Oracle® Communications Billing and Revenue Management

ECE Installation Guide

Release 15.2
G35888-01
January 2026

Oracle Communications Billing and Revenue Management ECE Installation Guide, Release 15.2

G35888-01

Contents

5 Installing Elastic Charging Engine

6 Upgrading Elastic Charging Engine

7 ECE Postinstallation Tasks

8 Verifying the ECE Installation

9 Uninstalling ECE

About This Content

This guide describes the system requirements and procedures for installing Oracle Communications Billing and Revenue Management Elastic Charging Engine (ECE).

Audience

This document is for system administrators who install and configure the ECE software and those involved in planning a charging system that includes ECE. The person installing the software should be familiar with the following topics:

- Operating system commands
- Database configuration
- Network management
- Oracle Coherence

Before reading this guide, you should have a familiarity with ECE. See *BRM Concepts*.

1

ECE Installation Overview

Learn about the Oracle Communications Billing and Revenue Management (BRM) Elastic Charging Engine (ECE) installed components and the ECE installation process.

> ⚠ **Caution**
>
> Deploying charging for 5G with HTTP Gateway (5G CHF) requires a cloud native deployment of ECE and BRM components. The HTTP Gateway can be used only on an ECE cloud native system.

Topics in this document:

For an overview of the ECE components, see "BRM System Architecture" in *BRM Concepts*.

About Installing ECE

When you install ECE, you are given the option to install individual ECE software components or to install all ECE software components at once. The components you choose to install depends on what you want to do with ECE. For a development system, you typically install the ECE Server component only.

This guide frequently refers to the *ECE_home* directory, which is the directory in which ECE is installed. This directory contains the ECE Server software directory, the SDK directory (*ECE_home***/oceceesdk**), and various installation-related files.

Overview of ECE Installed Components

The installed components depend on whether you perform an ECE development installation or perform an ECE production installation.

Installed Components in an ECE Standalone Installation

For an ECE development installation, you install and configure the following components:

- Third-party software, such as Groovy

  Groovy is a prerequisite for running the ECE installer. Groovy is also used for launching the Elastic Charging Controller (ECC), which is the ECE command line interface.

- Java Runtime Environment (JRE) from Java Development Kit (JDK), if it is not already installed
- ECE Server software

  ECE Server software includes the core processes required for receiving and processing requests, responding to systems that send requests, and publishing rated event data.

Installed Components in an ECE Integrated Installation

For an ECE production installation, you install and configure the following components:

- Third-party software, such as Groovy

  Groovy is a prerequisite for running the ECE installer. Groovy is also used for launching the Elastic Charging Controller (ECC), which is the ECE command line interface.
- Java Runtime Environment (JRE) from Java Development Kit (JDK), if it is not already installed
- The following products required in a production system, if they are not already installed:
  - PDC

    PDC requires that you also install Oracle WebLogic Server
  - Either Oracle WebLogic Server or Apache Kafka

    Apache Kafka and Oracle WebLogic Server are not part of the core ECE installation. However, ECE uses Apache Kafka or Oracle WebLogic Server when it is used in a production charging solution.
  - Oracle Database to persist the data in the database or Oracle NoSQL Database to persist the data in the cache
  - BRM server
  - Online or offline network mediation software

    Network mediation software is required for sending requests to ECE in a production charging solution. The ECE installation process does not have a dependency on network mediation software. The network mediation software is installed after ECE is installed since it is a client of ECE.
- The following ECE software components, which you install by running the ECE installer:
  - ECE Server software

    ECE Server software includes the core processes required for receiving and processing requests, responding to systems that send requests, and publishing rated event data.
  - ECE BRM Integration Pack
  - ECE PDC Integration Pack

Overview of the ECE Installation Procedure

The installation procedure follows these steps:

1. Plan your installation. When planning your installation, you do the following:
   - Determine the scale of your implementation, for example, a small test system or a large production system.

- Determine how many physical machines you need, and which software components to install on each machine.
- Plan the system topology, for example, how the system components connect to each other over the network.

2. Review system requirements. System requirements include:
   - Hardware requirements, such as disk space
   - System software requirements, such as operating system (OS) versions and OS patch requirements, and JVM process requirements (such as memory settings)
   - Information requirements, such as IP addresses and host names
3. Perform preinstallation tasks.
4. If you are installing an ECE production installation:
   - Ensure you have installed and configured the following products:
     - BRM
     - PDC
     - Oracle Database or Oracle NoSQL Database (based on your persistence requirement)
     - Oracle WebLogic
     - Apache Kafka and Apache ZooKeeper (if you are using them for ECE notifications)
   - Set up either a JMS Topic in Apache Kafka or a JMS queue in Oracle WebLogic for ECE notification events
   - Create the required Oracle Advanced Queueing (AQ) database queues (DBMS AQs) for BRM update requests
5. Install ECE.

   You may need to run the ECE installation multiple times. For example, when performing an ECE production installation, you run the installer to install all ECE software components, and then run the installer again to install the ECE Server component so that you can run Rated Event Formatter on a separate machine.
6. Perform postinstallation tasks.

   If you are installing an ECE production installation, do one of the following for handling ECE acknowledgment events and failed customer data updates.
   - If you are using Apache Kafka, create an Notification Topic and a Suspense Topic.
   - If you are using Oracle WebLogic Server, create an Acknowledgments Queue and a Suspense Queue.
7. Verify the installation.
8. If you are installing an ECE production installation, install and configure your network mediation software, such as Oracle Communications Offline Mediation Controller.

Overview of the ECE Installation Procedure for Upgrade

> **Note**
>
> A direct upgrade from an existing ECE release is not supported.

If you have an existing ECE installation (earlier release installation), and you are installing ECE, you need to follow these steps:

1. Plan your installation.
2. Review system requirements.
3. Back up your existing configuration.

   Back up all files of the existing ECE installation on the driver machine.
4. Create a new directory for the new installation on the driver machine.
5. Upgrade system requirements that are required by the new release:
   - Install the required version of JRE/JDK.
   - Do one of the following:
     - If you want to store all the ECE data in the database, use Oracle Database. You can use the BRM database to persist the ECE data.
     - If you want to continue to persist only the rated events in Oracle NoSQL database, install the required version of Oracle NoSQL Database.
   - Verify that you have installed the required version of Oracle WebLogic Server.

     Installing Oracle WebLogic Server is a prerequisite for PDC so this is the version that PDC requires.
   - Install Apache Kafka if you are using Topics rather than queues for handling notification events and BRM update requests.
   - Install the required version of BRM.
   - Install the required version of PDC.
   - Upgrade your network mediation software.
6. Install ECE.

   You install ECE in the new directory on the driver machine.
7. Perform the following postinstallation tasks:
   - Merge configurations from the existing installation into the new installation.
   - Upgrade extension code.
   - Update BRM configuration files.
   - Deploy the new ECE installation onto server machines.
   - Stop the ECE nodes of your existing installation.
   - Restore your ECE system by reloading data from BRM and PDC.
   - Start all ECE nodes of the new installation.

8. Verify the installation.

ECE Installation Options

You can install ECE in two ways:

- **GUI installation:** Use the GUI installation when you want to interact with the installer GUI during installation.
- **Silent installation:** The silent installation enables you to perform a non-interactive installation of ECE. The silent installer uses a response file that contains the installation parameters and values. Use the silent installation when you are repeatedly installing ECE using the same configuration. Silent installation is a way of setting installation configurations only once and then using those configurations to duplicate the installation on many machines.

  The silent installer runs in the background without requiring any user intervention. To obtain the silent installation response file, you run the GUI installation using the record option for the first install. The GUI installer creates a response file with the parameters and values that you specify during the installation. You can then copy and edit the response file to reflect the specifics of your target system, and to contain your preferred installation options.

Ensuring a Successful ECE Installation

The ECE installation should be performed only by qualified personnel. You must be familiar with your operating system.

Follow these guidelines:

- As you install each component (for example, Groovy and JDK), verify that the component installed successfully before continuing the installation process.
- Pay close attention to the system requirements. Before you begin installing the software, make sure your system has the required base software. In addition, make sure that you know all of the required configuration values, such as host names and port numbers.
- As you create new configuration values, write them down. In some cases, you need to re-enter configuration values later in the procedure.

2

Planning Your ECE Installation

Learn how to plan your Oracle Communications Billing and Revenue Management (BRM) Elastic Charging Engine (ECE) installation.

Topics in this document:

About Planning Your ECE Installation

When planning an ECE installation, you consider how many physical servers can handle your subscriber base and how many charging server nodes to include in your cluster. You decide what server to use as the primary administrator machine, referred to as the *driver machine*, and what ECE components to install on the other servers, referred to as *server machines*. You also consider security aspects of your system and how it communicates with other applications in your charging system, such as Oracle Communications Billing and Revenue Management (BRM) and Oracle Communications Offline Mediation Controller.

System Deployment Planning

When planning an ECE installation, you consider how many charging server nodes to include in your cluster. For any gateway servers that you use as your network integration for online charging, you also determine how many gateway nodes that you need.

When considering how many charging server and gateway nodes to include in your cluster, note the following points:

- You will want to determine the minimum number of charging server nodes needed for your customer base. If the minimum number is *N*, you need to run at least *n+ 1* nodes to have uninterrupted usage processing during a rolling upgrade.
- In an ECE distributed environment (multiple machines), the guideline is to have a minimum of two charging server nodes per machine (provided the total number of charging server nodes can handle the normal expected throughput for your system). The minimum configuration for gateway nodes is 2, this allows for failover plus additional nodes as needed to handle the expected throughput of the system..
- For a standalone installation (single machine) for a development or test environment, note the following guidelines:
  - Although you can use one charging server node in a development or test environment, having only one charging server node is not a valid configuration for deploying into a runtime environment.
  - The minimum configuration for an ECE standalone installation is **3** charging server nodes, which accounts for two charging server nodes plus an additional node if both

charging server nodes fail. The minimum configuration for an ECE standalone installation for gateway nodes is **2** to allow for failover.

- Server redundancy is a minimum requirement of ECE installations.

Coherence Planning

ECE nodes are based on Oracle Coherence. Decide how to configure Oracle Coherence settings for your ECE topology. For example, determine how many nodes to add to the cluster when a node failure occurs. See the discussion in the Oracle Coherence documentation for information about Oracle Coherence high availability and performance concepts.

About Installing a Secure System

In a production system, you must ensure that communication between components and access to the system servers are secure. When you install ECE, you will be prompted to select security options during the installer process. If you have not enabled SSL communication between ECE and BRM during installation, you can enable it after the installation.

3

ECE System Requirements

Learn about the software, hardware, and information requirements for Oracle Communications Billing and Revenue Management (BRM) Elastic Charging Engine (ECE).

Topics in this document:

Software Requirements

For information about the supported and required software, see "Common Software Compatibility" and "ECE Software Compatibility" in *BRM Compatibility Matrix*.

Hardware Requirements

The number and configuration of the computers that you employ for your ECE installation depend on the scale and the kind of deployment you have planned according to your charging requirements. Work with your performance team to determine your sizing requirements.

About Oracle Exadata

ECE is supported on Oracle Exadata systems. You can use an Oracle Exadata or non-Exadata database for creating the ECE schema. The Oracle database must be installed and configured with Oracle RAC on Exadata systems. See the Oracle Exadata documentation for more information on Exadata and how to create an Oracle RAC instance in Oracle Exadata.

4

ECE Preinstallation Tasks

Learn about the preinstallation tasks for Oracle Communications Billing and Revenue Management (BRM) Elastic Charging Engine (ECE).

Topics in this document:

- Preinstallation Tasks Common to All ECE Installations
- Preinstallation Tasks for an ECE Integrated Installation
- Preinstallation Tasks for ECE Software Upgrade

> **Note**
>
> (Linux) The **ece_provision** script is not supported in ECE 12.0 and later releases. You must manually apply the Oracle Linux network configuration changes on your environment to prepare machines in your topology for a distributed ECE installation.

Preinstallation Tasks Common to All ECE Installations

You must perform these preinstallation tasks for all ECE installation types:

1. Install Apache Groovy on the driver machine and set it in your PATH environment variable.

   Groovy is used for launching the Elastic Charging Controller (ECC), which is the ECE command line interface. ECC is an extension of the Groovy Shell (**groovysh**) for ECE. For information on how to install Groovy, see "Install Groovy" on the Apache Groovy website.

2. Install Oracle Java Development Kit (JDK) and set it in your PATH environment variable.

   The JRE is required for the installer process. See the Oracle JDK documentation for information about installing JDK.

3. Install Oracle Coherence and set the path to the Coherence libraries in your PATH environment variable.

   The Coherence libraries are required to install ECE. For information about installing Oracle Coherence, see "Installing Coherence for Java" in *Oracle Fusion Middleware Installing Oracle Coherence*.

4. Obtain the required JAR files and save them to a directory on the driver machine.

   Make a record of the location of the JAR files, because you are required to specify this location during the ECE installation process. For the list of required JAR files, see "Additional ECE Software Requirements" in *BRM Compatibility Matrix*.

> **Note**
>
> - You must change the name of the **kvclient-25.1.14.jar** file to **kvclient.jar**. If you do not rename this file, the ECE installer displays an error indicating that a required JAR file is missing.
> - The JAR files are digitally signed with a private key to ensure that the files are authentic and modified. For more information, see "About Enhanced Security for JAR Files" in *BRM Security Guide*.

5. Create an ECE user account. See "Creating the ECE User Account".
6. Establish two-way password-less SSH logins. See "Establishing Two-Way Password-less SSH Logins".
7. Install an Oracle database. See "Installing and Configuring Oracle Database".

Creating the ECE User Account

Create the user account that is to be the primary user running ECE in your environment. The ECE user is a Linux account used for password-less SSH.

You create the same user account on the driver machine (the primary administrator machine) and all machines that are running ECE.

Make a record of the user name. You will be required to specify the user name during the ECE installation process.

To create the user account:

1. Log in to the driver machine.
2. Enter the following commands:

   ```
   useradd user_name
   passwd user_name
   ```

   where *user_name* is the name of the user.
3. When prompted, enter the password for the user.

See the discussion in your Linux documentation for more information about the **useradd** command.

Establishing Two-Way Password-less SSH Logins

Establish two-way password-less SSH logins between all the physical servers in your cluster: between the driver machine and each server machine and between all server machines.

If you will install an ECE standalone system on one machine only, a password-less SSH login is also required for the ECE user on the standalone machine.

To establish two-way password-less SSH logins, perform the following steps on each machine:

1. Log in to the ECE machine as the ECE user.
2. Run the following commands:

   ```
   ssh-keygen -t dsa
   ssh-copy-id -i ~/.ssh/id_dsa.pub user@host
   ```

where:

- *user* is the name of the ECE user.
- *host* is the name of the server for which the password-less SSH is being established.

  If you will install an ECE standalone system on one machine, *host* in the **ssh-copy-id** command must be **localhost**.

The number of ECE nodes you can start simultaneously is affected by the limitation on how many simultaneous SSH connections the machines in your environment can make from or to another machine. The start command, by default, attempts to start ten nodes simultaneously using ten different threads. Ensure that your maximum number of open sessions permitted per network connection is less than the number of nodes you want to start simultaneously from the driver machine.

Installing and Configuring Oracle Database

> **Note**
>
> - If you want to persist all the ECE data, you must use Oracle Database. You can use the BRM database to persist the ECE data. However, you can also create a new database if required.
> - If you want to persist only rated events, you can use Oracle NoSQL Database. See "Installing and Configuring Oracle NoSQL Database" for more information.

Oracle recommends that the installation and configuration of Oracle Database be performed by an experienced database administrator. To install and configure Oracle Database, see the Oracle Database installation documentation.

When you install the software, do the following:

- Install Oracle Database Enterprise Edition.
- Create the ECE database.
- (Optional) Install Oracle Partitioning. You need this to partition the tables in your ECE database.
- (Optional) If you are using Oracle Database to persist data, create ECE tablespaces and temporary tablespaces for the ECE schema, to store the ECE data.

  Oracle recommends that you create separate ECE tablespaces and temporary tablespaces for each schema. However, you can use a single ECE tablespace and temporary tablespace to create all the schemas.

Using an Existing Schema User

You can use an existing schema for ECE persistence or create a new schema user during the ECE installation. If you are using existing schema user, the user must have granted select on v$database.

To grant select permission, log in to your database as user sysdba and run the following SQL grant select command:

```
SQL> grant select on v_$database to db_user
```

Preinstallation Tasks for an ECE Integrated Installation

Perform these preinstallation tasks before you install an integrated ECE system:

1. Ensure that you have performed all preinstallation tasks common to all ECE installations. See "Preinstallation Tasks Common to All ECE Installations".
2. Install an Oracle NoSQL database. See "Installing and Configuring Oracle NoSQL Database".
3. Install BRM. See "Installing and Configuring BRM".
4. Set up the Oracle Advanced Queuing (AQ) database queues (DBMS AQs). See "Setting Up Database Queues for ECE-to-BRM Mediation".
5. Install Pricing Design Center (PDC). See "Installing and Configuring Pricing Design Center".
6. Install the SCTP package if you will use Diameter Gateway for network integration. See "(Diameter Gateway) Installing SCTP Package".

Installing and Configuring Oracle NoSQL Database

ECE publishes rated events to a data store in Oracle NoSQL Database where the events are stored temporarily before being extracted and sent to the BRM system.

> **Note**
>
> ECE uses Oracle NoSQL Database only to temporarily store rated event information.
>
> To store all the ECE data including the rated event information in the database, you must use Oracle Database.

When you install Oracle NoSQL Database, note the database connection information (such as host name, port number, and data store name). You must specify this information during the ECE installation process.

When configuring NoSQL Database, set up the NoSQL data store to which ECE can publish rated events. Size the Oracle NoSQL database key-value data store installation to match your ECE charging server topology.

After you install an Oracle NoSQL database, you can start the Oracle NoSQL database data store with either a single-node or multiple-node configuration:

- A single-node data store configuration is included with the Oracle NoSQL database installation and can be started in a nonproduction ECE environment.
- A multiple-node NoSQL data store configuration is required for running ECE in a production environment and requires additional configuration to make multiple nodes work as an Oracle NoSQL database cluster.

See the discussion in the Oracle NoSQL Database documentation for information about installing NoSQL Database, setting up a NoSQL data store, and setting up high availability and performance for the Oracle NoSQL Database.

ECE uses the Oracle NoSQL database client library for connecting and interacting with the Oracle NoSQL database. The Oracle NoSQL database client library is installed when you

install the ECE server software. You provide the Oracle NoSQL database connection information when you install ECE.

About Oracle NoSQL Data Store Partitions

An Oracle NoSQL data store is divided into partitions. Partitions store the rated events processed by each Rated Event Formatter instance and are associated with the target BRM database schema to which the rated events are to be exported. The partitions are automatically created for each BRM database schema.

> **Tip**
>
> One BRM schema is *not* mapped to one Oracle NoSQL database partition. The Oracle NoSQL database can have any preconfigured number of partitions based on the data size. The Rated Event Formatter **partition** configuration entry actually refers to the BRM database schema, *not* the Oracle NoSQL partition.

Installing and Configuring BRM

Oracle Communications Billing and Revenue Management (BRM) is required in the charging system to perform billing, subscription management, and financial management.

