CA Embedded Entitlements Manager

Release Notes

Release 12.51

CA Technologies Product References

This document references the following CA Technologies products:

- CA Embedded Entitlements Manager (CA EEM)
- CA Directory
- CA SiteMinder®

Documentation Changes

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

- Operating System Support—Deleted. See the CA Embedded Entitlements Manager Compatibility Matrix on the CA Support site.
- Native 64-bit Support for UNIX Platforms (see page 21)—Added to describe that CA EEM now supports 64-bit UNIX platforms
- Certificates with Custom Key Length (see page 21)—Added to describe that CA EEM now supports certificates with custom key length.
- Support for Windows 2012 Server (see page 21)—Added to describe that CA EEM now supports Windows 2012 Server.
- Support for Kerberos Authentication (see page 22)—Added to describe that CA EEM now supports Kerberos authentication.
- CA EEM SDK Enhancement (see page 22)—Added to describe that CA EEM now provides an API to get CA EEM Server properties.
- Changes to the Failover Configuration Tool (see page 25)—Added to describe that the failover tool supports certificates with custom key length.
- Fixed Issues (see page 27)—Added to list the issues that were fixed in the previous releases.
- CA EEM Installation on Non-English Operating System (see page 42)—Added to describe that CA EEM installation can be performed only if certain conditions are met.

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Contents

Chapter 1: Welcome

Welcome to CA Embedded Entitlements Manager (CA EEM). This document contains information about product installation considerations, operating system support, new features, changes to existing features, known issues, third-party acknowledgments, and information about contacting CA Technical Support.

Note: We recommend that you refer the CA EEM documentation or the Authentication Server topics in your product documentation to understand the CA EEM features used by your product.

Chapter 2: System Requirements

This section contains the following topics:

Windows

The minimum system requirements are:

- An Intel Pentium or higher computer with a CD-ROM drive
- At least 4 GB of RAM
- 10GB of hard disk free space, plus enough space for the directory data
- At least 300 MB disk space required under the temporary directory %temp% (C:\Documents and Settings\Administrator\Local Settings\Temp\) where the CA EEM installation files are extracted during installation
- Windows updates applied, that is Windows Installer v3 or later
- Winsock-compatible TCP/IP installed and configured
- Windows administrator access to the system
- Adobe Acrobat Reader 8.0 to view the print format of the documentation
- Internet Browser to run the Web components (Microsoft Internet Explorer 7.0 or higher, or Firefox 3.0 or higher)

UNIX and Linux

The minimum system requirements are:

- At least 4 GB of RAM
- 10 GB of hard disk free space, plus enough space for the directory data
- At least 500-MB disk space required under the temporary directory (/tmp) where the CA EEM installation files are extracted during installation
- Adobe Acrobat Reader to view the print format of the documentation (Reader 5.0.10 for Solaris and Reader 7.0 for Linux)
- Internet Browser to run the Web components (Firefox 3.0 and higher).
- General UNIX system administration skills and Superuser (root) access to a computer to install CA EEM

Chapter 3: Installation Considerations

Installation and upgrade procedures for this release of CA EEM are described in the *Implementation Guide.*

Before you install and configure CA EEM, verify that you have installed the Windows Installer 3.1 on Windows platform.

This section contains the following topics:

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.

Chapter 4: Upgrade Considerations

This section contains the following topics:

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.

MDB Database Migration

When you upgrade to the current version of CA EEM, the data in the CA MDB database is migrated to CA Directory. After the upgrade, CA EEM Server accesses the data from CA Directory.

Chapter 5: New Features

This section contains the following topics:

Native 64 bit Support for UNIX Platforms

CA EEM now supports the native 64-bit architecture for the following UNIX platforms:

- Solaris
- Linux
- IBM AIX
- HP-UX Itanium

Both CA EEM SDK and the CA EEM server now support the 64-bit architecture.

Note: You can install only one instance of the CA EEM server, either the 64-bit or the 32-bit, in a computer. If your computer has an instance of a 32-bit CA EEM server, uninstall the 32-bit CA EEM server instance before installing the native 64-bit CA EEM server.

