CA Embedded Entitlements Manager

Getting Started Guide

r8.4

CA Product References

This document references the following CA products:

- CA® Embedded Entitlements Manager (CA EEM)
- CA® Directory
- CA® SiteMinder® Web Access Manager (CA SiteMinder)
- CA® Identity Manager
- CA® Security Command Center
- CA® Integrated Threat Management
- CA® Enterprise Log Manager

Contact CA

Contact Technical Support

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

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

Provide Feedback

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

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

Contents

Chapter 1: Introduction 9

Overview 9
Functions 9
Features 10
Client Access 11
Data Store Support 11

Chapter 2: Installing on Windows 13

Installation Overview 13
Install Server 14
Wizard Setup Checklist 14
How to Skip Selecting JRE Path Screen in Installation Wizard 15
    Set Javahome parameter 15
Install Server Using Installation Wizard 16
Upgrade Server 17
Start Server 18
Remove Server 18
Install SDK 19
Start SDK 19
Remove SDK 19
Server Installation Parameters 20
Install CA EEM Server in Silent Mode 21
    Create the Response File 22
    Run the Command Specifying the Response File 22
Remove CA EEM Server in Silent Mode 23

Chapter 3: Installing on Linux and UNIX 25

Installation Overview 25
Install Server 26
Upgrade Server 27
Remove Server 27
Install SDK 28
Start CA EEM SDK 28
Remove SDK 28
Server Installation Script Parameters 29
Install Server in Silent Mode 34

Remove CA EEM Server in Silent Mode 34

Chapter 4: Back Up and Restore CA EEM Server 35

File System Back Up 35
Back Up CA EEM Server Files and Folders 36
Restore Procedures 36
Start iGateway Service 37
Stop iGateway Service 37

Chapter 5: Backing Up CA EEM Data Stored in CA Directory 39

Introduction to CA Directory Terminology 39
How to Use the DXtools 40
DXHOME Environment Variable 40
Exit Status Codes for the DXtools 40
How to Back Up CA Directory Data 42
Connect to a Local DSA Console 42
Online Datastore Dump 43
dump dxgrid-db Command—Take a Consistent Snapshot Copy of a Datastore 44
Using an LDIF file to Back Up and Load Data 45
DXdumpdb Tool—Export Data from a Datastore to an LDIF File 45
How to Restore CA Directory Data 46
DXloaddb Tool—Load a Datastore from an LDIF File 47

Chapter 6: Integrating With CA SiteMinder 49

How You Integrate CA SiteMinder with CA EEM 49
How You Integrate CA SiteMinder r12 With CA EEM 50

Chapter 7: Configuring Failover 51

Failover 51
Data Store Failover 51
How You Configure CA Directory 52
CA EEM Server Failover 59
Configure CA EEM Files 60

Chapter 8: Configuring External Directory Server Support 63

Configure External Directory Server Support 63
Configure External Directory Failover Support 64
Connecting to LDAP Servers over SSL 64
How CA EEM Connects to LDAP Server Over SSL 65

How to Configure the SSL Connections 65
Configure the LDAP Server to Use SSL Certificates 65
Enable SSL in CA EEM Server 66

Chapter 9: Configuring Support for Large Numbers of Policies 67

Support for Large Number of Policies 67
Configure Additional Settings for CA EEM Server on AIX 67
Client Configuration 67
Configure Client for all Operating Systems 68

Chapter 10: Archiving Events 69

Overview 69
Utility to Defrost Cold DB Files 70
SEM Utility Syntax 71
Defrost Cold DB Files 72

Appendix A: Upgrading and Troubleshooting CA Directory Installation 73

Upgrade CA Directory 73
How to Estimate the Time to Upgrade a DSA From r8.1 74
Troubleshooting 74
Troubleshooting on UNIX 74
Troubleshooting on Windows 76

Chapter 1: Introduction

This section contains the following topics:

Overview (see page 9)
Functions (see page 9)
Features (see page 10)
Client Access (see page 11)
Data Store Support (see page 11)

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
- Integrated with CA Security Command Center and CA Audit for security event management
- Integration with CA SiteMinder to retrieve user and group information from CA 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
  - External global users from CA Identity Manager
- Integration with CA Identity Manager for role-based user provisioning and management
- 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

Client Access

You can access CA EEM Server through standard web and web services interfaces that provide third-party integration without requiring the client module. The interfaces are:

- HTML and iTechnology for configuration and administration
- iTechnology for delivering CA Audit events

iTechnology is a CA technology based on web standards such as HTTP, HTTPS, HTML, XML, and SSL. It provides a framework to create and deploy web services across the Internet.

Data Store Support

CA EEM supports identifying a single external user source, such as Microsoft Active Directory. CA EEM stores its configuration and policies in CA Directory regardless of where the user objects are stored.

Chapter 2: Installing on Windows

This section contains the following topics:

Installation Overview (see page 13)
Install Server (see page 14)
Wizard Setup Checklist (see page 14)
How to Skip Selecting JRE Path Screen in Installation Wizard (see page 15)
Install Server Using Installation Wizard (see page 16)
Upgrade Server (see page 17)
Start Server (see page 18)
Remove Server (see page 18)
Install SDK (see page 19)
Start SDK (see page 19)
Remove SDK (see page 19)
Server Installation Parameters (see page 20)
Install CA EEM Server in Silent Mode (see page 21)
Remove CA EEM Server in Silent Mode (see page 23)

Installation Overview

The CA EEM installation on Windows operating environments consists of installing the following applications:

CA EEM Server

You can use CA EEM Server to define authorization policies on application resources using a web interface. The web-based administrative interface lets you manage identities and access policies. The existing security infrastructure is used to implement rules based on business logic, using resources and user attributes, defined in centralized user stores and other enterprise systems.

CA EEM Software Development Kit (SDK)

You can use the CA EEM SDK to embed identity-based security controls within applications. The SDK is comprised of libraries, java classes, header files, and a tutorial. You can use the SDK to implement CA EEM in any application. For more information on how to implement CA EEM using SDK, see the *Programming Guide*.

Each application installs separately and functions independently of the other.

Install Server

You can install CA EEM server using the installation wizard or the command line. Use the command line to install CA EEM in the silent mode and use the installation wizard for an interactive install.

JRE is no longer a minimum requirement to install and use CA EEM. You can install and use CA EEM with or without JRE. If you want to install CA EEM without JRE as a minimum requirement, you must skip the JRE selection path screen in the installation wizard. If you want to install CA EEM server in a silent mode without JRE, you must use the javahome parameter set to "None".

The following sections describe how to install CA EEM server.

More Information

How to Skip Selecting JRE Path Screen in Installation Wizard (see page 15)
Wizard Setup Checklist (see page 14)
Install Server Using Installation Wizard (see page 16)
Install CA EEM Server in Silent Mode (see page 21)

Wizard Setup Checklist

While installing CA EEMserver on Windows, you need the following information:

Field	Value
CA EEM Installation Path	Location on your computer where you intend to install CA EEM.
JRE Installation Path	Location of JRE installation on your computer. **Note**: If you want to install and use CA EEM without JRE, you must set Javahome variable to None from command line before running the CA EEM installation wizard.
EiamAdmin Password	The password associated with the CA EEM administrator EiamAdmin

Field	Value
Backup Directory	The location on you computer where you intend to back up the files from an earlier installation of CA EEM. **Note:** You will need this information only if you upgrade a previous release of CA EEM to the current release.

How to Skip Selecting JRE Path Screen in Installation Wizard

JRE is no longer a minimum requirement to install and use CA EEM. If you want to install CA EEM without JRE, you must do the following:

1. Set javahome parameter equal to "None".

   Note: If you set javahome parameter to "None", the installation wizard does not display the Java Path selection screen.

2. Install CA EEM using the installation wizard.

Set Javahome parameter

You must set the javahome parameter to the value "None" before you use the installation wizard to install CA EEM. Set the javahome parameter, from the command line as follows:

```
EEMServer_[releasenumber].[build_number]_win32.exe -s -a /z"javahome=None; "
```

Install Server Using Installation Wizard

The CA EEM Server installation wizard guides you through the installation process and provides you with options to define the installation parameters.