Make a record of the BRM connection information (such as host names, port numbers, and passwords) when you install BRM. You will be required to specify this information during the ECE installation process.

See "Installing BRM" in *BRM Installation Guide* for more information.

Setting Up Database Queues for ECE-to-BRM Mediation

When configuring BRM, set up the following Oracle Advanced Queuing (AQ) database queues (DBMS AQs):

- A database queue to which the BRM Account Synchronization DM can publish business events for ECE to consume.
- A database queue to which ECE can move failed update requests from BRM (referred to as the Suspense Queue).
- A database queue to which ECE can publish acknowledgment events for BRM to consume (used when processing rating requests from BRM, such as during rerating).

See "Creating WebLogic JMS Queues for BRM" for details about the information you will need.

Installing and Configuring Pricing Design Center

Pricing Design Center (PDC) is required for creating the pricing data (pricing components and setup components) that is used by ECE for rating usage requests.

During the PDC installation process, when prompted to specify whether you want to integrate ECE with PDC, select **Yes**. PDC will create a JMS queue (a work item queue) where it will publish pricing data. The ECE Pricing Updater will listen on this queue for pricing updates so that it can load the data into ECE.

If you have already installed PDC but did not specify to integrate it with ECE, manually set up a JMS queue on a PDC WebLogic server and configure PDC to publish pricing data to this queue.

Make a record of the connection information (such as host name, port number, and password) for the WebLogic server where the JMS queue resides. You will be required to specify this information during the ECE installation process.

> **Note**
>
> During ECE installation, the ECE installer checks the connection to your WebLogic Server through TCP Port 7. Ensure that TCP Port 7 is open in your WebLogic server's firewall.

For information about installing and configuring PDC, see "Installing Pricing Design Center" in *PDC Installation Guide*.

(Diameter Gateway) Installing SCTP Package

If you plan to use Diameter Gateway for network integration for online charging, and you plan to use Stream Control Transmission Protocol (SCTP), verify that your operating system has SCTP support. If your operating system does not have SCTP, you must install the SCTP system package for your operating system version.

Preinstallation Tasks for ECE Software Upgrade

> **Note**
>
> If you have an existing ECE installation, note the following:
>
> - A direct upgrade from an existing ECE release is not supported.
> - ECE supports complete installation only. To upgrade ECE, you install the new version of ECE using the **Complete** option and reconfigure the configuration and mediation files to match your existing release.

If you have an existing ECE installation, perform these preinstallation tasks before upgrading ECE:

1. Make a complete offline backup of your existing ECE configuration (the ECE installation directory and its content: *ECE_home*). In particular, make sure you back up all customized files. Store this backup in a safe location. The data in these files are necessary if you encounter any issues during the installation process.
2. Create a home directory for the new version of ECE. Because your old release is on the same driver machine, be careful to specify the home details for the new version of ECE when you run the ECE Installer.

   The home details consist of the home directory path and a unique name you give to the new installation. When you run the installer, it displays the home details of any old release installations it detects on your driver machine in the **Specify Home Details** list.

3. To enable persistence of all the ECE data in the database, use Oracle Database. See "Installing and Configuring Oracle Database" for more information.
4. If you have an existing installation of ECE integrated with BRM and Pricing Design Center (PDC), do the following:
   a. Install the compatible version of BRM on the machine on which BRM is installed. See "Installing BRM" in *BRM Installation Guide*.
   b. Install the compatible version of PDC on the machine on which PDC is installed. See "Installing Pricing Design Center" in *PDC Installation Guide*.
5. Install the recommended version of the other required software on the machine on which ECE is installed. See "Software Requirements" for more information.
6. Install Oracle Coherence and set the path to the Coherence libraries in your PATH environment variable.

   The Coherence libraries are required to install ECE. For information about installing Oracle Coherence, see "Installing Coherence for Java" in *Oracle Fusion Middleware Installing Oracle Coherence*.
7. (Optional) Install the recommended version of Oracle NoSQL Database as applicable. See "Installing and Configuring Oracle NoSQL Database" for more information.
8. Obtain the required JAR files and save them to a directory on the driver machine.

   Note the location of the JAR files, because you are required to specify this location during the ECE installation process. For the list of required JAR files, see "Additional ECE Software Requirements" in *BRM Compatibility Matrix*.

> **Note**
>
> You must change the name of the **kvclient-25.1.14.jar** file to **kvclient.jar**. If you do not rename this file, the ECE installer displays an error indicating that a required JAR file is missing.

5

Installing Elastic Charging Engine

Learn about the tasks required to install Oracle Communications Billing and Revenue Management (BRM) Elastic Charging Engine (ECE).

Topics in this document:

> **Note**
>
> ECE supports complete installation only. To upgrade ECE, you install the new version of ECE using the **Complete** option and reconfigure the configuration and mediation files to match your existing release.

Downloading the ECE Software

You can download the ECE software from one of the following locations:

- For ECE 15.2.0 or any 15.2.*x* maintenance release: From the Oracle software delivery website (https://edelivery.oracle.com)
- For any 15.2.*x*.*y* patch set release: From the Oracle support website (https://support.oracle.com)

Search for and download the **Oracle Communications Elastic Charging Engine 15.2.*x*.*y*.0** software, where *x* refers to the maintenance release and *y* refers to the patch set release of ECE that you are installing.

The Zip archive includes the installer: **OCECE-15.2.*x*.*y*.0_generic.jar**.

Installing ECE by Using the GUI Installation

The steps for installing ECE by using the GUI installation depend on the ECE software components you choose to install:

- To install an ECE integrated system, select the **Complete** option.

  See "Installing an ECE Integrated System" for more information.

- To install an ECE standalone system, select the **Standalone** option.

  This option installs a self-contained, nonproduction version of ECE that is not integrated with Oracle Communications Billing and Revenue Management (BRM) or Pricing Design Center (PDC). Use the standalone system for evaluation, demonstration, and functional testing.

  See "Installing a Standalone ECE System" for more information.

Installing an ECE Integrated System

To install an ECE integrated system, select the **Complete** installation option. This installs ECE Server, ECE Diameter Gateway, ECE HTTP Gateway, and all ECE integration packs.

> **Note**
>
> If you are upgrading an existing ECE installation, select the same options and provide the same values that you provided during the previous installation.

To install an ECE integrated system:

1. On the server on which ECE is installed, create a temporary directory (*temp_dir*).
2. Download the ECE software. See "Downloading the ECE Software" for instructions.
3. Go to the *temp_dir* directory, and run one of the following commands:
   - To start the GUI installer:

     ```
     Java_home/bin/java -jar jarfile
     ```

     where:
     - *Java_home* is the directory in which you installed the latest supported Java version.
     - *jarfile* is the ECE installer file, for example **ocece-15.2.0.0.0_generic.jar**.
   - To start the GUI installer and create a silent installer response file during the installation:

     ```
     Java_home/bin/java -jar jarfile -record -destinationFile path
     ```

     where *path* is the response file location and name.

   The Welcome window appears.
4. In the Welcome window, click **Next**.

   > **Note**
   >
   > The installer creates an **Inventory** directory if it does not detect any installed Oracle products on the system. The **Inventory** directory manages all Oracle products installed on your system.

5. In the Installation Inventory window, enter the following if you do not want to accept the defaults and then click **Next**.
   - The full path of the inventory directory
   - The name of the operating system group that has write permission to the inventory directory
6. In the Installation Location window, enter the full path or browse to the directory in which you want to install ECE and then click **Next**.

> **Note**
>
> If you have an existing ECE installation, ensure that you do not enter the path to the same directory in which the existing ECE release is installed. You can install ECE in a different directory on the same machine.

7. In the Languages Selection window, select the languages you want ECE to use and then click **Next**.
8. In the Installation Type window, select **Complete** and then click **Next**.
9. In the Select ECE Security Options window, select one of the ECE security options listed in Table 5-1 and then click **Next**.

Table 5-1 ECE Security Options

Option	Description
Security enabled with SSL	Enables the following security configurations: • SSL encryption (Impacts overall system performance) • JMX security • Authorized hosts list • Coherence node authentication • BRM SSL security authentication • PDC SSL security authentication • EM Gateway SSL security authentication
Security enabled without SSL	Enables the following security configurations: • JMX security • Authorized hosts list • Coherence node authentication
Security disabled	Enables no security configurations (Single server installation only)

10. In the Enable Persistence window, do one of the following and then click **Next**.
    - To persist all of the ECE data in the database, select **Persistence enabled** and proceed to step 12.
    - To persist only rated events in the database, select **Persistence disabled** and proceed to the next step.
11. In the Oracle NoSQL Database Details window, specify the NoSQL database connection information in Table 5-2, click **Next**, and then proceed to step 17.

> **Note**
>
> This window appears only if you selected **Persistence disabled**.

Table 5-2 Oracle NoSQL Database Details

Field	Description
Host Name	The host name or IP address of the machine on which the Oracle NoSQL database is installed.
Port Number	The port number assigned to the Oracle NoSQL database.
NoSQL Datastore Name (database name)	The name of the Oracle NoSQL data store in which you want to persist ECE rated events. This is where Rated Event Publisher writes rated events generated by the ECE server.

12. In the ECE Persistence Schema Creation window, select one of the following options and then click **Next**.
    - To have the installer create the schema user and tables for the ECE persistence schema, select **Create schema user and tables** and proceed to the next step.
    - To have the installer create only the tables for the ECE persistence schema, select **Create tables only** and proceed to step 16.
    - If you want to use existing schema users and tables, select **Use existing schema user and tables** and proceed to step 17.
13. In the ECE Persistence Database Details window, specify the information in Table 5-3 and then click **Next**.

Table 5-3 ECE Persistence Database Details

Field	Description
Host Name	The host name or IP address of the machine on which the ECE persistence database is installed.
Port Number	The non-SSL port number assigned to the ECE persistence database service.
User Name	The user name for the ECE persistence database.
Password	The ECE persistence database user password.
Service Name	The name of the ECE persistence database service. This is where all ECE data is persisted by the ECE server.
SSL Enabled	Whether to enable SSL communication between ECE and the Oracle database. The **SSL Enabled** option must be selected for production systems. If **SSL Enabled** is not selected, the subsequent fields are disabled.
TLS Version	The version of TLS to use when connecting to the database. Select **1.2**.
ORA Files Location	The location of the tnsnames.ora and sqlnet.ora files.
SSL Type	The SSL type: **One Way** or **Two Way**.
SSL Server Cert DN	The SSL server certificate distinguish name.

Table 5-3 (Cont.) ECE Persistence Database Details

Field	Description
Wallet Location	The full path to the directory from where ECE will access the SSL DB wallets.
Wallet Type	The type of wallet: **SSO** or **PKCS12**.
Wallet Password	If you selected **PKCS12**, enter the password for the SSL DB PKCS12 wallet. If you selected **SSO**, this field is grayed out.

Ensure that the Oracle Database server is in the **Running** state. The installer connects to the Oracle Database server to verify the information you entered is valid.

14. In the ECE Persistence Schema Details window, specify the information in Table 5-4, which is required to create the ECE schema in the ECE persistence database, and then click **Next**.

Table 5-4 ECE Persistence Schema Details

Field	Description
User Name	The ECE persistence schema user name.
Password	The password for the ECE persistence schema user.
Confirm Password	Enter the password for the ECE persistence schema user again.
ECE Tablespace	The name of the tablespace for the ECE schema.
Temp Tablespace	The name of the temporary tablespace for the ECE schema.

15. In the Configure Rated Event Partitions window, specify the information in Table 5-5, click **Next**, and then proceed to step 17.

Table 5-5 Configure Rated Event Partitions

Field	Description
Storage INITIAL	The RatedEvent table Storage INITIAL field data.
Storage NEXT	The RatedEvent table Storage NEXT field data.
Storage SUBPARTITIONS	The RatedEvent table Storage SUBPARTITIONS field data.

16. In the Persistence Database Details window, specify the information in Table 5-6 and then click **Next**.

> **Note**
>
> This window appears only if you selected **Create Tables Only** for the ECE persistence schema.

Table 5-6 Persistence Database Details

Field	Description
User Name	The ECE persistence schema user name.
Password	The password for the ECE persistence schema user.

JDBC URL	The JDBC URL, in this format:
	`Driver:@HostName:Port:ServiceName`
	where:
	• *Driver* is the driver used to connect to Oracle Database.
	• *HostName* is the IP address or the host name of the computer on which the ECE persistence database is configured.
	• *Port* is the non-SSL port number assigned to the ECE persistence database service.
	• *ServiceName* is name of the ECE persistence database service.
	For example:
	`jdbc:oracle:thin:@localhost:1521:orcl`

SSL Enabled	Whether to enable SSL communication between ECE and the Oracle database. Select the **SSL Enabled** option for production systems. When disabled, the subsequent fields are disabled.
SSL Type	Select the SSL type: **One Way** or **Two Way**.
SSL Server Cert DN	The SSL server certificate distinguish name.
Wallet Location	The location of SSL database wallet.
Wallet Type	The type of SSL database wallet: **SSO** or **PKCS12**.
Wallet Password	The password of the SSL database wallet.

17. In the Config Data Details window, enter the path or browse to the directory in which ECE retrieves the XML files that contain your configuration data (mediation specifications). Click **Next**.

    After installation, when you load data into ECE, the loading utility reads and loads configuration data from this directory.

18. In the Pricing Data Details window, enter the path or browse to the directory in which ECE retrieves the XML files that contain your pricing data. Click **Next**.

    After installation, when you load data into ECE, the loading utility reads and loads pricing data from this directory.

19. In the Customer Data Details window, enter the path or browse to the directory in which ECE retrieves the XML files that contain your customer data. Click **Next**.

    After installation, when you load data into ECE, the loading utility reads and loads customer data from this directory.

20. In the CrossRef Data Details window, enter the path or browse to the directory in which ECE retrieves the XML files that contain your cross-reference data. Click **Next**.

After installation, when you load data into ECE, the loading utility reads and loads cross-reference data from this directory.

21. In the PayLoad Config file Details window, enter the path or browse to the directory in which ECE retrieves the XML files that contain your payloadconfig data. Click **Next**.

    After installation, when you load data into ECE, the loading utility reads and loads payloadconfig data from this directory.

22. In the Rated Event Manager Config File Details window, enter one of the following in the **REF MODE** field and then click **Next**.

    - **CDR** to only generate CDRs.
    - **DIRECT** to load data directly into BRM.
    - **CDR_DIRECT** to load data directly into BRM, and generate CDRs for audit purposes.

23. In the Persistence Data Details window, enter the path or browse to the directory into which the ECE BrmCdrPluginDirect Plug-in will write call detail record (CDR) files of rated events. Click **Next**.

    This is the directory where the plug-in stores completed CDR files that are ready to be processed by BRM.

24. In the ECE Cluster Details window, enter the information in Table 5-7 and then click **Next**.

Table 5-7 ECE Cluster Details

Field	Description
User Name for Host Machines	The user name you specified when you created the ECE user account prior to installation. All machines in the cluster must have the same user name. This is used by ECE to identify the remote machines on which to deploy ECE.
Java Heap Settings	The memory to allocate to each node in the ECE cluster. The memory applies to each node for the driver machine and all server machines.
Cluster Name	The cluster name used by applications to identify ECE in the cluster. For example, Oracle Enterprise Manager Cloud Control uses the cluster name to locate ECE nodes for monitoring. The cluster name must contain fewer than 32 characters.
Non Active-active multi site deployment	Select this if you do not plan to set up an active-active disaster recovery system. **Note**: If you select this option, skip to step 26.
Active-Active multi site deployment	Select this if you plan to set up an active-active disaster recovery system. This is selected by default.

25. In the ECE Active Active Clusters window, enter the names of all clusters in your active-active sites, separated by commas. Ensure that you enter the current cluster's name. Click **Next**.

> **Note**
>
> This window appears only if you selected **Active-Active multi site deployment**.

26. In the Coherence Grid Security window, specify the machines allowed to be part of the Coherence cluster and the credentials required for accessing the cluster, and then click **Next**.

> **Note**
>
> If you selected the **Security disabled** option, this window does not appear. Go to step 27.

To specify the machines, do one or both of the following:

- In the **Host Details in comma separated format** field, list the host names or IP addresses of all machines on which ECE nodes will reside. Separate each value with a comma.

  Include your computer name in this field. *Do not* enter **localhost** or a loopback address.

  Include all server machines across which the Coherence grid is deployed and any other machine that is to be part of the grid.
- Specify a range of allowed addresses for hosts in the same subnet as follows:

  In the **Host Details Range from IP Address** field, enter the valid IP address that starts the range.

  In the **Host Details Range to IP Address** field, enter the valid IP address that ends the range.

To specify the credentials required to access the cluster:

- In the **Alias Name for Coherence grid security** field, enter the account alias that defines the administrator for securing the Coherence cluster.
- In the **Password for the alias** field, enter the password used to access the cluster security key in the Coherence KeyStore (the *ECE_home***/oceceserver/config/server.jks** file).

  This is the password for Coherence cluster security.

  You use this password when enabling secure socket layer (SSL).

  For more information, see "Setting Up Cluster Security" in *BRM System Administrator's Guide*.

27. In the KeyStore Credentials window, specify the KeyStore credential information in Table 5-8 and then click **Next**.

Table 5-8 KeyStore Credentials

Field	Description
Key Password for boundary system alias	The password ECE uses to access the server JKS file.

Table 5-8 (Cont.) KeyStore Credentials

Field	Description
Certificate store password	The password used to access the server JKS file.

DName	The credentials that define what users are authorized to do regarding cluster security.
	Examples:
	`CN=Administrator,OU=Rating,O=CompanyB`
	Or:
	`CN=Developer,OU=ECE`
	where:
	• CN is the common name for the user.
	• OU is the organizational unit of the user.
	• O is the organization of the user.
	The combined **DName** values are similar to a group in Linux.
	Tip: The value set here (in creating the certificate) is used for authentication in the cluster and must be the same as the value used in the *ECE_home*/**oceceserver/config/permissions.xml** file, which is created after installation and used for authorization in the cluster.
	You use the DName value when enabling SSL.
	The DName value is used as a command line parameter for creating the **server.jks** keystore.

28. In the Oracle Wallet Details window, specify the ECE wallet details in Table 5-9 and then click **Next**.

Table 5-9 Oracle Wallet Details

Field	Description
Wallet Location	The full path or browse to the directory in which you want to store the Oracle wallet for ECE.
Wallet Password	The password for the ECE wallet.
Confirm Wallet Password	The password for the ECE wallet again.

29. In the Kafka or WebLogic JMS window, specify whether to use Apache Kafka topics or WebLogic JMS queues for ECE and then click **Next**.

    If you selected **Kafka**, proceed to the next step.

    If you selected **WebLogic JMS**, proceed to step 31.

30. In the Kafka Configuration Details window, enter the information in Table 5-10, click **Next**, and then proceed to step 33.