Certificates with Custom Key Length

CA EEM now supports certificates created using key lengths 1024, 2048, and 4096.

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

Support for Windows 2012 Server

The CA EEM Server now supports Windows 2012 Server.

Support for Kerberos Authentication

The CA EEM Server now supports Kerberos authentication against Microsoft Active Directory on Windows and Linux platforms.

CA EEM SDK Enhancement

The CA EEM SDK now provides a new API (SafeContext.getServerProperty) to get the CA EEM Server properties.

Chapter 6: Changes to Existing Features

This section contains the following topics:

Changes in CA EEM r12.0

Dynamic CPP SDK Libraries

CA EEM now provides dynamic linked-libraries for CPP SDKs instead of the static linked-libraries. Also, CA EEM no longer exposes iTech SDK objects in the APIs.

For information about CPP SDKs, see the *Implementation Guide*.

Search for Users in Global Groups

CA EEM no longer supports a search for users belonging to a global group.

Server Installer

The Server Installer now uses InstallAnywhere installer.

For information about the Server Installer, see the *Implementation Guide*.

SHA2 Support

CA EEM now uses SHA2 for the following tasks:

- Manage client-server communication
- Store user passwords
- Manage application certificates

Deprecated APIs

CA EEM does not provide the following deprecated APIs:

- SafeContext.authenticateWithPam
- SafeContext.submitAdminEvent
- SafeContxt.getCache
- SaefContext.setPersistentCacheFile
- SaefContext.getPersistentCacheFile
- SaefContext.synchronizeAll
- SaefContext.isPushSupported
- SaefContext.generatePassTicket
- SaefContext.configurePassTicket
- SaefContext.disablePassTicket
- SafeContext.getApplicationInstanceObject
- SafeContext.isExternalDirectory
- SafeContext.isSiteMinder
- SafeGlobalUser.setDirectoryPassword
- SafeGlobalUser.setDirectoryPasswordDigest
- SafeGlobalUser.getDirectoryPassword
- SafeUser.setSuspended
- SafeUser.isSuspended
- SafeSession.setIdentity
- SafeSession.addUserGroup
- SafeSession.clearUserGroupQ
- SafeSession.addGlobalUserGroup
- SafeSession.addDynamicUserGroup
- SafeSession.clearDynamicUserGroupQ
- SafeSession.addAttr
- SafeSession.clearAttrQ
- SafeSession.delAttr
- SafeSession.delnAttr
- SafeSession.clearAttrQ
- SafeSession.clearAttrQ

- SafeSession.clearAttrQ

CA User Activity Reporting Module Reporting Component

CA EEM no longer ships the CA User Activity Reporting Module Reporting Component. CA EEM now stores the security events in files under the default location CA EEM Installation Directory/logs. You can configure the default logging properties using the plugin.xml in the CA EEM Installation Directory/config/logger location.

External LDAP User and Group Caching

CA EEM no longer caches entire users, groups, and folders of the configured external LDAP directory. You can set a limit to caching.

For information about caching, see the *Online Help*.

Changes in CA EEM r12.51

Changes to the Failover Configuration Tool

The Failover tool has been updated to configure certificates with a custom key length in the CA EEM Server.

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

Chapter 7: Fixed Issues

The following issues have been fixed in this release:

