CA Access Control

Upgrade Guide

12.6.03

Third-Party Notices

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

Sample Scripts and Sample SDK Code

The Sample Scripts and Sample SDK code included with the CA Access Control product are provided "as is", for informational purposes only. Adjust them to your specific environment and do not use them in production without running tests and validations.

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

CA Technologies Product References

This document references the following CA Technologies products:

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

Documentation Conventions

The CA Access Control documentation uses the following conventions:

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

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

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

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

Example: Command Notation Conventions

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

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

In this example:

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

File Location Conventions

The CA Access Control documentation uses the following file location conventions:

- *ACInstallDir*—The default CA Access Control installation directory.
  - Windows—\ProgramFiles\CA\AccessControl
  - UNIX—/opt/CA/AccessControl/

- *ACSharedDir*—A default directory used by CA Access Control for UNIX.
  - UNIX—/opt/CA/AccessControlShared
- *ACServerInstallDir*—The default CA Access Control Enterprise Management installation directory.
  - /opt/CA/AccessControlServer
- *DistServerInstallDir*—The default Distribution Server installation directory.
  - /opt/CA/DistributionServer
- *JBoss_HOME*—The default JBoss installation directory.
  - /opt/jboss-4.2.3.GA

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: About this Guide

This guide provides information about how to upgrade CA Access Control server and endpoint components and how to migrate PMDs to Advanced Policy environment.

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

Chapter 2: Upgrading Server and Endpoint Components

This section contains the following topics:

Before You Begin to Upgrade

Review the following topics before you begin the upgrade process:

Upgrade an Existing Central Database to Microsoft SQL Server 2008

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

Follow these steps:

1. Stop all CA Access Control services on the Enterprise Management Server.
2. Stop JBoss. Do *one* of the following steps:
   - If JBoss is not installed as a service, interrupt the JBoss application server window (Ctrl+C).
   - If JBoss is installed as a service, stop the JBoss service from the Services panel.
3. Upgrade to Microsoft SQL Server 2008.
4. Download the Microsoft SQL Server JDBC Driver 2.0 from the Microsoft website.
5. Extract the file to a temporary directory on the Enterprise Management Server.
6. Do *one* of the following steps:
   - Locate the sqljdbc.jar file, if you are using JDK version 1.5.
   - Locate the sqljdbc4.jar file and rename it sqljdbc.jar, if you are using JDK version 1.6 or higher.

7. Copy the file into the following directory on the Enterprise Management Server:

   JBoss_HOME/server/default/lib

   Note: Overwrite the existing file in this directory.

8. Start the Microsoft SQL Server 2008 services.
9. Start JBoss.
10. Start CA Access Control Enterprise Management.

Prepare a CA Access Control Endpoint for Enterprise Management

You can install the Enterprise Management Server on a CA Access Control endpoint. The endpoint does not contain all the components that are required by the Enterprise Management Server. Before you can install the Enterprise Management Server on the endpoint, you prepare the endpoint.

Follow these steps:

1. Stop all CA Access Control services (Windows) or daemons (UNIX) on the endpoint
2. Install the Enterprise Management Server on the endpoint

   The web-based applications and the Distribution Server are installed. If not already installed, the latest version of CA Access Control is also installed.

3. Create a DMS on the Enterprise Management Server.

   The Enterprise Management Server installation does not create the DMS on the endpoint. Use the dmsmgr utility to create the DMS.

4. Start the Enterprise Management Server services or daemons.
5. Create a user account with the ADMIN, AUDITOR, and Logical authorization attributes.

   You use the logical user account when you define the DMS connection settings in CA Access Control Enterprise Management.

6. Create a host group on the DMS.
7. Add the node to the DMS using the dmsmgr utility.

8. Log in to CA Access Control Enterprise Management with the administrative user account that you specified when you installed the Enterprise Management Server.
9. In CA Access Control Enterprise Management, define the DMS connection settings.

   You specify the DMS you created on the endpoint.

   The Enterprise Management Server is installed and configured to use the DMS you created.

Note: For more information about the dmsmgr utility, see the *Reference Guide*. For more information about how to use selang to create and configure users, see the *selang Reference Guide*.

Preparing to Upgrade the Enterprise Management Server

Collect the following information before you begin to upgrade an r12.5.x Enterprise Management Server installation to r12.6.1:

- Message Queue password

  Obtain the administrative user, reportserver user, and +reportagent user passwords.
- Database connection information

  Obtain the host name, port number, database name, username, and password.
- Java Connector Server password

  Obtain the communication password that you used during the previous installation of CA Access Control Enterprise Management.
- (Optional) Java Connector Server (JCS) SSL certificate

  Import a new SSL certificate after you upgrade to CA Access Control Enterprise Management r12.5.x only if you used a custom SSL certificate.

Import the Java Connector Server SSL Certificate After Upgrade

Because of a change in the Java Connector Server (JCS) SSL certificate in CA Access Control r12.5 SP3, you must import a new SSL certificate after you upgrade from CA Access Control r12.5.x.

Important! Complete this procedure only if you used a custom JCS SSL certificate. You do not need to perform this procedure if you used the default SSL certificate.

Follow these steps:

1. Stop the JBoss application server.

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

   JBOSS_HOME/server/default/deploy/IdentityMinder.ear/custom/ppm/trusttore/

3. Back up the ssl.keystore file.
4. From the directory you navigated to previously, open a Command Prompt window.
5. Run the keytool utility to specify the custom SSL keystore to import, where *JAVA_HOME* indicates the directory where JDK is installed. For example:

   JAVA_HOME\bin\keytool.exe -import -alias eta_client -file c:\custom_certificate.der -keystore ssl.keystore

   A password prompt appears.

6. Enter the keystore password. The default password is *secret*.

   The keytool displays the certificate details and fingerprints.

7. Type Yes to add the certificate to the keystore.

   The keytool adds the new certificate.

8. Start the JBoss application server.

   You have loaded the new JCS SSL certificate file to CA Access Control Enterprise Management.

Chapter 3: How to Upgrade from CA Access Control r5.3

Due to additional components and changes in deployments, you cannot upgrade to CA Access Control 12.8 from CA Access Control r5.3. You upgrade your existing CA Access Control r5.3 deployment first to CA Access Control r8.0Sp1 and then you upgrade to CA Access Control 12.8.

You upgrade your existing CA Access Control r5.3 deployment by following these steps:

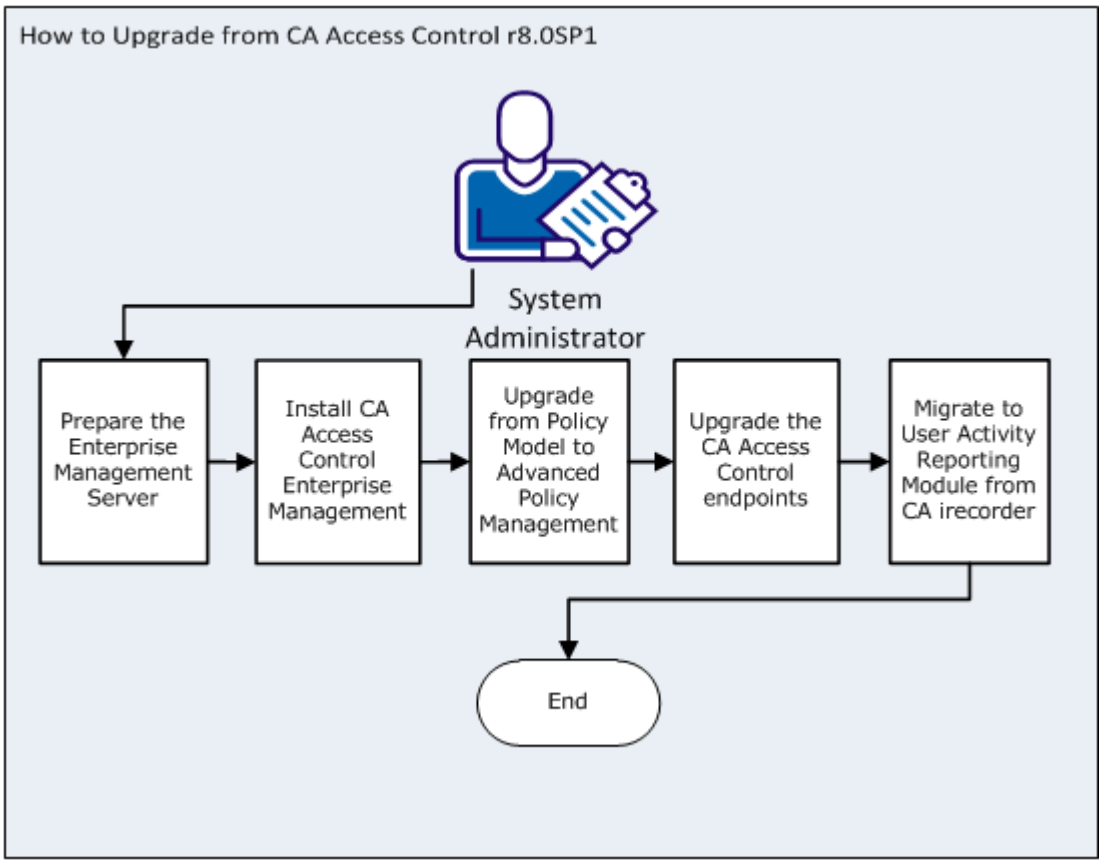
1. Back up all CA Access Control components before you start the upgrade process.
2. Upgrade to CA Access Control r8.0SP1 (see page 15)
3. Upgrade to CA Access Control 12.8

Chapter 4: Upgrading from CA Access Control r8.0SP1

The purpose of this scenario is to describe the steps that you follow to upgrade from CA Access Control r8.0SP1. The upgrade process in the chapter assumes that you installed CA Access Control r8.0SP1 components on separate computers.