Table 5-10 Kafka Configuration Details

Field	Description
Enable SSL Connection for Kafka	Whether to enable an SSL connection for Kafka.
Host Name and Port	The host name and port number of the machine on which Apache Kafka is installed.
Kafka TrustStore Location	(If you have selected to use SSL with Kafka) The directory in which the TrustStore file is located.
Kafka TrustStore Password	(If you have selected to use SSL with Kafka) The password for the TrustStore.
Topic Name	The name of the Kafka topic in which ECE will publish notifications.
Suspense Topic Name	The name of the Kafka topic in which BRM will publish failed notifications.
Failure Topic Persistence Enabled	Whether to save information about failed usage requests to the persistence database.
Failure Topic Name	(if failure topic persistence is enabled) The name of the Kafka topic in which ECE publishes failed ECE usage requests.
Overage Topic Name	The name of the Kafka topic in which ECE publishes overage records, which contain details about usage overage amounts for prepaid customers.
Partitions	The number of partitions to create in your Kafka topics. The recommended number to create is calculated as follows: [(Max HTTP Gateway Nodes) + (Max Diameter Gateway Nodes * Max Diameter Clients) + (1 for BRM Gateway) + (1 for Internal Notifications)] For example, if you have 2 HTTP Gateway nodes, 4 Diameter Gateway nodes, 10 Diameter Gateway clients, and a BRM Gateway, you would need [(2 + (4 * 10) + 1 + 1) = 44 Kafka partitions. Arbitrarily, you can set this to a maximum value.
Failure Partitions	The number of partitions to create in your failure topic.
Replication Factor	The number of replications to create.

31. In the ECE Notification Queue Details window, enter the Java Message Service (JMS) credentials in Table 5-11 and then click **Next**.

    ECE publishes notifications into this JMS queue, which external systems can use to obtain data for their own processing.

> **Note**
>
> After you enter the JMS credentials, the installer checks the connection to your WebLogic Server through TCP Port 7. Ensure that TCP Port 7 is open in your WebLogic server's firewall.

After you install ECE, you run a postinstallation script that creates the JMS queue on the server.

Table 5-11 ECE Notification Queue Details

Field	Description
Host Name	The host name of the server on which the JMS queue (JMS topic) resides.
Port Number	The port number of the server on which the JMS queue (JMS topic) resides.
User Name	The user name for logging in to the server on which the JMS queue (JMS topic) resides.
Password	The password for logging in to the server. on which the JMS queue (JMS topic) resides.
Connection Factory Name	The connection factory name used to create connections to the JMS queue (JMS topic) queue. After installing ECE, you run an ECE postinstallation script that creates the JMS queue (JMS topic) on the server. The connection factory name entered here is used by the script to create connections to the JMS queue.
Topic Name	The name of the JMS queue on the server, to which ECE publishes notification events. After installing ECE, you run a postinstallation script that creates the JMS queue (JMS topic) on the server. The topic name entered here is the name the ECE postinstallation script uses to create the JMS queue.
Suspense Queue Name	The name for the suspense queue to which ECE pushes the failed notifications.

32. In the ECE Notification Queue SSL Details window, enter the information in Table 5-12, which is required to connect to the Java Message Service queue to which ECE publishes notification events. Click **Next**.

Table 5-12 ECE Notification Queue SSL Details

Field	Description
Disable SSL	If you do not want to use SSL to encrypt communication between ECE and the JMS queue, select the **Disable SSL** option. If you select this option, do not enter values in the following fields.
Keystore password	The password used to access the SSL keystore file.
Keystore location	The full path to the SSL keystore file.

33. In the Diameter Gateway Details window, enter the information in Table 5-13 and then click **Next**.

    The Diameter Gateway details you enter in this window apply to one Diameter Gateway node instance that listens to *all* network interfaces for Diameter messages, which is suitable for basic testing directly after installation.

For a distributed environment, you must add Diameter Gateway node instances to your topology and configure a unique network interface for each instance after installation.

Table 5-13 Diameter Gateway Details

Field	Description
Skip	If you do not want Diameter Gateway to start when ECE starts, select the **Skip** option. If you select this option, do not enter values in the following fields.
Origin Host	The value for the Origin-Host attribute-value pair (AVP) to be sent in the Diameter request. This is a unique identifier that you assign your Diameter Gateway server on its host. It can be any string value. The value set here is used by the Diameter client to identify your Diameter Gateway server as the connecting Diameter peer that is the source of the Diameter message. For more information about how the Origin-Host AVP can be specified, refer to Internet Engineering Task Force (IETF) Network Working Group RFC 3588 (Diameter Base Protocol).
Origin Realm	The value for the Origin-Realm AVP to be sent by the Diameter Gateway in outgoing Diameter requests. This is the signaling realm (domain) that you assign your Diameter Gateway server. The value set here is used by Diameter clients to identify your Diameter Gateway server as the source of the Diameter message. For more information about how the Origin-Realm AVP can be specified, refer to Internet Engineering Task Force (IETF) Network Working Group RFC 3588 (Diameter Base Protocol).

34. In the RADIUS Gateway Details window, enter the information in Table 5-14 and then click **Next**.

The RADIUS Gateway details you enter in this window apply to a single RADIUS Gateway instance (node) that listens to *all* network interfaces for RADIUS messages, which is suitable for basic testing directly after installation.

For a distributed environment, you must add RADIUS Gateway instances (nodes) to your topology and configure a unique network interface for each instance after installation.

Table 5-14 RADIUS Gateway Details

Field	Description
Skip	If you do not want RADIUS Gateway to start when ECE starts, select the **Skip** option. If you select this option, do not enter values in the following fields.
Name	The name of the RADIUS Gateway instance.

Table 5-14 (Cont.) RADIUS Gateway Details

Field	Description
Port	The port number assigned to RADIUS Gateway.
Shared Secret	The common password shared between the RADIUS Gateway server and Network Access Server (NAS). It is used by the RADIUS protocol for security.
Wallet Location	The path to the Oracle wallet that contains the SSL authentication and signature credentials (such as private keys, and certificates) and the root key for the RADIUS Gateway server.

35. In the HTTP Gateway Details window, enter the information in Table 5-15 and then click **Next**.

Table 5-15 HTTP Gateway Details

Field	Description
Name	The name of the HTTP Gateway.
Enable HTTP2	If your HTTP Gateway server will communicate using the HTTP/2 protocol, select the **Enable HTTP2** option. Otherwise, the HTTP 1.1 protocol will be used.
Server Port	The HTTPS port number of the computer on which the HTTP Gateway resides. Enter a value only if SSL is enabled.
Server HTTP Port	The HTTPS port number of the computer on which the HTTP Gateway resides. Enter a value only if SSL is disabled.
Enable Server SSL	If you will use SSL to encrypt communication between the HTTP client and HTTP server, select the **Enable Server SSL** option. When selected, the **Server Port** is used for communication.
Enable NRF Registration	If you want this HTTP Gateway server to use NRF registration charging setting parameters for NRF registration, select the **Enable NRF Registration** option. Only one HTTP server can register to NRF. If more than one HTTP server has NRF registration enabled, the HTTP Gateway will throw an error and not start up. If NRF registration is disabled on all HTTP servers, NRF registration will not happen.

36. In the HTTP Gateway Server SSL Keystore Password Details window, specify the information in Table 5-16 and then click **Next**.

Table 5-16 HTTP Gateway Server SSL Keystore Password Details

Field	Description
Keystore Alias	The unique alias for the Keystore and trusted certificate entries. The default is **oracle**.
Keystore Type	The type of KeyStore, such as JCEKS, JKS, and PKCS12. The default is **PKCS12**.
Keystore Algorithm	The name of the algorithm used to generate the key such as RSA or DSA. The default is **RSA**.

Keystore DName	The credentials that define what users are authorized to do regarding cluster security.
	Examples:
	`CN=Administrator,OU=Rating,O=CompanyB`
	Or:
	`CN=Developer,OU=ECE`
	where:
	• CN is the common name for the user.
	• OU is the organizational unit of the user.
	• O is the organization of the user.
	The combined **DName** values are similar to a group in Linux.
	Tip: The value set here (in creating the certificate) is used for authentication in the cluster and must be the same as the value used in the *ECE_home***/ocfollowing/config/permissions.xml** file, which is created after installation and used for authorization in the cluster.
	You use the DName value when enabling SSL.
	The DName value is used as a command line parameter for creating the **server.jks** keystore.

Keystore Size	The size of the Keystore. The default is **1024**.
Keystore Password	The password used to access the SSL Keystore file.
Confirm Keystore Password	Enter the Keystore password again.

37. In the NRF, PCF and SMF SSL Configuration Details window, specify the information in Table 5-17 and then click **Next**.

Table 5-17 NRF, PCF and SMF SSL Configuration Details

Field	Description
Enable twoway SSL (mTLS)	If you will use two-way SSL between HTTP Gateway and the PCF, NRF, and SMF, select the **Enable twoway SSL (mTLS)** option.
Enable PCF SSL	If you will use SSL to encrypt communication between the HTTP Gateway and the PCF, select the **Enable PCF SSL** option.

Table 5-17 (Cont.) NRF, PCF and SMF SSL Configuration Details

Field	Description
Enable NRF SSL	If you will use SSL to encrypt communication between the HTTP Gateway and the NRF, select the **Enable NRF SSL** option.
Enable SMF SSL	If you will use SSL to encrypt communication between the HTTP Gateway and the SMF, select the **Enable SMF SSL** option.
Truststore location	The directory in which the TrustStore file is located.
Truststore type	The type of TrustStore: **SSO** or **PKCS12**. The default is **PKCS12**.
Truststore password	The password for the TrustStore.
Identity keystore location	The directory in which the Identity KeyStore certificate file is located. This field is required only when the **Enable twoway SSL (mTLS)** option is selected.
Identity keystore type	The type of KeyStore: **SSO** or **PKCS12**. The default is **PKCS12**. This field is required only when the **Enable twoway SSL (mTLS)** option is selected.
Identity keystore password	The password for the Identity KeyStore. This field is required only when the **Enable twoway SSL (mTLS)** option is selected.

38. In the Enter Details for enabling OAuth2 window, specify the information in Table 5-18 and then click **Next** if you want to enable OAuth 2.0 for 5G services in an on-premises environment.

> **Note**
>
> If **OAuth2enabled** is set to **true**, you must at least enter the **JWT Algorithm used** and **NRF Public Key Location** or **Symmetric key**.

Table 5-18 Enabling OAuth2

Field	Description
Enable OAuth2	If you want OAuth 2.0 security protocol to authenticate a 5G client's identity and authorize it to access the ECE REST API, select **Enable OAuth2**.
NRF Public Key Location	The path to the public key of the Network Repository Function. You use this when asymmetric cryptography is used to create the access token.
JWT Algorithm used	The algorithm used by the Network Repository Function to create the JSON Web Token (JWT). You use this when asymmetric cryptography is used to create the access token.

Table 5-18 (Cont.) Enabling OAuth2

Field	Description
Symmetric Key	The details of the symmetric key. It is used when you use symmetric cryptography to create the access token by the NRF. The symmetric key is stored in the ECE wallet as `oauth2.symmetric.key`.

> **Note**
>
> When you make access tokens by asymmetric cryptography, the following JWT Algorithms are supported:
>
> - RSA
> - ECDSA

39. In the BRM Database Connection Details window, specify the information in Table 5-19 and then click **Next**.

Table 5-19 BRM Database Connection Details

Field	Description
JDBC URL	The following colon-separated values: *Driver*:@*HostName*:*Port*:*ServiceName* where: • *Driver* is the driver used to connect to the BRM database. • *HostName* is the IP address or the host name of the computer on which the BRM database is configured. • *Port* is the port number assigned to the BRM database service. • *ServiceName* is name of the BRM database service. For example: jdbc:oracle:thin:@*localhost*:1521:PINDB
User Name	The BRM database schema user name.
Password	The password for the BRM database user.
Queue Name	The name of the Oracle Advanced Queuing (AQ) database queue that the Account Synchronization DM uses to publish business events for ECE to consume. ECE listens on this queue for loading update requests from BRM.

Table 5-19 (Cont.) BRM Database Connection Details

Field	Description
Suspense Queue Name	The name of the Oracle AQ database queue to which ECE moves events for failed update requests for later reprocessing. After installing ECE, you can use an ECE postinstallation script to create this queue. When prompted by the script, enter the queue name you entered here.
Acknowledgment Queue Name	The name of the Oracle AQ database queue to which ECE publishes acknowledgments for BRM. For example, ECE uses this queue to send acknowledgment events to BRM during the rerating process, indicating that the process can start or finish. After installing ECE, you can use an ECE postinstallation script to create this queue. When prompted by the script, enter the queue name you entered here.
AMT Queue Name	The name of the Oracle AQ database queue to which ECE publishes notifications for BRM.
SSL Enabled	Whether to enable SSL communication. Select the **SSL Enabled** option for production systems. If disabled, the subsequent fields are disabled.
TLS Version	The version of TLS to use when connecting to the database. Select **1.2**.
ORA Files Location	The location of the tnsnames.ora and sqlnet.ora files.
SSL Type	The SSL type: **One Way** or **Two Way**.
SSL Server Cert DN	The SSL server certificate distinguish name.
Wallet Location	The location of the SSL database wallet.
Wallet Type	The type of SSL database wallet: **SSO** or **PKCS12**.
Wallet Password	The password of the SSL database wallet.

40. In the BRM Gateway Details window, enter the information in Table 5-20 and then click **Next**.

Table 5-20 BRM Gateway Details

Field	Description
Host Name	The IP address or the host name of the computer on which BRM is configured.
CM Port	The port number assigned to the CM.
User Name	The BRM user name.
Password	The password for logging in to BRM.

Table 5-20 (Cont.) BRM Gateway Details

Field	Description
Disable SSL	If you will *not* use SSL to encrypt communication between ECE and BRM through BRM Gateway, select the **Disable SSL** option. If you select this option, do not change the value in the following field.
Wallet File Absolute Path	The path to the Oracle wallet file that contains the SSL trusted certificates for BRM Gateway. If SSL is enabled for BRM Gateway but the Oracle wallet file containing the SSL trusted certificates for BRM Gateway is not in the default location (**/opt/wallet/client/cwallet.sso**), replace the default path in the **Wallet File Absolute Path** field with the full path to the actual location.

41. In the External Manager (EM) Gateway Details window, specify the information in Table 5-21 and then click **Next**.

Table 5-21 External Manager (EM) Gateway Details

Field	Description
Number EM Gateways	The number of EM Gateway instances you want ECE to run automatically when you start EM Gateway.
Starting Port Number	The port number assigned to EM Gateway. If you have more than one EM Gateway instance, this is the starting port number. Subsequent port numbers increase by one for each additional EM Gateway instance. For example, if the starting port number is **15502** and you specify three EM Gateway instances, ports **15502**, **15503**, and **15504** are used by EM Gateway processes. Ensure that no other processes on the machine use port numbers assigned to EM Gateway instances.
Disable SSL	If you do *not* want to use SSL to encrypt communication between BRM and ECE through EM Gateway, select the **Disable SSL** option. If you select this option, do not enter or change values in the following fields.
Client Authentication Disabled	If you do *not* want authentication to be performed to check whether EM Gateway is allowed to communicate with ECE, select the **Client Authentication Disabled** option. If you select this option, do not change the value in the following fields.
Client wallet	If SSL is enabled for EM Gateway but the Oracle wallet file containing the SSL trusted certificates for EM Gateway is not in the default location (**/opt/wallet/server/cwallet.sso**), replace the default path in the **Client wallet** field with the full path to the actual location.

42. In the PDC Pricing Components Queue Details window, enter the system connection information in Table 5-22 for the server on which the JMS queue for PDC pricing component data resides. Click **Next**.

Table 5-22 PDC Pricing Components Queue Details

Field	Description
Host Name	The IP address or the host name of the computer on which the PDC JMS queue to which PDC publishes the pricing data resides.
Port Number	The port number of the computer on which the PDC JMS queue resides.
User Name	The user name for logging in to the server on which the PDC JMS queue resides.
Password	In the **Password** field, enter the password for logging in to the server on which the PDC JMS queue resides.
Disable SSL	If you will *not* use SSL to encrypt communication between BRM and PDC, select the **Disable SSL** option. If you select this option, do not enter values in the following fields.
PDC KeyStore password	The password used to access the SSL KeyStore file.
KeyStore Path	The full path to the SSL KeyStore file.

PDC publishes pricing component data into this queue. ECE will listen on this JMS queue to consume the pricing component data.

43. In the Third Party Component Details window, enter the path or browse to the directory that contains the third-party components required by ECE and then click **Next**.
44. In the Java Home Location window, enter the path or browse to the directory in which the compatible version of Java is installed and then click **Next**.
45. In the Installation Summary window, review the selections you have made in the preceding windows and then click **Install**.

    The Installation Progress window appears.

> **Note**
>
> After the installation begins, clicking **Stop installation** stops the installation process, but the files that are already copied are not removed.

46. When the installation is done, click **Next**.
47. In the Installation Complete window, click **Finish** to complete and exit.

The installer checks for all required software and displays errors if it detects any missing or unavailable components or if any connectivity issues occur.

For information about verifying the installation of ECE, see "Verifying the ECE Installation".

For information about ECE installer logs, see "Troubleshooting the ECE Installation".

Installing a Standalone ECE System

To install a standalone ECE system, select the **Standalone** installation option. An ECE standalone system is a self-contained, nonproduction version of ECE that is not integrated with BRM or Pricing Design Center (PDC). Use the standalone system for evaluation, demonstration, and functional testing.

To install a standalone ECE system:

1. On the server on which ECE is installed, create a temporary directory (*temp_dir*).
2. Download the ECE software. See "Downloading the ECE Software" for instructions.
3. Go to the *temp_dir* directory, and run one of the following commands:
   - To start the GUI installer:

     ```
     Java_home/bin/java -jar jarfile
     ```

     where:
     - *Java_home* is the directory in which you installed the latest supported Java version.
     - *jarfile* is the ECE installer file, for example **ocece-15.2.1.0.0_generic.jar**.
   - To start the GUI installer and create a silent installer response file during the installation:

     ```
     Java_home/bin/java -jar jarfile -record -destinationFile path
     ```

     where *path* is the response file location and name.

   The Welcome window appears.
4. In the Welcome window, click **Next**.

   > **Note**
   >
   > The installer creates an **Inventory** directory if it does not detect any installed Oracle products on the system. The **Inventory** directory manages all Oracle products installed on your system.

5. In the Installation Inventory window, enter the full path or browse to the directory in which you want to install ECE and then click **Next**.
   - Full path of the inventory directory
   - Name of the operating system group that has write permission to the inventory directory
6. In the Installation Location window, enter the full path or browse to the directory in which you want to install ECE and then click **Next**.

> **Note**
>
> If you have an existing ECE installation, ensure that you do not enter the path to the same directory in which the existing ECE release is installed. You can install ECE in a different directory on the same machine.

7. In the Languages Selection window, select the languages you want ECE to use and then click **Next**.
8. In the Installation Type window, select **Standalone** and then click **Next**.
9. In the ECE Security Options window, select one of the ECE security options listed in Table 5-23 and then click **Next**.

Table 5-23 ECE Security Options

Option	Description
Security disabled	Enables no security configurations. (Single server installation only)
Security enabled without SSL	Enables the following security configurations: • JMX security • Authorized hosts list • Coherence node authentication
Security enabled with SSL	Enables the following security configurations: • SSL encryption (Impacts overall system performance) • JMX security • Authorized hosts list • Coherence node authentication

10. In the Enable Persistence window, do one of the following and then click **Next**.
    - To persist all ECE data in the database, select **Persistence enabled** and proceed to step 12.
    - To persist only the rated events in the database, select **Persistence disabled** and proceed to the next step.
11. In the Oracle NoSQL Database Details window, specify the information in Table 5-24, click **Next**, and then proceed to step 16.

