CA Embedded Entitlements Manager

Implementation Guide

Release 12.51

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Documentation Changes

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

- Operating System Support (see page 11)—Updated the UNIX operating systems with 64-bit and deleted references to CA EEM running as a 32-bit application.
- Certificates with Custom Key Length for CA EEM Server (see page 62)—Added to describe that CA EEM supports custom key length certificates for the SSL communication.

Contents

Chapter 1: Understanding CA EEM 7

Overview 7
Functions 7
Features 8

Chapter 2: Implementing CA EEM Server 9

Installation Prerequisites 9

Chapter 3: Operating System Support 11

System Requirements 11
- Windows 12
- UNIX and Linux 12

Install Considerations 12
- Supported FIPS Modes 12

Windows Installation 13
- Installation Worksheet 13
- Install CA EEM Server Manually 14
- Install CA EEM Server Silently 15

UNIX Installation 16
- Installation Worksheet 16
- Install CA EEM Server Manually 18
- Install CA EEM Server Silently 18

CA EEM Server Installation Structure 20
Verify Installation 20

Chapter 4: Post-Installation Configuration Tasks 21

User Access Permissions 21
CA EEM Server User Stores Configuration 23
- Configure CA EEM with Internal Datastore 24
- Reference from an External LDAP Directory 24
- How You Integrate SiteMinder with CA EEM 32

Certificate Validation 35
- Prerequisites 35
- How to Validate a Certificate 36

FIPS 140-2 Support Configuration 40

FIPS 140-2 Overview 41
Supported Security Modes in CA EEM 42
Configuring CA EEM Server in FIPS-only Mode 42
Configure Your Application in FIPS-only Mode 46
Disaster Recovery Configuration 48
Overview 48
File System Back Up 49
Back up and Restore CA EEM Data 50
Failover Configuration 56
Prerequisites 56
How to Set Up a Failover Environment 56
How to Delete a Secondary Server 60
Certificates with Custom Key Length for CA EEM Server 62
Considerations for Using Higher Key Length Certificates 62
How to Generate the Certificates 63
Generate Certificates with Custom Key Length for CA EEM Servers in Failover or Cluster Environment 65
Configure SSL Communication between CA EEM Server and LDAP Server 68

Chapter 5: Upgrading CA EEM Server 71

Upgrade Considerations 71
Upgrade CA EEM Server 73
Upgrade CA EEM Server 73
How to Migrate CA EEM Server from an Unsupported Operating Systems 74

Chapter 6: Uninstalling CA EEM Server 77

Uninstall CA EEM Server Manually 77
Uninstall CA EEM Server Silently 78

Chapter 7: Appendix 79

Ports Used by CA EEM 79
CA EEM Services 79

Chapter 1: Understanding CA EEM

This section contains the following topics:

Overview (see page 7)
Functions (see page 7)
Features (see page 8)

Overview

CA Embedded Entitlements Manager (CA EEM) allows applications to share common access policy management, authentication, and authorization services.

Functions

CA EEM provides a set of security services. The following security services are available:

- Configuration services:
  - Registering and unregistering application instances
  - Administrative scoping of application administrators
  - Delegating administrative rights
  - Managing users and groups
- Administration security services:
  - Managing access, event, and obligation policies
  - Managing calendars
- Run-time security services:
  - Authenticating users
  - Authorizing access
  - Logging security events

Features

CA EEM consists of the following features:

General

- Policy isolation lets each registered application instance to use its own space for storing its application-specific data
- Run-time SDK available for Java, C++, and C#
- Administrative SDK available for Java, C++, and C#
- Command line interface support for administrative functions (insert/modify/remove objects):
  - XML export and import
  - Run-time checks
  - Migration tools
- Web interface support for standalone and launch-in-context access
- Secure HTTP communications
- Integration with SiteMinder to retrieve user and group information from SiteMinder data store

Identity Management

- Shared global users and attributes for all applications
- Support for different modes for global users
  - Internal global users, complete with password policy management
  - External global users from LDAP directory servers
- Support for portable session export and import for single sign-on

Access Management

- Access management covers both Access Control Lists (ACLs) and business policies
- Policy language allows the use of user, session, environment, and resource attributes in making policy decisions
- Built-in administrative scoping of all objects
- Built-in support for delegated administration
- Built-in support for custom obligation checks requiring application-specific actions
  - Local in-process evaluation of permission checks
  - SDK and Web interface for defining access policies, ACLs, administrative scoping policies, and delegated authority

Chapter 2: Implementing CA EEM Server

This section contains the following topics:

Installation Prerequisites (see page 9)
Operating System Support (see page 11)
System Requirements (see page 11)
Install Considerations (see page 12)
Windows Installation (see page 13)
UNIX Installation (see page 16)
CA EEM Server Installation Structure (see page 20)
Verify Installation (see page 20)

Installation Prerequisites

- Verify that the computer that hosts the CA EEM Server meets the minimum operating system and system requirements.
- Gather the required information about the installation options for the CA EEM Server.
- Verify that the following do not contain non-english letters in the names:
  - Host name of the computer where you want to install CA EEM server
  - Installation folders used by CA EEM
  - Temporary folder path

Chapter 3: Operating System Support

CA EEM Server and CA EEM SDK are supported on following platforms:

Platform	Architecture	Version
Windows	x86/64	Microsoft Windows 2008 Microsoft Windows 2008 R2 Microsoft Windows 7
Solaris	SPARC/64-bit	Oracle Solaris 11 Sun Solaris 10 (Ultra SPARC) with GNU tar 1.15.1 Sun Solaris 9 (Ultra SPARC) with GNU tar 1.15.1 Sun Logical Domains
Linux	x86/64	SUSE Linux Enterprise Server 10, SUSE Linux Enterprise Server 11 Red Hat Enterprise Linux Server 5, Red Hat Enterprise Linux Server 6 Ubuntu 10.04 LTS Server
IBM AIX	Power5/64-bit	IBM AIX 7 IBM AIX 6.1 IBM AIX 5.3 with Maintenance Level 9, libcompat.1.o library
HP-UX	PARISC/32-bit	HP 11.31
HP-UX	Itanium 2/64-bit	HP Itanium 11.31

CA supports these operating systems for the duration of their lifecycle (as determined by the operating system's manufacturer or until CA announces that we are dropping support). Visit our website http://ca.com/support for the latest information about supported operating systems.

System Requirements

The following section describes the CA EEM Server system requirements.

Windows

The recommended system requirements are as follows:

- An Intel Pentium processor
- 4GB RAM
- 10 GB of hard disk free space
- At least 300 MB disk space is required under the temporary directory %temp% (C:\Documents and Settings\Administrator\Local Settings\Temp\) where the CA EEM installation files are extracted during the installation
- Windows Installer v3 or later
- Winsock-compatible TCP/IP installed and configured

  Windows administrator access to the system
- Internet Browser to run the Web components (Microsoft Internet Explorer 7.0 or higher, or Mozilla Firefox 3.0 or higher).

UNIX and Linux

The recommended system requirements are as follows:

- 4GB RAM
- 10 GB of hard disk free space
- 500 MB disk space is required under the temporary directory (/tmp) where the CA EEM installation files are extracted during the installation.
- A Web browser to run the web components (Firefox 3.0 or higher).

Install Considerations

Review the following installation considerations before you install the CA EEM Server.

Supported FIPS Modes

By default CA EEM is installed in a non-FIPS mode. FIPS-only mode can be configured during installation or post-installation.

CA EEM does not support FIPS-only mode with SAML and SELinux operating systems.

Windows Installation

You can install CA EEM using one of the following methods:

- Manual Installation using the CA EEM install wizard
- Silent Installation using the CA EEM response file

Important! On a firewall enabled computer, verify that no application uses the port 5250, because CA iTechnology iGateway runs on this port.

Installation Worksheet

Before you install CA EEM, gather the information in the following table. After you complete the worksheet, you can use it as you work through the installation prompts.

Required Information	Response File Parameter	Comments
Shared Components Path	SHARED_COMPONENTS_PATH	Enter the path where you installed the CA EEM components. **Default**: C:\Program Files\CA\SC
CA Directory Path	CADIR_PATH	Enter the path where you installed CA Directory. **Default**: C:\Program Files\CA\Directory. **Note**: During installation, CA EEM creates an environmental variable %DXHOME% that points to the installation path.
Data DSA Port	DATA_DSA_PORT	Enter the port number that DSA uses to listen to requests. **Default**: 509
DB Size(in Mb)	DB_SIZE	Enter the maximum size of the datastore for CA EEM. **Default**: 256 MB
EiamAdmin Password	EIAMADMIN_PASSWORD	Enter the EiamAdmin password in clear text or munged format.
CA EEM Installation path	EIAM_PATH	Enter the path where you installed the CA EEM Server. **Default**: C:\Program Files\CA\SC\EmbeddedEntitlementManager

Required Information	Response File Parameter	Comments
CA iTechnology iGateway Installation Path	IGW_PATH	Enter the path where you installed CA iTechnology iGateway. **Default**: C:\Program Files\CA\SC\iTechnology **Note**: During installation, CA EEM creates an environmental variable %IGW_LOC% that points to the installation path.
Backup Directory Path	BACKUP_LOCATION	Enter the path where you want to store the backup files.

More information:

Install CA EEM Server Silently (see page 15)

Install CA EEM Server Manually

Use the installation wizard to manually install the CA EEM server. Before you perform the following procedure, verify that you have the CA EEM installer.

Follow these steps:

1. Navigate to the location where you stored the CA EEM installer.
2. Right-click the installer and select Run as administrator.

   The installation wizard opens.

   Note: You cannot install a 64-bit version of the CA EEM installer on a 32-bit operating system.
3. Follow the instructions on the installation wizard, and click Finish.

   The CA EEM server is installed.

More information:

Installation Worksheet (see page 13)

Install CA EEM Server Silently

CA EEM provides you a response file that you must configure to silently install the CA EEM server. You can use the response file to perform identical silent installations on various servers.

To install a CA EEM server, perform the following steps:

1. Configure the response file.
2. Invoke the silent installation.

More information:

Installation Worksheet (see page 13)
Configure the Response File (see page 15)
Invoke Silent Installation (see page 19)

Configure the Response File

CA EEM creates a Response File with default values. You can use the Response File with the default values or edit the Response File to silently install the CA EEM server.

Follow these steps:

1. Navigate to the location *EEMServer_home*\CA\SC\EmbeddedEntitlementManager.
2. Copy the response.properties file to the <install directory of target server>.
3. (Optional) Edit the response.properties file, and save the changes.

   The Response File is configured.

   Note: If you are using a non-English characters in the response ffile, save the response file in the UTF-8 encoded format.