The information in this section is intended for system or CA Access Control administrators that are tasked with managing CA Access Control.

The following diagram illustrates the steps to complete to upgrade from CA Access Control r8.0SP1:



Important!

- Back up all CA Access Control components before you start the upgrade process.
- Customize the software package to specify the 'eTrustAccessControl' path. 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.

You upgrade your existing CA Access Control r8.0SP1 deployment by following these steps:

1. Prepare the Enterprise Management Server.

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

2. Install CA Access Control Enterprise Management (see page 18).
3. Upgrade from Policy Model environment to an advanced policy management environment (see page 61).
4. Upgrade the CA Access Control endpoins:
   - Windows—Install using Product Explorer (see page 22)
   - UNIX—Install Using install_base script (see page 24)

   Note: The installation also upgrades the password PMD.
5. (Optional) Migrate (iRecorder product) to CA User Activity Reporting Module.

Note: You cannot upgrade the Policy Manager. Use CA ControlMinder Endpoint Management to manage policies on the endpoints.

Prepare the Central Database for Enterprise Management

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

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

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

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

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

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

Follow these steps:

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

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

2. Configure the RDBMS for CA Access Control Enterprise Management:

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

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

     This user must have the following permissions and settings:

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

   - For SQL Server:

     - Create a new case-*insensitive* database.

       The database must have the sort order SQL_Latin1_General_CP1_CI_AS.

     - Create a user, make the new database the default database of the user, and assign the user to the following privileges: DBCREATOR, SYSADMIN

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

   a. Customize the deployment scripts before you deploy them.

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

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

   b. Deploy the deployment scripts.

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

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

Install CA Access Control Enterprise Management on Windows

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

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

Follow these steps:

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

   The InstallAnywhere installation program starts.

a. (Optional) Specify the full pathname of a custom FIPS key to use during installation.

b. Open a Command Prompt window and navigate to the CA Access Control Enterprise Management installation executable on the CA Access Control Server Components DVD for Windows. This file is located under:

```
\EnterpriseMgmt\Disk1\InstData\NoVM
```

c. Run the CA Access Control Enterprise Management install executable with the following argument:

```
-DFIPS_KEY=full_pathname_to_FIPS_key
```

For example, to install with a custom FIPS key located at C:\tmp\FIPS.key:

```
E:\EnterpriseMgmt\Dis1\InstData\NoVM\install_EntM_r125.exe
-DFIPS_KEY=C:\tmp\FIPSkey.dat
```

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

The InstallAnywhere installation program starts.

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

Java Development Kit (JDK)

Defines the location of an existing JDK.

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

JBoss Application Server Information

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

To do this, define the:

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

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

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

- Port JBoss uses.

- Port JBoss uses for secure communications (HTTPS).

- Naming port number.

Communication Password

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

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

Database Information

Defines the connection details to the RDBMS:

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

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

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

User Store Type

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

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

Note: To deploy login authorization policies to [assign the value for unab in your book], you must select either Active Directory or Other User Store as the user store. If you select Active Directory or Other User Store as the user store, you cannot create or delete users and groups in CA Access Control Enterprise Management. For more information about [assign the value for unab in your book] and Active Directory restrictions, see the *Enterprise Administration Guide*.

Active Directory Settings

Defines the Active Directory user store settings:

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

  Note: Set the Search Root at least one node higher in the directory tree than the Distinguished Names (DNs) for the users specified for User DN and System User. Otherwise, Enterprise Management might launch without displaying any tabs.
- **User DN**—Defines the Active Directory user account name that is used to manage CA Access Control Enterprise Management. For example: CN=Administrator, cn=Users, DC=DomainName, DC=Com.

  Note: This user issues LDAP queries against Active Directory. You can choose to define a user with read-only privileges for this parameter. However, if you define a user with read-only privileges, you cannot assign admin roles or privileged access roles to users in CA Access Control Enterprise Management. Instead, you modify the member policy for each role to point to an Active Directory group.
- **Password**—Defines the password of the Active Directory user account that is used to manage CA Access Control Enterprise Management.

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

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

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

System User

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

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

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

Administrator Password

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

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

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

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

   You can now configure CA Access Control Enterprise Management for your enterprise.

Install Using Product Explorer

The CA Access Control Product Explorer lets you select between different architecture installations of CA Access Control and install the Runtime SDK. The Product Explorer uses a graphical interface to install CA Access Control and provides interactive feedback.

Follow these steps:

1. Log into the Windows system as a user with Windows administrative privileges (that is, as the Windows administrator or a member of the Windows Administrators group.)
2. Close any applications that are running on your Windows system.

3. Insert the CA Access Control Endpoint Components for Windows DVD into your optical disc drive.

   If you have autorun enabled, the Product Explorer automatically appears. Otherwise, navigate to the optical disc drive directory and double-click the PRODUCTEXPLORERX86.EXE file.

4. From the Product Explorer main menu, expand the Components folder, select CA Access Control for Windows (*my_architecture*), then click Install.

   You need to select the installation option that matches the architecture of the computer you are installing on (32-bit, 64-bit x64, or 64-bit Itanium).

   The Choose Setup Language window appears.

5. Select the language you want to install CA Access Control with and click OK.

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

   Note: If the installation program detects an existing installation of CA Access Control, you are prompted to select whether you want to upgrade CA Access Control.

6. Follow the instructions on the installation screens.

   During the installation, the installation program prompts you to supply information. For the information that you need when installing CA Access Control, refer to the installation worksheets.

   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.

   Note: If you choose to restart your computer later, an additional warning cautions you that the installation is not complete until your computer is rebooted. Some CA Access Control functionality, such as logon interception, does not work until after you restart your computer.

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.

Follow these steps:

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: Upgrade to CA Access Control r12.6SP1 for UNIX Using Silent Install

This example shows you how to upgrade an existing CA Access Control r8.0SP1 endpoint to CA Access Control r12.6SP1 for UNIX. In this example, you install CA Access Control using the parameters file that enables you to install new features on the endpoint.

1. Review the install_base script command.

   You use the install_base script to install CA Access Control r12.6SP1 in silent mode. For more information, refer to the *Implementation Guide*.

2. Extract the parameters file from the tar compressed file from the CA Access Control Endpoint Components for UNIX media. The file is located in the following directory:

   `\Unix\Access-Control\`

3. Install CA Access Control using the install_base script.

   Use the -autocfg command and specify to use the parameters file you customized.

   CA Access Control r12.6SP1 is installed with the options you specified.

Example: The parameters file

The parameters file lets you select the software components to add to the endpoint. If you install CA Access Control in native installation mode, you customize the file before you begin the installation. If you install CA Access Control in interactive mode, you can extract the installation parameters into a file and then customize the installation parameters.

The following is a snippet from the parameters file:

```
#  Specifies whether you want to configure PUPM Agent
#  Values: "yes", "no"
#  Default: "no"
INSTALL_PUPM="yes"

# Specifies whether  enables KBL audit records management
# Values: yes, no
# Default: no
ENABLE_KBL=yes
```

In this example, you specified to install the [assign the pupm variable value for your book] Integration on, (INSTALL_PUPM=yes). and enabled keyboard logging on the endpoint, (ENABLE_KBL=yes).