To install CA EEM Server

1. Do one of the following:
   - Open the Windows Explorer and double-click the install package EEMServer_[*releasenumber*].[*build_number*]_win32.exe on the target computer.
   - Enter the following command at the command prompt using installation parameters:

     `EEMServer_[releasenumber].[build_number]_win32.exe -s -a /z "eiampath=<Custom installation path for CA EEM>; etdirpath=<Custom installation path for CA Directory>; igpath=<Custom installation path for iGateway>;"`

     You can provide a custom installation path using installation parameters. For more details about installation parameters, see Server Installation Parameters (see page 20).

     The installation wizard appears.
2. Follow the instructions on the installation wizard to complete the installation.

More Information:

How to Skip Selecting JRE Path Screen in Installation Wizard (see page 15)

Upgrade Server

You can upgrade the existing installation of CA EEM Server to the current version.

To upgrade an existing installation of CA EEM Server

1. Run the EEMServer_[*releasenumber*].[*build_number*]_win32.exe on the target computer.
2. Depending on the version of CA EEM Server installed, one of the following occurs:
   - If the existing version of CA EEM Server is older than the version that is being installed, the installation wizard backs up the existing version and automatically upgrades to the newer version.
   - If the existing version of CA EEM Server is same as the version that is being installed, the installation wizard prompts to uninstall CA EEM Server. You can uninstall and re-install CA EEM Server.
   - If the version that is being installed is older than the existing version, the installation wizard displays an error and quits the installation.

Upgrading the CA EEM Server updates the following:

- CA EEM Server in \\CA\SharedComponents\iTechnology folder
- iGateway
- CA Directory

More Information:

Wizard Setup Checklist (see page 14)
Install Server Using Installation Wizard (see page 16)
Server Installation Parameters (see page 20)

Start Server

You must start the CA EEM Server to manage identities and access policies of registered applications.

To start using CA EEM Server

1. Do one of the following:
   - Enter the URL https://*hostname* or *ipaddress*:5250/spin/eiam in your browser. If you are on the CA EEM Server computer, specify http://l*ocalhost*:5250/spin/eiam.
   - Select Start, Programs, CA, Embedded Entitlements Manager, EEM UI on Windows operating environments.

     A login page appears.
2. Enter the following information in the login dialog:
   a. Select an application instance that you have registered from the Application drop-down. The default is <Global>. The default administrator username is EiamAdmin.

      Note: You can add other global users for login and set their usernames according to the preferences.

   b. Enter your password. This is the same password you specified during the installation of CA EEM Server for EiamAdmin.

   c. Select Remember my settings, if you want to log into the CA EEM Server with the same settings next time.
3. Click Log In.

   The CA EEM interface home page appears. For more information about how to use CA EEM Server, see the *Online Help*.

Remove Server

You can uninstall the CA EEM Server using the Add or Remove Programs of the Control Panel.

Note: You cannot remove CA EEM Server if applications are registered in CA EEM. You must unregister the applications before uninstalling CA EEM Server. For information about unregistering an application, see the *Online Help.*

Install SDK

The CA EEM SDK installation wizard guides you through the installation process.

To install the CA EEM SDK

1. Open the Windows Explorer and double-click the install package EEMSDK_[*releasenumber*].[*build_number*]_win32.exe, or run the installation file from the command prompt.

   The installation wizard appears.

2. Click I Agree to accept the Terms and Conditions.

   Note: The I Agree button is enabled only after you read, or scroll the text of the Terms and Conditions.

   The Choose Destination Location dialog appears. By default, the installation wizard installs the CA EEM SDK in the following location: C:\Program Files\CA\Embedded IAM SDK

3. Click Next.

   Or

   Click Browse and select a directory on your computer where the CA EEM SDK must be installed, and click Next.

   This starts installing the CA EEM SDK.

4. Click Finish.

   CA EEM SDK is installed.

Start SDK

To start CA EEM SDK click Start, Programs, CA, Embedded Entitlements Manager, EEM SDK.

The CA EEM SDK documentation window appears.

Remove SDK

You can uninstall the CA EEM SDK using the Add or Remove Programs of the Control Panel.

Server Installation Parameters

While installing CA EEM on Windows, you must collect information on the following command line parameters:

eiampath

Specifies the path where the CA EEM Server will be installed. The default is C:\Program Files\CA\SharedComponents\Embedded IAM.

etdirpath [path]

Specifies the path where CA Directory will be installed. The default is C:\Program Files\CA\Directory.

igpath [path]

Specifies the path where iGateway will be installed. The default is C:\Program Files\CA\SharedComponents\iTechnology.

backupdir

Specifies the location where the data from the existing installation is backed up.

-javahome [directory]

Sets the JAVA_HOME variable to [directory] when calling the iGateway installer. This parameter defaults to the contents of the JAVA_HOME environment variable and is prompted for only if $JAVA_HOME is null.

Note: If you want to install CA EEM without java, you must set javahome to None.

CA EEM uses the following parameters during CA Directory installation. You can configure the parameters based on your needs.

Important! Before customizing the default port numbers ensure that no other services are configured to use the same ports.

-dsaport

Specifies the port that the dsa uses to listen to any requests directed at it.

Default: 509

-ssldport

Specifies the port that the CA Directory uses to listen to the SSLD server. The SSLD server is a background process that handles SSL and TLS authentication, encryption, and decryption for CA Directory.

Default: 21847

-routerport

Specifies the port that the dsa uses to connect to the router dsa. A router DSA has no local data and no datastore. It can only route traffic to other DSAs.

Default: 1684

-dxdbsize

Specifies the maximum size of the datastore for CA EEM.

Default: 500 MB

-dxuser

Specifies a non-dsa user who can install, administer, and uninstall CA Directory. The dxuser can be a local system user or a network user.

Note: If you have installed CA Directory using a local system user as the dxuser, then during uninstallation that local system user may be deleted. So, if you are using a local system user as a dxuser to install CA Directory, ensure that the user is not setup to run any other programs.

Note: On a computer with Microsoft Windows Server 2003, the maximum length of the string that you can use at the command prompt is 8,191 characters. With Microsoft Windows 2000, the maximum length of the string that you can use at the command prompt is 2,047 characters. For more information about InstallShield command length, see the *Release Notes*.

Install CA EEM Server in Silent Mode

Installing the CA EEM Server in silent mode requires two tasks:

1. Create the response file.
2. Run the command specifying the response file.

   A log file eiaminstall.log is created during the silent installation to record any installation errors.

Note: If you install CA EEM Server silently, you can also remove it silently.

Create the Response File

You can record your installation inputs in a response file, which is used to install the CA EEM Server silently. You must create a new response file for each build that you want to install.

To create a response file

1. Run the CA EEM Server installation package on the target computer.
2. Enter the following command at the command prompt to create a response file in the specified directory.

   EEMServer_[*releasenumber*].[*build_number*]_win32.exe -s -a /r /f1"*pathname of response file*"

   Example:

   EEMServer_8.4.0.55_win32.exe -s -a /r /f1"c:\resp.iss"

3. Enter values for the installation parameters, which are stored in the response file.

Run the Command Specifying the Response File

The following examples illustrate options for performing a silent installation:

- To install the CA EEM Server in the silent mode enter the following command at the command prompt:

  EEMServer_[*releasenumber*].[*build_number*]_win32.exe -s -a /s /f1"*pathname of response file*"

  Example:

  EEMServer_8.4.0.55_win32.exe -s -a /s /f1"c:\resp.iss"

- To create an installation log file during the silent installation, enter the following command at the command prompt:

  EEMServer_[*releasenumber*].[*build_number*]_win32.exe -s -a /s /v"/qn /L*v <path to create log file>" /f1"*pathname of response file*"

  Example:

  EEMServer_8.4.0.55_win32.exe -s -a /s /v"/qn /L*v c:\install.txt" /f1"c:\resp.iss"

This installs the CA EEM Server in silent mode, using the specified response file.

Note: You can provide the installation parameters along with the install script. For more details about the parameters, see Server Installation Parameters (see page 20).

Remove CA EEM Server in Silent Mode

You must use a response file created from the same build of CA EEM Server to successfully remove the product. To remove CA EEM Server in the silent mode enter the following command at the command prompt:

EEMServer_[*releasenumber*].[*build_number*]_win32.exe -s -a /s /f1"*pathname of response file*" /z"uninstall"

Example:

EEMServer_8.4.0.55_win32.exe -s -a /s /f1"c:\resp.iss" /z"uninstall"

This removes CA EEM Server in silent mode.

