifies the Update Time property for each resource listed in the policy to the time the policy was deployed.

   Note: Because you changed commands that create objects to commands that modify objects, you should not see any deployment errors for the policy.

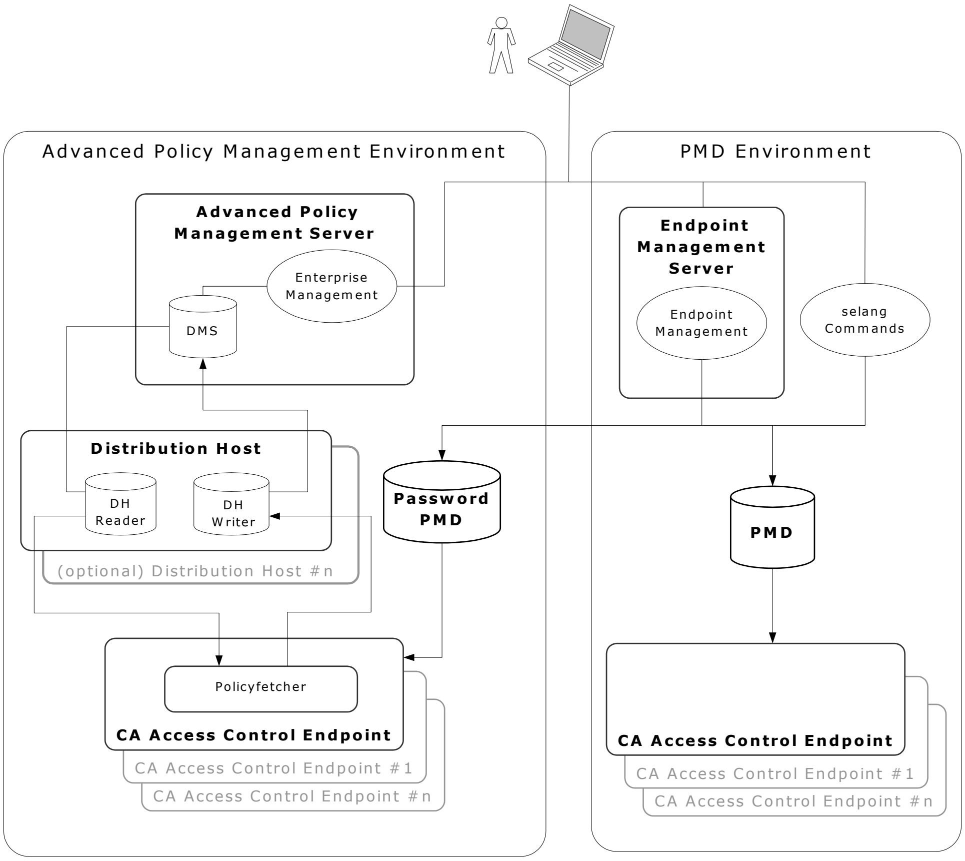
Note: For more information about policies and host groups, see the *Enterprise Administration Guide*.

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.


Advanced Policy Management Environment
Advanced Policy Management Server
Enterprise Management
DMS
Distribution Host
DH Reader
DH Writer
(optional) Distribution Host #n
Password PMD
Policyfetcher
CA Access Control Endpoint
CA Access Control Endpoint #1
CA Access Control Endpoint #n
PMD Environment
Endpoint Management Server
Endpoint Management
selang Commands
PMD
CA Access Control Endpoint
CA Access Control Endpoint #1
CA Access Control Endpoint #n

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.

To update endpoints in a mixed policy management environment

1. Create a new 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.