Example: Response file (Windows)

```
INSTALLER_UI=SILENT
SHARED_COMPONENTS_PATH=C:\\Program Files\\CA\\SC
EIAM_PATH=C:\\Program Files\\CA\\SC\\EmbeddedEntitlementManager
IGW_PATH=C:\\Program Files\\CA\\SC\\iTechnology
CADIR_PATH=C:\\Program Files\\CA\\Directory
DATA_DSA_PORT=509
DB_SIZE=256
FIPS_ENABLED=true
EIAMADMIN_PASSWORD={munged}GBUHA01AXQFY
BACKUP_LOCATION=C:\\Program Files\\CA\\SC\\Backup
```

Invoke Silent Installation

Follow these steps:

1. Open the command prompt from the target server.
2. Execute the following command:

   ```
   EEMServer<version_number>.exe –f responsefile.properties
   ```

Note: You can also use the command line parameters with the silent installation.

UNIX Installation

You can install CA EEM using one of the following methods:

- Manual Installation using the CA EEM installer
- Silent Installation using the CA EEM response file

Installation Worksheet

Before you install CA EEM, gather the information in the following table. After you complete the worksheet, you can use it as you work through the installation prompts.

Required Information	Response File Parameter	Comments
Shared Components Path	SHARED_COMPONENTS_PATH	Enter the path where you installed the CA EEM components. **Default**: /opt/CA/SharedComponents
CA Directory Path	CADIR_PATH	Enter the path where you installed CA Directory. **Default**: /opt/CA/Directory **Note**: During installation, CA EEM creates an environmental variable %DXHOME% that points to the installation path.
Data DSA Port	DATA_DSA_PORT	Enter the port number that DSA uses to listen to requests. **Default**: 509
DB Size(in Mb)	DB_SIZE	Enter the maximum size of the datastore for CA EEM. **Default**: 256 MB
EiamAdmin Password	EIAMADMIN_PASSWORD	Enter the EiamAdmin password in clear text or munged format. The password must be of minimum five characters, and can contain special characters and digits.

Required Information	Response File Parameter	Comments
CA EEM Installation path	EIAM_PATH	Enter the path where you installed the CA EEM Server. **Default**: /opt/CA/SharedComponents/EmbeddedEntitlementManager
CA iTechnology iGateway Installation Path	IGW_PATH	Enter the path where you installed CA iTechnology iGateway. **Default**: /opt/CA/SharedComponents/iTechnology **Note**: During installation, CA EEM creates an environmental variable %IGW_LOC% that points to the installation path.
CA iTechnology iGateway Username	IGWUSER	Enter the user name used to install CA iTechnology iGateway. The user must have the permission to administer and manage CA iTechnology iGateway. **Default**: root
CA iTechnology iGateway User Group	IGWGROUP	Enter the group name of CA iTechnology iGateway user. **Default**: root
CA Directory Username	DXUSER	Enter the name of a non-dsa user who can manage CA Directory. The dxuser can be a local system user or a network user. **Default**: dsa **Note**: Do not use the local system user to run any other programs.
CA Directory User Group	DXGROUP	Enter the group name of the dxuser. **Default**: etrdir
Backup Directory Path	BACKUP_LOCATION	Enter the path where you want to store the backup files.

Note: During silent installation, you can prefix a parameter with -D and pass on the parameters through a command prompt. For example, -DEIAMADMIN_PASSWORD.

More information:

Install CA EEM Server Manually (see page 18)
Install CA EEM Server Silently (see page 18)

Install CA EEM Server Manually

You must use the CA EEM installer to manually install the CA EEM server. During the installation process, the installer prompts you for inputs. Before you perform the following procedure, verify that you have the CA EEM installer.

Follow these steps:

1. Execute the following command on the target server:

   `EEMServer_<version number>_<operating system>`

   The installer displays the license agreement.

2. Type **Y** and press Enter.

   The installation begins and the installer prompts you for inputs.

3. Enter inputs as prompted.

   A confirmation message with entered inputs is displayed.

4. Click **Y** to confirm the inputs.

   The CA EEM server is silently installed.

More information:

Installation Worksheet (see page 16)

Install CA EEM Server Silently

CA EEM provides you a response file that you must configure to silently install the CA EEM server. You can use the response file to perform identical silent installations on various servers.

To install a CA EEM server, perform the following steps:

1. Configure the response file.
2. Invoke the silent installation.

More information:

Installation Worksheet (see page 16)
Configure the Response File (see page 19)
Invoke Silent Installation (see page 19)

Configure the Response File

CA EEM creates a response file with default values. You can use the response file with the default values or edit the response file to silently install the CA EEM server.

Follow these steps:

1. Navigate to the location *EEMServer_home*\CA\SC\EmbeddedEntitlementManager.
2. Copy the response.properties file to the installation directory of target server.
3. (Optional) Edit the response.properties file, and save the changes.

   The response file is configured.

Example: Response file (UNIX)

```
INSTALLER_UI=SILENT
SHARED_COMPONENTS_PATH=/opt/CA/SharedComponents
EIAM_PATH=/opt/CA/SharedComponents/EmbeddedEntitlementManager
IGW_PATH=/opt/CA/SharedComponents/iTechnology
CADIR_PATH=/opt/CA/Directory
DATA_DSA_PORT=509
DB_SIZE=256
IGWUSER=root
IGWGROUP=sys
DXUSER=dsa
DXGROUP=etrdir
FIPS_ENABLED=true
EIAMADMIN_PASSWORD={munged}GBUHA01AXQFY
BACKUP_LOCATION=/opt/CA/SharedComponents/Backup
```

Invoke Silent Installation

Follow these steps:

1. Open the command prompt from the target server.
2. Execute the following command:

   ```
   ./EEMServer_<version number>_<operating
   system>[-f<path_to_installer_properties_file>]
   ```

Note: You can also use the command line parameters with the silent installation.

CA EEM Server Installation Structure

CA EEM has the following installation folder structure:

bin

Contains CA EEM tools and utilities that manage the CA EEM server.

lib

Contains CA EEM libraries that run CA EEM.

config

Contains CA EEM configuration files.

logging

Contains the following logger configuration files:

plugin.xml

Controls security event logging properties.

server.xml

Controls server logging properties.

java.xml

Controls server java logging properties.

server

Contains the following server configuration file:

server.xml

Stores server configuration settings.

uninstall

Contains scripts that uninstall the CA EEM server.

Verify Installation

To determine if the installation is successful, log on to the CA EEM admin GUI. Successful login to CA EEM indicates that the installation is successful.

Chapter 4: Post-Installation Configuration Tasks

This section contains the following topics:

User Access Permissions (see page 21)
CA EEM Server User Stores Configuration (see page 23)
Certificate Validation (see page 35)
FIPS 140-2 Support Configuration (see page 40)
Disaster Recovery Configuration (see page 48)
Failover Configuration (see page 56)
Certificates with Custom Key Length for CA EEM Server (see page 62)

User Access Permissions

CA EEM independently manages the access to an application. You can assign a user with different permissions to access different applications. To define user permissions, create a scoping policy for each application with required permissions. The following table specifies the available user permissions to manage CA EEM:

Task	Scoping Policy Resource	Scoping Policy Action
Attach to an application	ApplicationInstance	read
Add, Modify, or Delete an Application	ApplicationInstance	read, write
View AppObjects	AppObject	read
Add, Modify, or Delete an AppObject	AppObject	read, write
View an Application User	User, iPoz	read
Add, Modify, or Delete an Application User	User iPoz	read, write read
View a Global User	GlobalUser, iPoz	read
Add, Modify, or Delete Global User	GlobalUser iPoz	read, write read
View an Application Group	UserGroup, iPoz	read
Add, Modify, or Delete an Application Group	UserGroup iPoz	read, write read

Task	Scoping Policy Resource	Scoping Policy Action
View a Global Group	GlobalUserGroup, iPoz	read
Add, Modify, or Delete a Global Group	GlobalUserGroup iPoz	read, write read
View a Calendar	Calendar	read
Add, Modify, or Delete a Calendar	Calendar	read, write
View a Policy	Policy	read
Add, Modify, or Delete a Policy	Policy	read, write
View an Application Folder	Folder	read
Add, Modify, or Delete an Application Folder	Folder	read, write
View a Global Folder	GlobalFolder	read
Add, Modify, or Delete a Global Folder	GlobalFolder	read, write
View a Server Configuration	iPoz	read
Add, Modify, or Delete a Server Configuration	iPoz	read, write
Perform Certificate Validation	CertificateValidation	read

Note: By default, EiamAdmin has all the permissions to manage the CA EEM server.

CA EEM Server User Stores Configuration

You can control how CA Embedded Entitlements Manager refers to global users and global groups from *one* of the following options:

- Store data internally in CA Embedded Entitlements Manager
- Refer data from an external LDAP directory
- Refer data from a CA SiteMinder Policy Server

You can use the settings on this page to configure the global users and groups settings.

Store in internal datastore

Specifies that the global users and global groups data is stored in an internal datastore in CA Embedded Entitlements Manager. Using this configuration, you can perform the following tasks:

- Manage the global users and global groups
- Authenticate users
- Assign access permissions to CA Embedded Entitlements Manager application policies
- Manage user passwords
- Manage password policies

Reference from an External Directory

Specifies that the global users and global groups data is referenced from an external LDAP directory. Using this configuration, you can retrieve global users and global groups from an external LDAP directory to perform the following tasks:

- Authenticate users
- Assign access permissions to CA Embedded Entitlements Manager application policies

You cannot manage the global users and global groups, manage passwords, or password policies.

Reference from CA SiteMinder Policy Server

Specifies that the global users and global groups data is referenced from a CA SiteMinder Policy Server. Using this configuration, you can retrieve global users and global groups from a CA SiteMinder Policy Server to perform the following tasks:

- Authenticate users
- Assign access permissions to CA Embedded Entitlements Manager application policies

You cannot manage the global users and global groups, manage passwords, or password policies.

Note: If you change a configuration type in an existing directory configuration, the existing user application details are still stored in CA EEM. You must manually delete the details from CA EEM.

More information:

Configure CA EEM with Internal Datastore (see page 24)
Reference from an External LDAP Directory (see page 24)
How You Integrate SiteMinder with CA EEM (see page 32)

Configure CA EEM with Internal Datastore

CA EEM uses CA Directory to internally store the global users and global groups.

Follow these steps:

1. Log on to the CA EEM Server as an EiamAdmin using the Application <Global>.

   The CA EEM home page appears.
2. Select Configure, EEM Server, Global Users/Global Groups.

   The Global Users/Global Groups page appears.
3. Select Store in internal datastore, and click Save.

   CA EEM is configured with internal datastore.

Reference from an External LDAP Directory

You can reference to a global user or global group from an external LDAP directory.