> **Note**
>
> This window appears only if you selected **Persistence disabled**.

Table 5-24 Oracle NoSQL Database Details

Field	Description
Host Name	The host name or IP address of the machine on which the Oracle NoSQL database is installed.
Port Number	The port number assigned to the Oracle NoSQL database.

Table 5-24 (Cont.) Oracle NoSQL Database Details

Field	Description
NoSQL Datastore Name (database name)	The name of the Oracle NoSQL data store in which you want to persist ECE rated events. This is where Rated Event Publisher writes rated events generated by the ECE server.

12. In the ECE Persistence Schema Creation window, do one of the following and then click **Next**.
    - To create user and tables for the ECE persistence schema, select **Create schema user and tables** and proceed to the next step.
    - To create only the tables for the ECE persistence schema, select **Create tables Only** and proceed to step 13.
    - If you want to use existing schema users and tables, select **Use existing schema user and tables** and proceed to step 16.
13. In the ECE Persistence Database Details window, specify the information in Table 5-25 and then click **Next**.

> **Note**
>
> Ensure that the Oracle Database server is in Running state. The installer connects to the Oracle Database server to verify the information you entered is valid.

Table 5-25 ECE Persistence Database Details

Field	Description
Host Name	The host name or IP address of the machine on which the ECE persistence database is installed.
Port Number	The non-SSL port number assigned to the ECE persistence database service.
User Name	The SYSDBA or system user name for the ECE persistence database.
Password	The ECE persistence database user password.
Service Name	The name of the ECE persistence database service. This is where all ECE data is persisted by the ECE server.
SSL Enabled	Whether to enable SSL communication between ECE and the Oracle database. The **SSL Enabled** option must be selected for production systems. If **SSL Enabled** is not selected, the subsequent fields are disabled.
TLS Version	The version of TLS to use when connecting to the database. Select **1.2**.
ORA Files Location	The location of the tnsnames.ora and sqlnet.ora files.

Table 5-25 (Cont.) ECE Persistence Database Details

Field	Description
SSL Type	The SSL type: **One Way** or **Two Way**.
SSL Server Cert DN	The SSL server certificate distinguish name.
Wallet Location	The full path to the directory from where ECE will access the SSL DB wallets.
Wallet Type	The type of wallet: **SSO** or **PKCS12**.
Wallet Password	If you selected **PKCS12**, enter the password for the SSL DB PKCS12 wallet. If you selected **SSO**, this field is grayed out.

14. In the ECE Persistence Schema Details window, specify the information in Table 5-26, click **Next**, and then proceed to step 16.

Table 5-26 ECE Persistence Schema Details

Field	Description
User Name	The ECE persistence schema user name.
Password	The password for the ECE persistence schema user.
Confirm Password	Enter the password for the ECE persistence schema user again.
ECE Tablespace	The name of the tablespace for the ECE schema.
Temp Tablespace	The name of the temporary tablespace for the ECE schema.

15. In the Persistence Database Details window, specify the information in Table 5-27 and then click **Next**.

Table 5-27 Persistence Database Details

Field	Description
User Name	The ECE persistence schema user name.
Password	The password for the ECE persistence schema user.

Table 5-27 (Cont.) Persistence Database Details

Field	Description

JDBC URL	The JDBC URL, in this format:
	`Driver:@HostName:Port:ServiceName`
	where:
	• *Driver* is the driver used to connect to Oracle Database.
	• *HostName* is the IP address or the host name of the computer on which the ECE persistence database is configured.
	• *Port* is the non-SSL port number assigned to the ECE persistence database service.
	• *ServiceName* is name of the ECE persistence database service.
	For example:
	`jdbc:oracle:thin:@localhost:1521:orcl`

SSL Enabled	Whether to enable SSL communication between ECE and the Oracle database. Select the **SSL Enabled** option for production systems. When disabled, the subsequent fields are disabled.
SSL Type	Select the SSL type: **One Way** or **Two Way**.
SSL Server Cert DN	The SSL server certificate distinguish name.
Wallet Location	The location of SSL database wallet.
Wallet Type	The type of SSL database wallet: **SSO** or **PKCS12**.
Wallet Password	The password of the SSL database wallet.

16. In the Config Data Details window, enter the path or browse to the directory where ECE retrieves the XML files that contain configuration data (mediation specifications). Click **Next**.

    After installation, when you load data into ECE, the loading utility reads and loads configuration data from this directory.

17. In the Pricing Data Details window, enter the path or browse to the directory where ECE retrieves the XML files that contain pricing data. Click **Next**.

    After installation, when you load data into ECE, the loading utility reads and loads pricing data from this directory.

18. In the Customer Data Details window, enter the path or browse to the directory where ECE retrieves the XML files that contain customer data. Click **Next**.

    After installation, when you load data into ECE, the loading utility reads and loads customer data from this directory.

19. In the PayLoad Config File Details window, enter the path or browse to the directory where ECE retrieves the XML files that contain payloadconfig data. Click **Next**.

    After installation, when you load data into ECE, the loading utility reads and loads payloadconfig data from this directory.

20. In the Rated Event Manager Config File Details window, enter one of the following in the **REF MODE** field and then click **Next**.
    - **CDR** to only generate CDRs.
    - **DIRECT** to load data directly into BRM.
    - **CDR_DIRECT** to load data directly into BRM, and generate CDRs for audit purposes.
21. In the Cross-Reference Data Details window, enter the path or browse to the directory where ECE retrieves the XML files that contain cross-reference data. Click **Next**.

    After installation, when you load data into ECE, the loading utility reads and loads cross-reference data from this directory.
22. In the Persistence Data Details window, enter the path or browse to the directory into which the ECE BrmCdrPluginDirect Plug-in will write call detail record (CDR) files of rated events. Click **Next**.

    This is the directory where the plug-in stores completed CDR files that are ready to be processed by BRM.
23. In the ECE Cluster Details window, enter the information in Table 5-28 and then click **Next**.

Table 5-28 ECE Cluster Details

Field	Description
User Name for Host Machines	The user name you specified when you created the ECE user account prior to installation. All machines in the cluster must have the same user name. This is used by ECE to identify the remote machines on which to deploy ECE.
Java Heap Settings	The memory to allocate to each node in the ECE cluster. The memory applies to each node for the driver machine and all server machines.
Cluster Name	The cluster name used by applications to identify ECE in the cluster. For example, Oracle Enterprise Manager Cloud Control uses the cluster name to locate ECE nodes for monitoring. The cluster name must contain fewer than 32 characters.
Non Active-active multi site deployment	Select this checkbox if you do not plan to set up an active-active disaster recovery system. Note: If you select this option, skip to step 25.
Active-Active multi site deployment	Select this checkbox if you plan to set up an active-active disaster recovery system. This is selected by default.

24. In the ECE Active Active Clusters window, click **Next**.

> **Note**
>
> This window appears only if you selected **Active-Active multi site deployment**.

25. In the Coherence Grid Security window, specify the machines allowed to be part of the Coherence cluster and the credentials required for accessing the cluster.

> **Note**
>
> If you selected the **Security disabled** option, this window does not appear. Proceed to step 26.

To specify the machines, do one or both of the following:

- In the **Host Details in Comma Separated Format** field, list the host names or IP addresses of all machines on which ECE nodes will reside. Separate each value with a comma.

  Include your computer name in this field. *Do not* enter **localhost** or a loopback address.

  Include all server machines across which the Coherence grid is deployed and any other machine that is to be part of the grid.
- Specify a range of allowed addresses for hosts in the same subnet as follows:

  In the **Host Details Range from IP Address** field, enter the valid IP address that starts the range.

  In the **Host Details Range to IP Address** field, enter the valid IP address that ends the range.

To specify the credentials required to access the cluster:

- In the **Alias Name for Coherence Grid Security** field, enter the account alias that defines the administrator for securing the Coherence cluster.
- In the **Password for the Alias** field, enter the password used to access the cluster security key in the Coherence KeyStore (the *ECE_home***/oceceserver/config/server.jks** file).

  This is the password for Coherence cluster security.

  You use this password when enabling SSL.

26. In the KeyStore Credentials window, specify the information in Table 5-29 and then click **Next**.

Table 5-29 KeyStore Credentials

Field	Description
Key Password for boundary system alias	The password ECE uses to access the server JKS file.
Certificate store password	The password used to access the server JKS file.

Table 5-29 (Cont.) KeyStore Credentials

Field	Description

DName	The credentials that define what users are authorized to do regarding cluster security.
	Examples:
	`CN=Administrator,OU=Rating,O=CompanyB`
	Or:
	`CN=Developer,OU=ECE`
	where:
	• CN is the common name for the user.
	• OU is the organizational unit of the user.
	• O is the organization of the user.
	The combined **DName** values are similar to a group in Linux.
	Tip: The value set here (in creating the certificate) is used for authentication in the cluster and must be the same as the value used in the *ECE_home*/**oceceserver/config/permissions.xml** file, which is created after installation and used for authorization in the cluster.
	You use the DName value when enabling SSL.
	The DName value is used as a command line parameter for creating the **server.jks** keystore.

27. In the Oracle Wallet Details window, specify the ECE wallet details in Table 5-30 and then click **Next**.

Table 5-30 Oracle Wallet Details

Field	Description
Wallet Location	The full path or browse to the directory in which you want to store the Oracle wallet for ECE.
Wallet Password	The password for the ECE wallet.
Confirm Wallet Password	The password for the ECE wallet again.

28. In the ECE Notification Queue Details window, enter the Java Message Service (JMS) credentials in Table 5-31 and then click **Next**.

    ECE publishes notification events into this JMS queue (JMS topic), which external systems can use to obtain data for their own processing.

    After you install ECE, you run a postinstallation script that creates the JMS queue (JMS topic) on the server.

Table 5-31 ECE Notification Queue Details

Field	Description
Host Name	The host name of the server on which the JMS queue (JMS topic) resides.

Table 5-31 (Cont.) ECE Notification Queue Details

Field	Description
Port Number	The port number of the server on which the JMS queue (JMS topic) resides.
User Name	The user name for logging in to the server on which the JMS queue (JMS topic) resides.
Password	The password for logging in to the server. on which the JMS queue (JMS topic) resides.
Connection Factory Name	The connection factory name used to create connections to the JMS queue (JMS topic) queue. After installing ECE, you run an ECE postinstallation script that creates the JMS queue (JMS topic) on the server. The connection factory name entered here is used by the script to create connections to the JMS queue.
Topic Name	The name of the JMS queue on the server, to which ECE publishes notification events. After installing ECE, you run a postinstallation script that creates the JMS queue (JMS topic) on the server. The topic name entered here is the name the ECE postinstallation script uses to create the JMS queue.
Suspense Queue Name	The name for the suspense queue to which ECE pushes the failed notifications.

29. In the ECE Notification Queue SSL Details window, enter the information in Table 5-32, which is required to connect to the Java Message Service queue to which ECE publishes notification events. Click **Next**.

Table 5-32 ECE Notification Queue SSL Details

Field	Description
Disable SSL	If you do not want to use SSL to encrypt communication between ECE and the JMS queue, select the **Disable SSL** option. If you select this option, do not enter values in the following fields.
Keystore password	The password used to access the SSL keystore file.
Keystore location	The full path to the SSL keystore file.

30. In the Diameter Gateway Details window, enter the information in Table 5-33 and then click **Next**.

Table 5-33 Diameter Gateway Details

Field	Description
Skip	If you do not want Diameter Gateway to start when ECE starts, select the **Skip** option. If you select this option, do not enter values in the following fields.
Origin Host	The value for the Origin-Host attribute-value pair (AVP) to be sent in the Diameter request. This is a unique identifier that you assign your Diameter Gateway server on its host. It can be any string value. The value set here is used by the Diameter client to identify your Diameter Gateway server as the connecting Diameter peer that is the source of the Diameter message. For more information about how the Origin-Host AVP can be specified, refer to Internet Engineering Task Force (IETF) Network Working Group RFC 3588 (Diameter Base Protocol).
Origin Realm	The value for the Origin-Realm AVP to be sent by the Diameter Gateway in outgoing Diameter requests. This is the signaling realm (domain) that you assign your Diameter Gateway server. The value set here is used by Diameter clients to identify your Diameter Gateway server as the source of the Diameter message. For more information about how the Origin-Realm AVP can be specified, refer to Internet Engineering Task Force (IETF) Network Working Group RFC 3588 (Diameter Base Protocol).

The Diameter Gateway details you enter in this window apply to one Diameter Gateway node instance that listens to *all* network interfaces for Diameter messages, which is suitable for basic testing directly after installation.

For a distributed environment, you must add Diameter Gateway node instances to your topology and configure a unique network interface for each instance after installation. See the discussion about adding Diameter Gateway nodes for online charging in "ECE Postinstallation Tasks".

31. In the RADIUS Gateway Details window, enter the information in Table 5-34 and then click **Next**.

Table 5-34 RADIUS Gateway Details

Field	Description
Skip	If you do not want RADIUS Gateway to start when ECE starts, select the **Skip** option. If you select this option, do not enter values in the following fields.
Name	The name of the RADIUS Gateway instance.
Port	The port number assigned to RADIUS Gateway.

Table 5-34 (Cont.) RADIUS Gateway Details

Field	Description
Shared Secret	The common password shared between the RADIUS Gateway server and Network Access Server (NAS). It is used by the RADIUS protocol for security.
Wallet Location	The path to the Oracle wallet that contains the SSL authentication and signature credentials (such as private keys, and certificates) and the root key for the RADIUS Gateway server.

The RADIUS Gateway details you enter in this window apply to a single RADIUS Gateway instance (node) that listens to *all* network interfaces for RADIUS messages, which is suitable for basic testing directly after installation.

For a distributed environment, you must add RADIUS Gateway instances (nodes) to your topology and configure a unique network interface for each instance after installation. See the discussion about adding RADIUS Gateway nodes in "ECE Postinstallation Tasks".

32. In the Third-Party Library Details window, enter the path or browse to the directory that contains the JAR files required by ECE and then click **Next**.
33. In the Java Home Location window, enter the path or browse to the directory in which the compatible version of Java is installed and then click **Next**.
34. In the Installation Summary window, review the selections you have made in the preceding windows and then click **Install**.
35. In the Installation Progress window, wait until the installation completes and then click **Next**.

> **Note**
>
> After the installation begins, clicking **Stop installation** stops the installation process, but the files that are already copied are not removed.

36. In the Installation Complete window, click **Finish** to complete and exit.

The installer checks for all required software and displays errors if it detects any missing or unavailable components or if any connectivity issues occur.

For information about verifying the installation of ECE, see "Verifying the ECE Installation".

For information about ECE installer logs, see "Troubleshooting the ECE Installation".

Installing ECE by Using the Silent Installation

The silent installation procedure enables you to perform a non-interactive installation of ECE. You can use the silent installation to install ECE quickly on multiple systems.

Silent install mode does not use the GUI and runs in the background. In this mode, you use a response file template that contains a predefined set of values to install ECE. You can generate a response file that contains the parameters and values during the ECE GUI installation.

Creating a Response File

To create a response file:

1. Create a copy of the response file that was generated during the GUI installation. See "Installing ECE by Using the GUI Installation" for more information.

   > **Note**
   >
   > The GUI installer does not store passwords provided during installation in the response file. You must manually add the passwords after creating a copy of the response file.

   You can create as many response files as needed.
2. Open the file in a text editor.
3. Modify the response file you copied by specifying the key-value information for the parameters you want in your installation.

   > **Note**
   >
   > - The response file template contains guidelines and examples on how to enter the values in the parameters.
   > - The installer treats incorrect context, format, and type values in a response file as if no value were specified.
4. Save and close the response file.

Performing a Silent Installation

To perform a silent installation:

1. Create a response file. See "Creating a Response File".
2. Copy the response file you created to the machine on which you are running the silent installation.
3. On the machine on which you are running the silent installation, go to the *temp_dir* directory to which you have downloaded the PDC server software pack, and run the following command:

   ```
   Java_home/bin/java -jar jarfile -debug -invPtrLoc Inventory_home/oraInventory/
   oraInst.loc [parameter=value] -responseFile path -silent
   ```

   where:

   - *Java_home* is the directory in which you installed the latest supported Java version.
   - *jarfile* is the ECE installer file, for example **ocece-15.2.0.0.0_generic.jar**.
   - *parameter* is the name of an installation parameter.
   - *value* is the value of the installation parameter.

- *path* is the absolute path to the response file.

For example:

```
Java_home/bin/java -jar ocece-15.2.0.0.0_generic.jar -debug -invPtrLoc
Inventory_home/oraInventory/oraInst.loc INSTALL_TYPE=Complete -responseFile /tmp/
oracle.communications.ocece.ece.rsp -silent
```

The installation runs silently in the background.

The ECE installer checks for all required software and writes errors to a log file if it detects any missing or unavailable components or if any connectivity issues occur.

For information about verifying the installation of ECE, see "Verifying the ECE Installation".

For information about ECE installer logs, see "Troubleshooting the ECE Installation".

6

Upgrading Elastic Charging Engine

Learn how to upgrade an existing Oracle Communications Billing and Revenue Management (BRM) Elastic Charging Engine (ECE) installation.

Topics in this document:

> **Note**
>
> When upgrading an existing ECE installation, note the following:
>
> - A direct upgrade from the ECE 11.1 or ECE 11.2 release is not supported. You must upgrade to ECE 12.0 before you can upgrade to ECE 15.2.
> - You can upgrade directly from ECE 12.0 Patch Set 4 or later to ECE 15.2. To upgrade from 12.0 Patch Set 3 or earlier to ECE 15.2, you must upgrade to the intermediate patch sets until you are at Patch Set 4, and then you can upgrade directly from 12.0 Patch Set 4 to 15.2.
> - The ECE Installer installs the complete ECE software and copies the configuration files to the new complete installation to match your existing ECE settings.

In this document, the current ECE release running on your system is called the *old release*. The ECE release you are upgrading to is called the *new release*.

Overview of Upgrading ECE

If you have an existing installation of ECE integrated with BRM and Pricing Design Center (PDC) and you are upgrading that installation, do the following:

> **Note**
>
> Ensure that you install these in the following order:
>
> 1. The new version of ECE.
> 2. A compatible version of BRM.
> 3. A compatible version of PDC.
>
> See "BRM Suite Compatibility" in *BRM Compatibility Matrix* for the compatible version of BRM and PDC.

1. Plan your installation. See "About Planning Your ECE Installation".
2. Review system requirements. See "ECE System Requirements".
3. Perform the pre-upgrade tasks. See "Performing the Pre-Upgrade Tasks".
4. Perform the upgrade tasks. See "Performing the Upgrade Tasks".
5. Perform the post-upgrade tasks. See "Performing the Post-Upgrade Tasks".

Performing Zero Downtime Upgrade

If you have created an active-hot standby disaster recovery system, you can use the zero downtime upgrade method to upgrade the existing ECE installation with very minimal disruption to the existing installation and the services that are provided to your customers.

> **Note**
>
> Zero downtime upgrade steps are applicable to **active-hot standby** and **active-active** systems. To upgrade an active-active system to 15.0, first mark a site as failed to put it in maintenance mode for the upgrade to 15.0.