Note: You cannot remove CA EEM Server if applications are registered in CA EEM. You must unregister the applications before uninstalling CA EEM Server. For information about unregistering an application, see the *Online Help.*

Chapter 3: Installing on Linux and UNIX

This section contains the following topics:

Installation Overview (see page 25)
Install Server (see page 26)
Upgrade Server (see page 27)
Remove Server (see page 27)
Install SDK (see page 28)
Start CA EEM SDK (see page 28)
Remove SDK (see page 28)
Server Installation Script Parameters (see page 29)
Install Server in Silent Mode (see page 34)
Remove CA EEM Server in Silent Mode (see page 34)

Installation Overview

The CA EEM installation on Linux and UNIX operating environments consists of installing the following applications:

CA EEM Server

You can use CA EEM Server to define authorization policies on application resources using a web interface. The web-based administrative interface lets you manage identities and access policies. The existing security infrastructure is used to implement rules based on business logic, using resources and user attributes, defined in centralized user stores and other enterprise systems.

CA EEM Software Development Kit (SDK)

You can use the CA EEM SDK to embed identity-based security controls within applications. The SDK is comprised of libraries, java classes, header files, and a tutorial. You can use the SDK to implement CA EEM in any application. For more information on how to implement CA EEM using SDK, see the *Programming Guide*.

Each application installs separately and functions independently of the other.

Install Server

CA EEM Server for Linux and UNIX uses a self-extracting shell script that guides you through the installation process. During the installation process, the script displays the license information and prompts for installation parameters. After the installation parameters are entered, the installation begins.

To install CA EEM Server for Linux and UNIX

1. Run the installation script EEMServer_[*releasenumber*].[*build_number*]_[*name of operating system*].sh on the target computer.

   Example:

   `EEMServer_8.4.0.55_sunos.sh`

   The file is decompressed and the installation begins.

2. Enter Y to accept the Terms and Conditions of the license agreement (or N to decline and abort the installation).

   The script prompts for the installation parameters.

3. Enter the installation parameters.

   Note: For more information on the available installation parameters, see Server Installation Script Parameters.

   Example:

   a. Enter the installation path for the CA EEM Server (or accept the default).

   A confirmation screen appears with the installation parameter values you entered.

4. Enter Y to continue the installation, if the information on the confirmation screen is correct (if you Enter N, the installer exits.).

5. Enter the EiamAdmin password.

   Note: The default administrator username is EiamAdmin.

   The installation procedure depends on the command line parameters and the type of CA EEM Server package being installed.

   The installer script completes the installation of CA EEM Server on your computer.

Upgrade Server

You can upgrade the existing installation of CA EEM Server to the current version.

To upgrade an existing installation of CA EEM Server

1. Run the EEMServer_[*releasenumber*].[*build_number*]_[*name of operating system*] on the target computer.
2. Depending upon the version of CA EEM Server installed, one of the following occurs:
   - If the existing version of CA EEM Server is older than the version that is being installed, the installation wizard automatically upgrades to the newer version.
   - If the existing version of CA EEM Server is same as the version that is being installed, the installation wizard prompts to uninstall CA EEM Server. You can uninstall and re-install CA EEM Server.
   - If the version that is being installed is older than the existing version, the installation wizard displays an error and quits the installation.

   For information about how to install CA EEM Server, see Install Server (see page 26).

Upgrading the CA EEM Server updates the following:

- CA EEM Server in \\CA\SharedComponents\iTechnology folder
- iGateway
- CA Directory

Remove Server

To remove CA EEM Server, run the eiamuninstall.sh script from the installation directory.

Note: You cannot remove CA EEM Server if applications are registered in CA EEM. You must unregister the applications before uninstalling CA EEM Server. For information about unregistering an application, see the *Online Help.*

Install SDK

CA EEM SDK for Linux and UNIX uses a self-extracting shell script that guides you through the installation process. During the installation process, the script displays the license information and prompts for the installation parameters. After the installation parameters are entered, the installation begins.

To install CA EEM SDK for Linux and UNIX

1. Run the installation script EEMSDK_[*releasenumber*].[*build_number*]_[*name of operating system*].sh on the target computer.

   Example:

   `EEM_8.4.0.55_sunos.sh`

   The file is decompressed and installation begins.
2. Enter Y to accept the Terms and Conditions of the license agreement (or N to decline and abort the installation).
3. Enter the installation path for the CA EEM SDK (or accept the default).
4. Select install product.

   CA EEM SDK is installed on your computer.

Start CA EEM SDK

To start CA EEM SDK, point your Web browser at /opt/CA/eIAMSDK/Doc/index.html (or wherever CA EEM SDK was installed).

Remove SDK

You can remove CA EEM SDK from Linux and UNIX operating systems.

To remove CA EEM SDK

1. Run the installation script EEMSDK_[*releasenumber*].[*build_number*]_[*name of operating system*].sh on the target computer.

   Example:

   `EEM_8.4.0.55_sunos_linux.sh`

   The file is decompressed.
2. Select uninstall/remove product.

   The installation script removes CA EEM SDK on your computer.

Server Installation Script Parameters

While installing CA EEM, you must collect information on the following command line parameters that the script prompts for during the installation.

The script accepts the following command line parameters:

-build_date

Displays the date this package was built.

backupdir

Specifies the location where the data from the existing installation is backed up.

-dumptar [filename]

These parameters dump the script or tar part of the installer to the filename specified. If the filename is -, the data is dumped to standard output device.

Note: Only one of these (script or tar) can be used at a time, as the script exits after completing one of them.

These options can be used to unpack the installer, allowing access to its contents without actually performing an installation. To reassemble an installer after modifying the tar file, assuming that the tar was extracted to files.tar.gz and the script to installer.sh, use the following command:

```
cat files.tar.gz >> installer.sh
```

Note: Making changes to the tar or the script might result in failed installs.

CA EEM uses the following parameters during CA Directory installation. You can configure the parameters based on your needs.

Important! Before customizing the default port numbers ensure that no other services are configured to use the same ports.

-dsaport

Specifies the port that the dsa uses to listen to any requests directed at it.

Default: 509

-ssldport

Specifies the port that the CA Directory uses to listen to the SSLD server. The SSLD server is a background process that handles SSL and TLS authentication, encryption, and decryption for CA Directory.

Default: 21847

-routerport

Specifies the port that the dsa uses to connect to the router dsa. A router DSA has no local data and no datastore. It can only route traffic to other DSAs.

Default: 1684

-dxdbsize

Specifies the maximum size of the datastore for CA EEM.

Default: 500 MB

-dxuser

Specifies a non-dsa user who can install, administer, and uninstall CA Directory. The dxuser can be a local system user or a network user.

Note: If you have installed CA Directory using a local system user as the dxuser, then during uninstallation that local system user may be deleted. So, if you are using a local system user as a dxuser to install CA Directory, ensure that the user is not setup to run any other programs.

-eiamadminpw [password]

Sets the EiamAdmin password to [password]

-eiampath

Sets the path where the CA EEM Server will be installed. The default is /opt/CA/SharedComponents/EmbeddedIAM.

-etdirpath [path]

Sets the path where CA Directory will be installed.

-external_type

Sets the type of external directory.

-external_branch

Sets the branch of external directory.

-external_userdn

Sets the userdn of the external directory.

-external_pw

Sets the password in the munged (encrypted) format.

-external_base

Sets the basedn of the external directory.

-external_host

Sets the host name where the external directory is installed.

-external_port

Sets the port number to which the external directory listens.

These parameters specify various configuration options for connecting the CA EEM Server to an external directory.

Note: The branch option defaults to /iTechPoz/Entities/Users and need not be changed; for Active Directory, the type is ADS.

-igpath [directory]

Sets the iGateway path. The path must be a fully qualified path, such as -iisystem. The default is /opt/CA/SharedComponents/iTechnology.

-javahome [directory]

Sets the JAVA_HOME variable to [directory] when calling the iGateway installer. This parameter defaults to the contents of the JAVA_HOME environment variable and is prompted for only if $JAVA_HOME is null.

Note: If you want to install CA EEM without java, you must set javahome=None.

-logfile [filename]

Causes the installer to write log information to [filename], defaults to /tmp/eiam-install.log.

-nocrc and -ignorechecksum

Forces the installer to skip checksum verification of the tar file contained within the script. This is required only by the teams producing a custom packaged installer.

-noetdir

Does not install CA Directory.

-noetdirsetup

Does not run programs to configure CA Directory.