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
```

Chapter 5: Upgrade from CA Access Control r12.0 SP1

This section details the steps an CA Access Control, or system administrator follows to upgrade an existing CA Access Control r12.0 SP1 deployment. The process in the chapter assumes that the administrator installed CA Access Control r12.0 SP1 components on separate computers.

For example, the Enterprise Management Server is installed on one computer, where as the DMS, DH and Report Server are also installed on separate computers.

The upgrade process described in this chapter instructs you how to upgrade each component separately.

Note: You can upgrade from CA Access Control Enterprise Management r12.0 SP1 only.

Before You Begin

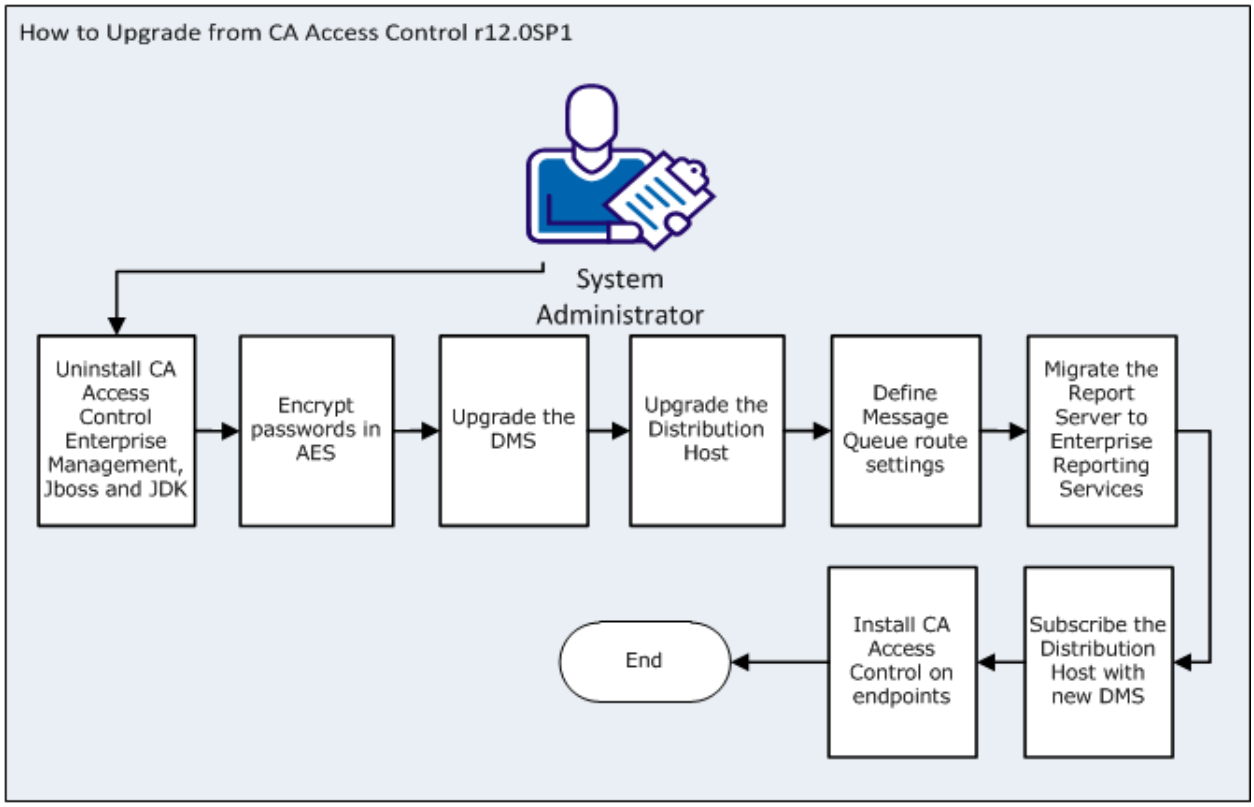
Before you begin the process of upgrading the current CA Access Control installation consider the following:

- We recommend that you backup CA Access Control components before starting the upgrade process. We recommend backing up the system files before starting the upgrade process, including all databases.
- CA Access Control Enterprise Management installs the following components: Enterprise Management Server, CA Access Control, Distribution Server, Enterprise reporting service.
- After upgrading the previous DMS is unavailable. You must upgrade the Enterprise Management Server, DMS and DH before starting the server.
- Specify to use an embedded user store when installing the Enterprise Management Server.

  Important! You cannot use [assign the value for unab in your book] reports and login authorization policies when you install the Enterprise Management Server on the embedded user store. To generate [assign the value for unab in your book] reports and configure login authorization policies, you must install Active Directory.

How to Upgrade from r12.0 SP1

The following steps describe how you upgrade an existing CA Access Control r12.0 SP1 deployment:



1. Upgrade the Enterprise Management Server.
    a. Uninstall CA Access Control Enterprise Management r12.0 SP1, JBoss and JDK.
    b. Install JDK 1.5.0 and JBoss 4.2.3 using the Prerequisite Installer (see page 31).
    c. install CA Access Control Enterprise Management.
2. Encrypt the existing passwords in AES (see page 40).

    In CA Access Control Enterprise Management r12.5 SP1, the encryption method was changed from RC2 to AES.
3. Upgrade the DMS computer (see page 41).

    Note: You do not need to complete this step if the DMS is installed on the same computer as CA Access Control Enterprise Management.
4. Upgrade the Distribution Host (see page 45).

    Note: Upgrade every DH in your enterprise. You do not need to complete this step if the DH is installed on the same computer as the Enterprise Management Server.
5. Define Message Queue (MQ) route settings (see page 46).
6. Migrate the Report Server to Enterprise Reporting Services (see page 59).
7. Subscribe the DH with the new DMS (see page 60).
8. (Optional) Upgrade CA Access Control endpoint (see page 60)s.

Upgrade the Enterprise Management Server

This procedure describes the steps you follow to upgrade the Enterprise Management Server and the post installation steps that you need to do.

Follow these steps:

1. Uninstall CA Access Control Enterprise Management r12.0 SP1.

    Note: For information about uninstalling CA Access Control Enterprise Management r12.0 SP1, see the *Implementation Guide* for that release.
2. Uninstall the existing JDK and JBoss.

3. Install prerequisite software (see page 31).
4. Install CA Access Control Enterprise Management (see page 18).

   CA Access Control Enterprise Management also installs the following:

   - Enterprise Management Server
   - CA Access Control
   - Enterprise reporting service.
   - Distribution Server

   Important! You must specify to use an embedded user store when you install CA Access Control Enterprise Management.
5. Update the database schema by running the supplied scripts if the reporting database schema is not identical to the schema on CA Access Control Enterprise Management.
6. (Optional) Configure secure communication for JBoss (see page 37).
7. Disable the DMS and DH on CA Access Control Enterprise Management. Run the following command:

   ```
   dmsmgr -remove -auto
   ```

   Important! Complete this step only if the DMS is installed on a separate computer than CA Access Control Enterprise Management.

   Note: After upgrading the existing DMS is no longer available. Upgrade the DMS after installing the new Enterprise Management Server. For more information about the dmsmgr utility, see the *Reference Guide*.

The new Enterprise Management Server is installed. You must now upgrade the DMS and Distribution Host before you start CA Access Control Enterprise Management.

Run the Prerequisite Software Installation Utility

Valid on Windows

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

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

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

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

Follow these steps:

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

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

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

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

   The prerequisite software installs. This can take some time.

5. Do *one* of the following:

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

     The prerequisite software installation process is complete.

Install CA Access Control Enterprise Management on Windows

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

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

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

Follow these steps:

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

   The InstallAnywhere installation program starts.

a. (Optional) Specify the full pathname of a custom FIPS key to use during the installation.

b. Open a command prompt window and navigate to the CA Access Control Enterprise Management installation executable on the CA Access Control Server Components DVD for Windows. This file is located under:

```
\EnterpriseMgmt\Disk1\InstData\NoVM
```

c. Run the CA Access Control Enterprise Management install executable with the following argument:

```
-DFIPS_KEY=full_pathname_to_FIPS_key
```

For example, to install with a custom FIPS key located at C:\tmp\FIPS.key:

```
E:\EnterpriseMgmt\Disk1\InstData\NoVM\install_EntM_r125.exe
-DFIPS_KEY=C:\tmp\FIPSkey.dat
```

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

The InstallAnywhere installation program starts.

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

Choose Install Folder

Defines the full path of the installation folder.

Default: \ProgramFiles\CA\AccessControlServer\

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

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

Java Development Kit (JDK)

Defines the location of an existing JDK.

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

JBoss Application Server Information

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

To do this, define the:

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

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

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

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

Communication Password

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

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

Database Information

Defines the connection details to the RDBMS:

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

- **Username**—Defines the name of the user that you created when you prepared the database.

  Note: You granted this user the appropriate database permissions when you prepared the database.

- **Password**—Defines the RDBMS password of the user that you created when you prepared the database.

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

User Store Type

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

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

Note: To deploy login authorization policies to [assign the value for unab in your book], you must select either Active Directory or Other User Store as the user store. If you select Active Directory or Other User Store as the user store, you cannot create or delete users and groups in CA Access Control Enterprise Management. For more information about [assign the value for unab in your book] and Active Directory restrictions, see the *Enterprise Administration Guide*.

Active Directory Settings

Defines the Active Directory user store settings:

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

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

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

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

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

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

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

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

System User

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

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

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

Administrator Password

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

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

CA Access Control Enterprise Management is installed after you complete the wizard.

6. To complete the installation, reboot the computer.

   After you reboot the computer, you can configure CA Access Control Enterprise Management for your enterprise.

SSL Communication for JBoss

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

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

Example: Configure JBoss for SSL Communication on Windows

This example shows you how to configure the JBoss application server to use SSL for secure communication.

Important! This procedure describes how to configure JBoss to use SSL for secure communication using JBoss version 4.2.3 and JDK version 1.5.0.

Follow these steps:

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

   JBoss_HOME\server\default\deploy\IdentityMinder.ear\custom\ppm\truststore

3. Enter the following command to change the default ssl,keystore password:

   `keytool -storepasswd -new password -keystore ssl.keystore -storepass secret`

   -storepasswd

   Specifies to change the keystore password. The password must be at least six (6) characters long.

   -keystore

   Specifies the keystore name to add the certificate.

   -keystore

   Specifies the keystore name.

   -storepass

   Defines the password used to protect the keystore.

4. Enter the following command to create a key for the Enterprise Management Server:

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

   -genkey

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

   -alias

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

   -keyalg

   Specifies the algorithm to use to generate the key pair.

   The keytool utility starts.

5. Enter the password *secret*.

6. Complete the prompts as required and press enter to verify the parameters you entered.

   The certificate is added to the keystore.

   Note: The keystore and key alias must use identical passwords.

7. Enter the following command to encrypt the keystore password to a file:

   `java -cp JBoss_HOME/server/default/lib/jbossx.jar org.jboss.security.plugins.FilePassword welcometojboss 13 passowrd <kestore_password> keystore.password`

   Note: The Salt and IterationCount are the variables that define the strength of the encrypted password. In the this example, "welcometojboss" is the salt and 13 is the iteration count.

8. Locate the file named server.xml in the following directory and open it for editing:

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

9. Locate the <Connector Port> tag in the following section:

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443
         This connector uses the JSSE configuration, when using APR, the
         connector should be using the OpenSSL style configuration
         described in the APR documentation -->
    <!--
    <Connector port="18443" protocol="HTTP/1.1" SSLEnabled="true"
               maxThreads="150" scheme="https" secure="true"
               clientAuth="false" sslProtocol="TLS" />
```

   Note: The connector port number corresponds to the JBoss HTTPS Port number that you specified during the prerequisite or CA Access Control Enterprise Management installation process.