Issue Number	Issue Description
19532370	The User Management page of the CA EEM Admin UI displays a Close button, which is not required by the embedding application.
21140937	The CA EEM Server logs the following error message repeatedly in the igateway.log file: sponsor[favicon.ico] not found and invocation returned 404 error.
21085791	The session not found error occurs when CA EEM Server is subjected to load.
20727736	CA EEM Server fails to check for the required disk space during installation.
21156973	When you create an Identity and Access Control List (IACL) policy with dug:GroupName as a filter, the User icon is displayed instead of the Dynamic User Group icon in the CA EEM Admin UI.
21130773	The authenticateWithDigest API fails with a NULL pointer exception during NTLM authentication.
21105722	When you define an Access Control List policy, a resource with an asterisk does not evaluate correctly.
20792264	The CA EEM SDK does not read and write the PEM and P12 certificate through streams
21181861	The policy evaluation of the CA EEM r12.0 policy attributes with the CA EEM r8.4 clients fails.
21165169	When you try to reset the user store configuration password using the CA EEM Admin UI, the current password is populated in the Password field.
21186119, 21227442	When you upgrade CA EEM from 32-bit to 64-bit, or from 64-bit to 32-bit, CA EEM displays an incorrect error message.
21176721	The CA EEM r8.4 clients cannot export or import global settings using safex.
21216193	The CA EEM upgrade using silent installation fails when the specified backup directory already exists.
21228012	When you select an unmapped attribute in the calculation editor in the CA EEM Admin UI, a textbox to enter the new attribute name is not displayed.
21236753	The isExternalDirectory API is not backward compatible with the CA EEM 8.4 SDK.
21111740	If the group name is specified in a case different from which it was originally created, safex does not delete the user group membership.
21290675, 21380942	CA EEM does not preserve the case in which the user session information was created.
21297455	When you upgrade from r8.4 to r12.0, the CA EEM client fails to attach to an application that has no policies.

Issue Number	Issue Description
21096390	The NTLM authentication fails when the browser sends multiple authentication requests simultaneously.
20991340	During CA EEM Server installation, if you specify the EiamAdmin password with multiple $ symbols, the CA EEM Server installer sets a wrong password.
21202610	The CA EEM SDK cache file is written to the root directory.
21176081	CA EEM does not support native 64-bit support on Linux and Unix.
21195305	CA EEM does not support 2048-bit certificates.
21232770	The CA EEM SDK does not support retrieval of active CA EEM backend server information.
21349772	The CA EEM Admin UI does not display a page to change the EiamAdmin password when connected to an external user directory.
21334062	CA EEM does not support retrieval of CA EEM Servers configured in the High Availability environment.

Chapter 8: Known Issues

This section contains the following topics:

CA EEM Java Authentication API Takes 20 Seconds

Valid on Linux

Symptom:

When I use BSAFE Crypto-J 4.0 as a JCE provider, the CA EEM authentication API takes 20 seconds to execute.

Solution:

This is an issue with Sun Java. The workaround for this issue is published on the following Sun site: http://bugs.sun.com/. Search for the bug ID: 4705093 to see the workaround. Follow the steps as a workaround:

- Set the EGD used by Java by setting the security property "java.security.egd" to "file:///dev/urandom"

or

- Set the system property, rather than the security property, "java.security.egd" from the command line as follows: -Djava.security.egd=file:///dev/./urandom

SAML Authentication and CA SiteMinder Integration Do Not Work When the CA EEM Server is in FIPS-only Mode

Valid on AIX

SAML authentication and CA SiteMinder integration fails when CA EEM Server is configured for FIPS-only mode.

Cannot Log Into CA EEM Server with a Custom Created User EiamAdmin

Valid on Windows and Linux

Symptom:

I cannot log into CA EEM server with a custom created user "EiamAdmin". I receive an incorrect password error message.

Solution:

By default, CA EEM creates a user 'EiamAdmin' with administrative privileges during installation. When you try to login as "EiamAdmin", CA EEM always tries to authenticate based on the credentials of the default "EiamAdmin" user. Therefore, if you have a custom user "EiamAdmin" in your external directory, you cannot log into CA EEM with the custom "EiamAdmin" credentials.

Error Using CA EEM Java SDK

Symptom:

When I use the CA EEM Java SDK on a computer with Tomcat 4.1, I receive the following browser error:

```
HTTP 404 Error
```

In the Tomcat log, I see the following exception:

```
org.apache.commons.logging.LogConfigurationException: Invalid class loader
hierarchy. You have more than one version of 'org.apache.commons.logging.Log'
visible, which is not allowed.
```

Solution:

To use the CA EEM Java SDK on a computer with Tomcat 4.1, do the following:

1. Stop Tomcat Server.
2. Delete the commons-logging-api.jar and commons-logging.jar files from the webapps/application_name/WEB-INF/lib/ directory.
3. Restart Tomcat Server.