-noexternal

Specifies that users will not be referred from an external source. This is the default option. However, you can use this parameter to prevent the installer from prompting the user about an external directory.

-noigateway

Skips execution of iGateway_40_linux.sh. The iGateway path provided must point to a pre-existing iGateway, or this installation will not function.

-nosanitytest

Skips the sanity test during installation.

-nosponsors

Skips installation of sponsors and spindles not normally considered part of iGateway. These are installed into the iGateway directory. This option can be used if only Ingres is installed. (By giving -nosponsors and -noigateway).

-silent

Runs the installation in silent mode. If a required parameter is not specified on the command line, the installation aborts and prints an appropriate message. It does not make any changes to the system unless all needed parameters are specified.

-tempdir [directory]

Specifies the directory to use for temp file storage. Default is /tmp/eiam_temp. This must be a fully-qualified path, and must be in its own subdirectory. This script uses rm -rf to remove the directory you specify hereupon script completion.

-useexternal

Specifies that the CA EEM Server should be set to refer an external directory. When this option is given, -external_type, -external_branch, -external_userdn, -external_pw, -external_base, -external_host, and -external_port must also be provided.

-upgrade and -noupgrade

These parameters override the script's default behavior depending on whether an upgrade should be performed or not. An upgrade means that the files in the iGateway directory will be upgraded to the version included in this installer. The iGateway installer will not be invoked, so -noigateway are implied. The igateway path to upgrade defaults to the path contained in the iTechnology location file, and not to /opt/CA/SharedComponents/iTechnology. (You can still use -igpath to force a different path.) This option works only on an iGateway installation that was created by the previous version of the CA EEM installer.

Install Server in Silent Mode

To install CA EEM Server in the silent mode on Linux or UNIX enter the following command at the command prompt:

EEMServer_[*releasenumber*].[*build_number*]_[*name of operating system*].sh -silent -eiamadminpw *password -javahome directory*

Example: The following command for Sun operating environments includes the minimum required parameters:

EEMServer_8.4.0.55_sunos.sh -silent -eiamadminpw *password -javahome directory*

You can specify additional installation parameters. Most install parameters have defaults. For more information about Script Parameters, see Server Installation Script Parameters.

The file is decompressed and the installation begins.

Remove CA EEM Server in Silent Mode

To remove CA EEM Server, run eiamuninstall.sh -silent from the installation directory.

Note: You cannot remove CA EEM Server if any applications are registered. You must unregister all applications before the uninstallation successfully completes. For information about unregistering an application, see the *Online Help*.

Chapter 4: Back Up and Restore CA EEM Server

This section contains the following topics:

File System Back Up (see page 35)
Back Up CA EEM Server Files and Folders (see page 36)
Restore Procedures (see page 36)
Start iGateway Service (see page 37)
Stop iGateway Service (see page 37)

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 in case it is corrupted.

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

Data Description	Files Names on Windows	File Names on Linux
Configuration files	■ iPoz.conf ■ Eiam.conf ■ iPoz.map ■ Spin.conf ■ iPozDsa.pem ■ iPozRouterDsa.pem ■ logDepot.conf ■ calmReporter.conf	■ iPoz.conf ■ Eiam.conf ■ iPoz.map ■ Spin.conf ■ iPozDsa.pem ■ iPozRouterDsa.pem ■ eiam-type ■ Sponsorfiles ■ logDepot.conf ■ calmReporter.conf
Event information	■ logdepotdb ■ calm_catalog folder ■ calm_archive folder	■ logdepotdb ■ calm_catalog folder ■ calm_archive folder

Data Description	Files Names on Windows	File Names on Linux
Folders	■ System Registry ■ iTechnology folder	■ iTechnology folder ■ Environment settings

Back Up CA EEM Server Files and Folders

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 in case it is corrupted.

To back up CA EEM server files and folders

1. Stop iGateway.
2. Back up CA EEM configuration files, event information, and folders.
3. Back up CA EEM data stored in CA Directory.

   The CA EEM server configuration files, events, and folders are backed up.

More Information:

File System Back Up (see page 35)
Backing Up CA EEM Data Stored in CA Directory (see page 39)

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.

More Information:

Backing Up CA EEM Data Stored in CA Directory (see page 39)

Start iGateway Service

You must enter the following commands to start iGateway service:

Windows

net start igateway

Linux and UNIX

$IGW_LOC/S99igateway start

Stop iGateway Service

You must enter the following commands to stop iGateway service:

Windows

net stop igateway

Linux and UNIX

$IGW_LOC/S99igateway stop

Chapter 5: Backing Up CA EEM Data Stored in CA Directory

This section contains the following topics:

Introduction to CA Directory Terminology (see page 39)
How to Use the DXtools (see page 40)
How to Back Up CA Directory Data (see page 42)
How to Restore CA Directory Data (see page 46)

Introduction to CA Directory Terminology

This section explains the CA Directory terminology used in this document:

DSA

A *DSA* is a process that manages some or all of a directory's namespace. When installing CA EEM server, you can configure the following CA Directory related parameters:

DXmanager

DXmanager is a web application that lets you create, configure, monitor, and control your directory backbone.

DSA console

The *DSA console* lets you connect to a DSA to give DXserver commands, receive trace information, and act as a user agent.

DXtools

The *DXtools* are a set of command-line utilities that come with CA Directory. These tools help you manage directory administration, work with LDIF data, load and unload data to and from a directory, and to extract and convert schemas for use with CA Directory.

LDIF (LDAP Data Interchange Format)

LDIF files are text files that store directory information in LDIF. You can use LDIF files to transfer directory information between LDAP directory servers or to describe a set of changes to be applied to a directory.

How to Use the DXtools

You can run the DXtools in the following ways:

- Run the DXtools commands on the host, using the DSA console.
- Run the DXtools commands on a remote host, using the DSA console over a TCP/IP network.
- Include the DXtools commands in your scripts.

All tools return zero on success and non-zero when an error occurs.

DXHOME Environment Variable

Some tools require that the DXHOME environment variable is set to the home path of DXserver. This is done automatically when CA Directory is installed.

Some tools expect the DSA configuration files to be located in the *config* folder under the path in DXHOME.

Exit Status Codes for the DXtools

The DXtools share common exit codes, though not all exit codes apply to all tools. The exit codes are as follows:

0

Success

1

The corresponding DSA is running.

2

One or more of the datastore files already exists.

3

The specified directory location either does not exist or is not a directory.

4

The specified file is the wrong type, for example is a directory.

5

There is a permissions problem with this file.

6

The full path name of the datastore file is too large. This may be because the location specified for the datastore directory is too long.

7

An error occurred when trying to remove the old datastore files.

8

An error occurred when trying to rename the old datastore files.

9

An error occurred when trying to create or pad one of the files.

10

The datastore size is less than or equal to zero.

11

There was not enough space on the device or no memory available when trying to create the file.

12

There was insufficient access (perhaps because permissions were insufficient) to create the file or to set the access on the file.

13

The DXHOME environment variable is not set.

14

The DXHOME environment variable is not valid.

15

The corresponding DSA already exists.

16

The created DSA failed to start. Check its log files for details.

17

Incorrect or unknown command line parameters were provided.

18

The corresponding DSA does not exist.

How to Back Up CA Directory Data

Use the following process to back up CA Directory data:

1. Connect to a local DSA.
2. Take a snapshot copy of the datastore of the running default DSA. This process is called an online dump. Use the following command to take the snapshot:

   `dump` *dxgrid-db*

   Note: Replace dxgrid-db with the dsa name iTechPoz-Servern for backing up CA EEM.
3. Use the DXdumpdb tool to back up the online dump (.ZDB files), that is the snapshot copy of the datastore to an LDIF file.

More Information:

Connect to a Local DSA Console (see page 42)
Online Datastore Dump (see page 43)
dump dxgrid-db Command—Take a Consistent Snapshot Copy of a Datastore (see page 44)

Connect to a Local DSA Console

You can connect to a DSA locally on UNIX or Windows if a console port has been set for that DSA.

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.

Online Datastore 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.

The datastore files are copied to files with extensions starting .z:

- A database file *dxgrid-db*.zdb
- An attributes file *dxgrid-db*.zat
- An object classes file *dxgrid-db*.zoc

Note: Each dump overwrites the previous backup files. If you want to save the backup files, copy them to another location before the next dump.

dump dxgrid-db Command—Take a Consistent Snapshot Copy of a Datastore

The *dump dxgrid-db* command takes a consistent snapshot copy of the datastore of a running DSA (an online dump). The DSA completes any updates before carrying out this command and does not start any more updates until the copy is finished.