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

    You can now edit this tag.

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

```
securityDomain="java:/jaas/encrypt-keystore-password"
SSLImplementation="org.jboss.net.ssl.JBossImplementation"
```

12. Save and close the server.xml file.

13. Navigate to the following directory to locate the jboss-service.xml file:

    JBOss_HOME/server/default/deploy/jboss-web.deployer/META-INF

14. Add the following mbean between the <server> and </server> tags:

```
<mbean code="org.jboss.security.plugins.JaasSecurityDomain"
name="jboss.security:service=PBESecurityDomain">
      <constructor>
         <arg type="java.lang.String" value="encrypt-keystore-password"></arg>
      </constructor>
      <attribute
name="KeyStoreURL">${jboss.server.home.dir}/deploy/IdentityMinder.ear/custom/
ppm/truststore/ssl.keystore</attribute>
      <attribute
name="KeyStorePass">{CLASS}org.jboss.security.plugins.FilePassword:${jboss.se
rver.home.dir}/deploy/IdentityMinder.ear/custom/ppm/truststore/keystore.passw
ord</attribute>
<attribute name="Salt">welcometojboss</attribute>
<attribute name="IterationCount">13</attribute>
 </mbean>
```

   Note: In the above example,welcometojboss is the salt and 13 is the iteration count.

15. Save and close the jboss-service.xml
16. Start and open CA Access Control Enterprise Management.

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

Encrypt Passwords in AES Encryption Method

In CA Access Control r12.0 SP1, passwords were encrypted using the RC2 encryption method. In CA Access Control r12.5 SP1,the password encryption method was changed to AES. Therefore, passwords that were encrypted using RC2 encryption method cannot work in newer versions of CA Access Control. To solve this problem, you encrypt the existing passwords in AES after you upgrade from CA Access Control r12.0SP1.

Follow these steps:

1. Stop all the CA Access Control services.
2. Do the following:
   a. Connect to the Enterprise Management Server database as a user with read and write access privileges.
   b. Run the following query to remove the password CA Access Control Enterprise Management use to connect to the user store:

      ```
      update IM_DIR_CONNECTION set password=null where
      connection_name='java:/userstore’;
      ```
3. Encrypt all the passwords in the database using the pwdtools utility.

   For each entry in the tlbusers table, change the password with the encrypted passwords that you generate.
4. Remove the DMS settings from the connection table. Run the following query:

   ```
   DELETE FROM connection WHERE connection_name='con1';
   ```
5. Start all CA Access Control services.
6. Configure the DMS connection settings in CA Access Control Enterprise Management.

   Note:For more information about the DMS connection settings, see the *Online Help*.

Example: Encrypt passwords using the pwdtools utility

This example shows you how to encrypt a user password in AES encryption mode using the pwdtools utility and set the encrypted password in the Enterprise Management Server database.

1. Open the pwdtool.bat for editing. The file is located in the following directory, where *ACServerInstallDir* is the directory where the Enterprise Management Server is installed:

   ACServerInstallDir/IAM_Suite/Access_Control/tools/PasswordTool/

2. Enter the JAVA_HOME path in the "::SET JAVA_HOME=<enter valid java home here>" token. For example:

   ```
   SET JAVA_HOME=C:\jdk1.5.0
   ```

3. From a command-line window, run the following command, where *password* is a clear text password and *JBOSS_Home* is the directory where JBoss is installed:

   ```
   pwdtools -FIPS -p <"password"> -k
   JBOSS_HOME\server\default\deploy\IdentityMinder.ear\config\com\
   netegrity\config\keys\FIPSkey.dat
   ```

   The encrypted password is displayed. Copy the password to a clipboard.

4. Connect to the Enterprise Management Server as a user with read and write access rights to the database.

5. Run the following query where *encrypted password* is the encrypted password that you previously copied to a clipboard and *username* is the name of the user account:

   ```
   update tblusers set password = '<encrypted password>' where
   loginid='<username>';
   ```

You have set the account password with an encrypted password.

Upgrade the DMS

After installing the new CA Access Control Enterprise Management Server, you must upgrade the existing DMS. You do not need to remove the existing installation of the DMS before upgrading.

Important! Complete this step only if the DMS is installed on a separate computer than CA Access Control Enterprise Management.

To upgrade the DMS, install CA Access Control on the DMS computer (see page 22).

You can now configure CA Access Control Enterprise Management to connect to the DMS (see page 43).

Install Using Product Explorer

The CA Access Control Product Explorer lets you select between different architecture installations of CA Access Control and install the Runtime SDK. The Product Explorer uses a graphical interface to install CA Access Control and provides interactive feedback.

To install using Product Explorer

1. Log into the Windows system as a user with Windows administrative privileges (that is, as the Windows administrator or a member of the Windows Administrators group.)
2. Close any applications that are running on your Windows system.
3. Insert the CA Access Control Endpoint Components for Windows DVD into your optical disc drive.

   If you have autorun enabled, the Product Explorer automatically appears. Otherwise, navigate to the optical disc drive directory and double-click the PRODUCTEXPLORERX86.EXE file.
4. From the Product Explorer main menu, expand the Components folder, select CA Access Control for Windows (*my_architecture*), then click Install.

   You need to select the installation option that matches the architecture of the computer you are installing on (32-bit, 64-bit x64, or 64-bit Itanium).

   The Choose Setup Language window appears.
5. Select the language you want to install CA Access Control with and click OK.

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

   Note: If the installation program detects an existing installation of CA Access Control, you are prompted to select whether you want to upgrade CA Access Control.
6. Follow the instructions on the installation screens.

   During the installation, the installation program prompts you to supply information. For the information that you need when installing CA Access Control, refer to the installation worksheets.

   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.

   Note: If you choose to restart your computer later, an additional warning cautions you that the installation is not complete until your computer is rebooted. Some CA Access Control functionality, such as logon interception, does not work until after you restart your computer.

Configure the Connection to the DMS

During installation, CA Access Control Enterprise Management is configured to work against the Deployment Map Server (DMS) that is installed on the Enterprise Server. To create a custom connection to a different DMS, you need to configure it for your environment by configuring the connection to the custom DMS.

Note: During installation, CA Access Control Enterprise Management creates a default connection to the DMS on the Enterprise Management Server using the *ac_entm_pers* user account.

To configure the connection to the DMS

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

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

   The Create Connection task page appears.
3. Complete the fields in the dialog. 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 (AC).

   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: DMS*Name*@*hostName*

   For example, to use the default DMS that installs when you install CA Access Control Enterprise Management 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.

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

Click Submit.

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.

Upgrade the Distribution Host (DH)

After successfully upgrading the DMS, you upgrade the Distribution Host (DH). You upgrade the DH by installing the Distribution Server on every computer that is running the Distribution Host.

After installing the Distribution Server, you configure the Message Queue routing settings to establish routes for sending and receiving messages between the Distribution Server and CA Access Control Enterprise Management.

Important! Complete this step only if the DH is installed on a separate computer than CA Access Control Enterprise Management.

To upgrade the distribution host

1. Install the Distribution Server on the DH computer (see page 45).

   The Distribution Server installs the Java Connector Server (JCS), the DH, and the Message Queue.

2. Define the Message Queue routing settings (see page 46) between the Distribution Server and CA Access Control Enterprise Management.

   The Distribution Server is now configured.

Install the Distribution Server

When you configure CA Access Control to work in a disaster recovery or high availability environment, you install the Distribution Servers on separate computers and configure the Distribution Servers to propagate files between them.

To install the Distribution Server

1. Insert the appropriate CA Access Control Server Components DVD for your operating system into your optical disc drive.
2. Do either of the following:
   - On Windows:

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

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

     b. Expand the Components folder in the Product Explorer, select CA Access Control Distribution Server, then click Install.

        The InstallAnywhere installation program starts.

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

     /DistServer/Disk1/InstData/NoVM

  c. Run the following command:

```
./install_DistServer.bin -i console
```

  The InstallAnywhere installation program starts.

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

   Message Queue Settings

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

   Limits: Minimum of six (6) characters

   Java Connector Server - Provisioning Directory Information

   Defines the password for the Java Connector Server.

   Note: The Java Connector Server provides CA Access Control Enterprise Management with privileged account management capabilities.

   The CA Access Control Distribution Server installation is complete.

   Note: You must complete additional steps if you install the Distribution Server as part of a disaster recovery implementation.

How to Configure Message Routing Settings

When working in an environment that consists of a single instance of the Enterprise Management Server and multiple Distribution Servers, you must configure the MQ routing settings on all the Distribution Servers to point to the MQ on the Enterprise Management Server. This helps ensure that all the messages that the CA Access Control endpoints send are ultimately routed to a single MQ, that is located on the Enterprise Management Server.