You can perform the following tasks on the Directory Information pane:

- Add an external LDAP directory
- Update an external LDAP directory
- Delete an external LDAP directory

Support for Multiple Active Directory Domains

CA EEM now supports the following LDAP directories configurations:

Basic LDAP directory

Specifies that CA EEM resolves the global users and global groups within a specified LDAP directory.

Multiple Microsoft Active Directory Domains

Specifies that CA EEM resolves the global users and global groups across the configured Active Directory domains or forest. CA EEM supports the following Active Directory configurations:

Active Directory Domain

Specifies that CA EEM resolves domain-qualified global users and global groups across the individually configured domains.

Active Directory Forest

Specified that CA EEM resolves domain-qualified global users and global groups across all the domains within the configured forest.

In a multiple Active Directory domain, verify that you do the following tasks:

- When authenticating and authorizing a user, use a user principal name in the following format:

  `domain\username`

- When defining access policies, use the principal name of a global user or global group to assign permissions, and use PrincipalName attribute to define filters.

You can configure an Active Directory Domain by performing the following steps:

1. Select Multiple Microsoft Active Directory from Configuration Type.
2. Click Add external LDAP directory.
3. Enter the external LDAP directory details in the LDAP Directory Configuration page.

You can configure an Active Directory Domain by performing the following steps:

1. Select Microsoft Active Directory Forest from Configuration Type.
2. Click Add external LDAP directory.
3. Enter the external LDAP directory details in the LDAP Directory Configuration page.

Add an External LDAP Directory

You can configure CA EEM to refer from a new external LDAP directory.

Follow these steps:

1. Select Reference from an external LDAP Directory from the Global Users/Global Groups pane of the Userstore Configuration page.

   The Directory Information pane appears on the Userstore Configuration page. By default, Basic LDAP Directory is selected as the Configuration Type.

2. Select a Configuration Type, and click Add external LDAP directory from the Directory Information pane.

   The LDAP Directory Configuration page appears.

3. Complete the following fields:

   General

   The following appear under the general section:

   Name

   Specifies a name for the external LDAP directory.

   Attribute Map

   Specifies the set of rules that define how the attributes of the external LDAP directory are mapped to the CA EEM domain. This field appears only if you have selected the Type as Custom Mapped Directory.

   Domain Settings

   The Domain Settings section appears only if you chose to configure an Active Directory domain or forest. The following appear under the domain settings section:

   Domain

   Specifies the name of the domain in the Active Directory Domain or Active Directory Forest.

   Base DN

   Specifies the Base DN of the domain within a forest. This field appears only if you chose to configure an Active Directory forest.

   If you chose to configure an Active Directory Forest, you can add more domains by clicking Add Domain Mapping and delete a domain by clicking the delete icon of the domain.

   Connection Settings

   The following appear under the connection settings section:

   Host and Port

Specifies a hostname of the external LDAP directory, and an LDAP port for CA EEM to communicate with the external LDAP directory host. When you enter a hostname and port, click the arrow to add the entered details into Selected Hostnames. You can specify multiple host configurations, which can act as failover servers. When you specify multiple host configurations, you can use the up and down arrows in Selected Hostnames to arrange the order of failover servers.

Protocol

Specifies an LDAP protocol that is used to connect to the external LDAP directory. Select *one* of the following protocols:

LDAP

Specifies an LDAP connection over an unsecured connection.

LDAP + TLS

Specifies an LDAP connection over Transport Layer Security (TLS).

LDAPS

Specifies an LDAP connection over Secure Sockets Layer.

Base DN

Specifies the Distinguished Name of the external LDAP directory from where the search for global users and global groups begins. Only global users and global groups that are discovered underneath this DN are mapped into CA EEM. Enter a value without spaces.

User DN

Specifies the Distinguished Name of a user to connect to the external LDAP directory. Do not enter a comma in the cn of the User DN. For example, if your User DN is cn=firstname,middlename,dc=foo,dc=com, prefix the comma with a backslash to make the User DN as cn=firstname\,middlename,dc=foo,dc=com.

Password and Confirm Password

Specifies the password that is associated with the user in User DN.

The following fields appear on selecting LDAP + TLS or LDAPS as the protocol.

Certificate Path

Type the relative location of the certificate file that is placed in the CA EEM installation folder.

Key Path

Type the relative location of the certificate key file that is placed in the CA EEM installation folder.

CA Certificate Path

Type the relative location of the certificate file that was obtained from the CA and placed in the CA EEM installation folder.

Advanced Configuration

The following appear under the advanced configuration section:

Follow LDAP Referrals

Specifies that CA EEM must follow LDAP referrals. If you enable this option and search for an object that does not exist in the LDAP directory, the LDAP server provides a reference to a location that might hold the object.

Max Bind Connections

Specifies the maximum number of concurrent LDAP connections that CA EEM supports for authenticating users.

Max search connections

Specifies the maximum number of concurrent LDAP connections that CA EEM supports for search operations.

Connection Timeout

Specifies the maximum time in seconds the CA EEM Server waits to connect to the LDAP server.

Request Timeout

Specifies the maximum time in seconds the CA EEM Server waits for the LDAP server to respond to requests.

Search Retry Count

Specifies the number of times the CA EEM Server tries to reconnect to the LDAP directory after a failed search operation.

4. Click Save.

   The external LDAP directory is added.

Update an External LDAP Directory

You can update a configured external LDAP directory.

Follow these steps:

1. Select Reference from an external LDAP Directory from Global Users/Global Groups pane of the Userstore Configuration page.

   The Directory Information pane appears on the Userstore Configuration page.

2. Select a Configuration Type.

   The configured external LDAP directories are displayed in a table.

3. Click the name of the external LDAP directory you want to edit from the Name column of the table.

   The LDAP Directory Configuration page appears.

4. Make the necessary changes, and click Save.

   The external LDAP directory is updated.

Delete an External LDAP Directory

You can delete a configured external LDAP directory.

Follow these steps:

1. Select Reference from an external LDAP Directory from Global Users/Global Groups pane of the Userstore Configuration page.

   The Directory Information pane appears on the Userstore Configuration page. By default, Basic LDAP Directory is selected as the Configuration Type.

2. Select a Configuration Type.

   The configured external LDAP directories are displayed in a table.

3. Click the delete icon of the external LDAP directory you want to delete from the Remove column of the table.

   The delete confirmation dialog appears.

4. Click OK.

   The external LDAP directory is deleted.

Custom Mapped Directory

You can use custom mapped directory configuration to map external LDAP directory attributes to CA EEM attributes. This configuration lets you work with CA EEM attributes without having knowledge about the underlying LDAP attribute definitions.

Custom mapped directory configuration lets you do the following tasks:

- Customize user authentication
- Retrieve user attribute and user group membership resolution
- Define customer attributes mapping for users and user groups

You can use the settings on this page to configure a custom mapped directory.

Mapping Name

Specifies a name for the mapping label to connect to an external LDAP directory.

The following appear in the LDAP Attribute Mapping page:

Save

Saves the configuration.

Save As

Saves the configuration with a different name.

Delete

Deletes the selected label.

The following fields appear in the User Attribute Mapping panel:

User Search Filter

Specifies a search filter used to search for a user in the external LDAP directory.

User Authentication Filter

Specifies a user search filter that controls how an external LDAP directory resolves usernames to LDAP DN. The search filter consists of prefilter and postfilter components. For example, if you specified the prefilter as “(cn=“ and the postfilter as “)” during user authentication, CA EEM performs an LDAP search with the search filter "(cn=loginname)”

User Attribute Mapping

Allows you to map the external LDAP directory user attributes to CA EEM user attributes. You must specify the User Name attribute, which uniquely identifies the users in CA EEM. You can add a user attribute by clicking Add attribute, and enter the user attribute details in the last row of the table. You can delete a user attribute by clicking the delete icon of the user attribute.

The following fields appear in the Group Attribute Mapping panel:

Group Search Filter

Specifies an LDAP group search filter used for user group resolution.

Group Naming Attribute

Specifies an LDAP attribute that uniquely identifies groups.

Group Member Attribute

Specifies an LDAP group attribute in the LDAP group entry. For example, “member” attribute in Active Directory group or “uniqueMember” attribute in SunONE Directory group.

How You Integrate SiteMinder with CA EEM

To integrate SiteMinder with CA EEM, perform the following in SiteMinder Administrator:

- Create an agent in SiteMinder for communication between CA EEM and SiteMinder policy server. Ensure the agent supports 4.x agents.
- Create an administrator or use the existing default administrator "SiteMinder" with system level scope.
- Create a SiteMinder User Directory for authorization, which is used by CA EEM to retrieve LDAP attributes.
- Set the UniversalID field to uniquely identifies a user in the directory such as sAMAccountName or UID. You can set the UniversalID from the SiteMinder UI, User Directories, Properties, User attributes tab.
- Set the Password Attribute (RW) on the User Attribute tab to userPassword.
- Create a SiteMinder data store for authentication, which is used by CA EEM to authenticate users.

  Note: If the authentication and authorization user store is same, use the existing user store created for authorization.
- Create a Realm with the Resource Filter as “/iamt.html”.
- Create a SiteMinder domain and add the User Directories, administrator, and Realm to the domain.

For more information about SiteMinder, see the SiteMinder documentation.

SiteMinder Configuration Parameters

SiteMinder consists of two components, policy server and web agents.

Policy server

Policy server provides policy management, authentication, authorization and accounting.

Web agents

Web agents assist SiteMinder to access to Web applications and content according to defined security policies.

To enable the protocol between the agent and server, the agent must have a unique name and a shared secret key along with information to define a connection between the client application and the policy server.

For information on parameters to define between the client application and the policy server, see *Online Help*.

How Single Sign-on Works between SiteMinder and CA EEM

If you use an application that has an existing SiteMinder session to access an CA EEM enabled application, CA EEM recognizes the SiteMinder session ticket and creates an CA EEM session without re-authentication.

The following is the basic flow of events for application created using CA EEM with SiteMinder integration:

Example: Protecting a web application using SiteMinder

A web application using CA EEM with web server pages protected by SiteMinder is considered.

1. A user accesses a web application.
2. SiteMinder prompts for user authentication and the user submits credentials and is authenticated.
3. The user tries to access the original web application created using CA EEM.
4. Servlet code accesses the HTTPServletRequest context and sends the SiteMinder session token to the CA EEM using authenticateWithArtifact.
5. CA EEM Server validates the SiteMinder session against the SiteMinder Policy Server.
6. An CA EEM session is created and the user identity is loaded, if validation succeeds.