The datastore files are copied to files with extensions starting .z:

- A database file *dxgrid-db*.zdb
- An attributes file *dxgrid-db*.zat
- An object classes file *dxgrid-db*.zoc

Note: Each dump overwrites the previous backup files. If you want to save the backup files, copy them to another location before the next dump.

The DXdumpdb tool can export data from a datastore created by the dump command.

The command has the following format:

```
dump dxgrid-db [period start period];
```

period *start period*

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

start

Defines the number of seconds since Sunday 00:00:00 am GMT.

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

period

Defines the number of seconds between online dumps.

Example: Perform an Online Dump Every Hour

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

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

Note: Make sure you create a cron job on UNIX or a scheduled task on Windows to copy the backed up files to a safe location. Each dump overwrites the previous backup files.

Using an LDIF file to Back Up and Load Data

LDIF files are text files that store directory information in LDIF. You can use LDIF files to transfer directory information between LDAP directory servers or to describe a set of changes to be applied to a directory.

CA Directory comes with the DXdumpdb tool, which lets you unload data from a datastore into an LDIF file. You can then later load the data from the LDIF file into a datastore to recover the directory content.

Back Up a Directory to an LDIF File

To back up a directory to an LDIF file

1. Log in as the user *dsa* (on UNIX) or the DXserver 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 where the data is dumped.

   -z

   Specifies that DXdumpdb dumps from the copy of the datastore that is produced by the console command dump dxgrid-db.

   dsaname

   Specifies the name of the DSA.

DXdumpdb Tool—Export Data from a Datastore to an LDIF File

Use the DXdumpdb tool to export data from a datastore to an LDIF file.

Note: For a list of the status codes returned by all the DXtools commands, including this command, see Exit Status Codes for the DXtools (see page 40).

This command has the following format:

dxdumpdb *options DSA*

options

Denotes one or more of the following options:

-f *filename*

Specifies the file to receive the exported data. If this option is not specified, the output goes to standard output or the screen.

-v

Runs in verbose mode. This option switches on error and status tracing. For the -v option to work, you must also specify the -f option.

-z

Specifies that DXdumpdb dumps from the copy of the datastore that is produced by the console command *dump dxgrid-db*.

DSA

Defines the DSA. DXdumpdb looks in the configuration files of this DSA to find the datastore to export to an LDIF file.

Example: Extract Democorp Data to Screen

The following example prints the LDIF format data from the datastore of the *democorp* DSA to the screen:

```
dxdumpdb democorp
```

Example: Back up an online data store dump

The following example exports an online data store dump to an LDIF file.

```
dxdumpdb -f eembackup -z iTechPoz-Servern
```

How to Restore CA Directory Data

Use the following process to restore CA Directory:

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

DXloaddb Tool—Load a Datastore from an LDIF File

Use DXloaddb to load a datastore from a LDIF file. The datastore must already exist. All previous information in the datastore is deleted.

Usage notes:

- The LDIF file does not need to be sorted.
- DXloaddb hashes any password entry in the LDIF file that is in clear text.

  If a hash algorithm is specified in the DSA configuration, DXloadbdb uses that. Otherwise it uses SHA-1.
- By default, DXloaddb uses the DSA's configuration for operational attribute handling:
  - If *op-attrs* = *true* then any operational attributes in the LDIF file are loaded into the datastore.

    Any entries in the LDIF file that do not have a createTimestamp, have a creatTimestamp added to the datastore.
  - If *op-attrs* = *false* then operational attributes in the LDIF file are ignored and no operational attributes are created by the DXloaddb.

This command has the following format:

`dxloaddb [options] dsa ldif-file`

options

Denotes one or more of the following options:

-n

Specifies that DXloaddb does not do any actions.

-O

Specifies that DXloaddb includes standard operational attributes, such as password policy (for example, number of login attempts), and time stamp attributes. If this option is specified, DXloaddb creates any operational attributes that are not defined in the LDIF file.

-s

Specifies that DXloaddb produces the following statistics concerning the datastore:

- Total data size in MB
- Total number of entries
- Number of entries ignored
- Amount of padding in the datastore file in KB
- Average number of entries per MB

-v

Specifies verbose output.

ldif-file

The name of the LDIF file to load into the datastore.

DSA

Defines the DSA whose datastore is to be loaded.

Example: Create and Load a Datastore

The correct sequence in which to create and load a datastore is:

```
dxnewdb
dxloaddb
```

Example: Load LDIF Data into Datastore

The following example loads the data from democorp.ldif file to datastore democorp:

```
dxloaddb democorp democorp.ldif
```

The following is a possible part of democorp.ldif :

```
dn: o=Democorp, c=US
oc: organization
dn: ou=Administration, o=Democorp, c=US
oc: organizationalUnit
dn: cn=Fred Jones, ou=Administration, o=Democorp, c=US
oc: organizationalPerson
postalAddress: 11 Main Street $ Newtown
surname: Jones
title: Manager
telephonenumber: +1 (123) 456 7890
telephonenumber: +1 (987) 654 3210
dn: ou=Sales, o=democorp, c=US
oc: organizationalUnit
```

Telephonenumber appears twice because it is a multi-valued attribute

Chapter 6: Integrating With CA SiteMinder

This section contains the following topics:

How You Integrate CA SiteMinder with CA EEM (see page 49)
How You Integrate CA SiteMinder r12 With CA EEM (see page 50)

How You Integrate CA SiteMinder with CA EEM

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

- Create an agent in CA SiteMinder for communication between CA EEM and CA 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 CA SiteMinder User Directory for authorization, which is used by CA EEM to retrieve LDAP attributes. Ensure the UniversalID field uniquely identifies a user in the directory on the User attributes tab.
- Create a CA 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 CA SiteMinder domain and add the User Directories, administrator, and Realm to the domain.

For more information about CA SiteMinder, see the CA SiteMinder documentation.

How You Integrate CA SiteMinder r12 With CA EEM

You must use the following procedure to integrate CA SiteMinder r12 with CA EEM.

Note: You cannot use this procedure to integrate CA SiteMinder r12 with CA EEM on Solaris and AIX platforms.

To integrate with CA SiteMinder r12 with CA EEM, you must perform the following steps on the CA EEM server:

1. Stop iGateway service.
2. Go to the iTechnology folder, and replace the following folders or files with the corresponding files extracted from CA SiteMinder r12 SDK:

   UNIX

   Replace bin, EPTKI libs, and Java so files.

   Windows

   Replace bin, EPTKI libs, and Java SMr12 dlls.
3. Start iGateway service.

More Information:

Start iGateway Service (see page 37)
Stop iGateway Service (see page 37)

Chapter 7: Configuring Failover

This section contains the following topics:

Failover (see page 51)
Data Store Failover (see page 51)
CA EEM Server Failover (see page 59)
Configure CA EEM Files (see page 60)

Failover

Failover is the ability to ensure uninterrupted data flow and operability even when the data becomes unavailable.

For the CA EEM failover to work, you must attach an application to the CA EEM installed on a server to obtain information about other servers. The information about other server configuration is available in the iPoz.conf file that is used for failover.

Note: When you configure servers for failover, an application instance registered in the iPoz.conf file of the CA EEM server is not automatically updated in the iPoz.conf file of the replicated servers. You must manually add an entry for the application instance in the iPoz.conf file of each replicated server.

You can configure CA EEM to support two types of failover scenarios:

- Data store failover (see page 51)
- Server failover (see page 59)

Note: In this scenario, we assume the host names are Server1 and Server2.

Data Store Failover

The CA EEM Server uses CA Directory as its data store. The directory provides built-in support for failover and recovery.

How You Configure CA Directory

To configure CA Directory to support replication and failover, with Server1 as the preferred master:

1. Install CA EEM Server on the server hosts (Server1 and Server2) and synchronize their system time.
2. Configure data stores for replication.
3. Enable Failover.