To route messages from the MQ on every Distribution Server to the Enterprise Management Server, do the following:

- On each Distribution Server in your enterprise, do the following:
  - Stop the Message Queue service.
  - Modify the routing to the Enterprise Management Server Message Queue.
  - Define the parameters of the Enterprise Management Server Message Queue.
  - Configure the names of the Distribution Server message queues.
  - Specify the location of the Enterprise Management Server Message Queue.
  - Start the Message Queue service.
- On the Enterprise Management Server, do the following:
  - Stop the Message Queue service.
  - Modify the routing to the Distribution Server Message Queue.
  - Define the parameters of the Distribution Server Message Queue.
  - Configure the names of the Enterprise Management Server message queues.
  - Specify the location of the Enterprise Management Server Message Queue.
  - Start the Message Queue service.

Note: For information about message routing, refer to the *TIBCO Enterprise Message Service User's Guide*. Tibco documentation is installed as part of the Message Queue and is located at *ACServerInstallDir*/MessageQueue/tibco/ems/5.1/doc.

Modify the Message Queue Settings on the Distribution Server

By default, every Distribution Server is configured to work with the Message Queue that is running on that server. To route messages to another Message Queue, you must reconfigure the Message Queue settings.

This procedure shows you how to modify the Message Queue settings on the Distribution Server to enable communication with the CA Access Control Enterprise Management Message Queue. Complete this procedure for every Distribution Server in your enterprise.

To modify the Message Queue settings on the Distribution Server

1. Stop the CA Access Control Message Queue service.

   Important! When you stop the CA Access Control Message Queue service, the CA DSM r11Common Application Framework service is also stopped.

2. On the Distribution Server, open the file tibemsd.conf file, located by default in the following directory, where *DistServerInstallDir* is the directory in which you installed the Distribution Server:

   DistServerInstallDir/ACMQ/tibco/cfgmgmt/ems/data

3. Enter the Distribution Server short host name in the 'server' parameter.
4. Change the 'routing' parameter value to enabled.
5. Start the CA Access Control Message Queue service.

   You have modified the message queue settings on the Distribution Server.

Note: For information about message routing, refer to the *TIBCO Enterprise Message Service User's Guide*. Tibco documentation is installed as part of the Message Queue and is located at *ACServerInstallDir*/MessageQueue/tibco/ems/5.1/doc.

Example: tibemsd.conf file

The example shows you a snippet from the tibemsd.conf file after you modify the routing settings for a Distribution Server named DS_Example:

```
#####################
# Server Identification Information.
# server:    unique server name
# password:  password used to login into other routed server
#####################
server                 = DS_Example
password               =
#####################
…
#####################
# Routing. Routes configuration is in 'routes.conf'. This enables or
# disables routing functionality for this server.
#####################
routing                = enabled
#####################
```

Modify the Message Queue Settings on the Enterprise Management Server

This procedure shows you how to modify the Message Queue settings on the Enterprise Management Server to enable communication with the Distribution Server.

To modify the Message Queue settings on the Enterprise Management Server

1. Stop the CA Access Control Message Queue service.

   Important! When you stop the CA Access Control Message Queue service, the CA DSM r11Common Application Framework service is also stopped.

2. On the Enterprise Management Server, open the tibemsd.conf file for editing. This file is located in the following directory, where *ACServerInstallDir* is the directory in which you installed the Enterprise Management Server:

   ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

3. Enter the Enterprise Management Server short host name, not separated by dots, in the 'server' parameter.

4. Change the 'routing' parameter value to enabled.

5. Start the CA Access Control Message Queue service.

   You have modified the message queue settings on the Enterprise Management Server.

Note: For information about message routing, refer to the *TIBCO Enterprise Message Service User's Guide*. Tibco documentation is installed as part of the Message Queue and is located at *ACServerInstallDir*/MessageQueue/tibco/ems/5.1/doc.

Example: tibemsd.conf file

The example shows you a snippet from the tibemsd.conf file after you modify the routing settings for a CA Access Control Enterprise Management Server named ENTM_Example:

```
#####################
# Server Identification Information.
# server:    unique server name
# password:  password used to login into other routed server
#####################
server                 = ENTM_Example
password               =
#####################
…
#####################
# Routing. Routes configuration is in 'routes.conf'. This enables or
# disables routing functionality for this server.
#####################
routing                = enabled
#####################
```

Message Queue Connection Configuration

To route messages from the Message Queue on the Distribution Server to the Enterprise Management Server conversely, you modify the existing Message Queue settings in your enterprise.

Example: Configuring the Message Queue Connection Settings on the Distribution Server

This example shows you how to configure the Message Queue server settings on the Distribution Server. You configure the Message Queue to send messages to the Enterprise Management Server by defining the parameters of the Message Queue that is running on the Enterprise Management Server.

Follow these steps:

1. On the Distribution Server, do one of the following:
   - (Windows 2003 Server) Select Start, Programs, TIBCO-CA_AC, TIBCO EMS 5.1, Start EMS Administration Tool.
   - (UNIX) Do the following:
     a. Navigate to the following directory, where *DistServerInstallDir* is the directory in which you installed the Distribution Server:

        `DistServerInstallDir/MessageQueue/tibco/ems/5.1/bin`

     b. Run the following command:

        `tibemsadmin`

        The TIBCO EMS Administration Tool command prompt window opens.
2. Connect to the Message Queue using either of the following:
   - Enter the following command to connect using SSL:

     `connect ssl://localhost:7243`
   - Enter the following command to connect using TCP:

     `connect tcp://localhost:7222`

   A login name prompt appears.
3. Enter **admin**.

   A password prompt appears.
4. Enter the password that you provided when you installed the Distribution Server.
5. When prompted, enter a new password for the Message Queue server.
6. Define the Message Queue password.

   `set server password=`

   Example: set server password=*<C0mp1ex>*
7. Create a user named ENTM-NAME and assign a password to the user.

   `create user ENTM-NAME password=acserver_user-passwd`

   Example: create user EMS-SERVER password=*<acserver_user-passwd>*

   Important! Specify the same name that you defined in the 'server' parameter of the tibemsd.conf file on the Enterprise Management Server.

8. Do the following:
   a. Enter the following command:

      `add member ac_server_users ENTM_NAME`

      The user you created is added to the ac_server_users group.
   b. Enter the following command:

      `add member ac_endpoint_users ENTM_NAME`

      The user you created is added to the ac_endpoint_users group.
   c. Enter the following command:

      `add member report_publishers ENTM_NAME`

      The user you created is granted permissions to read and publish messages to CA Access Control queues.
9. Restart the Distribution Server.

   The changes you made are applied.

Example: Configure the Message Queue Connection Settings on the Enterprise Management Server

This example shows you how to configure the Message Queue server settings on the Enterprise Management Server. You configure the Message Queue to send messages to the Distribution Server.

In this example the term *DS-NAME* relates to the name of the Distribution Server computer and the term *ENTM-NAME* relates to name of the Enterprise Management Server. When you define the message queue server settings, you replace the name with the server actual names, as defined in the 'server' token in the *tibemsd.conf* file.

Follow these steps:

1. On the Enterprise Management Server, do one of the following:
   - (Windows 2003 Server) Select Start, Programs, TIBCO-CA_AC, TIBCO EMS 5.1, Start EMS Administration Tool.
   - (UNIX) Do the following:
     a. Navigate to the following directory, where *ACServerInstallDir* is the directory in which you installed the Enterprise Management Server:

        ACServerInstallDir`/MessageQueue/tibco/ems/5.1/bin`
     b. Run the following command:

        `tibemsadmin`

        The TIBCO EMS Administration Tool command prompt window opens.

2. Connect to the Message Queue using either of the following:
   - Enter the following command to connect using SSL:

     `connect ssl://localhost:7243`
   - Enter the following command to connect using TCP:

     `connect tcp://localhost:7222`

   A login name prompt appears.
3. Enter **admin**.

   A password prompt appears.
4. Enter the password that you provided when you installed the Enterprise Management Server.
5. Define the Message Queue password.

   `set server password=entm_server-passwd`

   Example: set server password=*<ENTM_SERVER_NAME-passwd>*
6. For each Distribution Server, create a user named DS-NAME and assign a password to the user.

   `create user DS-NAME password=dist_server_user`

   Example: create user EMS-Server password=*<C0mp1ex>*

   Important! Specify the same name that you defined in the 'server' parameter of the tibemsdf.conf file on the Enterprise Management Server.

7. Do the following:
   a. Enter the following command:

      `add member ac_server_users DS_NAME`

      The user you created is added to the ac_server_users group.

   b. Enter the following command:

      `add member ac_endpoint_users DS_NAME`

      The user you created is added to the ac_endpoint_users group.

   c. Enter the following command.

      `add member report_publishers DS_NAME`

      The user you created is granted permissions to read and publish messages to CA Access Control queues.

8. Restart the Distribution Server for the changes to take effect.

   You have configured the message queue connection settings on the Enterprise Management Server.

Note: For information about message routing, refer to the *TIBCO Enterprise Message Service User's Guide*. Tibco documentation is installed as part of the Message Queue and is located at *ACServerInstallDir*/MessageQueue/tibco/ems/5.1/doc.