How Authentication Works Using SiteMinder Authentication Schemes

The following process describes how authentication is performed using SiteMinder APIs:

- A user calls the authenticateWithPassword method by providing the username and password.
- CA EEM sends this information to the CA EEM Server.
- Based on the information, the authentication is performed by calling the SiteMinder APIs.
- The group and user information is loaded for the authenticated user.

Note: When CA EEM is connected to a SiteMinder user directory, the search calls use the SiteMinder APIs instead of the CA EEM search calls.

Reference from SiteMinder

You can reference to a global user or global group from a CA SiteMinder Policy Server.

The CA SiteMinder Configuration page contains the following fields:

Name

Specifies a name for the CA SiteMinder Policy Server.

Type

Specifies a type for the LDAP directory configured in CA SiteMinder Policy Server.

Attribute Map

Specifies the set of rules that define how the attributes of the CA SiteMinder Policy Server are mapped to CA EEM. This field appears only if you have selected the Type as Custom Mapped Directory.

Host

Specifies a hostname of the computer where CA SiteMinder Policy Server is installed.

Authentication Directory

Specifies the name of the user authentication directory configured in CA SiteMinder.

Authorization Directory

Specifies the name of the user authorization directory configured in CA SiteMinder.

Admin name

Specifies the name of CA SiteMinder Administrator who has privileges to manage system and domain objects.

Admin Password and Confirm Password

Specifies the password associated with the Administrator.

Agent name

Specifies the agent name mentioned in the CA SiteMinder Policy Server.

Agent Secret and Confirm Secret

Specifies the shared secret specified in the CA SiteMinder user interface.

Note: Agent Secret is case-sensitive.

Authorization Port

Specifies the authorization port used by CA SiteMinder.

Authentication Port

Specifies the authentication port used by CA SiteMinder.

Accounting Port

Defines the accounting port used by CA SiteMinder.

Search Time Out

Specifies the maximum time in seconds the CA EEM Server waits for CA SiteMinder to respond to requests.

Minimum Connections

Specifies the minimum number of concurrent LDAP connections that CA EEM supports for CA SiteMinder Policy Server.

Max Connection

Specifies the maximum number of concurrent connections that CA EEM supports for CA SiteMinder Policy Server.

Certificate Validation

After the embedding application has verified that the caller has the private key corresponding to the public key of the certificate, you can use CA EEM to perform the following steps:

1. Validate a certificate against trusted Certification Authorities (CAs)
2. Validate the revocation status of the certificate using the following revocation mechanisms:
   - Certificate Revocation List (CRL)
   - CRL Distribution Point (CRLDP)
   - Online Certificate Status Protocol (OCSP)

Prerequisites

Before you validate a certificate, perform the following steps:

- Create a jks file that contains a list of trusted CA.
- If you want to use a subordinate CA, add the entire CA hierarchy to the keystore.
- Verify that all the CA certificates including the intermediate CAs are trusted.
- Store the jks file in the relative path from the CA EEM installation directory.
- Configure server.xml with the location and password of the jks file.

How to Validate a Certificate

You can validate a certificate by performing the following steps:

1. Log on to CA EEM.
2. Click Configure, EEM Server, Certificate Validation.
3. The Certification Validation pane appears on the right pane.
4. Select Enable Certificate Validation.

   The certificate validation configuration panes appear.
5. Configure CA EEM with a trusted CA.
6. Select a revocation mechanism.
7. Select a user mapping attribute you want to extract from the certificate.
8. (Optional) Map the keystore with an external LDAP directory.
9. Invoke the ValidateUserCertificate API. For information about invoking the ValidateUserCertificate API, see the Programming Guide.

More information:

Configure CA EEM with a Trusted CA (see page 37)
Select a Revocation Mechanism (see page 38)
Extract a User Mapping Attribute (see page 39)
Map a Certificate with a User (see page 40)

Configure CA EEM with a Trusted CA

Map CA EEM with a keystore for CA EEM to search for the certificates in the keystore.

Follow these steps:

1. Log on to CA EEM.
2. Click Configure, EEM Server, Certificate Validation.

   The Certification Validation section appears on the right pane.
3. Select Enable Certificate Validation.

   The certificate validation configuration sections appear.
4. Navigate to the Trusted Keystore section.
5. Type the relative location of the jks file from the CA EEM Installation Directory in Keystore file location.
6. Type the jks file password in Keystore Password and Confirm Keystore Password.
7. Click Save.

   CA EEM is configured with the trusted CA.

Select a Revocation Mechanism

You can select one or more revocation mechanisms. If you enable all three mechanisms, CA EEM validates the certificates in the following order of priority:

- Online Certificate Status Protocol (OCSP)
- CRL Distribution Point (CRLDP)
- Certificate Revocation List (CRL)

CA EEM proceeds to validate a certificate with the next mechanism only if the validation with the previous mechanism fails.

Follow these steps:

1. Log on to CA EEM.
2. Click Configure, EEM Server, Certificate Validation.

   The Certification Validation section appears on the right pane.
3. Select Enable Certificate Validation.

   The certificate validation configuration sections appear.
4. Navigate to the Revocation Mechanism section.
5. Click Enable OCSP.

   CA EEM displays the OCSP Server, Verify OCSP Response, and Certificate Alias Name fields.
6. Type the URL of the OCSP Server.
7. (Optional) If you want to verify the OCSP response, select Verify OCSP Response.
8. Type the alias name of the certificate as configured in the keystore in OCSP Responder Certificate.
9. Select Enable CRLDP.
10. Select Enable CRL files.

    CA EEM displays the CRL Folder Location and CRL File Update Interval fields.
11. Type the CRL Folder Location.
12. Type the time period in seconds CA EEM waits to verify the certificate for updates in the folder in CRL file update interval.
13. Click Save.

    The revocation mechanisms are selected.

Extract a User Mapping Attribute

CA EEM extracts a user mapping attribute after validating a certificate. You can use the extracted user mapping attribute to map the certificate with a user from the configured external LDAP directory.

Follow these steps:

1. Log on to CA EEM.
2. Click Configure, EEM Server, Certificate Validation.

   The Certification Validation section appears on the right pane.
3. Select Enable Certificate Validation.

   The certificate validation configuration sections appear.
4. Navigate to the Username Extraction section.
5. Select a field from User mapping field.
6. Type a regular expression pattern that CA EEM must use to extract the user mapping attribute from the certificate.
7. Click Save.

   The user mapping attribute is extracted.

Example 1: Extract User DN from the Certificate Subject

If you want to extract the user DN cn=user, ou=org, o=com from a certificate, perform the following steps:

1. Select subject from User mapping.
2. Type the following regular expression:

   ```
   (.*)
   ```
3. Click Save.

Example 2: Extract User Attribute from the Certificate Subject

If you want to extract cn of the User DN cn=user, ou=org, o=com from a certificate, perform the following steps:

1. Select subject from User mapping.
2. Type the following regular expression:

   ```
   cn=(.*), ou.*
   ```
3. Click Save.

Map a Certificate with a User

If you have configured a custom mapping for an external LDAP directory, you can use the extracted user mapping attribute to map the certificate with a user from the external LDAP directory.

Follow these steps:

1. Log on to CA EEM.
2. Click Configure, EEM Server, Certificate Validation.

   The Certification Validation section appears on the right pane.
3. Select Enable Certificate Validation.

   The certificate validation configuration sections appear.
4. Navigate to the LDAP Mapping section.
5. Select Perform LDAP lookup to resolve users.
6. Select the LDAP user store.
7. Select one of the following mapping options:

   User certificate DN as LDAP DN

   Specifies that CA EEM uses the DN of the certificate to retrieve user details from the LDAP directory.

   Use LDAP Attribute

   Specifies that CA EEM searches the LDAP directory with the following search format:

   `(LDAP Attribute Name)=(Extracted User Mapping Attribute)`

   Use LDAP search expression

   Specifies that CA EEM searches the LDAP directory with the following search format:

   `(`*`prefilter of search criteria`*`)(`*`Extracted User Mapping Attribute`*`)(`*`postfilter of search criteria`*`)`
8. Click Save.

   The certificate is mapped with a user.

FIPS 140-2 Support Configuration

CA EEM can operate in a non-FIPS mode or in a FIPS-only mode. The cryptographic boundaries, that is, the way CA EEM applies encryption, are the same in both modes, but the algorithms are different.

FIPS 140-2 Overview

The Federal Information Processing Standards (FIPS) 140-2 publication specifies the requirements for using cryptographic algorithms within a security system protecting sensitive, unclassified data. CA EEM Server embeds Crypto-C ME v2.0 cryptographic library from RSA, which has been validated as meeting the FIPS 140-2 *Security Requirements for Cryptographic Modules.* The validation certificate number for this module is 608.

CA EEM Java SDK uses a FIPS-compliant version of the BSAFE Crypto-J 4.0 cryptographic library from RSA. CA EEM C++ SDK embeds ETPKI 4.1.x, which uses RSA cryptography libraries.

Computer products that use FIPS 140-2 accredited cryptographic modules in their FIPS-accredited mode can only use FIPS approved security functions such as AES (Advanced Encryption Algorithm), SHA-1 (Secure Hash Algorithm), and higher level protocols such as TLS v1.0 as explicitly allowed in the FIPS 140-2 standard and implementation guides.

In FIPS-only mode, CA EEM uses the following algorithms:

- SHA1, SHA256, SHA384—For managing client-server communication.
- SHA512—For storing user passwords.

  Note: CA EEM applies SHA512 to the password digest only if you update the password digest. Until you update, CA EEM accepts the existing password in the password digest.
- SHA256—For managing application certificates.
- TLS v1.0—For communication with external LDAP directories if the LDAP connection is over TLS.

Supported Security Modes in CA EEM

CA EEM supports the following modes of operation.

non-FIPS

This mode uses non-FIPS compliant techniques for cryptography. In this mode MD5 is the default algorithm that is used to encrypt and decrypt sensitive data. The CA EEM installer always install the CA EEM Server in a non-FIPS mode. In this mode, the CA EEM Server is backward compatible with the CA EEM clients. For example, you can use the CA EEM r8.4 SDK to connect to a CA EEM r8.4 SP3 Server.

FIPS-only

This mode uses only FIPS-compliant techniques for cryptography. This mode is not compatible with clients running in non-FIPS mode. You must use only CA EEM r8.4 SP3 SDK FIPS-only clients with CA EEM r8.4 SP3 Servers or later running in FIPS-only mode. In this mode, the CA EEM Server supports the following algorithms to encrypt and decrypt data:

- SHA1
- SHA256
- SHA384
- SHA512
- TLS v1.0 for communication with external LDAP directories if the LDAP connection is over TLS.

Note: SHA1 is the default algorithm.