Configure the Knowledge Files

The knowledge files provide reference to servers for data store replication configuration. You must configure the following knowledge files:

- Data knowledge file (iTechPoz-Server1.dxc) to add the host name of server

To configure knowledge files

1. Open the knowledge directory.
   - **Windows:** use the Run command in Start menu and enter %DXHOME%\config\knowledge
   - **Linux and UNIX:** ~dsa/config/knowledge
2. Open and edit the Server1 knowledge file (iTechPoz-Server1.dxc) as follows:
   - Modify the following entries:

```
tcp localhost port 509

dsa-name = <cn iTechPoz><cn PozDsa>
```

   - To read:

```
tcp "Server1" port 509, tcp localhost port 509

dsa-name = <cn iTechPoz><cn PozDsaServer1>
```

- Add the following entry after the auth-levels line and before the link-flags line

```
dsa-flags = multi-write
```

3. Save and close the Server1 knowledge file.
4. Open and edit the Server2 knowledge file as follows:
   - Modify the following entries:

```
tcp localhost port 509

dsa-name = <cn iTechPoz><cn PozDsa>
```

   - To read:

```
tcp "Server2" port 509, tcp localhost port 509

dsa-name = <cn iTechPoz><cn PozDsaServer2>
```

   - Add the following entry after the auth-levels line and before the link-flags line.

```
dsa-flags = multi-write
```

5. **(Optional)** To enable one way replication, set the dsa-flags on Server2 as follows:

```
dsa-flags = multi-write, shadow
```

   Note: In one way replication, updates between servers always occurs in only one direction. For example, if you set up Server1 and Server2 in a one way replication set up with Server1 as the master, then whenever Server1 is updated the changes are replicated on Server2; any updates on Server2 are not replicated on Server1.
6. Save and close the Server2 knowledge file.
7. Copy the following knowledge files from Server1 to knowledge directory of Server2:
   `iTechPoz-Server1.dxc`
   `iTechPoz-Server2.dxc`
8. (Optional) To enable one way replication, edit the file iTechPoz-Server1.dxc, copied from Server1, as following:
   - dsa-flags = multi-write

   To read:
   - dsa-flags = multi-write, read-only

   Note: This makes sure that changes from the Server2 do not get propagated to Server1.
9. Copy the certificate files of Server1 to Server2 and from Server2 to Server1 as follows:

   Note: Certificate files are found in the %DXHOME%\config\ssld\personalities directory

- Copy the files itechpoz-server1.pem and itechpoz-server1-router.pem from Server1 to Server2
- Copy the files itechpoz-server2.pem and itechpoz-server2-router.pem from Server2 to Server1

10. Create a new iTechPoz-trusted.pem file by concatenating the contents of iTechPoz-trusted.pem of Server1 and iTechPoz-trusted.pem of Server2.

    Note: iTechPoz-trusted.pem file can be found in %DXHOME%\config\ssld directory.

11. Copy the new iTechPoz-trusted.pem to both Server1 and Server2 to overwrite the existing files.
12. Backup the Server1 data store.
13. Copy the LDIF file creates as part of the Server1 backup.
14. Load the LDIF file from Server1 backup into Server2.

More Information:

How to Back Up CA Directory Data (see page 42)
Examples for Configuring Knowledge Files (see page 55)

Examples for Configuring Knowledge Files

The following examples contain sample code for configuring the following files for data store failover:

- Data knowledge file (iTechPoz-Server1.dxc) to add the host name of server
- Router knowledge file (iTechPoz-Server1-Router.dxc) to add the host information in the router
- Group knowledge file (iTechPoz.dxg) to achieve group knowledge that all (Directory System Agent) DSAs in the domain can access

Example: Configuring Server1 Router Knowledge File

```
#
# iTechPozRouter - iTechnology rePOZitory
#
set dsa "iTechPoz-Server1-Router" =
{
prefix       = <cn iTechPozRouter>
dsa-name     = <cn iTechPozRouter><cn PozDsaServer1>
dsa-password = "{MD5}rMx+fEvmsStrQzYrrrhjjQ=="
…
};
```

Example: Configuring Server1 Knowledge File

```
#
# iTechPoz - iTechnology rePOZitory
#
set dsa "iTechPoz-Server1" =
{
prefix       = <cn iTechPoz>
dsa-name     = <cn iTechPoz><cn PozDsaServer1>
dsa-password = "{MD5}rMx+fEvmsStrQzYrrrhjjQ=="
address      = tcp "Server1" port 509, tcp localhost port 509
…
dsa-flag = multi-write
link-flags   = ssl-encryption-remote
};
```

Example: Configuring Server2 Router Knowledge File

```
#
# iTechPozRouter - iTechnology rePOZitory
#
set dsa "iTechPoz-Server2-Router" =
{
prefix       = <cn iTechPozRouter>
dsa-name     = <cn iTechPozRouter><cn PozDsaServer2>
dsa-password = "{MD5}rMx+fEvmsStrQzYrrrhjjQ=="
```

```
address      = tcp localhost port 1684
…
};
```

Example: Configuring Server2 Knowledge File

```
#
# iTechPoz - iTechnology rePOZitory
#
set dsa "iTechPoz-Server2" =
{
prefix       = <cn iTechPoz>
dsa-name     = <cn iTechPoz><cn PozDsaServer2>
dsa-password = "{MD5}rMx+fEvmsStrQzYrrrhjjQ=="
address      = tcp "Server2" port 509, tcp localhost port 509
…
dsa-flag = multi-write
link-flags   = ssl-encryption-remote
};
```

Example: Configuring Group Knowledge File

```
# iTechPoz - iTechnology rePOZitory
# Source the knowledge files of the iTechPozRouter and iTechPoz DSAs.
source "iTechPoz-Server1-Router.dxc";
source "iTechPoz-Server2-Router.dxc";
source "iTechPoz-Server1.dxc";
source "iTechPoz-Server2.dxc"
```

Enable Failover

You must enable failover to successfully configure the data store failover. You must modify the following files to enable failover:

- Router knowledge file (iTechPoz-Server1-Router.dxc) to add the host information in the router
- Group knowledge file (iTechPoz.dxg) to achieve group knowledge that all (Directory System Agent) DSAs in the domain can access

Note: Ensure that you have configured the data stores for replication before enabling failover.

To enable failover

1. Open and edit the Server1 router knowledge file (iTechPoz-Server1-Router.dxc) as follows:
   - Modify the following entry:

     ```
     dsa-name = <cn iTechPozRouter><cn PozDsa>
     ```

   - To read:

     ```
     dsa-name = <cn iTechPozRouter><cn PozDsaServer1>
     ```

2. Save and close the Server1 router knowledge file.
3. Open and edit the Server2 router knowledge file (iTechPoz-Server2-Router.dxc) as follows:
   - Modify the following entry:

     ```
     dsa-name = <cn iTechPozRouter><cn PozDsa>
     ```

   - To read:

     ```
     dsa-name = <cn iTechPozRouter><cn PozDsaServer2>
     ```

4. Save and close the Server2 router knowledge file.
5. Edit the group knowledge file (iTechPoz.dxg) and set the preferences to the new data and router knowledge files on Server1 and Server2.
6. Copy the certificate files of Server1 to Server2 and from Server2 to Server1 as follows:

   Note: Certificate files are found in the %DXHOME%\config\ssld\personalities directory
   - Copy the file itechpoz-server1-router.pem from Server1 to Server2
   - Copy the file itechpoz-server2-router.pem from Server2 to Server1
7. Enter the following commands to stop and start all services:

   Windows

   ```
   dxserver stop all
   ```

```
ssld stop
ssld start
dxserver start all
```

Linux and UNIX

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

CA EEM Server Failover

Note: Ensure you install the same version of CA EEM Server on both the server hosts (Server1 and Server2) and synchronize their system time.

You can configure Server1 to trust the sessions and certificates of Server2.

To configure server1 for failover

1. Enter the URL https://server1:5250/spin.
2. Select iTech Administrator, and click Go.

   The Login screen appears.
3. Enter the login credentials as follows based on your selection of the option Type in the Login screen:

   Host

   Login as root or administrator.

   iAuthority

   Login as eiamadmin.
4. Click the Configure tab, add Server2 as Hostname in the Trusted iAuthority Hosts pane and click Trust.

   An entry in added in iControl.conf file and Server1 starts trusting sessions from Server2.
5. Click the iAuthority tab, enter Label as Server2, browse to the location of PEM Certificate file in the Add Trusted Root pane and click Add Trusted Root.

   Note: The PEM certificate file (rootcert.pem) is located in the iTechnology directory of Server2.

   An entry is added in iAuthority.conf and Server1 starts trusting certificates from Server2.