Configure the Names of the Message Queues on the Distribution Server

To forward messages from the Distribution Server to the Enterprise Management Server, configure each messages route to forward the messages from the Message Queue on the Distribution Server to the Message Queue on the Enterprise Management Server.

In this procedure you define the message queue settings on the Distribution Server. You modify the message queue settings file to provide the settings of the Message Queue on the Enterprise Management Server.

To configure the names of the Message Queue on the Distribution Server

1. On the Distribution Server, open the file queues.conf. The file is located by default in the following directory, where *DistServerInstallDir* is the directory in which you installed the Distribution Server:

   DistServerInstallDir/ACMQ/tibco/cfgmgmt/ems/data

2. Locate the queue named 'queue/snapshots' and add the ENTM-NAME value at the end of the queue name, preceded by a @ sign as follows:

   queue/snapshots@*ENTM-NAME*

   ENTM-NAME

   Defines the short name of the Enterprise Management Server.

   Important! Specify the same name that you defined in the 'server' parameter of the tibemsd.conf file on the Enterprise Management Server.

3. Locate the queue name 'queue/audit' and add the ENTM-NAME value at the end of the queue name, preceded by a @ sign as follows:

   queue/audit@*ENTM-NAME*

4. Locate the queue named 'ac_endpoint_to_server' and add the ENTM-NAME value at the end of the queue name, preceded by a @ sign as follows:

   ac_endpoint_to_server@*ENTM-NAME*

5. Locate the queue named 'ac_server_to_endpoint' and add the ENTM-NAME value at the end of the queue name, preceded by a @ sign as follows:

   ac_server_to_endpoint@*ENTM-NAME*

6. Save and close the file.

Note: For information about message routing, refer to the *TIBCO Enterprise Message Service User's Guide*. Tibco documentation is installed as part of the Message Queue and is located at *ACServerInstallDir*/MessageQueue/tibco/ems/5.1/doc.

Configure the Names of the Message Queues on the Enterprise Management Server

In this procedure you define the message routing settings on the Enterprise Management Server. You configure the Message Queue settings on the Enterprise Management Server to identify this Message Queue as the primary server.

To configure the names of the Message Queues on the Enterprise Management Server

1. On the Enterprise Management Server, open the file queues.conf in an editable form. The file is located in the following directory, where *ACServerInstallDir* is the directory in which you installed the Enterprise Management Server:

   ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

2. Locate the queue named 'queue/snapshots' and add the word 'global' after the word 'secure' at the end of the queue name, as follows:

   ```
   queue/snapshot secure, global
   ```

3. Locate the queue named 'queue/audit' and add the word 'global' after the word 'secure' at the end of the queue name, as follows:

   ```
   queue/audit secure, global
   ```

4. Locate the queue named 'ac_endpoint_to_server' and add the word 'global' after the word 'secure' at the end of the queue name, as follows:

   ```
   ac_endpoint_to_server secure, global
   ```

5. Locate the queue named 'ac_server_to_endpoint' and add the word 'global' after the word 'secure' at the end of the queue name, as follows:

   ```
   ac_server_to_endpoint secure, global
   ```

6. Save and close the file.

Note: For information about message routing, refer to the *TIBCO Enterprise Message Service User's Guide*. Tibco documentation is installed as part of the Message Queue and is located at *ACServerInstallDir*/MessageQueue/tibco/ems/5.1/doc.

Message Routing Configuration

After you have configured the Message Queue settings and configured the message queue routing settings on the Distribution Server and on the Enterprise Management Server, you set up the message routes on the Distribution Server and on the Enterprise Management Server.

Example: Set Up Message Routes on the Distribution Server

This example shows you how to set up the message route settings on the Distribution Server. You set up a route between the Distribution Server and the Enterprise Management Server to route messages arriving from CA Access Control endpoints to the Message Queue on the Enterprise Management Server. Complete this procedure on every Distribution Server in your enterprise.

1. On the Distribution Server, open the file routes.conf for editing. The file is located by default in the following directory, where *DistServerInstallDir* is the directory in which you installed the Distribution Server:

   DistServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

2. Add the following entries:

   ```
   [ENTM-NAME]
   url          = ENTM-URL
   ssl_verify_host = disabled
   ssl_verify_hostname = disabled
   ```

   ENTM-NAME

   Defines the short name of the Enterprise Management Server.

   ENTM_URL

   Defines the Enterprise Management Server URL.

3. Save the file.
4. Restart the CA Access Control Message Queue service.

Example: Set Up Message Routes on the Enterprise Management Server

This example shows you how to set up the message route settings on the Enterprise Management Server. You set up a route between the Enterprise Management Server and the Distribution Server to send messages from the Enterprise Management Server to the Distribution Server and from there to the endpoints.

1. On the Enterprise Management Server, open the file routes.conf. The file is located by default in the following directory, where *ACServerInstallDir* is the directory in which you installed the Enterprise Management Server:

   ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

2. Add the following entries:

   ```
   [DS-NAME]
   url          = DS-URL
   ssl_verify_host = disabled
   ssl_verify_hostname = disabled
   ```

   DS_NAME

   Defines the short name of the Distribution Server.

   DS_URL

   Defines the Distribution Server URL.

3. Save the file.
4. Restart the CA Access Control Message Queue service.

Note: For information about message routing, refer to the *TIBCO Enterprise Message Service User's Guide*. Tibco documentation is installed as part of the Message Queue and is located at *ACServerInstallDir*/MessageQueue/tibco/ems/5.1/doc.

Migrate the Report Server to the Enterprise Reporting Services

The Enterprise Reporting services bundle the Report Server functionality into a single enterprise wide reporting service. Due to architectural changes, the Report Server is now a part of CA Access Control Enterprise Management and is no longer an individual component. You migrate the Report Server by installing Distribution Server on the Report Server and reconfiguring the Message Queue settings.

Note: This migration process lets existing endpoints continue using the Message Queue on the Report Server computer. You do not need to reconfigure the ReportAgent settings on the endpoints after you complete this procedure.

Important! Complete this step only if the Report Server is installed on a separate computer than CA Access Control Enterprise Management.

Follow these steps

1. Install the Distribution Server on the Report Server computer (see page 45).
2. Disable the JBoss service.
3. Define Message Queue route settings (see page 46) between the Distribution Server and CA Access Control Enterprise Management.

   The Enterprise Reporting services (including the Report Server) are installed. You can now configure the Enterprise Reporting server components.

   Note: For more information about the Enterprise Reporting Server components, see the *Enterprise Administration Guide*.
4. Subscribe the DH on the new DMS (see page 60).

Subscribe a DH to a DMS

After you have completed upgrading CA Access Control Enterprise Management components, you cannot continue working with the previous DMS. You must configure the upgraded DH to work with the new DMS before starting CA Access Control Enterprise Management.

Important! Complete this step only if you installed the Distribution Server on the Report Server computer.

Follow these steps:

1. Open a command prompt window on the Distribution Server.
2. Subscribe the new DMS with the Distribution Host.

   sepmd -s DH__WRITER DMS__@<entm>
3. Add the new DMS as the Distribution Host parent.

   sepmd -s DMS__ DH__@<host_name>
4. On the Enterprise Management Server, open a command prompt window and create a new subscriber.

   sepmd -n DH__@<host_name>

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

Upgrade CA Access Control Endpoints

After upgrading CA Access Control Enterprise Management, the DMS, the Distribution Host and the Report Server, you can now upgrade the existing CA Access Control r12.0 SP1 endpoints.

To upgrade CA Access Control endpoints install CA Access Control on the endpoints (see page 22).

Chapter 6: Migrating PMDs to an Advanced Policy Management Environment

This section contains the following topics:

Migration to an Advanced Policy Management Environment

When you migrate from a Policy Model (PMD) environment to an advanced policy management environment, you change the way you deploy rules to your endpoints:

- In a PMD environment, regular rules you define in a central database (PMDB) are automatically propagated to databases in a configured hierarchy.
- In an advanced policy management environment, you assign policies (groups of rules) to one or more host or host groups. You can also undeploy (remove) policies and view deployment status and deployment deviation.

When you migrate from a PMD environment to an advanced policy management environment, you:

- Install additional components
- Create policies from the rules in the PMDB
- Upgrade the endpoints
- Flatten your PMD structure

Advanced policy management does not support hierarchical host groups. If your PMD architecture contains hierarchical PMDBs, you must flatten your PMD hierarchy.

Note: Advanced policy management does not support policies with password management commands. You must use a password PMD to synchronize passwords between endpoints and to distribute password management rules. You cannot migrate a password PMD to the advanced policy management environment. Instead, you apply a filter file to the password PMD so that it only sends password rules to its subscribers.

How the Migration Process Works

Migrating to an advanced policy management environment lets you deploy and undeploy policies, and check the deployment and deviation status of policies. While you use CA Access Control to perform most migration tasks, there are still some tasks you must perform yourself. Understanding how the migration process works helps you troubleshoot any problems that may arise.

The following process gives you an overview of the stages in the migration process:

1. You install the Enterprise Management server components.

   The advanced policy management environment is set up as part of the Enterprise Management installation process.

