Contents

Note: This document contains details on new and changed features specific to CA Embedded Entitlements Manager (EEM). Any new or changed features related to CA Workload Automation engines or other products that use EEM can be found in the respective product documentation.

New Features in EEM Release 12.0

This section contains the following topics:

Support for Multiple Domains

CA EEM now supports the following LDAP directories configurations:

Basic LDAP directory

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

Multiple Active Directory domains

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

Active Directory Domain

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

Active Directory Forest

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

For information about the multiple domain support, see the Implementation Guide or the Online Help.

Failover Tool

CA EEM provides a command line tool for automating the failover configuration process. Using the failover tool, you can configure a primary server and various failover nodes.

For information about the failover tool, see the Implementation Guide.

Certificate Validation

After you verify the public key and private key of a certificate in an SSL handshake, you can use CA EEM to validate the revocation status of a certificate. CA EEM uses the validateUserCertificate API to validate a certificate. If the validation of a certificate is successful, CA EEM extracts the username and initiates a safe session.

CA EEM supports the following revocation mechanisms:

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

For information about the certificate validation, see the Implementation Guide or the Online Help, and the Programming Guide.

Changes in EEM Release 12.0

This section contains the following topics:

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.

New Features in EEM Release 12.0 CR01

No new features were added in EEM Release 12.0 CR01.

Changes in EEM Release 12.0 CR01

No features were changed in EEM Release 12.0 CR01.

New Features in EEM Release 12.0 CR02

No new features were added in EEM Release 12.0 CR02.

Changes in EEM Release 12.0 CR02

This section contains the following topics:

Changes to the CA EEM Installer

Before installing any CA Embedded Entitlements Manager components on a system, the CA Embedded Entitlements Manager installer verifies that the localhost binds to all addresses it resolves. If the localhost fails to bind, the installation is aborted and an error message is logged in the eiam-install.log file.

New Features in EEM Release 12.0 CR03

This section contains the following topics:

Support for PEM Certificate Authentication

The CA EEM JAAS module supports PEM certificates for authentication.

Changes in EEM Release 12.0 CR03

This section contains the following topics:

Changes to the CA EEM Java SDK jars

CA EEM upgraded the following JAVA SDK jars:

- httpclient-4.0 to httpclient-4.1.2
- httpcore-4.0.1 to httpcore-4.1.2
- commons-codec-1.3 to commons-codec-1.4

Changes to the eiam.config file

In the earlier releases, CA EEM cores on any UNIX machine when the SIGPIPE signal is generated in a process of the embedding application using the CA EEM CPP SDK. To resolve the issue, you can add the <signalhandling> tag to the eiam.config file.

Follow these steps:

Open the eiam.config file and navigate to the <TransportConfig> section.

Add the following line to the <TransportConfig> section:

<signalhandling>SIGPIPE</signalhandling>

Save the changes.

Changes to CA EEM High Availability

The existing CA EEM High Availability feature is modified to support the following modes of High Availability configuration:

Internal High Availability mode, in which CA EEM servers are configured in a High Availability environment. If server communication fails, a CA EEM SDK fails over to the other CA EEM servers.

External High Availability mode, in which CA EEM servers are configured behind an Apache reverse proxy server. If server communication fails, the Apache reverse proxy server fails over to the CA EEM servers.

Configure a CA EEM Primary Server

Configure a CA EEM primary server in a High Availability configuration mode.

Follow these steps:

Open the command prompt from the primary server, and navigate to the EiamInstallation\bin location.

Execute the following command:

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

The message "Enter EiamAdmin password" appears.

Type the EiamAdmin password, and press Enter.

Execute the following command:

```
resetprimary
```

Note: Reset a primary server only once in a high-availability setup.

The message "Enter DSA port" appears.

Do one of the following steps:

To use the default 509 as the DSA port, press Enter.

To use a different port as the DSA port, type the port number and press Enter.

The message "Specify high-availability mode" appears.

Do one of the following steps:

To use the internal High Availability mode, type 1 and press Enter.

To use the external High Availability mode, type 2 and press Enter.

The primary server is configured.

Note: For information about CA EEM High Availability, see the CA EEM Implementation Guide.

New Features in EEM Release 12.0 CR04

No new features were added in EEM Release 12.0 CR04.

Changes in EEM Release 12.0 CR04

This section contains the following topics:

Support for the isExternalDirectory() Method

CA EEM supports the isExternalDirectory() method to check if a CA EEM server is configured to an external user store.

Support for Java Stream in PEM and P12 Certificates

CA EEM updated the following APIs to provide Java stream support for PEM and P12 certificates:

- readPEM()
- writePEM()
- readP12()
- writeP12()

New Features in EEM Release 12.0 CR05

No new features were added in EEM Release 12.0 CR05.

Changes in EEM Release 12.0 CR05

This section contains the following topics:

Changes to the pingEiam Method

The pingEiam method in the CA EEM CPP SDK is enhanced to support the HTTPS protocol.

New Features in EEM Release 12.0 CR06

This section contains the following topics:

New Tag in the eiam.config File

You can configure the CA EEM Java SDK to restrict the maximum number of connections to CA EEM Server. The following attribute is added to the Network tag:

maxconnections

Defines the maximum number of connections to CA EEM Server.

Example: <Network sockettimeout="120000" retrycount="2" maxconnections="100" />

Changes in EEM Release 12.0 CR06

This section contains the following topics:

Changes to Server Logging

You can configure the different log levels of CA EEM server installer logging. CA EEM supports all log levels that are supported by log4j. By default, INFO is set as the log level.