You must also configure Server2 to trust the sessions and certificates of Server1.

To configure server2 for failover

1. Enter the URL https://server2:5250/spin.
2. Select iTech Administrator.
3. Log in as root or administrator by selecting Host or as eiamadmin by selecting iAuthority.
4. Click the Configure tab, add Server1 as Hostname in the Trusted iAuthority Hosts pane and click Trust.

An entry is added in iControl.conf file and Server2 starts trusting sessions from Server1.

5. Click the iAuthority tab, enter Label as Server1, browse to the location of PEM Certificate file in the Add Trusted Root pane and click Add Trusted Root.

   Note: The PEM certificate file (rootcert.pem) is located in the iTechnology directory of Server1.

   An entry is added in iAuthority.conf and Server2 starts trusting certificates from Server1.

Configure CA EEM Files

You must configure CA EEM Server1 to receive the list of available servers to fall back on, which are replicated versions.

To configure CA EEM Server1

1. Open the iTechnology directory of Server1.
   - **Windows**: %IGW_LOC%
   - **Linux and UNIX**: /opt/CA/SharedComponents/iTechnology (Default)
2. Open the iPoz.conf file and add the following tag:

   ```
   <BackboneMember>Server2</BackboneMember>
   ```

3. Stop and start iGateway.

   Windows

   ```
   net stop igateway
   net start igateway
   ```

   Linux and UNIX

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

You must also configure CA EEM Server2 to receive the list of available servers to fall back on, which are replicated versions.

To configure CA EEM Server2

1. Open the iTechnology directory of Server2.
   - **Windows**: %IGW_LOC%
   - **Linux and UNIX**: /opt/CA/SharedComponents/iTechnology (Default)
2. Open the iPoz.conf file and add the following tag:

   ```
   <BackboneMember>Server1</BackboneMember>
   ```
3. Stop and start iGateway.

   Windows

   ```
   net stop igateway
   net start igateway
   ```

   Linux and UNIX

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

Chapter 8: Configuring External Directory Server Support

This section contains the following topics:

Configure External Directory Server Support (see page 63)
Configure External Directory Failover Support (see page 64)
Connecting to LDAP Servers over SSL (see page 64)

Configure External Directory Server Support

You can use CA EEM to communicate with an external directory server for user authentication and authorization using the LightWeight Directory Access Protocol (LDAP).

You must enter the values for external directory servers in the iPoz.conf file located in /CA/SharedComponents/iTechnology folder after the installation.

Note: You must stop iGateway before making any changes to the iPoz.conf file and restart it afterwards.

UseExternalAuthDirectory

Specifies whether you want to use a different external directory for Authentication. Type True to use a different external directory. The default is False.

ExternalAuthDirType:

Specifies the type of external directory. Currently supported types include CA Identity Manager, Custom Mapped Directory, Microsoft Active Directory, Novell eDirectory, Novell eDirectory-CN, and Sun One Directory.

ExternalAuthDirUserDn

Specifies the UserDn for the type of external directory specified.

ExternalAuthDirPassword

Specifies the user password in the encrypted format.

Note: You must munge the password using the following command and paste it in the ipoz.conf file.

```
/iTechnology/safex -munge <password in clear text>
```

ExternalAuthDirHost

Specifies the host name on which the external directory has been configured.

ExternalAuthDirPort

Specifies the port to which the external directory listens.

ExternalAuthDirUserSearchPreFilter

Specifies the pre search filter as per the external directory. You can search for any object class such as, users.

ExternalAuthDirUserSearchPostFilter

Specifies the post search filter as per the external directory. You can search for any object class such as, users.

Configure External Directory Failover Support

You can extend the capability of CA EEM to fall back on another external directory server that is a replicated version of the server.

This can be accomplished by providing the mapping in the iPoz.conf.

Note: You must stop iGateway before making any changes to the iPoz.conf file and restart it afterwards.

ExternalDirHostBackup

Specifies the host name of the replicated external directory server.

ExternalAuthDirHostBackup

Specifies the host name of the different external directory server to be used for user authentication.

Connecting to LDAP Servers over SSL

To establish an SSL connection to LDAP servers you must have the following certificates:

Certificate Authority Certificate

You can obtain this certificate from a Certificate Authority, for example Verisign or Thwate. This certificate indicates that certificates issued by this Certificate Authority are valid and can be trusted.

LDAP Server Certificate

You must obtain this certificate from a trusted Certificate Authority. This certificate contains information about the LDAP server and identifies the LDAP server with the client.

Note: CA EEM supports only .pem certificates for SSL connections.

How CA EEM Connects to LDAP Server Over SSL

The following process explains how the CA EEM server and the LDAP server communicate over SSL.

1. The CA EEM server connects to the LDAP server using a Certificate Authority certificate.
2. The LDAP server verifies the Certificate Authority certificate, and if the certificate is valid establishes a handshake with the CA EEM server.
3. The LDAP server sends its public key to the CA EEM server during the handshake. The public key is used to encrypt data that is sent to the LDAP server.
4. The CA EEM server uses the public key to encrypt data and sends the data to the LDAP server.
5. The CA EEM server send username and password to authenticate against LDAP server.

How to Configure the SSL Connections

You must follow the following process to configure SSL communication between the LDAP server and the CA EEM server:

1. Configure the LDAP server to use certificates
2. Configure the CA EEM server to communicate over SSL

Configure the LDAP Server to Use SSL Certificates

To configure the LDAP server to use SSL, you must do the following steps:

1. Obtain a Certificate Authority certificate and install the certificate in the trusted certificate store on your LDAP server.
2. Obtain a server certificate from the Certificate Authority and install the certificate in the server certificate store of your LDAP server.
3. Enable the LDAP server to accept SSL connections.

Enable SSL in CA EEM Server

To enable SSL in the server

1. Copy the certificate of Certificate Authority from the LDAP server and save it to the computer where CA EEM server is running.
2. Open the ipoz.conf file and edit the following tags:

   <ExternalDirSSL>

   Specifies if SSL communication is enabled or disabled. You must set this tag to "true" to enable SSL communication.

   <ExternalDirCACertPath>

   Specifies the path where the certificate of Certificate Authority is stored on the computer where CA EEM server is running.
3. Restart igateway.

Chapter 9: Configuring Support for Large Numbers of Policies

This section contains the following topics:

Support for Large Number of Policies (see page 67)
Configure Additional Settings for CA EEM Server on AIX (see page 67)
Client Configuration (see page 67)

Support for Large Number of Policies

Note: CA EEM provides support for large number of policies only in C++ SDK enabled client environment.

You must configure the CA EEM Server and clients before registering applications that use a large number of policies.

Note: CA EEM supports up to 20,000 policies on the HP-UX platform.

Configure Additional Settings for CA EEM Server on AIX

You must perform the following additional steps to configure the CA EEM Server to support the use of a large number of policies on AIX.

To configure CA EEM Server on AIX

1. Modify the network settings using the following command at the AIX command prompt:

   ```
   no -o tcp_nodelayack=1
   ```

2. Increase the process limit using the following command at the AIX command prompt:

   ```
   ulimit -d unlimited
   ulimit -f unlimited
   ```

Client Configuration

You must configure client to support the use of a large number of policies.

Configure Client for all Operating Systems

To support the deployment of a large number of policies, you must configure clients for all operating systems:

- Increase the application cache update time to avoid cache updates during registering applications using Safex.

  For more information about cache update, see the *Programming Guide.*

  Note: We recommend setting the cache update time to 3600 seconds during registration to avoid cache updates during registration. After registration, change the cache update time to 30 seconds, which is the default setting.

- Enable Reliable Event Delivery.

  For more information about Reliable Event Delivery, see the *Programming Guide*.

Chapter 10: Archiving Events

This section contains the following topics:

Overview (see page 69)
Utility to Defrost Cold DB Files (see page 70)

Overview

CA EEM lets you generate and manage reports for events generated by the CA EEM Server. The archiving system organizes archived files into the following three states:

Warm db Files

Refers to the archive files created once the number of events exceeds Maximum Rows in an event database. Warm archived files are available for querying and reporting from CA EEM server. No data can be inserted into a warm db file. Warm db files are available in CA EEM server only for the number of days specified as Max Archive Days in Event Log Settings.

Cold db Files

Refers to the archive files in warm state that are backed up manually to another location. You cannot query or create reports from a cold db file. The cold db files need to be defrosted before they can be used for querying or reporting.