For more information on creating an active-hot standby disaster recovery system, see "Configuring ECE for Disaster Recovery" in *BRM System Administrator's Guide*.

Before you perform the zero downtime upgrade, ensure the following:

- You have the same instances of ECE, BRM, and PDC installed in your production and backup sites.
- Both the instances of ECE, BRM, and PDC installed in your production and backup sites and all the components connected to your ECE system are currently running.

To perform the zero downtime upgrade:

1. Ensure that all the requests and updates (such as usage requests, top-up requests, and pricing and customer data updates) are routed to your production site.
2. In your backup site, do the following:
   a. Stop the BRM and PDC instances.
   b. Upgrade the BRM instance to the version compatible with your *new* release.
   c. Upgrade the PDC instance to the version compatible with your *new* release.

d. Stop replicating the ECE cache data to your production site by running the following command:

```
gridSync stop [ProductionClusterName]
```

where *ProductionClusterName* is the name of the ECE cluster in your production site.

3. In your production site, do the following:

a. Stop replicating the ECE cache data to your backup site by running the following command:

```
gridSync stop [BackupClusterName]
```

where *BackupClusterName* is the name of the ECE cluster in your backup site.

b. Verify that the ECE and BRM data updates are synchronized in real time and all the rated events are getting published to the persistence database or Oracle NoSQL database.

4. In your backup site, do the following:

a. Start the BRM and PDC instances and their processes.

b. Upgrade ECE directly to the *new* release. You can skip the "Performing a Rolling Upgrade" task.

c. Start ECE. See "Starting ECE" in *BRM System Administrator's Guide* for more information.

d. Start the following ECE processes and gateways:

> **Note**
>
> Depending on your installation, you start Diameter Gateway, RADIUS Gateway, or both.

```
start emGateway
start brmGateway
start ratedEventFormatter
start diameterGateway
start radiusGateway
```

5. Delete the **NFProfileConfiguration** and **NFServiceConfiguration** ECE Configuration MBeans from the site running the ECE 12.0 patch set (production site) before federating cache data to the backup site from the production site.

6. Start replicating the ECE cache data to your backup site by running the following commands:

```
gridSync start
gridSync replicate
```

7. If you are upgrading from ECE 12.0 Patch Set 7 or earlier, update the Kafka partitions by doing the following:

a. On your backup site, log on to the driver machine.

b. Start a JMX editor, such as JConsole, that enables you to edit MBean attributes.

c. Connect to the ECE charging server node set to start **CohMgt = true** in the *ECE_home***/oceceserver/config/eceTopology.conf** file, where *ECE_home* is the directory in which you installed the new release.

d. In the editor's MBean hierarchy, expand the **ECE Configuration** node.

e. Use the JMX editor to update the following values:

- Under **brmGatewayConfigurations** set the **kafkaPartition** value to **3**.
- Under **httpGatewayConfigurations** set the **kafkaPartition** value to **5,6,7,8,9**.

8. Repeat steps 1 through 7 for your production site. If required, you can switch the traffic from production site to the newly upgraded backup site, and perform the upgrade for the former.
9. Verify that the ECE data is automatically replicated to both sites.
10. Once the upgrade is done, you can switch the Coherence federation unidirectionally (for an **active-hot standby** system) or bidirectionally (for an **active-active** system) based on the setup.

Performing the Pre-Upgrade Tasks

Before upgrading your existing ECE system, perform these tasks:

1. Backing Up Your Existing Configuration
2. Creating the Home Directory for the New Release

Backing Up Your Existing Configuration

Back up your existing configuration and installation area (the ECE installation directory and its content: *ECE_home*). In particular, make sure you back up all customized files.

> **Note**
>
> Store this backup in a safe location. The data in these files are necessary if you encounter any issues in the installation process.

Creating the Home Directory for the New Release

Create a directory to be the new ECE home directory, *ECE_new_home*; for example, ECE_150. Because you have your old release on the same driver machine, be careful to specify the home details for the new release when you run the ECE installer. The home details consist of the home directory path and a unique name you give to the new installation.

When you run the installer, it displays the home details of any old release installations it detects on your driver machine in the **Specify Home Details** list.

Performing the Upgrade Tasks

To upgrade your existing ECE system, perform these tasks:

1. Installing the New Version of ECE for Your Upgrade
2. Reconfiguring Configuration File Settings to Match Your Old Release
3. Copying the Mediation Specification Data to the New Installation
4. Upgrading Extension Code

5. Verifying the New Parameters in the Upgraded ECE Configuration Files

Installing the New Version of ECE for Your Upgrade

Download the ECE software from the Oracle Support website (https://support.oracle.com). Then, install the ECE software into *ECE_New_home*.

Follow the instructions in "Installing Elastic Charging Engine" to install ECE.

In the **Existing ocece Installation Details** window, ensure that you enter the full path or browse to the directory in which you installed the existing ECE installation.

Reconfiguring Configuration File Settings to Match Your Old Release

After installing the new release, reconfigure the default system and business configuration files of the new installation to match the settings in your old release configuration files.

Reconfigure all settings in the files of the following directories to match your old installation settings:

- *ECE_New_home***/oceceserver**
- *ECE_New_home***/oceceserver/config**
- *ECE_New_home***/oceceserver/brm_config**

You must move the configuration data, such as your custom customer profile data and request specification files, into *ECE_New_home*.

You can also use a merge tool to merge the configuration files you have changed in your old installation with the configuration files in the new installation.

> **Note**
>
> Do not use a merge tool for reconfiguring the settings in the *ECE_home***/oceceserver/config/management/charging-settings.xml** file. New and changed properties can be introduced in this file, which would make the file difficult to merge.

To reconfigure settings of the *ECE_New_home***/config/management/charging-settings.xml** file:

1. On the driver machine, Open the *ECE_New_home***/oceceserver/config/eceTopology.conf** file.
2. For each physical server machine or unique IP address in the cluster, enable charging server nodes (such as the **ecs1** node) for JMX management by specifying a port for each node and setting it to **start CohMgt = true**.

   > **Note**
   >
   > Do not specify the same port for the JMX management service that is used by your old ECE installation. Enable charging server nodes on your new installation for JMX management by using unique port numbers.

3. Save and close the file.

4. Start the JMX-management-enabled charging server nodes by doing the following:
   a. Change directory to the *ECE_New_home***/oceceserver/bin** directory.
   b. Start Elastic Charging Controller (ECC):

      ```
      ./ecc
      ```

   c. Run the following command:

      ```
      start server
      ```

5. Access the ECE MBeans:
   a. Log on to the driver machine.
   b. Start a JMX editor, such as JConsole, that enables you to edit MBean attributes.
   c. Connect to the ECE charging server node set to **start CohMgt = true** in the *ECE_New_home***/oceceserver/config/eceTopology.conf** file.

      The **eceTopology.conf** file also contains the host name and port number for the node.
   d. In the editor's MBean hierarchy, expand the **ECE Configuration** node.
6. Use the JMX editor to enter values for all settings associated with your old release's *ECE_home***/config/management/charging-settings.xml** file and enter values for new settings introduced in the new release.

   Your configurations are saved to the *ECE_New_home***/oceceserver/config/management/charging-settings.xml** file.
7. Stop the JMX-management-enabled charging server nodes.

Copying the Mediation Specification File to the New Installation

When installing the new release, the mediation specification file is not automatically copied to the new installation.

You must manually copy the mediation specification file (for example, **diameter_mediation.spec**) in your old release's *ECE_home***/oceceserver/config/management** directory to the new installation.

Upgrading Extension Code

If you customize rating by implementing extensions using the ECE extensions interface, apply the customizations to the corresponding files of the new installation.

Upgrade your extension code and recompile it. Recompile *ECE_home***/oceceserver/config/extensions** with the new library. Ensure that the packaged extensions JAR files are available to the ECE runtime environment in the *ECE_home***/lib** folder.

Verifying the New Parameters in the Upgraded ECE Configuration Files

The upgrade process automatically adds or updates parameters in the following configuration files:

- **JMSConfiguration.xml:** The following **JMSDestination name** sections in this configuration file are updated or added:
  - **NotificationQueue:** New parameters read by the ECE charging nodes.
  - **BRMGatewayNotificationQueue:** New section read by BRM Gateway.

  - **DiameterGatewayNotificationQueue:** New section read by Diameter Gateway.
- **migration-configuration.xml:** The **pricingUpdater** section in this configuration file is updated.

Perform the following procedures to verify that the new parameters were successfully added to the configuration files and that the default values of the new and updated parameters are appropriate for your system. If necessary, change the values.

- Verifying New and Updated Parameters in the Upgraded JMSConfiguration.xml File
- Verifying New and Updated Parameters in the Upgraded migration-configuration.xml File

Verifying New and Updated Parameters in the Upgraded JMSConfiguration.xml File

To verify the new and updated parameters in the upgraded **JMSConfiguration.xml** file:

1. Open the *ECE_New_home***/config/JMSConfiguration.xml** file in a text editor.
2. Locate the **<MessagesConfigurations>** section and its three **JMSDestination name** sections.
3. In each **JMSDestination name** section, verify that the values of the following parameters are appropriate for your system:

```
<JMSDestination name="JMS_destination_name">
    <HostName>host_name</HostName>
    <Port>port_number</Port>
    <UserName>user_name</UserName>
    <Password>password</Password>
    <ConnectionFactory>connection_factory_name</ConnectionFactory>
    <QueueName>queue_name</QueueName>
    <SuspenseQueueName>suspense_queue_name</SuspenseQueueName>
    <Protocol>protocol</Protocol>
    <ConnectionURL>connection_URL</ConnectionURL>
    <ConnectionRetryCount>connection_retry_count</ConnectionRetryCount>
    <ConnectionRetrySleepInterval>connection_retry_sleep_interval
        </ConnectionRetrySleepInterval>
    <InitialContextFactory>initial_context_factory_name
        </InitialContextFactory>
    <RequestTimeOut>request_timeout</RequestTimeOut>
    <KeyStorePassword>keystore_password</KeyStorePassword>
    <keyStoreLocation>keystore_location</keyStoreLocation>
</JMSDestination>
```

   where:

   - *JMS_destination_name* is one of the following names:
     - **NotificationQueue**
     - **BRMGatewayNotificationQueue**
     - **DiameterGatewayNotificationQueue**

     > **Note**
     >
     > Do not change the value of the **JMSDestination name** parameters.

   - *host_name* specifies the name of a WebLogic server on which a JMS topic resides.

If you provided a value for the **Host Name** field on the ECE Notification Queue Details installer window, that value appears here. Add this host to the **ConnectionURL** parameter, which takes precedence over **HostName**.

- *port_number* specifies the port number on which the WebLogic server resides.

  If you provided a value for the **Port Number** field on the ECE Notification Queue Details installer window, that value appears here. Add this port number to the **ConnectionURL** parameter, which takes precedence over **Port**.

- *user_name* specifies the user for logging on to the WebLogic server.

  This user must have write privileges for the JMS topic.

- *password* specifies the password for logging on to the WebLogic server.

  When you install ECE, the password you enter is encrypted and stored in the KeyStore. If you change the password, you must run a utility to encrypt the new password before entering it here. See "About Encrypting Passwords" in *BRM Developer's Guide*.

- *connection_factory_name* specifies the connection factory used to create connections to the JMS topic on the WebLogic server to which ECE publishes notification events.

  You must also configure settings in Oracle WebLogic Server for the connection factory.

- *queue_name* specifies the JMS topic that holds the published external notification messages.

- *suspense_queue_name* specifies the name of the queue that holds failed updates sent through the BRM Gateway. This parameter is applicable only for the **BRMGatewayNotificationQueue** section.

- *protocol* specifies the wire protocol used by your WebLogic servers in the **ConnectionURL** parameter, which takes precedence over **Protocol**. The default is **t3**.

- *connection_URL* lists all the URLs that applications can use to connect to the JMS WebLogic servers on which your ECE notification queue (JMS topic) or queues reside.

> **Note**
>
> – When this parameter contains values, it takes precedence over the deprecated **HostName, Port,** and **Protocol** parameters.
>
> – If multiple URLs are specified for a high-availability configuration, an application randomly selects one URL and then tries the others until one succeeds.

Use the following URL syntax:

```
[t3|t3s|http|https|iiop|iiops]://address[,address]. . .
```

where:

– **t3, t3s**, **http**, **https**, **iiop**, or **iiops** is the wire protocol used.

For a WebLogic server, use **t3**.

– *address* is *hostlist*:*portlist*.

– *hostlist* is *hostname*[,*hostname*.]

– *hostname* is the name of a WebLogic server on which a JMS topic resides.

– *portlist* is *portrange*[+*portrange*.]

– *portrange* is *port*[-*port*.]

– *port* is the port number on which the WebLogic server resides.

Examples:

```
t3://hostA:7001
t3://hostA,hostB:7001-7002
```

The preceding URL is equivalent to all the following URLs:

```
t3://hostA,hostB:7001+7002
t3://hostA:7001-7002,hostB:7001-7002
t3://hostA:7001+7002,hostB:7001+7002
t3://hostA:7001,hostA:7002,hostB:7001,hostB:7002
```

- *connection_retry_count* specifies the number of times a connection is retried after it fails. The default is **10**.

  This applies only to clients that receive notifications from BRM.

- *connection_retry_sleep_interval* specifies the number of milliseconds between connection retry attempts. The default is **10000**.
- *initial_context_factory_name* specifies the name of the initial connection factory used to create connections to the JMS topic queue on each WebLogic server to which ECE will publish notification events.
- *request_timeout* specifies the number of milliseconds in which requests to the WebLogic server must be completed before the operation times out. The default is **3000**.
- *keystore_password* specifies the password used to access the SSL KeyStore file if SSL is used to secure the ECE JMS queue connection.
- *keystore_location* specifies the full path to the SSL KeyStore file if SSL is used to secure the ECE JMS queue connection.

4. Save and close the file.

For more information about these parameters, see "Configuring Notifications in ECE" in *ECE Implementing Charging*.

Verifying New and Updated Parameters in the Upgraded migration-configuration.xml File

To verify the new and updated parameters in the upgraded **migration-configuration.xml** file:

1. Open the *ECE_New_home***/oceceserver/config/management/migration-configuration.xml** file.
2. Locate the **pricingUpdater** section.
3. Verify that the default values of the following parameters are appropriate for your system:

```
<pricingUpdater
  . . .
  hostName="host_name"
  port="port_number"
  . . .
  connectionURL="connection_URL"
  connectionRetryCount="connection_retry_count"
  connectionRetrySleepInterval="connection_retry_sleep_interval"
```

```
. . .
protocol="protocol"
. . .
requestTimeOut="request_timeout"
. . .
</pricingUpdater>
```

where:

- *host_name* specifies the name of the server on which a JMS queue to which PDC publishes pricing data resides.

  If you provided a value for the **Host Name** field on the PDC Pricing Components Queue Details installer window, that value appears here. Add this host to the **ConnectionURL** parameter, which takes precedence over **HostName**.

- *port_number* specifies the port number of the server on which the PDC JMS queue resides.

  If you provided a value for the **Port Number** field on the PDC Pricing Components Queue Details installer window, that value appears here. Add this port number to the **ConnectionURL** parameter, which takes precedence over **Port**.

- *connection_URL* lists all the URLs that applications can use to connect to the servers on which the PDC JMS queue or queues reside.

  > **Note**
  >
  > – When this parameter contains values, it takes precedence over the deprecated **hostName, port,** and **protocol** parameters.
  >
  > – If multiple URLs are specified for a high-availability configuration, an application randomly selects one URL and then tries the others until one succeeds.

  Use the following URL syntax:

  ```
  [t3|t3s|http|https|iiop|iiops]://address[,address]. . .
  ```

  where:

  – **t3, t3s**, **http**, **https**, **iiop**, or **iiops** is the wire protocol used. For a WebLogic server, use **t3**.

  – *address* is *hostlist*:*portlist*.

  – *hostlist* is *hostname*[,*hostname*.]

  – *hostname* is the name of a server on which a PDC JMS queue resides.

  – *portlist* is *portrange*[+*portrange*.]

  – *portrange* is *port*[-*port*.]

  – *port* is the port number of the server on which the PDC JMS queue resides.

  Examples:

  ```
  t3://hostA:7001
  t3://hostA,hostB:7001-7002
  ```

  The preceding URL is equivalent to all the following URLs:

```
t3://hostA,hostB:7001+7002
t3://hostA:7001-7002,hostB:7001-7002
t3://hostA:7001+7002,hostB:7001+7002
t3://hostA:7001,hostA:7002,hostB:7001,hostB:7002
```

- *connection_retry_count* specifies the number of times a connection is retried after it fails. The default is **10**.

  This applies only to clients that receive notifications from BRM.

- *connection_retry_sleep_interval* specifies the number of milliseconds between connection retry attempts. The default is **10000**.
- *protocol* specifies the wire protocol used by the servers listed in the **ConnectionURL** parameter, which takes precedence over **Protocol**. The default is **t3**.
- *request_timeout* specifies the number of milliseconds in which requests to the PDC JMS queue server must be completed before the operation times out. The default is **3000**.

4. Save and close the file.

Performing the Post-Upgrade Tasks

After upgrading ECE, perform these tasks:

1. Deploying the New Version onto Server Machines
2. Creating Database Configurations for Multi-Site Deployments
3. Performing a Rolling Upgrade
4. Enabling Per Site Rated Event Formatter Instances in Persistence-Enabled Active-Active Systems
5. Stopping and Restoring Your ECE System

Deploying the New Version onto Server Machines

If you installed an ECE standalone installation, you can skip this task.

Deploying the new version onto the server machines means that you distribute the Elastic Charging Server node instances (charging server nodes) and other nodes defined in your topology file across the server machines.

To deploy the new version onto your server machines:

1. Open the *ECE_New_home***/config/eceTopology.conf** file and your old release topology file.
2. Verify the following:
   a. The settings in the *ECE_New_home***/config/eceTopology.conf** file are the same as specified in your old release topology file.

      Your topology configuration must be identical to that of your old installation. Oracle recommends that you copy the topology file from your old installation.

   b. All the hosts included in the *ECE_New_home***/config/eceTopology.conf** file have the same login ID (user ID) and the password-less SSH has been configured to all hosts from the driver machine.
3. Save and close the files.

4. Verify that all of the custom files and system and business configuration files of the new installation match the settings of your old installation configuration files and that your custom request specification files and custom customer profile data is being carried over.
5. Open the *ECE_New_home***/config/management/migration-configuration.xml** file.
6. Verify that the **configObjectsDataDirectory** parameter is set to the directory where you store your configuration data (mediation specification used by Diameter Gateway).
7. Save and close the file.
8. Log on to the driver machine.
9. Go to the *ECE_New_home***/bin** directory.
10. Start Elastic Charging Controller (ECC):

    ```
    ./ecc
    ```

11. Run the following command, which deploys the ECE installation onto server machines:

    ```
    sync
    ```

    The **sync** command copies the relevant files of the ECE installation onto the server machines in the ECE cluster.

Creating Database Configurations for Multi-Site Deployments

Perform this task only if your environment meets all of the following conditions:

- You are upgrading from ECE 12.0 Patch Set 3 or later to ECE 15.2.x.
- You are using Oracle Database for persistence.
- You have a multi-site deployment (either active-active or active-non-active).