Error Using Pre-Deployment Labels in Scoping and Dynamic User Group Policies

Symptom:

When I try to define pre-deployment labels for scoping and dynamic user group policies, the evaluation result is invalid.

Solution:

CA EEM server now evaluates the scoping and dynamic user group policies. So, pre-deployment labels do not reflect in the new authorization checks.

CA EEM UI Displays the CAELM Application

Symptom:

When I upgraded to CA EEM r12.0, CA EEM still displays CAELM application on the UI.

Solution:

To unregister the CAELM application, perform the following steps:

1. Log on to the Global Application as an EiamAdmin.

   The CA Embedded Entitlements Manager application window opens.
2. Click Configure, Applications.

   The available applications are displayed in the left pane.
3. Click CAELM.

   The Application Instance details are displayed on the right pane.
4. Click Unregister.

   A delete confirmation dialog opens.
5. Click OK.

Error Using WebLogic 8.1 Application Server

Symptom:

When I deploy an application that uses the CA EEM Java SDK, on a WebLogic 8.1 Application server, I receive a ClassCastException.

Solution:

You receive this error if the WebLogic server is configured to use its own implementation of HTTPSUrlConnection for HTTP handlers.

To avoid this error, configure the WebLogic server to use the SUN handlers by adding the -DUseSunHttpHandler=true parameter to the JVM options.

For information on how to set the parameters, see the JVM documentation.

Attach Operation Fails on CA EEM 8.4

Symptom:

When I define attach permissions for a group, and a user from the group tries to attach to an SDK, the attach operation failed.

Solution:

As a workaround, perform *one* of the following steps:

- Use the latest SDK for your application.
- Define a scoping policy for a user with read permission to the global groups and application groups.

CA SiteMinder Configuration Fails Intermittently on UNIX

Symptom:

When I try to connect CA EEM server to the configured CA SiteMinder Policy Server, the operation fails.

Solution:

This issue occurs when there is a low entropy on the CA EEM server. To resolve the issue, perform *one* of the following steps:

1. Add a symbolic link from /dev/random to /dev/urandom.
2. Perform the following steps:
   a. Install the mgd daemon.
   b. Execute the following command:

      ```
      #cat /proc/sys/kernel/random/entropy_avail
      ```

      The entropy value is displayed.
   c. Execute the following command:

      ```
      #rngd -r /dev/urandom -o /dev/random -f -t 1
      ```

      The mgd daemon is started.
   d. (Optional) Execute the following command to monitor the entropy value:

      ```
      #watch -n 1 cat /proc/sys/kernel/random/entropy_avail
      ```

Unable to Launch CA EEM GUI After Installing CA Integrated Threat Management

Symptom:

I am unable to launch CA EEM GUI after installing CA Integrated Threat Management on the same server as CA EEM.

Solution:

You may be unable to launch CA EEM GUI because CA Integrated Threat Management during installation removes a <Spindle> tag from the Spin.conf file.

You must add the <Spindle> tag before the following section in the Spin.conf file to launch CA EEM GUI:

```
                    <version>8.1</version>
                    <directory/>
                    <config/>
                    <redirecthttps>true</redirecthttps>
                    <sendevents>true</sendevents>
</Spindle>
```

To look like:

```
<Spindle>
                    <version>8.1</version>
                    <directory/>
                    <config/>
                    <redirecthttps>true</redirecthttps>
                    <sendevents>true</sendevents>
</Spindle>
```

Unable to Launch CA EEM GUI After Uninstalling CA Integrated Threat Management

Symptom:

I am unable to launch CA EEM GUI after uninstalling CA Integrated Threat Management that is installed on the same server as CA EEM.

Solution:

You may be unable to launch CA EEM GUI because CA Integrated Threat Management during uninstallation removes a <Spindle> tag from the Spin.conf file.