Defrosted db Files

Refers to the archive files in cold state that are restored so that users can query or generate reports from CA EEM server. Defrosted db files are available in the archive directory only for the number of hours specified as Event Policy in Event Log Settings.

To change Event Log Settings

1. Log in to CA EEM.

   The CA EEM home page appears.

2. Click Manage Reports, Configuration, Services, Event Log Settings.

   The event log settings appear.

Note: For more information about configuring services to manage reports, see the *Online Help*.

More Information:

Defrost Cold DB Files (see page 72)

Utility to Defrost Cold DB Files

CA EEM provides a utility to defrost cold db files. You must both restore and defrost the files from cold to warm state before you can run queries against the files and view live reports. The sem utility provides this functionality. You can download the sem utility from support at http://ca.com/support.

To set up sem utility

1. Extract the sem utility compressed files.
2. Set environment variables based on your operating system:

   Linux or Solaris

   ```
   Export LD_LIBRARY_PATH = <sem_Extraction_Folder>:$LD_LIBRARY_PATH
   ```

   AIX

   ```
   Export LIBPATH = <sem_Extraction_Folder> :$LIBPATH
   ```

   HP-UX

   ```
   Export SHLIB_PATH= <sem_Extraction_Folder> :$SHLIB_PATH
   ```

Note: For Windows, to set up sem utility, from the command line you must navigate to the extracted folder and run sem.exe.

More Information:

Defrost Cold DB Files (see page 72)

SEM Utility Syntax

The sem utility has the following syntax:

sem -h <hostname> -u <user> -p <password> -listcolddb | -defrost <archive>

-h

Specifies the hostname of the computer where the cold db files are stored.

-u

Specifies the user name used to authenticate with CA EEM server.

-p

Specifies the password for a user name used to authenticate with CA EEM server.

-listcolddb

Lists all the cold db files stored on the host computer.

-defrost <archive>

Defrosts the specified archive file.

The following table explains return values of the sem utility:

Return Value	Description
0	Success
1	Invalid arguments
2	Invalid username
3	Authentication Failed
4	Failed to list cold db files
5	Failed to defrost a cold db file

Defrost Cold DB Files

You must both restore and defrost the files from cold to warm state before you can run queries against the files and view live reports.

Note: Before defrosting, the cold db files must be copied to the archive directory iTechnology\calm_archive.

To restore and defrost cold db files

1. Run the sem utility from the command line to retrieve a list of all cold db files.

   sem -h <*hostname*> -u <*username*> -p <*password*> -listcolddb

2. Run the sem utility to defrost cold db files.

   sem -h <*hostname*> -u <*username*> -p <*password*> -defrost <*archive*>

   The cold db files are restored and defrosted.

More Information:

Overview (see page 69)

Appendix A: Upgrading and Troubleshooting CA Directory Installation

Upgrade CA Directory

This procedure covers the case where you have an older release of CA Directory running on a Windows computer, and you want to upgrade it to the latest version.

Note: Before you start, ensure that each database has only one DSA.

To upgrade Directory

1. Log in as a user with Administrator privileges.
2. Download the latest versions of CA Directory from the following location:

   https://support.ca.com/irj/portal/anonymous/prdxrefsoln?productID=160
3. Navigate to the downloaded folder and run DXSetup.exe.

   The installation wizard starts.
4. When prompted, specify the location of the backup.
5. Click Migrate.

   The upgrade process backs up your data in the location you specified.
6. When prompted to choose an installation type, we recommend that you choose a custom installation.
7. When prompted, supply the requested information as required.

   The installation process completes the upgrade and creates a backup as requested.
8. When prompted, confirm that you want to restore your configuration and databases.

   The installation process restores the data that the installation process backed up in step 4.

   The message Restoration is complete appears.
9. Click OK and exit the installation wizard.

   The installation process completes and installs the product on your computer.

How to Estimate the Time to Upgrade a DSA From r8.1

To estimate the time you need to do the upgrade, add the time it takes to complete each of the following tasks:

- Data dump to an LDIF file

  The installation process does this. Allow about five minutes per million entries.

- Software installation

  This takes less than half an hour.

- Data load from the LDIF file

  The installation process does this. Allow between one and five minutes per million entries.

Note: The times to dump and load vary, depending on your hardware configuration.

Troubleshooting

This section describes how to deal with problems that might occur during or after installing or upgrading CA Directory.

Troubleshooting on UNIX

This section describes how to deal with problems that might occur during or after installing or upgrading CA Directory.

DXadmind Times Out after Upgrading

Valid on UNIX

Symptom:

After I upgrade CA Directory, DXadmind times out when started.

Solution:

This problem occurs because DXadmind is already running.

In a standard upgrade for DXserver, the upgrade process stops and restarts DXadmind when the upgrade is complete. However, if you cancel the installation for DXserver during the process, DXadmind may not have stopped. As a result, it times out when it tries to restart.

To fix the problem, you need to stop and restart DXadmind.

To stop and restart DXadmind

1. Enter the following command:

   ```
   dxadmind status
   ```

   The status of Dxadmind appears.

2. Log in as the DXserver administrator.

   Note: You need to be logged in as the DXserver administrator to run the command dxadmind start.

   By default, the user name for the DXserver administrator is dsa.

3. Enter the following command:

   ```
   dxadmind stop
   ```

   DXadmind stops.

4. Enter the following command:

   ```
   dxadmind start
   ```

   DXadmind restarts.

5. If DXadmind times out again, do the following:

   a. Enter the following command:

      ```
      ps -ef | grep dxadmind
      ```

      The command finds the Dxadmind process and a response which includes a line similar to the following appears:

      ```
      dsa 6204 1 0 21:23:34 ? 0:00 dxadmind start
      ```

      In this example, the process name is dxadmind, and the process number is 6204.

   b. Enter *either* of the following commands:

      ```
      pkill dxadmind
      ```

      ```
      kill 6204
      ```

      DXadmind ends.

   c. Enter the following command:

      ```
      dxadmind start all
      ```

      DXadmind restarts.

Troubleshooting on Windows

This section describes how to deal with problems that might occur during or after installing or upgrading CA Directory.

Note: For descriptions of messages that can appear during installation, see Installation Error Messages on Windows in the *Reference Guide*.

Cannot Connect to CA Directory from Remote Computer

Valid on Windows

Symptom:

I am not able to connect to CA Directory from another computer.

Solution:

This happens because the firewall is on by default.

Disable the firewall. This means all ports are open and you do not need to configure any port

If you do not want to disable the firewall completely, use one of the following solutions:

To allow access to all ports used by CA Directory

1. Open Control Panel.
2. Click Windows Firewall.

   The Windows Firewall dialog appears.
3. Click the Exceptions tab, and then click Add Program.

   The Add a Program dialog box appears.
4. Click Browse to locate dxserver.exe and then click OK.

   Windows adds the program to the list on the Exceptions tab.

   This opens all the ports that CA Directory uses.
5. Click OK.
6. On the Exceptions tab, select the check box next to dxserver.exe, and then click OK.

   If you later decide that you do not want the program to be an exception, clear this check box.

To open a single port

1. Open Control Panel.
2. Click Windows Firewall.

   The Windows Firewall dialog appears.
3. Click the Exceptions tab, then click Add Port.

   The Add a Port dialog box appears.
4. Complete the following fields in the Add a Port dialog box:

   Port Number

   Specifies the number of the port you want to open.

   Example: Port 2125 specifies DXadmind.

   Name

   Specifies the name of the port.

   Example: DXadmind.

   TCP

   Specifies a TCP port.

   The new service is added to the Exceptions list.

   Click OK.

To permit connections to a specific DSA only, add the port number for that specific DSA. For example, add port number 19389 for access to the Democorp DSA only.

Note: In this case, do not add dxserver.exe to the exception list.

Need to Diagnose a CA Directory Startup Problem

Valid on UNIX

Symptom:

I am having a problem with CA Directory startup that I need to diagnose.

Solution:

The /etc/init.d/dxserver script starts and stops CA Directory at system boot and shutdown. This starts and stops SSL daemons, DXadmind, and any DSAs marked for autostart.

The script writes a log called dxserver-rc.log, usually in the DXserver logs directory, DXHOME/logs (if DXHOME is not defined, then look for this file in the /tmp directory). This log shows each of the processes started or stopped.