To perform this configuration, run the following commands in SQL*Plus using the ECE persistence schema user

```
create table InvalidRatedEvent_BRM1(created_time number, session_id
varchar2(4000),
    schema_id int, rated_event blob, partition_time number);

create table InvalidRatedEvent_BRM2(created_time number, session_id
varchar2(4000),
    schema_id int, rated_event blob, partition_time number);

create table RatedEvent_BRM1(
    created_time number,
        session_id varchar2(4000),
        schema_id int,
        rated_event blob,
  partition_time number)
  SEGMENT CREATION IMMEDIATE
  PCTFREE 10 PCTUSED 60 INITRANS 80 MAXTRANS 255 NOCOMPRESS LOGGING
  STORAGE(INITIAL 10485760 NEXT 10485760 MINEXTENTS 1 MAXEXTENTS 2147483645
  PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1
  BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT)
  LOB (RATED_EVENT) STORE AS SECUREFILE (
    ENABLE STORAGE IN ROW CHUNK 8192 RETENTION
    NOCACHE LOGGING
    STORAGE(INITIAL 65536 NEXT 20971520 MINEXTENTS 1 MAXEXTENTS 2147483645
```

```
    PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1
    BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT))
  PARTITION BY LIST (partition_time) AUTOMATIC
  SUBPARTITION BY HASH (SESSION_ID) SUBPARTITIONS 8
  (
  PARTITION old_time VALUES (-1)
  );

create table RatedEvent_BRM2
        (created_time number,
        session_id varchar2(4000),
        schema_id int,
        rated_event blob,
  partition_time number)
  SEGMENT CREATION IMMEDIATE
  PCTFREE 10 PCTUSED 60 INITRANS 80 MAXTRANS 255
  NOCOMPRESS LOGGING
  STORAGE(INITIAL 10485760 NEXT 10485760 MINEXTENTS 1 MAXEXTENTS 2147483645
  PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1
  BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT)
  LOB (RATED_EVENT) STORE AS SECUREFILE (
    ENABLE STORAGE IN ROW CHUNK 8192 RETENTION
    NOCACHE LOGGING
    STORAGE(INITIAL 65536 NEXT 20971520 MINEXTENTS 1 MAXEXTENTS 2147483645
    PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1
    BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT))
  PARTITION BY LIST (partition_time) AUTOMATIC
  SUBPARTITION BY HASH (SESSION_ID) SUBPARTITIONS 8
  (
  PARTITION old_time VALUES (-1)
  );

commit;

create index ib_RatedEvent_BRM1 on RatedEvent_BRM1(partition_time,
created_time, schema_id)
  PCTFREE 10 INITRANS 80 MAXTRANS 255 COMPUTE STATISTICS
  STORAGE(INITIAL 20971520 NEXT 20971520 MINEXTENTS 1 MAXEXTENTS 2147483645
  PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1
  BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT)
  LOCAL;

create unique index nb1_RatedEvent_BRM1 on
RatedEvent_BRM1(partition_time,session_id)
  PCTFREE 10 INITRANS 80 MAXTRANS 255 COMPUTE STATISTICS
  STORAGE(INITIAL 20971520 NEXT 20971520 MINEXTENTS 1 MAXEXTENTS 2147483645
  PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1
  BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT)
  LOCAL;

create index ib_RatedEvent_BRM2 on RatedEvent_BRM2
  (partition_time, created_time, schema_id)
  PCTFREE 10 INITRANS 80 MAXTRANS 255 COMPUTE STATISTICS
  STORAGE(INITIAL 20971520 NEXT 20971520 MINEXTENTS 1 MAXEXTENTS 2147483645
  PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1
  BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT)
```

```
  LOCAL;

create unique index nb1_RatedEvent_BRM2 on RatedEvent_BRM2
(partition_time,session_id)
  PCTFREE 10 INITRANS 80 MAXTRANS 255 COMPUTE STATISTICS
  STORAGE(INITIAL 20971520 NEXT 20971520 MINEXTENTS 1 MAXEXTENTS 2147483645
  PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1
  BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT)
  LOCAL;

commit;
quit;
```

Performing a Rolling Upgrade

A rolling upgrade gracefully shuts down processes of an old ECE installation and starts up the processes of the new ECE installation while maintaining the operation of the overall ECE system.

> **Note**
>
> Rolling upgrades are supported for upgrades to ECE 15.2 only from ECE 15.1. Rolling upgrades from earlier releases are not supported due to updates in the supported versions of third-party software.

Rolling upgrades are intended for production systems to prevent interruption of service for customers during the upgrade. Rolling upgrades are also useful for test systems to avoid tedious restarts of ECE charging server nodes that would require reloading data from BRM and PDC to re-prime ECE caches.

> **Caution**
>
> (Productions systems) To mitigate charging server node failures that might threaten your system's ability to handle your customer base:
>
> - Schedule the rolling upgrade outside of your regular peak processing time.
> - Ensure that you have an appropriate number of charging server nodes for your customer base. If the minimum number of charging server nodes needed for your customer base is *N*, you must run at least *N+1* nodes to have uninterrupted usage processing during a rolling upgrade.

To perform a rolling upgrade:

1. Ensure that the new release is installed in a different directory from the old release.
2. Start ECC using the new installation.
3. Run the rolling upgrade script. See "Starting the Rolling Upgrade Process".
4. Verify that your new ECE installation is using the correct configuration data. See "Verifying the Configuration Data Path".

To roll back the upgrade, see "Rolling Back an Upgrade".

Starting the Rolling Upgrade Process

To start the rolling upgrade process:

1. Ensure that you deploy the new release onto server machines. See "Deploying the New Version onto Server Machines".
2. Open the *ECE_home*/**oceceserver/config/ece.properties** file in a text editor.
3. Specify the amount of time, in seconds, that the **rollingupgrade** script waits after a node has finished upgrading before starting the upgrade process for the next node by using this parameter:

   ```
   numberOfPauseSecondsForRollingUpgrade = PauseSeconds
   ```

   This is also the wait time used between rolling restarts of successive nodes.
4. Specify the maximum amount of time, in seconds, that the **rollingupgrade** script will wait for a node to start up (that is, enter the NODE_SAFE state) by setting this parameter:

   ```
   rollingUpgradePauseSecondsPerNode = MaxSeconds
   ```

   If a node's start-up time exceeds the specified number of seconds, the rolling upgrade fails.
5. (For all gateway nodes) To specify the number of seconds that the utility waits for each gateway node to restart before continuing to the next gateway node, add the following line:

   ```
   rollingUpgradeGatewayReadinessWait=seconds
   ```

   The default is 12 seconds.
6. (For individual gateway nodes) To specify the number of seconds the utility waits for a specific gateway node to restart before continuing to the next gateway node, add one or more of the following lines:

   ```
   rollingUpgradeEmGatewayReadinessWait=seconds
   rollingUpgradeCdrGatewayReadinessWait=seconds
   rollingUpgradeDiameterGatewayReadinessWait=seconds
   rollingUpgradeRadiusGatewayReadinessWait=seconds
   rollingUpgradeHttpGatewayReadinessWait=seconds
   ```

   These values override the value set in **rollingUpgradeGatewayReadinessWait**.
7. Save and close the **ece.properties** file.
8. Specify the order in which to restart nodes in the *ECE_New_home*/**config/eceTopology.conf** file. Nodes are started in the order in which they are listed in the configuration file.
9. Start the rolling upgrade in the new release while ECE is still operating on the old release by doing one of the following:
   - To upgrade all running nodes, run the following command:

     ```
     groovy:000> rollingUpgrade
     ```

All running nodes are upgraded (charging server nodes, data-loading utility nodes, data updating nodes, and so on) except for simulator nodes. Each node on the old location is brought down, upgraded, and joined back to the cluster.

- To upgrade nodes (bring them down, upgrade them, and join them back to the cluster) by node *role*, run the following commands:

  ```
  rollingUpgrade ratedEventFormatter
  rollingUpgrade server
  rollingUpgrade updater
  rollingUpgrade diametergateway
  ```

  It is recommended to first upgrade all nodes for role **ratedEventFormatter**, followed by all nodes for role **server**, followed by all nodes for role **updater**, and then followed lastly by all nodes for role **diametergateway**.

After the upgrade is completed, the new release is used. You can decide what to do with the old directory installation.

Verifying the Configuration Data Path

Before you use the new release, verify that the path to your configuration data (the path to your custom customer profile data and request specification data) is specified correctly for where the data lives on your new release.

To verify the path to the configuration data:

1. Access the ECE MBeans by launching a JMX editor and entering the IP address (or host name) and port of your JMX-management-enabled charging server node on the running new release.
2. Click the **MBeans** tab.
3. Expand **ECE Configuration**.
4. Expand **migration.loader**.
5. In the Name column, select **configObjectsDataDirectory**.
6. In the Value column, enter the directory where you store your configuration data (your mediation specification files).

   Your configuration is saved to the *ECE_New_home***/config/management/migration-configuration.xml** file (do not edit this file directly).

Rolling Back an Upgrade

To roll back an upgrade:

1. Go to the *ECE_New_home***/bin** directory.
2. Start ECC.

   ```
   ./ecc
   ```

3. Run the following command to start rolling back the upgrade:

   ```
   groovy:000> rollingUpgrade server
   ```

   One by one, each charging server node is rolled back.

4. After all charging server nodes are rolled back, restart the following nodes in the given order:

a. Pricing Updater
b. Customer Updater
c. BRM Gateway
d. Rated Event Formatter

See "Starting and Stopping ECE" in *BRM System Administrator's Guide* for information about starting these nodes.

Enabling Per Site Rated Event Formatter Instances in Persistence-Enabled Active-Active Systems

After upgrading all sites in an active-active system, you may still have a single primary Rated Event Formatter instance used by all sites. When data-persistence is enabled, you can change to the recommended architecture of one primary Rated Event Formatter instance and one secondary instance for each site. To make this change, do the following:

1. Configure your Rated Event Formatter instances in the **charging-settings.xml** file as described in "Configuring an Active-Active System" in *BRM System Administrator's Guide*.
2. Start the primary Rated Event Formatter instance on each site. You can optionally start the secondary instances as well, or you can wait until you need them for failover.

Stopping and Restoring Your ECE System

You can perform restarts of the ECE system for test systems only when it is intended to remove all data from Coherence caches.

> **Note**
>
> Restarts of the ECE system are not intended for production systems. If you are upgrading a production system, perform a rolling upgrade. See "Performing a Rolling Upgrade" for information.

To restore an upgraded ECE system:

1. Stop all ECE nodes of the old ECE installation.
2. In PDC, publish all PDC pricing data (the metadata, setup, pricing, and profile data) from the PDC database to ECE by running the following command:

   ```
   ImportExportPricing -publish -metadata -config -pricing -profile -target [ece]
   ```

   Running this command publishes all metadata, setup, pricing, and profile data from the PDC database to ECE.
3. Reconfigure the *ECE_New_home***/config/management/charging-settings.xml** file to match the settings (including customizations) in your old release and enter values for settings introduced in the new release.
4. On the driver machine, go to the *ECE_New_home***/bin** directory.
5. Start ECC:

   ```
   ./ecc
   ```

6. Enable real-time synchronization of BRM and ECE customer data updates. See "Synchronizing Data Between ECE and the BRM Database" in *ECE Implementing Charging* for more information.
7. Start ECE processes and gateways in the following order:

```
start server
start configLoader
start pricingUpdater
start customerUpdater
start emGateway
start brmGateway
start ratedEventFormatter
start diameterGateway
start radiusGateway
```

   All data is now back in the ECE data grid.

   Real-time data updates, which had been temporarily disrupted due to the shutdown, are processed upon restart.

Verifying the Installation After the Upgrade

> **Note**
>
> Test the release that you installed on a non-production system with a copy of your production data before you deploy it on a production system.

Verify the ECE installation by starting the ECE nodes in the cluster, loading the data needed for rating, and generating usage to verify that usage requests can be processed and customer balances can be impacted.

See "Verifying the ECE Installation" for information about verifying the ECE installation.

7

ECE Postinstallation Tasks

Learn about the postinstallation tasks required for Oracle Communications Billing and Revenue Management (BRM) Elastic Charging Engine (ECE). You must install or upgrade ECE before following these procedures.

Topics in this document:

Postinstallation Tasks Common to All ECE Installations

Perform the following postinstallation tasks for all ECE installation types:

1. Set the properties for your driver machine. See "Specifying Driver Machine Properties".
2. Set the properties for your server machine. See "Specifying Server Machine Properties".
3. Expose the ECE MBeans, so you can configure ECE nodes through a JMX editor. See "Enabling Charging Server Nodes for JMX Management".
4. Configure ECE to use multicast or unicast communication. See "Configuring ECE for Multicast or Unicast".
5. Configure any Diameter Gateway nodes. See "Adding and Configuring Diameter Gateway Nodes for Online Charging".
6. Configure any RADIUS Gateway nodes. See "Adding and Configuring RADIUS Gateway Nodes for Authentication and Accounting".
7. Set your system's default currency. See "Configuring Default System Currency".
8. Configure the ecs service for TLS 1.2. See "Configuring ecs for TLS 1.2".
9. Deploy ECE from the driver machine onto the server machines in the cluster. See "Deploying ECE onto Server Machines".

Specifying Driver Machine Properties

The driver machine is the machine on which you installed ECE, and it is the machine used to administer the ECE system. You specify the driver machine properties in the **ece.properties** file.

If you installed an ECE standalone installation, you must add an entry to the properties file that specifies that Oracle Communications Billing and Revenue Management (BRM) is not installed; if you do not, ECE tries to load BRM update events and cannot transition into a usage processing state.

To specify the ECE driver machine properties:

1. Open the *ECE_home***/oceceserver/config/ece.properties** file.
2. Specify the driver machine:

- For a standalone installation, set the **driverIP** parameter either to **localhost** or to the explicit IP address or hostname of the machine. For example:

  ```
  driverIP = localhost
  ```

- For an ECE system that has more than one machine, set **driverIP** to the explicit IP address value of the driver machine.

3. (ECE standalone installation) Specify that BRM is not installed by adding the following entry:

   ```
   java.property.skipBackLogProcessing=true
   ```

4. For an ECE system that has more than one machine, specify that configuration settings of a secondary machine should not be loaded into the driver machine by adding the following entry:

   ```
   loadConfigSettings = false
   ```

5. Save and close the file.

Specifying Server Machine Properties

You specify server machine properties to configure your ECE topology and tune the nodes in the cluster for garbage collection and heap size.

When you configure your ECE topology, you specify the ECE nodes in the cluster. This includes the physical host machines, or *server machines*, on which to deploy ECE nodes and the nodes themselves. Each server machine is a part of the Coherence cluster.

For an ECE standalone installation, you can accept all default values in the topology file if desired. You can add any number of charging server nodes (nodes that have the role **server** specified) and modify or delete existing charging server nodes. You must have at least one charging server node.

> **Note**
>
> The topology file is preconfigured with several nodes that are required by ECE. Do not delete existing rows in this file.

To specify server machine properties:

1. Open the *ECE_home***/oceceserver/config/eceTopology.conf** file.
2. Add a row for *each* Coherence node for each physical host computer (server machine) in the cluster.

   For example, if you have three physical server machines and each physical server machine has three nodes, you require nine rows.

3. For each row, enter the following information:

   - Name of the JVM process for that node.

     You can assign an arbitrary name. This name is used to distinguish processes that have the same role.

   - Role of the JVM process for that node.

     Each node in the ECE cluster plays a certain role.

   - Host name of the physical server machine on which the node resides.

For a standalone system, enter **localhost**.

A standalone system means that all ECE-related processes are running on a single physical server machine.

- (For multihomed hosts) IP address of the server machine on which the node resides.

  For those hosts that have multiple IP addresses, enter the IP address so that Coherence can be pointed to a port.

- Whether you want the node to be JMX-management enabled.

  See "Enabling Charging Server Nodes for JMX Management".

- The JVM tuning file that contains the tuning profile for that node.

4. (For Diameter Gateway nodes) For one Diameter Gateway node, specify a JMX port.

   Choose a port number that is not in use by another application.

   By specifying a JMX port number for one Diameter Gateway node, you expose MBeans for setting performance-related properties and collecting statistics for all Diameter Gateway node processes.

5. (For SDK sample programs) To run the SDK sample programs by using the **sdkCustomerLoader**, uncomment the line where the **sdkCustomerLoader** node is defined.

6. Save the file.

   You must specify the JVM tuning parameters (the number of threads, memory, and heap size) for each Coherence node that you specified in the **eceTopology.conf** file by editing or creating the JVM tuning file(s).

7. Open the *ECE_home***/ocecerver/config/defaultTuningProfile.properties** file.

   You can create your own JVM tuning file and save it in this directory. You can name the file what you want.

8. Set the parameters as needed.

9. Save the file.

10. In the topology file (*ECE_home***/ocecerver/config/eceTopology.conf**), ensure your JVM tuning file is associated with the node to which you want the tuning profile (as set by these parameters) to apply.

    The JVM tuning file is referenced by name in the topology file as mentioned earlier in this procedure.

Enabling Charging Server Nodes for JMX Management

After installing ECE, you may reset system configurations, such as connection parameters for connecting to other applications, and set business configurations, such as charging-related rules you want to apply at run time. To set most configuration parameters, you use a JMX editor such as JConsole. Before you can use a JMX editor to set configuration parameters, you must expose ECE MBeans. You expose ECE MBeans by enabling one ECE node for JMX management for each unique IP address in your topology. When a JMX-management-enabled node starts, it provides a JMX management service on the specified host and port which is used to expose the ECE configuration MBeans.

Though any ECE node can be enabled for JMX management, you enable charging-server nodes for JMX management to support central configuration of the ECE system. Charging-server nodes are always running, and enabling them for JMX management exposes MBeans

for all ECE node processes (such as Diameter Gateway node instances, simulators, and data loaders).

To enable a charging server node for JMX management:

1. Open the *ECE_home*/**ocecеserver/config/eceTopology.conf** file.
2. For *each* physical server machine or unique IP address in the cluster, provide the following information for *one* charging server node (node with role **server**):
   - JMX port of the JVM process for that node.

     Enter any free port, such as **9999**, for the charging server node to be the JMX-management enabled node.

     Choose a port number that is not in use by another application.

     The default port number is **9999**.
   - Specify that you want the node to be JMX-management enabled by entering **true** in the **start CohMgt** column.

     For charging server nodes (nodes with the role **server**), always enable JMX-management for the node for which a JMX port is supplied.

     Enable only one charging server node per physical server for JMX management.

     Because multiple charging server nodes are running on a single physical machine, you set **CohMgt=true** for only one charging server node on each physical machine. Each machine must have one charging server node with **CohMgt=true** for centralized configuration of ECE to work.
3. Save the file.

Configuring ECE for Multicast or Unicast

You can configure ECE for multicast or unicast communication. Oracle Coherence uses the TCMP protocol, which can use the UDP/IP multicast or UDP/IP unicast methods of data transmission over the network. See the discussion about network protocols in *Oracle Coherence Getting Started Guide* for detailed information about how Oracle Coherence uses the TCMP protocol.