You must add the <Spindle> tag before the following section in the Spin.conf file to launch CA EEM GUI:

```
                    <version>8.1</version>
                    <directory/>
                    <config/>
                    <redirecthttps>true</redirecthttps>
                    <sendevents>true</sendevents>
</Spindle>
```

To look like:

```
<Spindle>
                    <version>8.1</version>
                    <directory/>
                    <config/>
                    <redirecthttps>true</redirecthttps>
                    <sendevents>true</sendevents>
</Spindle>
```

Search for Users or Groups When Connected to CA SiteMinder Takes a Long Time to Complete

When you use a regular expression * (asterisk) to search for users or groups through CA SiteMinder, CA EEM may take 20 minutes to 45 minutes, based on your system configuration, to display the results.

Memory Size on HP-UX

By default, HP-UX allocates 256 MB of memory for processes such as iGateway. CA EEM will run out of memory and iGateway may crash if you perform tasks using CA EEM that may require memory of more than 256 MB. So, you must increase the memory size allocated by HP-UX to iGateway process based on your requirement.

Authentication to an SSL Enabled Directory over Non-SSL Port Fails

Symptom:

When I disable SSL connections to an external directory and later try connecting to that external directory using SSL port 636, the authentication fails, and I am unable to login to CA EEM GUI.

Solution:

You cannot use an SSL port to connect to an external directory even if the SSL connection is disabled. To connect to an external directory that is configured for SSL connections, over non-SSL ports, you must do the following:

1. Open server.xml file and edit the following entry to reflect any valid non-SSL port:

   <host>*ldaphostname*:*port*</host>

2. Restart iGateway

   You can now connect to an SSL enabled external directory over non-SSL ports. The authentication is successful and you can login to CA EEM GUI.

Communication between CA EEM Server and Client Is Broken in an IPv6 Environment

Valid on Windows

Symptom:

The communication between a client and its server is broken in an IPv6 environment.

Solution:

In an IPv6 environment, the aforementioned platforms cannot communicate with the DNS server to resolve IPv6 addresses to host names. Hence, the communication between a client and its server is broken. You must perform the following steps to enable communication:

1. Open the hosts file located in the following folder:

   <*Windows_install_drive*>\WINDOWS\system32\drivers\etc

2. Add the IP address and host name of the destination computer to the existing IP addresses and host names in the following format:

   IPv6_Address Hostname

   For example, 2002:9b23:2d52::b892:c8f3:5695:fd5c GPC00015, where 2002:9b23:2d52::b892:c8f3:5695:fd5c is the IP Address and GPC00015 is the host name of the corresponding computer.

3. Save and close the hosts file.

   The IPv6 address of the destination computer is mapped to the host name of the destination computer.

Note: You must repeat this procedure on all client and their corresponding server computers. For more information on IPv6 and Windows, see the following link: http://www.microsoft.com/technet/network/ipv6/ipv6faq.mspx

User Authentication and Authorization Fails after CA EEM Upgrade

Valid on RHEL 5 and Solaris

Symptom:

When I upgraded to CA EEM r12.0 from an earlier version and tried to authenticate and authorize a user using SiteMinder, the operations fail.

Solution:

This is a known issue. A fix for this issue will be available in a future release of CA EEM.

Search for Users and Groups Fails

Symptom:

When I search for users or groups, and click a user or group from the search results page, a blank page appears.

Solution:

To resolve this issue, add a scoping policy for the iPoz resource with read action to a user who wants to view the search results.

Export of Server Configuration Fails

Symptom:

When I export an application from CA EEM server, the server configuration details in the imported XML are not updated.

Solution:

By default, CA EEM r12.0 does not export the server configuration details. To resolve this issue, perform the following steps:

1. Configure the destination server with the server configuration details of the source server.
2. Export an application into XML from the source server.
3. Import the XML into the destination server.

User Authentication and Authorization Fails on CA SiteMinder

Symptom:

When I use CA SiteMinder to authenticate and authorize a user belonging to a user group name with "–", the operations fail.