Configuring CA EEM Server in FIPS-only Mode

To configure the CA EEM Server in FIPS-only mode, do the following:

1. Verify prerequisites for configuring CA EEM Server in FIPS-only mode
2. Configure CA EEM Server in FIPS-only mode

Prerequisites for Configuring CA EEM Server in FIPS-only Mode

Review the following prerequisites before configuring the CA EEM Server in FIPS-only mode:

☐ Verify the minimum operating system and hardware requirements needed for the FIPS-only mode.

- ☐ Verify that the other CA products using iGateway such as CA ITM, CA ELM, and so on, are in FIPS-only mode. iGateway cannot be initialized both in FIPS-only mode and non-FIPS mode. When iGateway is initialized in FIPS-only mode, all products using iGateway must be in FIPS-only mode. Open the iGateway.conf file and verify the value for the following tag:

  `FIPSMode`

  If the value of this tag is set to False, it means that product using iGateway is in non-FIPS mode. Based on the existing configuration of iGateway decide appropriately if you want to enable CA EEM in FIPS-only mode.

- ☐ Upgrade your CA EEM Sever.

- ☐ Verify if the communication channel between the CA EEM Server and the external LDAP directory is encrypted.

Before Configuring CA EEM in FIPS-only Mode

Verify that your environment meets the minimum requirements before migrating the environment to use FIPS-only mode. Print the following to use as a checklist:

- ☐ Upgrade your CA EEM Sever to CA EEM r8.4 SP3 or later versions.

- ☐ Verify that the products that are integrated or connected with CA EEM are configured to use FIPS-only mode.

Configure CA EEM Server in FIPS-only Mode

When you configure the CA EEM Server in FIPS-only mode, CA EEM uses only FIPS 140-2 compliant cryptographic libraries to encrypt and decrypt sensitive data.

Note: The following procedure is also valid for changing the security mode of the CA EEM Server from FIPS-only to non-FIPS or non-FIPS to FIPS -only.

To configure the CA EEM Server in FIPS-only mode

1. Stop the iGateway service.
2. Open the iGateway.conf file and set the following tag to ON:

   `<FIPSMode>ON<FIPSMode>`

   Note: To change the mode from FIPS-only to non-FIPS, set FIPSMode tag to OFF.
3. Start the iGateway service.

   The CA EEM server is configured in a FIPS-only mode.

Verify CA EEM Server is in FIPS-only Mode

In FIPS-only mode, use IE7 (or above) or Firefox 3.0 (or above) to view the CA EEM admin GUI.

Note: For more information about how to configure Firefox in FIPS 140-2 mode, see the Firefox support site.

To verify that the CA EEM Server is in FIPS-only mode

1. Enter the following URL in your browser:

   `https://`*`hostname`* `or IP` *`address`*`:5250/spin/eiam/about.csp`

   The CA EEM Server About page opens.

2. Verify if the FIPS: label is set to Enabled.

   If the label is set to Enabled, it indicates that the CA EEM Server is in FIPS-only mode.

Configure the CA EEM to use Server certificates in a PKCS#11 Device

To use nCipher PKCS#11 devices with the CA EEM Server or the CA EEM SDK, configure the nCipher device and set the following property is set as follows:

```
CKNFAST_OVERRIDE_SECURITY_ASSURANCES=all
```

Note: For more information about how to configure the nCipher device with a hard token, see the nCipher documentation.

To configure the CA EEM Server to use certificates stored in a PKCS#11 devices, do the following:

1. Stop the iGateway service.
2. Open the iGateway.conf file and edit the <Connector name="defaultport"> CA Portal5250</port> tags to set the following values:

   certType

   Defines the type of certificate to be used. Supported certificate types are p12, pem, and p11.

   Default: pem

   Type: Childnode

Using P11 certificate

<pkcs11Lib/>—Path to PKCS11 library provided by token

<token/>—Token id

<userpin/>—Munged user pin

<id/>—Certificate and private key id

<sensitive/>—Private key is sensitive. Sensitive keys are not converted as software keys and crypto operation are performed using the cryptopki hardware (nonsensitive key can be treated as sensitive, but sensitive keys cannot be converted or treated as nonsensitive key)

Default: False

3. Save and close the iGateway.conf file.
4. Start the iGateway services.

Configure the CA EEM to Store Server Certificates in a PKCS#11 Device

To store the CA EEM certificates in a PKCS#11 device, do the following:

1. Stop the iGateway service.
2. Open the iGateway.conf file and edit the <CertificateManager> tags to set the following values:

   certType

   Defines the type of certificate to be used. Supported certificate types are p12, pem, and p11.

   Default: pem

   Type: Childnode

   Using P11 certificate

   <pkcs11Lib><pkcs11Lib/>—Path to PKCS11 library provided by token

   <token><token/>—Token id

   <userpin><userpin/>—Munged user pin

   <id><id/>—Certificate and private key id

   <sensitive><sensitive/>—Private key is sensitive. Sensitive keys are not converted as software keys and cryptographic operation are performed using the cryptoki hardware (nonsensitive key can also be treated as sensitive but sensitive keys cannot be converted/treated as nonsensitive key) – optional defaults to false
3. Save and close the iGateway.conf file.
4. Start the iGateway services.

Configure Your Application in FIPS-only Mode

To configure your application in FIPS-only mode, verify that the CA EEM SDK is in FIPS-only mode, CA EEM SDK uses only FIPS-compliant techniques for cryptography. The CA EEM SDK configuration file, eiam.config controls the secure mode of operation of the CA EEM SDK. Before configuring the CA EEM SDK in FIPS-only mode, verify the following:

- Verify that your CA EEM SDK is at version r8.4 SP3 or later.
- Migrate any existing P12 certificates used by CA EEM to PEM certificates.
- Initialize the CA EEM SDK in FIPS-only mode.

Migrate P12 certificates used by Your Application to PEM certificates.

CA EEM supports P12, PEM, and PKCS#11 certificates with the following considerations:

- P12 support is disabled (not available) under FIPS-only mode. As an alternative, in FIPS-only mode, PEM and PKCS#11 certificate support has been added.

Note: CA EEM C# SDK supports only PEM certificates in FIPS-only mode, P12 and PEM certificates in non-FIPS mode.

So, if you are using any P12 certificates, migrate these certificates to one of the supported certificate formats in the FIPS-only mode. Use the igwCertUtil utility to convert P12 certificates to pem certificates. The igwCertUtil is a utility to convert, create, or delete certificates. The igwCertUtil is located in the following folder:

Windows

%IGW_LOC%

UNIX and LINUX

$IGW_LOC

igwcertutil Utility—Create, Copy, Convert, and Delete Certificates

Valid on Windows, UNIX, and Linux

The create command has the following format:

```
igwCertUtil -version version -create -cert inputcert-params -issuer issuercert
-params [-debug] [-silent]
```

The convert command has the following format:

```
igwCertUtil -version version -conv -cert inputcert-params -target newcert-params
[-debug] [-silent]
```

The copy command has the following format:

```
igwCertUtil -version version -copy -cert inputcert-params -target newcert-params
[-debug] [-silent]
```

The delete command has the following format:

```
igwCertUtil -version version -delete -cert cert-params [-debug] [-silent]
```

-version *version*

Specifies the version of igwCertUtil used when creating, converting, copying, or deleting certificates. Version is used for backward compatibility. If igwCertUtil is modified, the version tag gets the old behavior.

-cert *inputcert*-parms

Specifies the certificate as an XML string when creating, converting, or copying certificates.

-issuer *issuercert*-parms

Specifies the certificate that is used to sign the newly generated certificate when creating a certificate. If no certificate is specified, a self-signed certificate is created.

-target *newcert*-parms

Specifies the configuration for the new certificate when converting (or copying) an existing certificate.

-cert *cert*-parms

-debug

(Optional) Turns on debugging for igwCertUtil.

-silent

(Optional) Turns on silent mode for igwCertUtil.

The following error codes are returned by igwCertUtil:

- CERTUTIL_ERROR_UNKNOWN (-1): unknown or undefined error happened
- CERTUTIL_SUCCESS (0): successful operation
- CERTUTIL_ERROR_USAGE (1): wrong command line arguments passed
- CERTUTIL_ERROR_READCERT (2): unable to read certificate
- CERTUTIL_ERROR_WRITECERT (3): unable to write certificate
- CERTUTIL_ERROR_DELETECERT (4): unable to delete certificate

Example: Convert P12 certificates to PEM certificates

The following example describes usage of converting a P12 certificate to a PEM certificate:

```
igwCertUtil -version 4.6.0.0 -conv  -cert
"<Certificate><certType>p12</certType><certURI>testCert.p12</certURI><certPW>pass
word</certPW></Certificate>" -target "<Certificate><certType>pem</certType>
<certURI>testCert.cer</certURI><keyURI>testCert.key</keyURI></Certificate>"
```

Example: Convert P12 Certificates to PKCS#11 certificate:

```
igwCertUtil -version 4.6.0.0 -conv  -cert
"<Certificate><certType>p12</certType><certURI>testCert.p12</certURI><certPW>pass
word</certPW></Certificate>" -target "<Certificate><certType>p11</certTyp
><pkcs11Lib>pathto-pkcs11Lib</pkcs11Lib><token>pkcs11token</token><userpin>user
in</userpin><id>certid</id></Certificate>"
```

Initialize the CA EEM SDK in FIPS-only Mode

The CA EEM SDK can be initialized in the FIPS-only mode by configuring the eiam.config file. To configure the eiam.config file, see the chapter, Configuring CA EEM SDK.

Disaster Recovery Configuration

Backing up the following CA EEM data ensures that you can restore CA EEM Server installations if they are corrupted:

- Configuration files and folders
- CA EEM data stored in the internal datastore

Overview

Backing up the following CA EEM data ensures that you can restore CA EEM Server installations if they are corrupted:

- Configuration files and folders
- CA EEM data stored in the internal datastore

File System Back Up

We recommend that you back up CA EEM servers regularly or whenever you have administered a change in the CA EEM servers environments. You can use the CA EEM server backups to restore your CA EEM server if it is corrupted.

You must back up the following CA EEM files and folders:

- CA iTechnology iGateway
- CA EEM
- CA Directory

Restore Procedures

You must restore your CA EEM data so that you can:

- Recover a CA EEM installation that is corrupted
- Recover a CA EEM server environment that is not working as desired

To recover CA EEM configuration files and data

1. Stop iGateway.
2. Rename all the backed up CA EEM .conf files to .conf.merge, and copy the renamed configuration files to the iTechnology folder. The .conf.merge files are required to merge the backed up configuration files with the new configuration files.
3. Restore CA EEM data.
4. Start iGateway.

Stop iGateway Service

Do the following commands to stop iGateway service:

Windows

1. Click Start, Run, and enter the following command:

   `services.msc`

   The Services panel appears.
2. Select CA iTechnology iGateway 4.7 service in the right pane of the Services panel, right-click, and select Stop.