When ECE is deployed in a distributed environment (multiple machines), it uses multicast or unicast for discovering other nodes when forming a cluster; for example, for allowing an newly started node to discover a preexisting cluster. Multicast is preferred because it allows packets to be sent only one time rather than sending one packet for each node. Multicast can be used only if it is enabled in the operating system and the network.

To configure ECE for multicast or unicast, see the following topics:

- To test that multicast is enabled in the operating system, see "Determining Whether Multicast Is Enabled".
- To configure ECE when using multicast, see "Configuring ECE for Multicast".
- To configure ECE when not using multicast, see "Configuring ECE for Unicast".

Determining Whether Multicast Is Enabled

To determine whether multicast is enabled in the operating system, use the Oracle Coherence multicast test utility. See "Performing a Multicast Connectivity Test" in *Oracle Coherence Administrator's Guide* for detailed information about using the multicast test utility and how to understand the output of the test.

If multicast is enabled, also use this test to determine the appropriate time-to-live value for messages on your servers. Record this information for use later.

Configuring ECE for Multicast

To configure ECE when using multicast:

1. Verify the TTL value you must use in your environment.

   See "Determining Whether Multicast Is Enabled".

2. Open the ECE Coherence override file your ECE system uses (for example, *ECE_home*/**oceceserver/config/charging-coherence-override-prod.xml**).

   To confirm which ECE Coherence override file is used, refer to the **tangosol.coherence.override** parameter of the *ECE_home*/**oceceserver/config/ece.properties** file.

   > **Tip**
   >
   > When using multicast, using **charging-coherence-override-prod.xml** enables **multicast** across multiple computers within a single sub-network.

3. In the **multicast-listener** section, update the **tangosol.coherence.ttl** parameter to match the TTL value you must use in your environment.

   For example, to set a TTL value of **4**:

   ```
   <multicast-
   listener>

      <address system-property="tangosol.coherence.clusteraddress">ip_address</
   address>
      <port system-property="tangosol.coherence.clusterport">port</
   port>
      <time-to-live system-property="tangosol.coherence.ttl">4</time-to-
   live>
   </multicast-listener>
   ```

   > **Note**
   >
   > You can segregate multiple ECE clusters within the same subnet by assigning distinct **tangosol.coherence.clusteraddress** values for each cluster.

4. Save the file.

Configuring ECE for Unicast

If multicast is not used, you must set up the Well Known Addresses (WKA) mechanism for your ECE cluster. Configuring a list of well known addresses prevents Coherence from using multicast.

To configure ECE when not using multicast:

1. Open the ECE Coherence override file your ECE system uses (for example, *ECE_home*/**oceceserver/config/charging-coherence-override-prod.xml**).

To confirm which ECE Coherence override file is used, refer to the **tangosol.coherence.override** parameter of the *ECE_home***/oceceserver/config/ece.properties** file.

2. Comment out the **multicast-listener** section.
3. Add the following **unicast-listener** section to the file:

```
<unicast-listener>
  <well-known-addresses>
    <socket-address id="id">
      <address system-propety="tangosol.coherence.wka">ip_address</address>
      <port system-property="tangosol.coherence.wka.port">port</port>
    </socket-address>
    ...
  </well-known-addresses>
  <port system-property="tangosol.coherence.localport">port</port>
</unicast-listener>
```

where:

- *id* is the ID for a particular cluster member
- **"tangosol.coherence.wka"** must refer to the machine that runs the first Elastic Charging Server node (the **ecs1** charging server node).
- *ip_address* is the IP address of the cluster member
- *port* is the value specified in the member's unicast listener port

4. Save the file.

Adding and Configuring Diameter Gateway Nodes for Online Charging

During ECE installation, if you specified that Diameter Gateway must be started when ECE is started, the ECE Installer creates a single instance (node) of Diameter Gateway (**diameterGateway1**) that is added to your topology. By default, this instance listens to all network interfaces for Diameter messages.

For a standalone installation, a single node is sufficient for basic testing directly after installation; for example, to test if the Diameter client can send a Diameter request to the Diameter Gateway node. Add additional Diameter Gateway nodes to your topology, configure them to listen on the different network interfaces in your environment, and perform performance testing. For information, see "Adding Diameter Gateway Nodes for Online Charging" in *BRM System Administrator's Guide*.

> **Note**
>
> When configuring additional Diameter Gateway nodes, ensure that you configure the Diameter peers and alternative peers for routing notifications. See "Configuring Alternative Diameter Peers for Notifications" in *ECE Implementing Charging* for more information.

Adding and Configuring RADIUS Gateway Nodes for Authentication and Accounting

During ECE installation, if you specified that RADIUS Gateway must be started when ECE is started, the ECE Installer creates a single instance (node) of RADIUS Gateway (**radiusGateway1**) that is added to your topology. By default, this instance listens to RADIUS messages.

For a standalone installation, a single node is sufficient for basic testing directly after installation; for example, to test if the RADIUS client can send a RADIUS request to the RADIUS Gateway node. Add additional RADIUS Gateway nodes to your topology and configure them to listen on the different network interfaces in your environment. For information, see "Adding RADIUS Gateway Nodes" in *BRM System Administrator's Guide*.

Configuring Default System Currency

During rating, ECE uses the subscriber's primary currency or the secondary currency for charging subscribers. If the currency used in the rate plans does not match the subscriber's primary or secondary currency, ECE uses the default system currency, US dollars.

For more information, see "Configuring Default System Currency" in *BRM System Administrator's Guide*.

Configuring ecs for TLS 1.2

To configure the ecs service for TLS 1.2:

1. Open the following files in a text editor:
   - *ECE_home*/**bin/environment.sh**
   - *ECE_home*/**config/defaultTuningProfile.properties**
   - *SDK_home*/**bin/launcher.sh**
2. Add the following lines to each file.

   ```
   -Djdk.tls.client.protocols=TLSv1.2 \
   -Djdk.tls.server.protocols=TLSv1.2
   ```

3. Save and close the files.

Deploying ECE onto Server Machines

If you installed an ECE standalone installation on a single machine only, you can skip this task.

If your ECE cluster includes multiple physical server machines, you run the ECE **sync** command to deploy ECE from the driver machine onto the server machines in the cluster.

Deploying ECE onto the server machines (in your distributed environment) means that you distribute the Elastic Charging Server node instances (charging server nodes) and other nodes defined in your topology file across the server machines.

> **Tip**
>
> For the **sync** command to work as expected, all the hosts included in the **eceTopology.conf** file must have the same login ID (user ID) and from the driver machine password-less SSH must be configured to all hosts.

To deploy ECE onto server machines:

1. Log on to the driver machine.
2. Change directory to the *ECE_home*/**oceceserver**/**bin** directory.
3. Start Elastic Charging Controller (ECC):

   ```
   ./ecc
   ```

4. Deploy the ECE installation onto server machines:

   ```
   sync
   ```

   The **sync** command copies the relevant files of the ECE installation onto the server machines you have defined to be part of the ECE cluster.

Postinstallation Tasks for an ECE Integrated Installation

For an ECE integrated installation, you perform the postinstallation tasks common to all ECE installations and also the tasks described in this section. See "Postinstallation Tasks Common to All ECE Installations" for information on common postinstallation tasks.

> **Note**
>
> HTTP Gateway does not support WebLogic JMS queues. Use Apache Kafka topics with HTTP Gateway.

For an integrated installation, after you install ECE, you must do the following:

1. If you specified to use WebLogic JMS queues during the ECE installation process, do this:
   a. Create a separate WebLogic domain for your ECE Notification queues.

      > **Note**
      >
      > Do not create your ECE notification queues in an existing WebLogic domain.

   b. Create the queues in Table 7-1 for BRM, ECE, and Pricing Design Center (PDC).

Table 7-1 WebLogic JMS Queues

Queue Name	Description
Suspense queue	Set up a suspense queue on a server running Oracle WebLogic Server where ECE publishes failed data updates from Customer Updater. See "Configuring the Customer Updater Suspense Queue" in *BRM System Administrator's Guide* for more information.
Acknowledgment queue	Set up an acknowledgment queue where ECE publishes acknowledgments for BRM. For example, ECE uses this queue to send acknowledgment events to BRM during the rerating process, indicating that the process can start or finish.
ECE notification queue (JMS topic)	Set up an ECE notification queue on a server running Oracle WebLogic Server where ECE can publish notification events for consumption by external systems, such as Oracle Communications Offline Mediation Controller. The ECE notification queue is a JMS topic; it can be on the same WebLogic server as the JMS queue where PDC publishes pricing updates. **Note:** You must create the ECE Notification queue in its own WebLogic domain. If you set up multiple JMS WebLogic servers for failover, you must enter their connection information in the *ECE_home*/**oceceserver/config/JMSConfiguration.xml** file. See "Configuring Credentials for Multiple JMS WebLogic Servers". See "Configuring Notifications in ECE" in *ECE Implementing Charging* for more information.

For instructions on creating these queues, see "Creating WebLogic JMS Queues for BRM".

2. If you specified to use Apache Kafka topics during the ECE installation process, do this:
   - Create the following Kafka topics for ECE: ECE Notification topic, ECE failure topic, Suspense topic, and ECE overage topic. For instructions on creating Kafka topics, see "Creating Kafka Topics for ECE".
   - Create the following queue for BRM: an Acknowledgment queue. For instructions on creating the queue, see "Creating WebLogic JMS Queues for BRM" except, when prompted, create only the Acknowledgment queue.
3. Install and configure your network mediation software. For example:
   - If you use Diameter Gateway as your network integration for online charging, ensure that you have added and configured Diameter Gateway nodes to listen on the different network interfaces in your environment. See "Adding and Configuring Diameter Gateway Nodes for Online Charging" for more information.
   - If you use Offline Mediation Controller as network mediation software for offline charging, see *Offline Mediation Controller Cartridge Packs* for instructions on installing and configuring Offline Mediation Controller to access ECE SDK libraries and send usage requests for offline CDRs.
4. Enable secure communication between components in the ECE integrated installation. See the following topics for more information:
   - Generating Java KeyStore Certificates
   - Exporting Java KeyStore Certificates

- Importing Java KeyStore Certificates

Creating WebLogic JMS Queues for BRM

Use the **post_Install.pl** script to create the required WebLogic JMS queues: Suspense queue, Acknowledgment queue, and Notification queue. After you use the script to create the queues, configure the queues using WebLogic Remote Console.

> **Note**
>
> If you have a multischema BRM environment, you must manually create suspense, acknowledgment, and notification queues for each secondary BRM schema by using the **pin_ifw_sync_oracle.pl** script. See "Creating Additional Queues for Multischema BRM Systems" in *BRM Installation Guide* for more information.

Location

*ECE_home***/oceceserver/post_installation/**

Syntax

```
perl post_Install.pl
```

You are prompted to install the BRM Suspense queue, Acknowledgment queue, and Notification queue. You can choose to install one, two, or all three queues.

> **Note**
>
> If you are using Kafka topics for HTTP Gateway, install only the Acknowledgment queue.

The queue names are specified during the ECE installation process and are used by the postinstallation script.

If queues are already created, you see a message in the log files. Alternatively, you can check if the BRM queues exist by querying the **user_queues** table on your BRM machine. If the suspense and acknowledgment queues are already created, a note will be logged in **brm_queue.log**. If the notification queue is already created, a note will be logged in **output.log**.

Parameters

For the BRM suspense and acknowledgment queues, you also need to enter the BRM machine password in addition to entering the following parameters:

- **BRM_HOSTNAME**: The IP address or the host name of the computer on which the BRM database is configured.
- **BRM_USER**: The BRM user name on the specified host.
- **BRM_DB_PASSWORD**: The password for the BRM database user.

For the ECE notification queue, you enter the following WebLogic server parameters:

- **JMS_PASSWORD**: The password for logging on to the WebLogic server on which the JMS queue resides.
- **JMS _MODULE NAME**: The JMS system module name of the module that has already been created on the WebLogic server.
- **JMS_SUBDEPLOYMENT**: The name of the subdeployment target in the JMS system module that has already been created on the WebLogic server.

After the JMS ECE notification queue is created, do the following in WebLogic Server:

1. Log in to WebLogic Remote Console for the domain on which the JMS topic for the ECE notification queue resides.
2. Click **Edit Tree**, then **Services**, and then **JMS Modules**.

   The Summary of JMS Modules page appears.
3. In the JMS Modules table, click the JMS topic used for ECE notifications.
4. Click **Connection Factories** in the tree in the left pane.
5. In the JMS Connection factories table, click **NotificationFactory**.
6. On the **Client** tab, do the following:
   a. Set **Client ID Policy** to **Unrestricted**.
   b. Set **Subscription Sharing Policy** to **shareable**.
   c. Click **Save**.
7. On the **Transactions** tab, do the following:
   a. Set **Transaction Timeout** to **2147483647**.
   b. Click **Save**.
8. Click the shopping cart at the top right, and then click **Commit Changes** to commit your changes.

Creating Kafka Topics for ECE

Use the **kafka_post_install.sh** script to create the ECE Notification topic, ECE failure topic, ECE External topic, Suspense topic, and ECE overage topic in Apache Kafka.

Location

*ECE_home***/ocecеserver/post_installation/**

Syntax

```
sh kafka_post_install.sh
```

When running the script, enter your Kafka **bin** path when prompted to do so.

The script creates the Kafka topics using the Kafka host name, topic names, number of partitions, and replication factor details that you specified during the ECE installation process.

Configuring Credentials for Multiple JMS WebLogic Servers

The ECE installer gathers connection information for only one JMS WebLogic server on which the ECE notification queue (JMS topic) is to reside. If your ECE system includes multiple ECE notification queue hosts for failover, you must specify connection information for *all* hosts.

To configure credentials for multiple JMS WebLogic servers:

1. Open the *ECE_home*/**ocececeserver/config/JMSConfiguration.xml** file.
2. Locate the **<MessagesConfigurations>** section.
3. Specify values for the parameters in the following **JMSDestination name** sections:
   - **NotificationQueue:** Read by the ECE charging nodes.
   - **BRMGatewayNotificationQueue:** Read by BRM Gateway.
   - **DiameterGatewayNotificationQueue:** Read by Diameter Gateway.

   > **Note**
   >
   > Do not change the value of the **JMSDestination name** parameter.

   Each **JMSDestination name** section contains the following parameters:

   - **HostName:** If you provided a value for the **Host Name** field on the ECE Notification Queue Details installer window, that value appears here. Add this host to the **ConnectionURL** parameter, which takes precedence over **HostName**.
   - **Port:** If you provided a value for the **Port Number** field on the ECE Notification Queue Details installer window, that value appears here. Add this port number to the **ConnectionURL** parameter, which takes precedence over **Port**.
   - **Protocol:** Specify the wire protocol used by your WebLogic servers in the **ConnectionURL** parameter, which takes precedence over **Protocol**.
   - **ConnectionURL:** List all the URLs that applications can use to connect to the JMS WebLogic servers on which your ECE notification queue (JMS topic) or queues reside.

     > **Note**
     >
     > When this parameter contains values, it takes precedence over the deprecated **HostName, Port,** and **Protocol** parameters.

     Use the following URL syntax:

     ```
     [t3|t3s|http|https|iiop|iiops]://address[,address]. . .
     ```

     where:

     – **t3**, **t3s**, **http**, **https**, **iiop**, or **iiops** is the wire protocol used.

     For a WebLogic server, use **t3**.

     – *address* is *hostlist*:*portlist*.

     – *hostlist* is *hostname*[,*hostname*.]

     – *hostname* is the name of a WebLogic server on which a JMS topic resides.

     – *portlist* is *portrange*[+*portrange*.]

     – *portrange* is *port*[-*port*.]

     – *port* is the port number on which the WebLogic server resides.

     Examples:

```
t3://hostA:7001
t3://hostA,hostB:7001-7002
```

The preceding URL is equivalent to all the following URLs:

```
t3://hostA,hostB:7001+7002
t3://hostA:7001-7002,hostB:7001-7002
t3://hostA:7001+7002,hostB:7001+7002
t3://hostA:7001,hostA:7002,hostB:7001,hostB:7002
```

> **Note**
>
> If multiple URLs are specified for a high-availability configuration, an application randomly selects one URL and then tries the others until one succeeds.

- **ConnectionRetryCount:** Specify the number of times a connection is retried after it fails.

  This applies only to clients that receive notifications from BRM.

- **ConnectionRetrySleepInterval:** Specify the number of milliseconds between connection retry attempts.

4. (Optional) Modify the values of the following parameters in the **JMSDestination name** section:

   - **UserName:** Specify the user for logging on to the WebLogic server.

     This user must have write privileges for the JMS topic.

   - **Password:** Specify the password for logging on to the WebLogic server.

     When you install ECE, the password you enter is encrypted and stored in the KeyStore. If you change the password, you must run a utility to encrypt the new password before entering it here. See "About Encrypting Passwords" in *BRM System Administrator's Guide*.

   - **ConnectionFactory:** Specify the connection factory used to create connections to the JMS topic on the WebLogic server to which ECE publishes notification events.

     You must also configure settings in Oracle WebLogic Server for the connection factory. See the discussion about setting up a JMS topic on a WebLogic server, see the Oracle WebLogic Server documentation.

   - **QueueName:** Specify the JMS topic that holds the published external notification messages.

   - **InitialContextFactory:** Specify the name of the initial connection factory used to create connections to the JMS topic queue on each WebLogic server to which ECE will publish notification events.

   - **RequestTimeOut:** Specify the number of milliseconds in which requests to the WebLogic server must be completed before the operation times out.

   - **KeyStorePassword:** If SSL is used to secure the ECE JMS queue connection, specify the password used to access the SSL KeyStore file.

   - **KeyStoreLocation:** If SSL is used to secure the ECE JMS queue connection, specify the full path to the SSL KeyStore file.

5. Save and close the file.

Generating Java KeyStore Certificates

To generate Java KeyStore certificates for connecting to the WebLogic server, PDC, BRM, and the HTTP Gateway:

1. Log on to the driver machine.
2. Go to the *Java_home***/bin** directory, where *Java_home* is the directory in which you installed the latest supported Java version.
3. Run the following commands:

```
keytool -genkey -alias weblogic -dname CN=commonName OU=organizationalunit
o=organization c=countryname -keyalg RSA -keypass mykeypass -keystore
mykeystore -storepass mystorepass -validity valdays

keytool -genkey -alias pdc -dname CN=commonname OU=organizationalunit
o=organization c=countryname -keyalg RSA -keypass mykeypass -keystore
mykeystore -storepass mystorepass -validity valdays

keytool -genkey -alias brm -dname CN=commonname OU=organizationalunit
o=organization c=countryname -keyalg RSA -keypass mykeypass -keystore
mykeystore -storepass mystorepass -validity valdays

keytool -genkey -alias http_gateway -dname CN=commonname
OU=organizationalunit o=organization c=countryname -keyalg RSA -keystore $
{oracleHome}/oceceserver/config/httpGatewayServer.jks -keypass mykeypass -
storepass mystorepass
```

where:

- *commonName* is the first and last name.
- *Organizationalunit* is the container within a domain which can hold users, groups, and computers.
- *Organization* is the name of the organization.
- *countryname* is the name of the country.
- *mykeypass* is the key password for the certificate.
- *mykeystore* is the KeyStore.
- *mystorepass* is the KeyStore password.
- *valdays* is the number of days that the KeyStore is valid.