2. You upgrade the PMD to CA Access Control r12.5 or later.
3. You migrate the endpoints that subscribe to the PMD to the advanced policy management environment.
4. In CA Access Control Enterprise Management, you export the rules in the PMDB to policy files.
5. CA Access Control Enterprise Management creates the following on the DMS:
   - A host group (GHNODE object) that corresponds to the migrated PMDB
   - Hosts (HNODE objects) that correspond to the endpoint subscribers of the PMDB
   - POLICY objects that contain the rules in the policy files
6. In CA Access Control Enterprise Management, you join the hosts to the host group. CA Access Control assigns the POLICY objects to the host group and deploys the POLICY objects to the hosts that correspond to the endpoint subscribers of the PMDB.
7. In CA Access Control Enterprise Management, you do *one* of the following:
   - If the PMD is a password PMD, you apply a filter file to the PMD.
   - If the PMD is not a password PMD, you delete the PMD.

Note: You can also use the policydeploy utility to perform migration tasks.

More information:

How to Migrate to Advanced Policy Management (see page 65)

How Policies Are Created and Assigned

When you migrate from a PMD environment to an advanced policy management environment, you use CA Access Control to create policies from the rules in the PMDB and assign the policies to host groups on the DMS.

The following process explains how CA Access Control creates and assigns policies:

1. CA Access Control exports the rules in the PMDB to a policy file.

   Note: You can specify that CA Access Control only exports rules that modify resources in a particular class.

2. CA Access Control changes each rule that creates a new resource or accessor to a rule that modifies the resource or accessor. For example, CA Access Control changes all newres rules to editres rules.

   This step prevents the deployment errors that result if you deploy a rule that creates a new resource or accessor more than once to the same endpoint.

3. CA Access Control creates a host group (GHNODE object) that corresponds to the PMD on the DMS.

4. For each endpoint subscriber that is listed in the PMDB, CA Access Control checks if a corresponding host (HNODE object) is already created in the DMS.

   - For each subscriber that is listed in the PMDB and that has a corresponding host in the DMS, CA Access Control joins the host to the host group created in Step 3.
   - For each subscriber that is listed in the PMDB and that does not have a corresponding host in the DMS, CA Access Control creates a host that corresponds to the endpoint and joins the host to the host group created in Step 3.

   Note: CA Access Control does not create hosts that correspond to subscriber PMDBs.

5. CA Access Control uses the rules in the exported policy file to create a POLICY object in the DMS.

   Note: CA Access Control does not create an undeploy script for the POLICY object.

6. CA Access Control assigns the POLICY object to the host group that it created in Step 3.

More information:

Migrate a PMDB (see page 67)

How Policies Are Initially Sent to a Migrated Endpoint

When you migrate from a PMD environment to an advanced policy management environment, CA Access Control creates policies from the rules in the PMDB and sends them to the migrated endpoints. Understanding how CA Access Control initially sends the policies to the migrated endpoint may help you troubleshoot any errors that occur during the migration process.

The following process explains how policies are initially sent to a migrated endpoint after you start CA Access Control on the endpoint:

1. CA Access Control starts and invokes policyfetcher, which sends a heartbeat notification to the DMS.
2. The DMS receives the heartbeat notification and checks if a corresponding host (HNODE) object exists on the DMS.
3. *One* of the following happens:
   - If a corresponding host exists on the DMS, and the host is part of the host group that corresponds to the PMD that you migrated:
     a. CA Access Control associates the endpoint and the host.
     b. CA Access Control deploys the policies that are assigned to the host group to the endpoint.
   - If a corresponding host does not exist on the DMS:
     a. CA Access Control creates the host.
     b. When you create and assign policies, CA Access Control joins the host to the host group that corresponds to the PMD that you migrated.
     c. CA Access Control deploys the policies that are assigned to the host group to the endpoint.
4. CA Access Control modifies the Update Time property for each resource listed in the policy to the time the policy was deployed.

   Note: Because CA Access Control changed commands that create objects to commands that modify objects, you should not see any deployment errors for the policy.

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

How CA Access Control Applies a Filter File to a Password PMD

Advanced policy management does not support policies with password management commands. Use a password PMD to synchronize passwords between endpoints and to distribute password management rules. When you migrate a password PMD to the advanced policy management environment, you apply a filter file to the password PMD so that it only deploys password rules to its subscribers.

The following process explains how CA Access Control applies a filter file to a password PMD:

1. CA Access Control creates a text file named filter.flt and adds the following lines to it:

```
#-------------------------------------------------------------------------
--
# access    env     class   objects properties              pass/nopass
#-------------------------------------------------------------------------
--
  *         *       USER    *       OLD_PASSWD;CLR_PASSWD   PASS
  *         *       *       *       *                       NOPASS
#-------------------------------------------------------------------------
--
```

2. CA Access Control saves filter.flt in the password PMD directory.
3. CA Access Control adds the full path of filter.flt to the "filter" configuration setting in the following location:
   - (UNIX) The [pmd] section of the pmd.ini file
   - (Windows) The following registry key:

     HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Pmd*PMDB_Name*

How to Migrate to Advanced Policy Management

Migrating to an advanced policy management environment lets you deploy and undeploy policies, and check the deployment and deviation status of policies.

Note: Advanced policy management does not support policies with password management commands. You must use a password PMD to synchronize passwords between endpoints and to distribute password management rules. You cannot migrate a password PMD to the advanced policy management environment.

Before you begin the migration process, verify that:

- All subscribers are available
- The subscribers have received all updates from the PMDB
- No subscribers are synchronized with the PMDB

Important! We strongly recommend that you back up the PMDB before you begin the migration process.

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

1. Install the Enterprise Management server components.

   The advanced policy management environment is set up as part of the Enterprise Management installation process.
2. Upgrade the PMD host to CA Access Control r12.5 or later.
3. Migrate the endpoints (see page 66).
4. Migrate the PMDB (see page 67).

More information:

How the Migration Process Works (see page 62)

Migrate an Endpoint

Migrating the endpoints is the third step in the process to migrate from a PMD environment to an advanced policy management environment. In the preceding steps, you:

- Installed the Enterprise Management server components
- Upgraded the PMD host to CA Access Control r12.5 or later

In this step, you migrate the endpoints that subscribe to the migrated PMDB.

To migrate an endpoint

1. Upgrade the endpoint to CA Access Control r12.0 or later.
2. Run the following commands on the endpoint to configure advanced policy management client components:

   ```
   dmsmgr -config -endpoint
   dmsmgr -config -dh dh_name@host_name
   ```

   The endpoint is upgraded to the advanced policy management environment.

Migrate a PMDB

We recommend that you understand the steps you must perform at each stage of the overall migration process before you migrate a PMDB. Migrating a PMDB is only one step in the process to migrate an enterprise deployment of CA Access Control to an advanced policy management environment.

Migrating a PMDB is the final step in the process to migrate from a PMD environment to an advanced policy management environment. In the preceding steps, you:

- Installed the Enterprise Management Server
- Upgraded the PMD host to CA Access Control r12.5 or later
- Migrated an endpoint (upgraded the endpoint to CA Access Control r12.0 or later and configured advanced policy management client components)

In this step, you use CA Access Control Enterprise Management to create a policy from the rules in the PMDB, create a host group for the migrated PMDB, and join the hosts that correspond to the PMDB subscribers to this host group. You can also choose to assign the new policy to the host group.

Important! Each time you click the Next button, CA Access Control Enterprise Management completes an action in the DMS or in the PMDB. It may be difficult to undo the result of these actions.

To migrate a PMDB

1. In CA Access Control Enterprise Management, click the Policy Management tab, click the Policy sub-tab, expand the Policy tree, and click PMDB Migrate.

   The PMDB Host Login page appears.

2. Type a user name and password that is authorized to access the PMDB and the name of the PMDB that you want to migrate, and click Log In.

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

   The PMDB Migrate Process page appears at the General task stage.

3. Complete the following fields, and click Next:

   Name

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

   Description

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

Policy Classes

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

Export dependent classes

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

The Policy Script task stage appears.

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

   CA Access Control Enterprise Management creates a policy from the rules. The Host Group task stage appears.

5. Complete the dialog and click Next, as follows:

   Host Group

   Specifies the name of the host group to add the hosts to. You can specify an existing host group or create a new host group.

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

   Assign Policy

   (Optional) Specifies to assign the policy to the host group.

   Assigned Hosts

   Specifies the hosts to add to the host group.

   Note: By default, this table contains all subscribers of the migrated PMDB that you have authority to access. You can add and remove hosts from the Assigned Hosts list; however, you cannot add a host to the host group if you do not have authority to access the host.

   CA Access Control Enterprise Management adds the hosts to the hosts group and, if specified, assigns the policy to the host group. The PMD Options task stage appears.

6. Select any of the following options that you want to apply to the migrated PMDB:

   Unsubscribe the hosts that you specified in step 3 (Host Group step)

   Specifies to unsubscribe the endpoints that you selected in the previous task stage from the migrated PMDB.

   Unsubscribe all of the PMDB subscribers

   Specifies to unsubscribe all subscribers from the migrated PMDB.

Delete the PMD

Specifies to delete the migrated PMDB.

Important! Do not delete the PMDB if you use it to propagate user password commands.

Add PMD filter file

Specifies to add a filter file to the migrated PMDB so that the PMDB only propagates user password commands to its subscribers. If you select this option, the migrated PMDB becomes a password PMDB.

7. Click Next.

   CA Access Control performs the actions that you specified. The Migration Actions Summary task stage appears and the migration process is complete.