   The iGateway service is stopped.

Linux and UNIX

$IGW_LOC/S99igateway stop

Start iGateway Service

Do the following commands to start iGateway service:

Windows

1. Click Start, Run, and enter the following command:

   ```
   services.msc
   ```

   The Services panel appears.

2. Select CA iTechnology iGateway 4.7 service in the right pane of the Services panel, right-click, and select Start.

   The iGateway service is started.

Linux and UNIX

```
$IGW_LOC/S99igateway start
```

Back up and Restore CA EEM Data

The CA EEM Server uses CA Directory as an internal data store to store the following data:

- Global users
- Global user groups
- Application users
- Application user groups
- Application policies

Note: If you have connected the CA EEM Server to an external LDAP directory, the global users are not stored in the internal data store.

The CA EEM Server data is stored in a directory namespace with the following DSA name:

```
itechpoz
```

Where, DSA is a process that manages the internal data store's namespace. The itechpoz DSA manages the CA EEM Server data.

The backup process involves dumping the data from this DSA to an LDIF file. And, the restore process involves loading the backed up LDIF file into the DSA.

Back Up CA EEM Data

Use one of the following procedures to back up CA EEM data:

- Create an online dump of the datastore and convert the dump to an LDIF file.
- Create an offline dump of the datastore.

Create a Backup from an Online Dump

You can take a consistent snapshot copy of the datastore of a running DSA (an online dump). The DSA completes any updates before carrying out the online dump and does not start any more updates until the copy is finished.

Note: Each dump overwrites the previous dump. If you want to save the online dump, copy it to another location before the next dump.

You can create a backup of an online dump using the following process:

1. Generate an online dump from the dsa console port on demand (see page 51).

   Or

   Schedule an online dump.

2. Convert the online dump to an LDIF file (see page 54).

Generate an Online Dump from the DSA Console

To generate the online dump from the DSA console, you must do the following:

1. Set a local DSA console port.
2. Connect to a local DSA and dump the data store.

Set Local DSA Console Port

To set the local DSA console port

1. Stop the local DSA services using the following commands:

   Windows

   ```
   dxserver stop dsaname
   ```

   Linux and UNIX

   ```
   su - dsa -c "dxserver stop dsaname"
   ```

2. Open the itechpoz.dxc configuration file and add the local console port entry immediately after the snmp-port entry:

   ```
   console-port = 10510
   ```

   Note: The configuration file is located in the following folders:

   Windows

   ```
   %DXHOME%\config\knowledge\itechpoz.dxc
   ```

   Linux and UNIX

   ```
   $DXHOME/config/knowledge/itechpoz.dxc
   ```

3. Save the itechpoz.dxc configuration file.

4. Start the local DSA services using the following commands:

   Windows

   ```
   dxserver start dsaname
   ```

   Linux and UNIX

   ```
   su - dsa -c "dxserver start dsaname"
   ```

Connect to a Local DSA Console and Dump the Data Store

To connect to a local DSA Console

1. Open a command prompt on the host on which the DSA is running.

2. Enter the following command:

   ```
   telnet localhost local-port-number
   ```

   local-port-number

   Specifies the console port number of the DSA to which you want to connect.

3. Enter the following command:

   ```
   dump dxgrid-db;
   ```

   An online dump *itechpoz.zdb* is created in the %DXHOME%\Data folder for Windows and $DXHOME/Data folder for UNIX platforms.

   Note: The online dump process is finished only when the .ZDB file size is equal to your data store (*.db) size.

Schedule an Online Dump

You can schedule the CA EEM Server to generate an online dump at a specifc time or to create the online dump at regular intervals.

Note: Each dump overwrites the previous backup file. Create a cron job on UNIX or a scheduled task on Windows to copy the backed up file to a safe location before the next dump.

To schedule an online dump

1. Stop the local DSA services using the following commands:

   Windows

   `dxserver stop dsaname`

   Linux and UNIX

   `su - dsa -c "dxserver stop dsaname"`

2. Open the itechpoz.dxc configuration file and add the following lines:

   `dump dxgrid-db period <start> <period>`

   where

   period *start period*

   (Optional) Specifies that the online dump is performed at regular intervals.

   start

   Defines the number of seconds from Sunday 00:00:00 a.m. GMT.

   Note: The start time is defined using GMT and not your local time.

   period

   Defines the number of seconds between online dumps.

   Note: The start time is relative to the period and should be lower than it. If you specify a start time that is greater than the period, the actual start is *start* - *period*. For example, if the *period* is 3600 seconds (one hour) and *start* is 3610 seconds, the online dump starts 10 seconds from midnight GMT and continues every hour from then on.

3. Save the itechpoz.dxc file.

4. Start the local DSA services using the following commands:

   Windows

   `dxserver start dsaname`

   Linux and UNIX

   `su - dsa -c "dxserver start dsaname"`

Example: Perform an Online Dump Every Hour

The following command takes a snapshot copy of the datastore every hour:

```
dump dxgrid-db period 0 3600
```

Example: Perform an Online Dump Every Night

The following command takes a snapshot copy of the datastore every night at 3 a.m. in a GMT+10:00 time zone:

```
dump dxgrid-db period 61200 86400
```

In this example, the start time is the number of seconds from Sunday midnight GMT to the first 3 a.m. slot, corrected by the time zone value, as follows:

```
(3 am – 10 time zone + 24 hours) * 60 minutes * 60 seconds = 61,200
```

The 24 hour period is calculated as follows:

```
24 hours * 60 minutes * 60 seconds = 86,400
```

Convert the Online Dump to an LDIF File

To create a backup of the data store from an online dump, you must convert the .ZDB files to an LDIF file.

To back up a directory to an LDIF file

1. Log in as the user dsa (on UNIX) or the administrator (on Windows).
2. Use the following command to back up the datastore to the LDIF file:

   dxdumpdb -f *filename* -z *dsaname*

   -f *filename*

   Specifies the file path and name of the LDIF file.

   -z

   Specifies that DXdumpdb dumps from the online dump.

   dsaname

   Specifies the name of the DSA.

   The LDIF file is created at the specified path.

Create an Offline Backup of the Data Store

An offline backup requires that you stop and start the DSA services every time you take a backup.

To create an offline backup

1. Login as the user dsa (on UNIX) or the administrator (on Windows).
2. Stop the local DSA services using the following commands:

   Windows

   ```
   dxserver stop dsaname
   ```

   Linux and UNIX

   ```
   su - dsa -c "dxserver stop dsaname"
   ```

3. Run the following command from the command line:

   ```
   dxdumpdb -f filename  dsaname
   ```

   -f *filename*

   Specifies the file path and name of the LDIF file.

4. Start the local DSA services using the following commands:

   Windows

   ```
   dxserver start dsaname
   ```

   Linux and UNIX

   ```
   su - dsa -c "dxserver start dsaname"
   ```

   The LDIF file is created at the specified path and the offline backup is successful.

Restore CA EEM Data

Use the following procedure to restore CA EEM data:

1. Stop the local DSA services using the following commands:

   Windows

   ```
   dxserver stop dsaname
   ```

   Linux and UNIX

   ```
   su - dsa -c "dxserver stop dsaname"
   ```

2. Use the DXloaddb to a datastore from an LDIF file.

   ```
   dxloaddb dsaname ldif-file
   ```

3. Start the local DSA services using the following commands:

   Windows

   ```
   dxserver start dsaname
   ```

   Linux and UNIX

   ```
   su - dsa -c "dxserver start dsaname"
   ```

Failover Configuration

CA EEM provides a command line tool for automating the failover configuration process.

Prerequisites

Before you execute the failover tool, perform the following steps:

- Synchronize the system time of all servers in the failover setup.
- Verify that all CA EEM Servers are configured in the same security mode, non-FIPS or FIPS-only.
- Verify that DNS lookup resolves hostnames of all the servers in the failover setup.
- Set the following environment variable:

  ```
  EIAM_HOME=<installation_path_of_CA EEM>
  ```

- Set JAVA_HOME as follows:

  Windows

  ```
  set JAVA_HOME=%EIAM_HOME%/jre
  ```

  ```
  set PATH=%EIAM_HOME%/jre/bin;%PATH%
  ```

  UNIX

  ```
  export JAVA_HOME=$EIAM_HOME/jre
  ```

  ```
  export PATH=$EIAM_HOME/jre/bin:$PATH
  ```

How to Set Up a Failover Environment

As an Administrator, you can plan a failover setup environment by performing the following steps:

1. Identify the servers that must act as a primary server and secondary servers.
2. Configure the primary server.
3. Add secondary servers to the primary server.
4. Synchronize the secondary servers with the primary server.

Configure a Primary Server

Configure a CA EEM primary server to invoke the failover tool and select a failover mode.

Follow these steps:

1. Open the command prompt from the primary server, and navigate to the EiamInstallation\bin location.
2. Execute the following command:

   ```
   java -jar eiam-clustersetup.jar
   ```

3. Type **Y** and press Enter.
4. Execute the following command:

   ```
   resetprimary
   ```

   Note: Reset a primary server only once in a failover setup.
5. Do *one* of the following steps:
   a. To use the default 509 as the DSA port, press Enter.
   b. To use a different port as the DSA port, type the port number and press Enter.
6. Do *one* of the following steps:
   a. To use the internal failover setup that consists of CA EEM servers which support CA EEM failover, type 1 and press Enter.
   b. To use an external failover setup that consists of CA EEM servers which are configured for CA EEM failover and a load balancer (hardware or software), type 2 and press Enter.

      Note: To use an external failover setup, ensure that the load balancer is configured.
7. Type **Y** and press Enter.

   The primary server is configured.

Add a Secondary Server to the Primary Server

You can use the failover tool to add a secondary server to the primary server.

Follow these steps:

1. Open the command prompt from the primary server, and navigate to the EiamInstallation\bin location.
2. Execute the following command:

   ```
   java -jar eiam-clustersetup.jar
   ```

3. Type **Y** and press Enter.
4. Execute the following command:

   ```
   add
   ```

5. Type the fully-qualified hostname of the secondary server, and press Enter.

   The message "Enter DSA Port [default=509]" appears.

6. Do *one* of the following steps:
   a. If you want to accept the default port, press Enter.
   b. If you want to enter a different DSA port, type the port number and press Enter.
7. Type **Y** and press Enter.

   The failover tool starts validating the entered details. After the validation, the secondary server is added to the primary server.

8. Repeat the Steps 4–8 to add another secondary server to the primary server.

Synchronize a Secondary Server with the Primary Server

Synchronize the configuration of the primary server with the secondary servers in a failover setup. After the synchronization, the configuration of each secondary server in the failover setup is overwritten with the configuration of the primary server.