You can configure the log levels in one of the following methods:

- Set the EIAMINSTALL_LOGLEVEL environment variable as follows:

  EIAMINSTALL_LOGLEVEL=log_level

- Run the following command from the command prompt:

  <CA EEMServer_installer.exe> -DEIAMINSTALL_LOGLEVEL=log_level

Changes to the VPAT Compliance Configuration

You can enable or disable the VPAT compliance feature. To enable the feature, select Activate Accessibility in the CA EEM UI login page. To disable the feature, clear Activate Accessibility in the CA EEM UI login page.

New Features in EEM Release 12.0 CR07

No new features were added in EEM Release 12.0 CR07.

Changes in EEM Release 12.0 CR07

No features were changed in EEM Release 12.0 CR07.

New Features in EEM Release 12.5

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.

Customized Key Length for SSL Certificates

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

Note: For more information, see the Implementation Guide.

Kerberos Authentication Support

CA EEM now supports Active Directory Kerberos based authentication on Linux platform.

Note: For more information, see the Implementation Guide.

EEM and SSO Server Integration

CA EEM includes functionality to integrate with SSO server.

Note: For more information, see the Implementation Guide.

Changes in EEM Release 12.5

This section contains the following topics:

Changes to the Failover Configuration Tool

Failover tool is modified to configure higher bit key length certificates in EEM server.

Note: For more information, see the Implementation Guide.

New Features in EEM Release 12.51

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.

Changes in EEM Release 12.51

No features were changed in EEM Release 12.51.

New Features in EEM Release 12.51 CR01

This section contains the following topics:

Support for Virtual IP (VIP) Address

The CA EEM server is certified on Apache reverse proxy cluster that is configured with virtual IP.

Import Audit Events into a Database

You can use the Safe Audit Import tool (tool) to import the audit events from the audit log files to a database for persistence or to generate reports.

For information on importing audit events, see the CA EEM Implementation Guide.

Changes in EEM Release 12.51 CR01

No features were changed in EEM Release 12.51 CR01

New Features in EEM Release 12.51 CR02

This section contains the following topics:

DataDirect JDBC Driver Support for Safe Audit Import Tool

The Safe Audit Import tool is enhanced to support the DataDirect JDBC Drivers for database communication.

Silent Failover Configuration

You can configure the Failover Configuration tool silently using the silent switch option that uses a response file. A sample response file is provided with the CA EEM installation.

Support for JRE 1.7.0

CA EEM Server supports JRE 1.7.0. By default, CA EEM provides JRE 1.6.0 with installation. To use JRE 1.7.0, update the value of JREpath in the igateway.conf file.

Support for Oracle Enterprise Linux 6

You can install CA EEM on Oracle Enterprise Linux (OEL) 6.

Support for Microsoft Windows 2012 R2

You can install CA EEM on Microsoft Windows 2012 R2.

Third Party Upgrades

CA EEM is upgraded to support CA Directory Release 12.0 SP13 and CAPKI 4.3.4.

Changes in EEM Release 12.51 CR02

No features were changed in EEM Release 12.51 CR02

New Features in EEM Release 12.51 CR03

This section contains the following topics:

Support Search of Application Groups

You can search for the application groups in Admin UI.

Support for Preserving CA EEM 8.4 Attributes

You can preserve the CA EEM 8.4 attributes during the export of applications from CA EEM 12.0. If you select the option, the attributes are not converted to the equivalent 12.x attributes.

Support of SDKs on RHEL7, OEL7, and SUSE12

The Java and CPP SDKs are certified to run on RHEL7, OEL7, and SUSE12.

Support of Oracle Enterprise Linux 6 and CentOS 6.0

CA EEM is certified on Oracle Enterprise Linux 6 (OEL6) with Kernel 3.0 and CentOS 6.0.

Upgrade of Third Party Components

CA EEM is upgraded to support CAPKI 4.3.8.

Changes in EEM Release 12.51 CR03

No features were changed in EEM Release 12.51 CR03

New Features in EEM Release 12.51 CR04

This section contains the following topics:

TLSv1.2 and TLSv1.1 Support

The EEM enhancement supports the TLSv1.2 and TLSv1.1 communication protocols. Secure Protocol tag in igateway.conf file now accepts the following values to support the new protocols added in the current release:

- SSLV23
- TLSV1_2
- TLSV1_1
- TLSV1

Note: SSLv2 and SSLv3 protocols are not supported from this release.

EEM Server Support on RHEL7, OEL7, and SUSE12

Modified and Certified the EEM r12.51 CR04 Server to run on the following operating systems:

•RHEL7

•OEL7

•SUSE12

Support for JRE 1.8.0

CA EEM provides JRE 1.6.0 with installation by default. CA EEM Server now supports JRE 1.8.0. To use JRE 1.8.0, update the value of JREpath in the igateway.conf file.

RSA Bsafe Crypto-J 6.2

Certified the EEM Java SDK with Bsafe Crypto-J 6.2 for FIPS communication.

Cipher Suite Option

Use the Cipherlist tag in igateway.conf file to allow/restrict the cipher suite in the SSL communication between the EEM SDK client/browser and the EEM server.

Changes in EEM Release 12.51 CR04

This section contains the following topics:

New tags added to Spin.conf

The following new tags have been added to Spin.conf file:

uicompat

The tag specifies whether uicompat check is configured. When this tag is set to true, EEM UI does not allow special characters in folders and resource classes.

Default: false

xframeoption

The tag specifies whether EEM UI can be loaded in an iframe. When this tag is set to true, EEM UI is not loaded in a different frame.

Default: false