More information:

How Policies Are Created and Assigned (see page 63)

Class Dependency

When you export the rules for specified classes from a PMDB, you can choose to also export the rules for dependent classes. If you specify that CA Access Control should export dependent classes, CA Access Control exports the following:

- If you export rules that modify resources in a particular class, and the class has a corresponding resource group, CA Access Control also exports the rules that modify resources in that resource group.

  For example, if you specify to export FILE class rules, CA Access Control exports the rules that modify resources in the FILE and GFILE classes.

- If you export rules that modify resources in a particular resource group, CA Access Control also exports the rules that modify the member resource of the resource group.

  For example, if you specify to export GFILE class rules, CA Access Control exports the rules that modify resources in the GFILE and FILE classes.

- If you export rules that modify resources in a particular class and that class has a PACL, CA Access Control also exports the rules that modify resources in the PROGRAM class.

- If you export rules that modify resources in a particular class and that class has a CALACL, CA Access Control also exports the rules that modify resources in the CALENDAR class.
- If you export rules that modify resources in a particular class, and one of the resources in that class is a member of a CONTAINER resource group, CA Access Control exports the rules that modify resources in the CONTAINER class and the rules that modify the resources that are members of each CONTAINER resource group.

  For example, if you specify to export CONTAINER class rules, and the CONTAINER object holds FILE objects, CA Access Control exports the rules that modify resources in the CONTAINER and FILE classes.

Duplicate HNODEs Appear In DMS

Symptom:

After I migrated a PMD to an advanced policy management environment, two HNODEs that represent the same endpoint are created in the DMS.

Solution:

The fully qualified host name of the endpoint is not the same on the DMS and on the endpoint. To fix this problem, delete one of the HNODE objects in the DMS.

Note: For more information about HNODE objects and the DMS, see the *Enterprise Administration Guide*.

Migrate Hierarchical PMDBs

Advanced policy management does not support hierarchical host groups. If your PMD architecture contains hierarchical PMDBs, you must flatten your PMD hierarchy during the migration process.

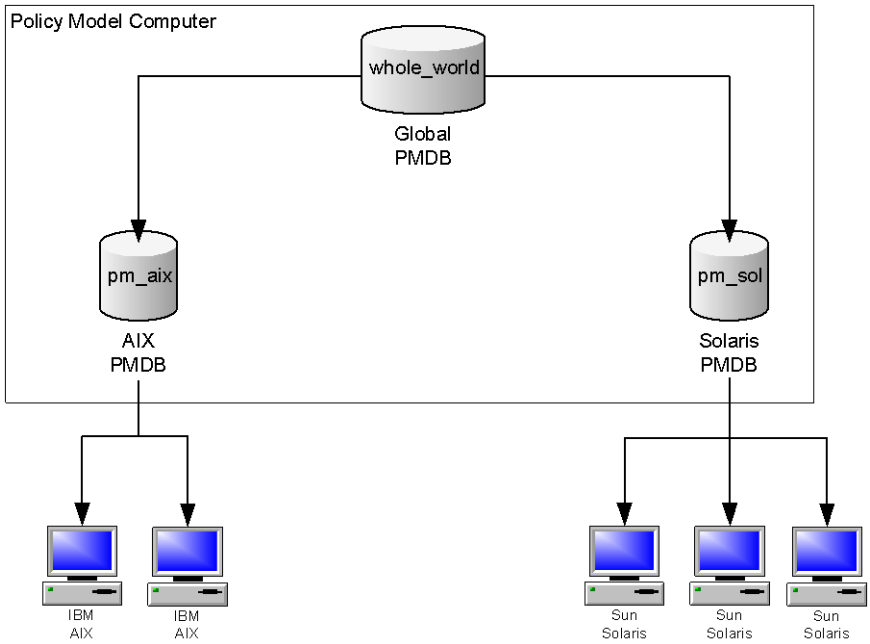
When you flatten the PMD hierarchy, you migrate each PMDB separately. During the migration CA Access Control creates a host group for each PMDB in the hierarchical environment and adds each endpoint to all the host groups that correspond to the PMDBs to which it was subscribed.

To migrate hierarchical PMDBs

1. Migrate the master PMDB.
2. Migrate each subscriber PMDB.

Example: Migrate Hierarchical PMDBs

The following diagram shows an example of a PMD environment with hierarchical PMDBs.



In this example, the PMDBs pm_aix and pm_solaris are subscribers of the PMDB whole_world. All IBM AIX endpoints are subscribers of pm_aix. All Sun Solaris endpoints are subscribers of pm_sol. Effectively, all endpoints are subscribers of whole_world.

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

1. Migrate the whole_world PMDB.

   CA Access Control creates the whole_world host group. All endpoints are members of this host group.

2. Migrate the subscriber PMDBs:

   - Migrate the pm_aix PMDB.

     CA Access Control creates the pm_aix host group. IBM AIX endpoints are members of this host group.

   - Migrate the pm_sol PMDB.

     CA Access Control creates the pm_sol host group. Sun Solaris endpoints are members of this host group.

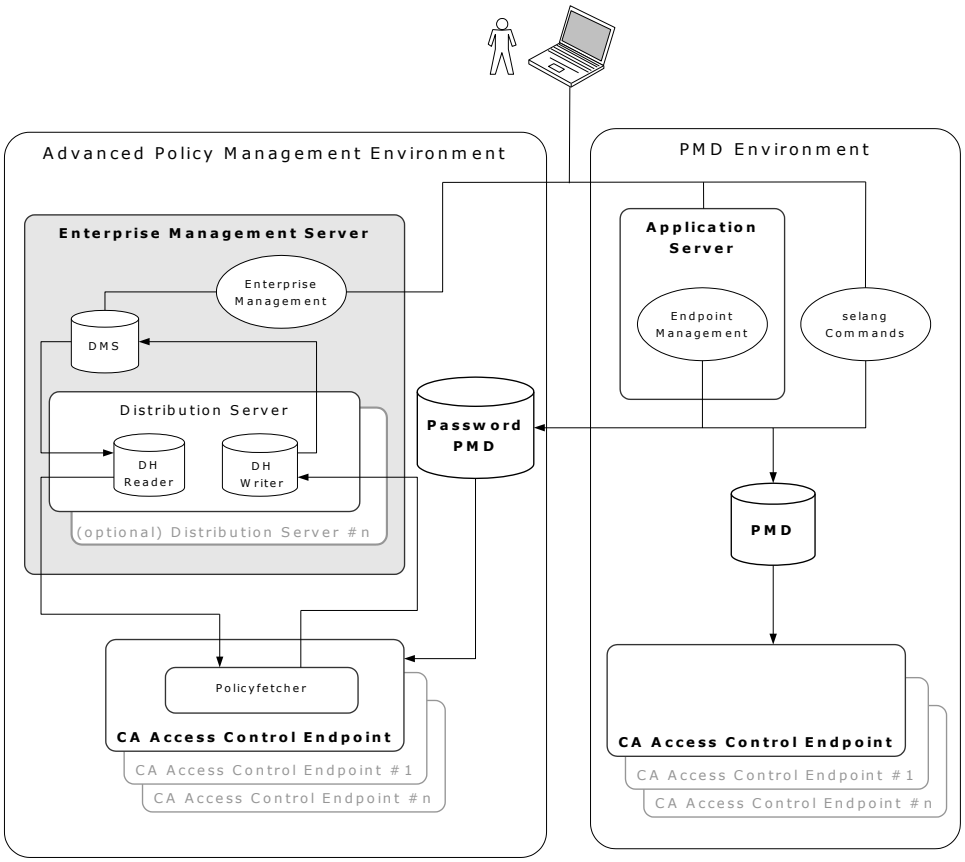
Note: In a PMD environment, if you apply a filter file to the pm_aix PMDB, the filter file may prevent the rules that you deploy from the whole_world PMDB from reaching the IBM AIX endpoints. In an advanced policy management environment, the IBM AIX endpoints are members of the whole_world host group. All the rules that you deploy to the whole_world host group are deployed to all the endpoints without filtering. You should be aware of this changed behavior when you deploy rules in an advanced policy management environment.

Mixed Policy Management Environments

A mixed policy management environment is a CA Access Control deployment in which some endpoints subscribe to a PMD and some endpoints are defined in an advanced policy management environment.

The following diagram shows an example of a CA Access Control deployment with a mixed policy management environment.

Note: Although it is not shown in this diagram, an endpoint can subscribe to a PMD and also be defined in an advanced policy management environment. For example, you can deploy policies to an endpoint in an advanced policy management environment, and also propagate selang rules from a PMD to the same endpoint.



Update Endpoints in a Mixed Policy Management Environment

When you update endpoints in a mixed policy management environment, you update the endpoints in each environment separately.

Note: Endpoints cannot accept rules that modify classes that were introduced in a later CA Access Control version. For example, an r8 endpoint can only accept rules that change r8 functionality, even though you deploy the rules from an r12.5 PMD or DMS.

To update endpoints in a mixed policy management environment

1. Create a script file with the selang deployment commands you want to deploy to the endpoints.
2. In CA Access Control Enterprise Management, do the following:
   a. Store the policy version on the DMS.
   b. Assign the stored policy version to the host groups you want to update.

   CA Access Control deploys the policy to the endpoints in the host group.
3. Update the PMDB with the selang commands in the script file.

   The PMDB propagates the commands to its endpoints.

Note: For more information about how to store and assign policy versions, see the *Enterprise Administration Guide*. For more information about how to update the PMDB, see the *Endpoint Administration Guide* for your OS.