Follow these steps:

1. Open the command prompt from a secondary server, and navigate to the EiamInstallation\bin location.
2. Execute the following command:

   `java -jar eiam-clustersetup.jar -p <fullyqualifiedhostname_of_primaryserver>`

   The installation paths of CA EEM, CA Directory, and CA iTechnology iGateway and the status of the failover tool on the secondary server details are displayed. The command-line interpreter changes from $ to the hostname of the secondary server.
3. Type the EiamAdmin password and press Enter.
4. Type **Y** and press Enter.
5. Execute the following command:

   sync
6. Type the number corresponding to the current hostname, and press Enter.
7. Do *one* of the following steps:
   a. If you are synchronizing the secondary server with the primary server for the first time, type 1 and press Enter.
   b. If you are synchronizing the secondary server with the primary server for latest configuration changes, type 2 and press Enter.
8. Type **Y** and press Enter.

   The failover tool starts validating the synchronization process. After the validation, the secondary server is synchronized with the primary server.

   Note: If you are not able to execute the sync command, execute the following cluster setup command again on the secondary server:

   ```
   java -jar eiam-clustersetup.jar -h
   <fullyqualifiedhostname_of_secondaryserver> -p
   <fullyqualifiedhostname_of_primaryserver>
   ```
9. Repeat the Steps 1–8 on each secondary server in the failover setup to synchronize all secondary servers with the primary server.

How to Delete a Secondary Server

You can delete a secondary server from the primary server in a failover setup. To delete a secondary server, perform the following steps:

1. Delete a secondary server from the primary server.
2. Synchronize the remaining secondary servers in the failover setup with the primary server.

Delete a Secondary Server from the Primary Server

You can use the failover tool to delete a secondary server from the primary server.

Follow these steps:

1. Open the command prompt from the primary server, and navigate to the EiamInstallation\bin location.
2. Execute the following command:

   ```
   java -jar eiam-clustersetup.jar
   ```

3. Type **Y** and press Enter.
4. Execute the following command:

   ```
   remove
   ```

   The available secondary servers are displayed. Each secondary server is numbered.
5. Type the number corresponding to the secondary server you want to delete, and press Enter.
6. Type **Y** and press Enter.

   The secondary server is removed from the primary server.
7. (Optional) To view the current secondary servers of the primary server, type list and press Enter.

Synchronize a Secondary Server with the Primary Server

Synchronize the configuration of the primary server with the secondary servers in a failover setup. After the synchronization, the configuration of each secondary server in the failover setup is overwritten with the configuration of the primary server.

Follow these steps:

1. Open the command prompt from a secondary server, and navigate to the EiamInstallation\bin location.
2. Execute the following command:

   `java -jar eiam-clustersetup.jar -p <fullyqualifiedhostname_of_primaryserver>`

   The installation paths of CA EEM, CA Directory, and CA iTechnology iGateway and the status of the failover tool on the secondary server details are displayed. The command-line interpreter changes from $ to the hostname of the secondary server.
3. Type the EiamAdmin password and press Enter.
4. Type **Y** and press Enter.
5. Execute the following command:

   sync
6. Type the number corresponding to the current hostname, and press Enter.
7. Do *one* of the following steps:
   a. If you are synchronizing the secondary server with the primary server for the first time, type 1 and press Enter.
   b. If you are synchronizing the secondary server with the primary server for latest configuration changes, type 2 and press Enter.
8. Type **Y** and press Enter.

   The failover tool starts validating the synchronization process. After the validation, the secondary server is synchronized with the primary server.

   Note: If you are not able to execute the sync command, execute the following cluster setup command again on the secondary server:

   ```
   java -jar eiam-clustersetup.jar -h
   <fullyqualifiedhostname_of_secondaryserver> -p
   <fullyqualifiedhostname_of_primaryserver>
   ```
9. Repeat the Steps 1–8 on each secondary server in the failover setup to synchronize all secondary servers with the primary server.

Certificates with Custom Key Length for CA EEM Server

CA EEM supports certificates that are created with key lengths of 1024, 2048, and 4096 and with digest algorithms SHA1, SHA256, SHA384, and SHA512.

Certificates are used for the SSL communication between the following components for enhanced security:

- CA EEM SDK and CA EEM Server
- CA EEM Server and LDAP Server

The following changes take place when you upgrade CA EEM to the r12.51 version:

- By default, the generated certificates have the 1024 key length and the SHA1 digest algorithm.
- The certificates in the iTechnology folder are migrated from the .conf file to .cer and .key files.

CA EEM Server uses the following certificates:

igateway.cer

For the SSL communication between the following:

- CA EEM Server and CA EEM SDK
- CA EEM Server and browser

icontrol.cer

For decrypting the CA EEM credentials.

iauthority.cer

For establishing trust between the CA EEM Servers.

rootcert.cer

For use as the root certificate of a certificate authority such as iAuthority.

Considerations for Using Higher Key Length Certificates

Following are the considerations for using higher key length certificates:

CA EEM SDK Prior to r12.51

The communication between the CA EEM Server and CA EEM SDK versions prior to r12.51 continue to work if the CA EEM Server is configured for 1024 key length.

If the CA EEM Server is configured for a higher key length, the communication between the CA EEM Server and CA EEM SDK versions prior to r12.51 fails.

CA EEM Application Certificates

If you use application certificates to connect to the CA EEM Server, regenerate the application certificates if the CA EEM Server certificates are modified.

Note: For more information about generating application certificates, see the *Programming Guide*.

How to Generate the Certificates

You can use the eiam-clustersetup utility to generate certificates with the required key length and digest algorithm. Executing the eiam-clustersetup utility updates the following files in the iTechnology and CA Directory folders:

The following certificate and key files that are availble in the iTechnology installation folder are modified:

- igateway.cer, igateway.key
- icontrol.cer, icontrol.key
- iauthority.cer, iauthority.key
- rootcert.cer, rootcert.key

The following configuration files that are available in the iTechnology installation folder are modified with the required key length and digest algorithm:

- igateway.conf
- iAuthority.conf
- iContol.conf

The following certificates available in the CA Directory folder are modified:

- itechpoz.pem
- itechpoz-trusted.pem

Prerequisites

Before you execute the eiam-clustersetup utility, perform the following steps:

1. Back up the .cer and .key files available in the following iTechnology installation path:

   ```
   C:\Program Files\CA\SC\iTechnology
   ```

2. Back up the itechpoz.pem and itechpoz-trusted.pem files.

   The location of the itechpoz.pem file is as follows:

   ```
   $DXHOME/dxserver/config/ssld/personalities/
   ```

   The location of the itechpoz-trusted.pem file is as follows:

   ```
   $DXHOME/dxserver/config/ssld/
   ```

3. Set the environment variable EIAM_HOME as follows:

   ```
   EIAM_HOME =<installation_path_of_CA EEM Server>
   ```

4. Set the environment variable JAVA_HOME as follows:

   In Windows

   ```
   Set JAVA_HOME=%EIAM_HOME%/jre
   ```

   ```
   Set PATH=%EIAM_HOME%/jre/bin;%PATH%
   ```

   In UNIX

   ```
   Export JAVA_HOME=$EIAM_HOME/jre
   ```

   ```
   Export PATH=$EIAM_HOME/jre/bin:$PATH
   ```

Generate the Certificates

The eiam-clustersetup utility generates the server certificates with the specified key length and digest algorithm and replaces the existing certificates with the new certificates in the iTechnology folder.

Follow these steps:

1. On the CA EEM Server where the certificates have to be issued, navigate to the following location:

   ```
   EIAM_HOME/bin
   ```

2. Execute the following command:

   ```
   java -jar eiam-clustersetup.jar
   ```

   A confirmation message appears.

3. Type Y and press Enter.

4. Execute the following command

   ```
   modifycerts
   ```

   The following message appears:

   ```
   Enter Certificate KeyLength [default = 1024]
   ```

5. Do *one* of the following steps:

   - To accept the default KeyLength, press Enter.

- To specify a different KeyLength, type the desired option and press Enter.

  The following message appears:

  ```
  Enter Digest Algorithm [default = SHA256]
  ```

6. Do *one* of the following steps:
   - To accept the default Digest Algorithm, press Enter.
   - To specify a different Digest Algorithm, type the desired option and press Enter.

     A confirmation message appears.
7. Type Y and press Enter.
8. Execute the following command to close the eiam-clustersetup utility:

   ```
   exit
   ```

   The certificates are generated with custom key length.

CA EEM Server uses the newly generated certificates.

Generate Certificates with Custom Key Length for CA EEM Servers in Failover or Cluster Environment

To use certificates with a custom key length for CA EEM Servers in a failover or cluster environment, do the following steps:

1. On the primary CA EEM Server, remove all the secondary CA EEM Servers.
2. Reset all the secondary CA EEM Servers.
3. Generate certificates with custom key length on all the CA EEM Servers.
4. Reconfigure the failover configuration.

Remove Secondary CA EEM Servers from Primary CA EEM Server and Reset Primary CA EEM Server

Important! Verify that the prerequisites for generating the certificates are met before you perform this procedure.

You can use the eiam-clustersetup utility to remove the secondary CA EEM Servers from the primary CA EEM Servers. After you remove the secondary CA EEM Servers, reset the primary CA EEM Server.

Follow these steps:

1. On the primary CA EEM Server, navigate to the following location:

   ```
   EIAM_HOME/bin
   ```

2. Execute the following command:

   ```
   java -jar eiam-clustersetup.jar
   ```

   A confirmation message appears.

3. Type Y and press Enter.

4. Execute the following command:

   ```
   remove
   ```

   The following message appears.

   ```
   select hostname
   ```

5. Type the number corresponding to the secondary CA EEM Server that you want to remove and press Enter.

   A confirmation message appears.

6. Type Y and press Enter.

7. Repeat steps 4 through 6 for all the secondary CA EEM Servers.

8. Execute the following command

   ```
   list
   ```

   Only the primary CA EEM Server is displayed. The secondary CA EEM Servers are removed from the primary CA EEM Server.

9. To reset the primary CA EEM Server, execute the following command:

   ```
   resetprimary
   ```

   The following message appears:

   ```
   Enter DSA Port [default = 509]
   ```

10. If necessary, update the default DSA port number and press Enter.

    The following message appears:

    ```
    Specify high-availability mode
    ```

11. Select a high-availability mode and press Enter.

    A confirmation message appears.

12. Type Y and press Enter.

    The primary CA EEM Server is reset.

13. To close the eiam-clustersetup utility, execute the following command:

    ```
    exit
    ```

    The secondary CA EEM Servers are removed from the primary CA EEM Server and the primary CA EEM Server is reset.