The Java KeyStore certificates for the WebLogic server, PDC, and BRM are generated.

Exporting Java KeyStore Certificates

To export the Java KeyStore certificates to a file:

1. Log on to the driver machine.
2. Go to the *Java_home***/bin** directory, where *Java_home* is the directory in which you installed the latest supported Java version.

3. Run the following commands:

```
keytool -export -alias weblogic -keystore mykeystore -storepass
mystorepass -rfc -file certificatename

keytool -export -alias pdc -keystore mykeystore -storepass mystorepass -
rfc -file certificatename

keytool -export -alias brm -keystore mykeystore -storepass mystorepass -
rfc -file certificatename

keytool -export -alias http_gateway -keystore mykeystore -storepass
mystorepass -rfc -file certificatename
```

where:

- *certificatename* is the name of the file to store the Java KeyStore certificates for connecting to the WebLogic server, PDC, and BRM.
- *mykeystore* is the KeyStore.
- *mystorepass* is the KeyStore password.

The Java KeyStore certificates are exported to the certificate file. For example: **public-admin.cer**.

Importing Java KeyStore Certificates

To import the Java KeyStore certificates into the default Java KeyStore:

1. Log on to the driver machine.
2. Go to the *Java_home***/bin** directory, where *Java_home* is the directory in which you installed the latest supported Java version.
3. Run the following commands:

```
keytool -import -alias weblogic -keystore Java_home/jre/lib/security/
cacerts -storepass mystorepass -file certificatename -noprompt rm
mykeystore certificatename

keytool -import -alias pdc -keystore Java_home/jre/lib/security/cacerts -
storepass mystorepass -file certificatename -noprompt rm mykeystore
certificatename

keytool -import -alias brm -keystore Java_home/jre/lib/security/cacerts -
storepass mystorepass -file certificatename -noprompt rm mykeystore
certificatename

keytool -import -alias http_gateway -keystore Java_home/jre/lib/security/
cacerts -storepass mystorepass -file certificatename -noprompt rm
mykeystore certificatename
```

where:

- *certificatename* is the name of the certificate file in which the Java KeyStore certificates for connecting to the WebLogic server, PDC, BRM, and the HTTP Gateway are stored.

- *mykeystore* is the KeyStore.
- *mystorepass* is the KeyStore password.

The Java KeyStore certificates are imported into the default Java KeyStore.

Postinstallation Tasks for ECE Software Upgrade

After upgrading ECE, perform the following postinstallation tasks:

> **Note**
>
> Rolling upgrades are supported for upgrades to ECE 15.2 only from ECE 15.1. Rolling upgrades from earlier releases are not supported due to updates in the supported versions of third-party software.

1. Reconfigure the default system and business configuration files. See "Reconfiguring Configuration File Settings to Match Your Old Release".
2. Manually copy your existing mediation specification data to the new installation. See "Copying the Mediation Specification Data to the New Installation".
3. Apply any ECE extensions to the new installation. See "Upgrading Elastic Charging Engine".
4. Merge your existing ECE configuration files with the new installation files. See "Updating the BRM Configuration Files".
5. Deploy ECE onto your server machines. See "Deploying ECE Onto Server Machines".
6. Restore your upgraded ECE system. See "Stopping and Restoring Your ECE System".

Reconfiguring Configuration File Settings to Match Your Old Release

After installing your new version of ECE, reconfigure the default system and business configuration files of the new installation to match the settings in your old release configuration files.

Reconfigure all settings in the files of the following directories to match your old installation settings:

- *ECE_home*/**oceceserver/**
- *ECE_home*/**oceceserver/config**
- *ECE_home*/**oceceserver/brm_config**

You must move the configuration data, such as your custom customer profile data and request specification files, into the *ECE_new_home* created for the new version of ECE.

You can also use a merge tool to merge the configuration files you have changed in your old installation with the configuration files in the new installation.

> **Note**
>
> Do not use a merge tool for reconfiguring the settings in the *ECE_home***/oceceserver/config/management/charging-settings.xml** file. New and changed properties can be introduced in this file, which would make the file difficult to merge.

To reconfigure settings of the *ECE_home***/config/management/charging-settings.xml** file on your new installation:

1. On the driver machine, open the (*ECE_new_home***/oceceserver/config/eceTopology.conf**) file.
2. For each physical server machine or unique IP address in the cluster, enable charging server nodes (such as the **ecs1** node) for JMX management by specifying a port for each node and setting it to **start CohMgt = true**.

   > **Note**
   >
   > Do not specify the same port for the JMX management service that is used by your old ECE installation. Enable charging server nodes on your new installation for JMX management by using unique port numbers.

3. Save and close the file.
4. Start the JMX-management-enabled charging server nodes by doing the following:
   a. Change directory to the *ECE_new_home***/oceceserver/bin** directory.
   b. Start Elastic Charging Controller (ECC):

      ```
      ./ecc
      ```

   c. Run the following command:

      ```
      start server
      ```

5. Access the ECE MBeans:
   a. Log on to the driver machine.
   b. Start a JMX editor, such as JConsole, that enables you to edit MBean attributes.
   c. Connect to the ECE charging server node set to **start CohMgt = true** in the *ECE_home***/oceceserver/config/eceTopology.conf** file, where *ECE_home* is the directory in which you installed the old release.

      The **eceTopology.conf** file also contains the host name and port number for the node.
   d. In the editor's MBean hierarchy, expand the **ECE Configuration** node.
6. Use the JMX editor to enter values for all settings associated with your old release's *ECE_home***/config/management/charging-settings.xml** file and enter values for new settings introduced in the new release.
7. Stop the JMX-management-enabled charging server nodes.

Copying the Mediation Specification Data to the New Installation

The mediation specification data is not automatically copied to the new installation.

You must manually copy the mediation specification data (for example, **diameter_mediation.spec**) in your old release's *ECE_home***/oceceserver/config/management** directory to the new installation.

Upgrading Extension Code

If you customize rating by implementing ECE extensions using the ECE extensions API, apply the customizations to the corresponding files of the new installation.

Upgrade your extension code and recompile it. Recompile *ECE_home***/oceceserver/config/extensions** with the new library. Ensure that the packaged extensions JAR files are available to the ECE runtime environment in the *ECE_home***/lib** folder.

Updating the BRM Configuration Files

Update the BRM configuration files on your BRM installation.

Copy the *ECE_home***/oceceserver/brm_config/payloadconfig_ece_sync.xml** file to your BRM environment and merge it with the version you are currently running on the BRM installation. Add your customizations to this file.

Deploying ECE Onto Server Machines

If you installed an ECE standalone installation, you can skip this task.

Deploying ECE onto the server machines means that you distribute the Elastic Charging Server node instances (charging server nodes) and other nodes defined in your topology file across the server machines.

To deploy ECE onto your server machines:

1. Open the *ECE_new_home***/oceceserver/config/eceTopology.conf** file and your old release topology file.
2. Verify the following:
   a. The settings in the *ECE_new_home***/oceceserver/config/eceTopology.conf** file are the same as specified in your old release topology file.

      Your topology configuration must be identical to that of your old installation. Oracle recommends that you copy the topology file from your old installation.

   b. All the hosts included in the *ECE_new_home***/oceceserver/config/eceTopology.conf** file have the same login ID (user ID) and the password-less SSH has been configured to all hosts from the driver machine.
3. Save and close the files.
4. Verify that all the custom files and system and business configuration files of the new installation match the settings of your old installation configuration files. Also, ensure that your custom request specification files and custom customer profile data are being carried over.
5. Open the *ECE_new_home***/oceceserver/config/management/migration-configuration.xml** file.
6. Verify that the **configObjectsDataDirectory** parameter is set to the directory where you store your configuration data (mediation specification used by Diameter Gateway).
7. Save and close the file.

8. Log on to the driver machine.
9. Change directory to *ECE_new_home***/oceceserver/bin**.
10. Start ECC:

    ```
    ./ecc
    ```

11. Run the following command, which deploys the ECE installation onto server machines:

    ```
    sync
    ```

    The **sync** command copies the relevant files of the ECE installation onto the server machines in the ECE cluster.

Stopping and Restoring Your ECE System

Perform this task only if you want to restore the upgraded ECE system.

> **⚠ Caution**
>
> Restarting the ECE system removes all data from Coherence caches (stopping all charging server nodes removes all data from Coherence caches).

To restore an upgraded ECE system:

1. Stop all ECE nodes of the old ECE installation.
2. In PDC, publish all the PDC pricing data (the metadata, setup, pricing, and profile data) from the PDC database to ECE by running the following command:

    ```
    ImportExportPricing -publish -metadata -config -pricing -profile -target [ece]
    ```

    Running this command publishes all the metadata, setup, pricing, and profile data in the PDC database to ECE.
3. Ensure that you have reconfigured the *ECE_new_home***/config/management/charging-settings.xml** file to match the settings (including customizations) in your old release and enter values for settings introduced in the new release.
4. On the driver machine, go to the *ECE_new_home***/oceceserver/bin** directory.
5. Start ECC:

    ```
    ./ecc
    ```

6. Enable real-time synchronization of BRM and ECE customer data updates. See "Synchronizing Data Between ECE and the BRM Database" in *ECE Implementing Charging* for more information.
7. Start ECE processes and gateways in the following order:

> **ⓘ Note**
>
> Depending on your installation, you start Diameter Gateway, RADIUS Gateway, or both.

```
start server
start configLoader
start pricingUpdater
start customerUpdater
start emGateway
start brmGateway
start ratedEventFormatter
start diameterGateway
start radiusGateway
```

All data is now back in the ECE data grid.

Real-time data updates, which had been temporarily disrupted due to the shutdown, are processed upon restart.

8

Verifying the ECE Installation

Learn how to verify that Oracle Communications Billing and Revenue Management (BRM) Elastic Charging Engine (ECE) was installed correctly.

Topics in this document:

About Verifying the ECE Installation

In general, you verify the ECE installation by starting the ECE nodes in the cluster, loading the data needed for rating, and generating usage to verify that usage requests can be processed and customer balances can be impacted.

The specific tasks involved in verifying the ECE installation depend on whether you installed an ECE standalone installation or an ECE integrated installation.

About Verifying an ECE Standalone Installation

Verifying an ECE standalone installation involves using sample data to verify that ECE can process requests when working with other applications such as Pricing Design Center (PDC) and Oracle Communications Billing and Revenue Management (BRM) without having to connect to those applications. The ECE installer installs the sample data that you need for verifying the installation. Sample data includes request specification data, sample customer accounts, sample configuration data (such as credit card profile information), and sample pricing data.

About Verifying an ECE Integrated Installation

Verifying an ECE integrated installation involves performing tasks that require all products in the integrated system so you can verify that all product integration points are configured correctly.

The following are some general tasks involved in verifying an ECE integrated installation.

- Defining your pricing in PDC and successfully loading the pricing data into ECE
- Extracting data from BRM and successfully loading it into ECE
- Creating a new customer in BRM and having the customer successfully updated in ECE
- Rating usage requests in ECE and successfully creating CDR files of the rated events by the BrmCdrPluginDirect Plug-in
- Loading CDR files into BRM and successfully updating the customer balances in BRM from the loading of those files into the BRM database

- Generating usage to verify that usage requests can be processed and customer balances can be impacted
- Create usage requests and successfully submitting them to ECE for processing
- Rating usage requests in ECE and successfully created CDR files containing the rated events
- Loading the CDR files into BRM and successfully updating the customer balances in BRM

For verifying an integrated installation in the most minimal way, you need only set up one product offering in PDC and create one customer account in BRM.

Verifying an ECE Standalone Installation

To verify an ECE standalone installation, perform these tasks:

1. Starting ECE Nodes in the Cluster
2. Loading Sample Data
3. Verifying that Usage Requests Can Be Processed for a Standalone Installation

Starting ECE Nodes in the Cluster

To start all ECE charging server nodes in the cluster:

1. Log on to the driver machine.
2. Change directory to the *ECE_home*/**oceceserver/bin** directory.
3. Start the Elastic Charging Controller (ECC):

   ```
   ./ecc
   ```

4. Start the ECE nodes by running the following command:

   ```
   start
   ```

To verify that the ECE nodes are running:

1. Access the ECE MBeans:
   a. Log on to the driver machine.
   b. Start the ECE charging servers (if they are not started).
   c. Start a JMX editor, such as JConsole, that enables you to edit MBean attributes.
   d. Connect to the ECE charging server node set to **start CohMgt = true** in the *ECE_home*/**oceceserver/config/eceTopology.conf** file.

      The **eceTopology.conf** file also contains the host name and port number for the node.
   e. In the editor's MBean hierarchy, expand the **ECE State Machine** node.
2. Expand **StateManager**.
3. Expand **Attributes**.
4. Verify that the **stateName** attribute is set to **Initial**.

   This means the ECE nodes are running.

Loading Sample Data

You load sample data so that you can rate simulated usage by using the ECE simulator.

This procedure assumes you are in the *ECE_home*/**ocececeserver/bin** directory and have started the ECE nodes. See "Starting ECE Nodes in the Cluster" for instructions on starting the ECE nodes.

To load sample data, run the following commands:

```
start configLoader
start customerLoader
```

The **loader** utility generates and loads the sample data and puts the nodes in a usage processing state. The **customerLoader** utility loads both the cross-reference data and the customer data.

To verify that the ECE nodes are in a usage processing state:

1. Access the ECE MBeans:
   a. Log on to the driver machine.
   b. Start the ECE charging servers (if they are not started).
   c. Start a JMX editor, such as JConsole, that enables you to edit MBean attributes.
   d. Connect to the ECE charging server node set to **start CohMgt = true** in the *ECE_home*/**ocececeserver/config/eceTopology.conf** file.

      The **eceTopology.conf** file also contains the host name and port number for the node.
   e. In the editor's MBean hierarchy, expand the **ECE State Machine** node.
2. Expand **StateManager**.
3. Expand **Attributes**.
4. Verify that the **stateName** attribute is set to **UsageProcessing**.

   This means the ECE nodes are running in a usage processing state.

Verifying that Usage Requests Can Be Processed for a Standalone Installation

You use the ECE simulator to run a sample workload and verify that usage requests can be processed. The simulator emulates network traffic coming from network mediation software and uses the sample data that you loaded to process the usage requests. You use the Coherence query tool to verify that the usage has impacted the sample customer's balance.

The simulator allows you to control the types of usage requests sent and the number and type of subscribers sending the usage requests. See "Running the Simulator to Send Usage Requests" in *ECE Implementing Charging* for more information.

This procedure assumes you are in the *ECE_home*/**ocececeserver/bin** directory and have started the ECE nodes and loaded sample data. See "Starting ECE Nodes in the Cluster" and "Loading Sample Data" for instructions.

To verify that usage requests can be processed:

1. Start the ECE simulator:

```
start simulator
```

2. Initialize the simulator:

   ```
   init simulator
   ```

3. Run the sample workload:

   ```
   simulate simulator
   ```

   The simulator will take a few seconds to complete processing the workload.

   This command sends requests to the ECE charging server.

4. Open the **invocation.log** file located in *ECE_home***/oceceserver**. You should see statistics for the sample workload.

5. From the *ECE_home***/oceceserver/bin** directory, enter the following commands to run the Coherence query tool:

   ```
   ./query.sh
   select * from Customer
   ```

   This command returns all customer information.

6. In the results of the query that are returned, locate the following string:

   ```
   {currentBalance=UnitValue{quantity=amount, unit=Money{cur=USD}
   ```

   where *amount* shows the quantity amount of the balance impact.

Verifying an ECE Integrated Installation

To verify that you can start charging server nodes in an integrated installation, see "Starting Charging Server Nodes in a Distributed Environment".

Starting Charging Server Nodes in a Distributed Environment

To start all ECE charging server nodes across the cluster in a distributed environment (over multiple physical server machines):

1. Log on to the driver machine.
2. Change directory to the **bin** directory:

   ```
   cd ECE_home/oceceserver/bin
   ```

3. Start ECC:

   ```
   ./ecc
   ```

4. Start ECE charging server nodes on all server machines in your distributed environment by running the following command:

   ```
   start
   ```

To verify that the ECE charging server nodes are running:

1. Access the ECE MBeans:
   a. Log on to the driver machine.
   b. Start the ECE charging servers (if they are not started).
   c. Start a JMX editor, such as JConsole, that enables you to edit MBean attributes.

d. Connect to the ECE charging server node set to **start CohMgt = true** in the *ECE_home***/oceceserver/config/eceTopology.conf** file.

   The **eceTopology.conf** file also contains the host name and port number for the node.

e. In the editor's MBean hierarchy, expand the **ECE State Machine** node.

2. Expand **StateManager**.
3. Expand **Attributes**.
4. Verify that the **stateName** attribute is set to **Initial**.

   This means the ECE charging server nodes are running.

Troubleshooting the ECE Installation

The ECE installer writes information to log files. You can check these log files for information about errors and actions performed during the installation.

Installation Log Files

The ECE installation logs can be found at *CentralInventorylocation***/oraInventory/logs**, where *CentralInventorylocation* is the directory path to the **oraInventory** directory. You can specify any inventory path.

You use the following log files to monitor installation and postinstallation steps:

- **installAction***TimeStamp***.log**
- **oraInstall***TimeStamp***.err**
- **oraInstall***TimeStamp***.out**
- **silentInstall***TimeStamp***.log** (for silent mode installation)

Next Steps

After installing and verifying the ECE installation, you perform additional tasks to set up your test or production system:

- Complete the integration between ECE, BRM, and PDC:
  - Define your event definitions in PDC.
  - Set up all your product offerings in PDC and publish them to the JMS pricing component queue.
  - Synchronize your PDC product offerings with BRM.
- Set up ECE system security.
- Configure the ECE system.
- Configure ECE to purge rated events that are no longer needed from the Oracle NoSQL Database so that rated events can be maintained at a manageable level.

9

Uninstalling ECE

Learn about the tasks you perform to uninstall the Oracle Communications Billing and Revenue Management (BRM) Elastic Charging Engine (ECE) software from your computer.

Topics in this document:

- Uninstalling the ECE Software
- Uninstalling ECE in Silent Mode

To uninstall the Oracle database, see the database vendor's documentation for your platform.

Uninstalling the ECE Software

You can use Oracle Universal Installer to uninstall the ECE software.

> **Note**
>
> Uninstalling ECE does not uninstall the configuration files generated during the ECE installation. You must remove these files manually.

To uninstall ECE:

1. Go to the *ECE_home***/oui/bin** directory, where *ECE_home* is the directory in which you installed ECE.
2. Run the following command:

   ```
   ./deinstall.sh
   ```

   The Distribution to Uninstall window appears.
3. Select the ECE software.
4. Click **Uninstall**.

   The Welcome window appears.
5. Click **Next**.

   The Uninstallation Summary window appears.
6. Click **Uninstall**.

   The Uninstallation Progress window appears.
7. Click **Next**.

   The Uninstallation Complete window appears.
8. Click **Finish**.

Uninstalling ECE in Silent Mode

To uninstall ECE in the silent mode:

1. Go to the *ECE_home***/oui/bin** directory.
2. Run the following command:

   ```
   ./deinstall.sh -responseFile path -silent -uninstall
   ```

   where *path* is the absolute path to the response file that you created in the root directory during the GUI installation of ECE.