Solution:

This is a known issue. A fix for this issue will be available in a future release of CA EEM.

Failover Configuration Fails after CA EEM Upgrade

Symptom:

When I upgraded to CA EEM r12.0 from an earlier release, the failover configuration fails.

Solution:

This is a known issue. A fix for this issue will be available in a future release of CA EEM. As a workaround, reconfigure the failover configuration.

Executing Failover Tool on Non-English Platform

Valid on Windows

Symptom:

On a non-English platform, when you execute the failover tool using the following command, garbage characters are displayed in the console.

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

Solution:

Execute the eiam-clustersetup.bat command to fix the issue.

Chapter 9: Limitations

This section contains the following topics:

CA Integrated Threat Management r8.0

CA EEM is incompatible with CA Integrated Threat Management r8.0. Therefore, if you need to run the CA EEM Server on the same computer as the CA Integrated Threat Management product, you must upgrade your computer to CA Integrated Threat Management r8.1.

Display Limitations in User Interface

The use of non-alphanumeric characters, such as double quotes, \ or / cause display problems in the user interface. Use only alphanumeric characters for the following objects:

- Actions
- Calendars
- Custom Mapped Directory Label
- Global Groups
- Global Users
- Folders
- Named Attributes
- Obligation Names
- Policies
- Resource Classes
- Users
- User Attributes
- User Groups

Policy Limitation on HP-UX

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

Username and Groupname Limitation

CA EEM reads a "\" as a domain name separator. So, when you try to authenticate or authorize a username or a group with a "\" in the basic LDAP user store, the operation fails.

CA EEM Installation on Non-English Operating System

CA EEM installation can be performed on a non-English operating system, *only* if the following conditions are met:

- The host name of the computer must be in English
- The installation path must be in English.

Chapter 10: Documentation

This section contains the following topics:

CA HTML Bookshelf

This release contains the CA HTML Bookshelf, which is an HTML help system that provides access to all deliverables in the product documentation set in both HTML and PDF. HTML provides robust online viewing and search capabilities, while PDF provides a print-friendly option.

The HTML bookshelf features include:

- A single help screen that displays all documentation for this release.
- An all-in-one search tool that searches the entire documentation set and returns matches found in both the HTML and PDF formatted documentation, without the need for a specialized .PDX index file.
- Additional links for using the Bookshelf, downloading Acrobat Reader, and contacting CA.

Search the Bookshelf

The bookshelf includes a search facility that helps you locate information throughout the set.

To search the bookshelf

1. Enter your search criteria in the Search field in the upper right corner of the bookshelf and press Enter.

   The search returns HTML results listed by topic and PDF results listed by guide. The results are sorted by date so that the most recently updated topics or PDFs appear at the top of the list. To find a topic in a PDF, open the PDF and view the list of topics within the PDF that match the search criteria.

2. (Optional) Click Sort by Relevance.

   The list is reordered so that the HTML topics or PDFs that contain the most matches appear at the top of the list.

Documentation Deliverables

The CA EEM documentation set contains the following document deliverables:

- CA EEM Programming Guide, which contains information about SDKs.
- CA EEM Implementation Guide that replaces the CA EEM Getting Started Guide, which contains information about the CA EEM Server.
- CA EEM Release Notes, which contains information about the current release such as highlights of the new features, enhancements to existing features, known issues, and so on.

Chapter 11: International Support

An *internationalized* product is an English product that runs correctly on local language versions of the required operating system and required third-party products, and supports local language data for input and output. Internationalized products also support the ability to specify local language conventions for date, time, currency and number formats.

A *translated* product (sometimes referred to as a *localized* product) is an internationalized product that includes local language support for the product user interface, online help and other documentation, local language default settings for date, time, currency, and number formats.

CA EEM is internationalized but not translated.

Note: The CA EEM SDK is not translated.

Appendix A: Third–Party Software Acknowledgements

CA EEM incorporates software from third–party companies. To view the licensing agreement information for a third-party software in HTML format, click Third Party Software Acknowledgements.