Reset the Secondary CA EEM Servers

Important! Verify that the prerequisites for generating the certificates are met before you perform this procedure.

You can use the eiam-clustersetup utility to reset the secondary CA EEM Servers.

Follow these steps:

1. On a secondary CA EEM Server, navigate to the following location:

   `EIAM_HOME/bin`

2. Execute the following command:

   `java -jar eiam-clustersetup.jar`

   A confirmation message appears.

3. Type Y and press Enter.

4. Execute the following command

   `resetprimary`

   The following message appears:

   `Enter DSA Port [default = 509]`

5. If necessary, update the default DSA port number and press Enter.

   The following message appears:

   `Specify high-availability mode`

6. Select a high-availability mode and press Enter.

   A confirmation message appears.

7. Type Y and press Enter.

   The CA EEM Server is reset.

8. To close the eiam-clustersetup utility, execute the following command:

   `exit`

Repeat the procedure on all the secondary CA EEM Servers.

Generate Certificates with Custom Key Length on all CA EEM Servers

Generate the certificates with the required key length and digest algorithm after verifying that the prerequisites are met.

Perform the prerequisite steps and generate the certificate on all the CA EEM Servers that are part of the failover or cluster environment.

Important! All the CA EEM Servers must have the certificates with the same key length and digest algorithm.

More information:

Prerequisites (see page 63)
Generate the Certificates (see page 64)

Reconfigure Failover Configuration

See the Failover Configuration section for configuring the failover or cluster environment.

Important! When you reconfigure the servers for failiover, specify the following value for the synchronization mode to sync the secondary servers with the primary server:

```
[2] [DELTA] secondary node is being synced to update configurations:
```

More information:

Failover Configuration (see page 56)

Configure SSL Communication between CA EEM Server and LDAP Server

You can use certificates with a custom key length for the SSL communication between the CA EEM Server and an LDAP Server.

When you configure the CA EEM Server using the CA EEM User Interface (UI) to reference an external LDAP Directory, you can set the CA EEM Server to communicate with LDAP Server over SSL or TLS.

Custom certificates can be used between the CA EEM Server and the LDAP Server *only* if the following conditions are met:

- The certificate must be obtained from a CA that the LDAP Server trusts.
- The certificate and key must be in the PEM format.

The following files are required for configuring the SSL communication between CA EEM Server and LDAP Server:

- A certificate file
- A key file
- A CA Certificate

Note: Copy these certificates to the location where CA EEM Server is installed.

Follow these steps:

1. Log in to CA EEM UI as EiamAdmin.
2. On the Configure tab, click User Store.
3. In the User Store section, click User Store.
4. On the right pane, under User Store Configuration, select Reference from an external LDAP Directory.
5. Select the Configuration Type and click Add external LDAP directory.
6. Fill the fields and select the Protocol as LDAP + TLS or LDAPS.
7. Specify the certificate name in Certificate Path.
8. Specify the key file name in Key Path.
9. Specify the CA certificate name in CA Certificate Path.
10. Click Save.

    CA EEM Server is configured to use custom certificates for the SSL communication with LDAP Server.

Chapter 5: Upgrading CA EEM Server

This section contains the following topics:

Upgrade Considerations (see page 71)
Upgrade CA EEM Server (see page 73)

Upgrade Considerations

Important! When you are upgrading CA EEM, ensure that the operating system on which you want to upgrade, is supported by CA EEM.

You can upgrade from CA EEM r8.3 Server or higher to CA EEM r12.0 Server. Before you upgrade:

- Back up CA EEM server data, configuration files, CA Directory and iTechnology folders.
- In a failover setup, verify that you have performed the following tasks in the CA Directory knowledge file:
  - Set all the failover servers to use the same DSA password (dsa-password). If the CA Directory knowledge file does not contain a dsa-password, add a password.
  - Set auth-levels to anonymous, clear-password.

Example: Sample CA Directory Knowledge File

```
# eiam repository

#

set dsa "iTechPoz-hostname" =

{

prefix       = <cn iTechPoz>

dsa-name     = <cn iTechPoz><cn PozDsa><cn "hostname">

dsa-password = newpassword

address      = tcp "hostname" port 509

auth-levels  = anonymous, clear-password

dsp-idle-time = 120

dsa-flags   = multi-write

link-flags   = ssl-encryption-remote

};
```

Note: For more information about how to back up your CA EEM data and configuration files, see Back Up and Restore CA EEM Data.

The following components are updated when you perform an upgrade:

- CA EEM Server
- iGateway
- CA Directory

After the upgrade, CA EEM performs the following tasks:

- Changes the installation folder from Embedded EIAM to EmbeddedEntitlementsManager.
- Uses the builtin failover mechanism instead of CA Directory routers.
- Restores the default configuration settings.
- Migrates all P12 certificates to PEM certificates.

Upgrade CA EEM Server

Follow these steps:

1. Run the installer on the target computer.

   Windows

   EEMServer_<version number>_win32.exe

   UNIX and Linux

   EEMServer_<version number>_<operating system>.bin

2. Depending on the installed version of CA EEM Server, the installer does one of the following:

   - If the existing version is older than the version that is being installed, the installation wizard backs up the existing version, and upgrades to the newer version.
   - If the version that is being installed is older than the existing version, the installation wizard displays an error and quits the installation.
   - If the existing version is same as the version that is being installed, the installer displays a message indicating that no upgrade is necessary. The installer exits after displaying the message.

Upgrade CA EEM Server

If you upgrade a CA EEM server to r12.0 from an earlier version, CA Directory performs the following tasks:

- Continues replicating data between the failover servers.
- Stops supporting failover mechanism until you upgrade all CA EEM servers to the current release.

How to Migrate CA EEM Server from an Unsupported Operating Systems

If you have installed CA EEM server on an operating system that CA EEM r12.0 does not support, perform the following steps to migrate data from the older CA EEM server to CA EEM r12.0:

1. Export the CA EEM database to an LDIF file from the existing CA EEM server.
2. Install CA EEM r12.0 on a supported operating system.
3. Import the LDIF file on the CA EEM r12.0 server.
4. Configure the user store. For information about configuring user store, see the CA EEM Server User Stores Configuration.
5. Issue new certificate for each registered application using safex.

Export CA EEM Database to an LDIF File

Perform the following steps on the unsupported operating system where you installed an older version of CA EEM server.

Follow these steps:

1. Execute the following command:

   Windows

   ```
   dxserver stop all
   ```

   UNIX

   ```
   su - dsa -c "dxserver stop all"
   ```

   The dxserver is stopped.

2. Execute the following command:

   Windows

   ```
   net stop igateway
   ```

   UNIX

   ```
   /opt/CA/SharedComponents/iTechnology/S99igateway stop
   ```

   The iTechnology iGateway is stopped.

3. Navigate to the following directory:

   CADirectory_installation_directory/dxserver

4. Execute the following command:

   CA EEM r8.4

   Windows

   ```
   dxdumpdb -x createTimestamp,modifyTimestamp -f iTechPoz-export.ldif
   iTechPoz-current_hostname
   ```

   UNIX

   ```
   su - dsa -c "dxdumpdb -x createTimestamp,modifyTimestamp -f
   iTechPoz-export.ldif iTechPoz-current_hostname"
   ```

   CA EEM r8.3

   Windows

   For CA EEM MDB version

   ```
   dxdumpdb -p "cn=iTechPoz" -f iTechPoz-export.ldif mdb
   ```

   For CA EEM non-MDB version

   ```
   dxdumpdb -p "cn=iTechPoz" -f iTechPoz-export.ldif itechpoz
   ```

   UNIX

For CA EEM MDB version

```
su - dsa -c "dxdumpdb -p "cn=iTechPoz" -f iTechPoz-export.ldif mdb"
```

For CA EEM non-MDB version

```
su - dsa -c "dxdumpdb -p "cn=iTechPoz" -f iTechPoz-export.ldif itechpoz"
```

An LDIF file is created in the dxserver folder of the CA Directory installation directory. The database is exported to the LDIF file.

Import the LDIF File

Perform the following steps on the computer where you installed CA EEM r12.0 on a supported operating system.

Follow these steps:

1. Copy the exported LDIF file to the dxserver folder of the CA Directory installation directory.
2. Open the command prompt and navigate to the CA Directory installation directory.
3. Execute the following command:

   dxmodify –a –c –H ldap://*current_fullyqualifiedhostname*:*dsaport* –D “cn=EiamAdmin,cn=Admins,cn=Entities,cn=iTechPoz” –w *eiamadminpassword* –f iTechPoz-export.ldif

   The LDIF file is imported.

Chapter 6: Uninstalling CA EEM Server

You can install CA EEM using *one* of the following methods:

- Manually
- Silently

Before you uninstall a CA EEM server, verify that no applications are registered with the CA EEM server. You must unregister all applications before you proceed to uninstall the CA EEM server. For information about unregistering an application, see the *Online Help*.

Note: If you want to forcefully uninstall a CA EEM server when an application is still registered with the CA EEM server, you can execute the command **eiamunstall -DFORCE_UNINSTALL=true** at the command prompt. This forceful uninstallation deletes the data of all the application that are registered with the CA EEM server.

This section contains the following topics:

Uninstall CA EEM Server Manually (see page 77)
Uninstall CA EEM Server Silently (see page 78)

Uninstall CA EEM Server Manually

Use the uninstallation wizard to uninstall the CA EEM server.

Follow these steps:

1. Log on to the console and navigate to the EiamHome\Uninstall location.
2. Run eiamuninstall.
3. Follow the instructions on the wizard.

   The CA EEM server is uninstalled.

Uninstall CA EEM Server Silently

Use the command prompt to uninstall the CA EEM server.

Follow these steps:

1. Log on to the console.
2. Execute the following command

   ```
   ./eiamuninstall -i silent
   ```

   The CA EEM server is uninstalled.

Chapter 7: Appendix

This section contains the following topics:

Ports Used by CA EEM (see page 79)
CA EEM Services (see page 79)

Ports Used by CA EEM

The CA EEM Server uses the following default ports:

Service	Port Number	Configurable
Administration Port	5250	No
Data DSA (itechpoz) Port	509	Yes. Edit the DXHOME/config/knowledge/ itechpoz.dxc file

CA EEM Services

The following services are installed with the CA EEM Server:

Windows

- CA Directory - itechpoz—Embedded CA Directory DSA (directory service agent) for the CA EEM LDAP repository.
- CA iTechnology iGateway 4.7— iTechnology iGateway service that handles the requests coming from CA EEM clients, processes the requests, and sends responses to the clients.

UNIX

- For CA Directory:
  - dxserver start itechpoz
- For iGateway:
  - ./igateway –b
  - /bin/sh ./WDigateway.sh