Oracle® Communications Billing and Revenue Management

Elastic Charging Engine 11.3 Installation Guide

Release 7.5

E70767-10

November 2018

ORACLE

Oracle Communications Billing and Revenue Management Elastic Charging Engine 11.3 Installation Guide, Release 7.5

E70767-10

Contents

7 ECE Post-Installation Tasks

8 Verifying the ECE Installation

A Elastic Charging Engine Installer Screens

Preface

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 Elastic Charging Engine Concepts*.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Accessing Oracle Communications Documentation

ECE documentation and additional Oracle documentation; such as Oracle Database documentation, is available from Oracle Help Center:

- http://docs.oracle.com

Additional Oracle Communications documentation is available from the Oracle software delivery Web site:

- https://edelivery.oracle.com

Document Revision History

The following table lists the revision history for this book.

Version	Date	Description
E70767-01	April 2016	Initial release.
E70767-02	September 2016	Documentation updates for ECE 11.3 Patch Set 1. ■ Renamed and updated the following chapters: Upgrading to ECE 11.3 Patch Set 1 ■ Updated the following sections: Software Requirements Required BRM Information Installing All ECE Components Installing a Standalone ECE System Installing Individual ECE Components Performing a Silent Installation ■ Updated the following information: All procedures involving MBeans
E70767-03	December 2016	Documentation updates for ECE 11.3 Patch Set 2. ■ Added the following chapter: Upgrading From ECE 11.3 Patch Set 1 to ECE 11.3 Patch Set 2 ■ Updated the following sections: Software Requirements Reconfiguring Configuration File Settings to Match Your Old Release Installing All ECE Components Installing a Standalone ECE System Installing Individual ECE Components Performing a Silent Installation
E70767-04	April 2017	Documentation updates for ECE 11.3 Patch Set 3. ■ Added the following chapter: Upgrading From ECE 11.3 Patch Set 2 to ECE 11.3 Patch Set 3 ■ Updated the following sections: Software Requirements Installing All ECE Components Installing a Standalone ECE System Installing Individual ECE Components Performing a Silent Installation

Version	Date	Description
E70767-05	August 2017	Documentation updates for ECE 11.3 Patch Set 4. ■ Added the following chapter: Upgrading From ECE 11.3 Patch Set 3 to ECE 11.3 Patch Set 4 ■ Updated the following sections: Software Requirements Installing All ECE Components Installing a Standalone ECE System Installing Individual ECE Components Performing a Silent Installation
E70767-06	December 2017	Documentation updates for ECE 11.3 Patch Set 5. ■ Added the following chapter: Upgrading From ECE 11.3 Patch Set 4 to ECE 11.3 Patch Set 5 ■ Updated the following sections: Software Requirements Installing All ECE Components Installing a Standalone ECE System Installing Individual ECE Components Performing a Silent Installation
E70767-07	March 2018	Documentation updates for ECE 11.3 Patch Set 7. ■ Added the following chapter: Upgrading Existing ECE 11.3 Installation ■ Updated the following sections: Software Requirements Installing All ECE Components Installing a Standalone ECE System Installing Individual ECE Components Performing a Silent Installation ■ Removed the following chapters: Upgrading to ECE 11.3 Patch Set 1 Upgrading From ECE 11.3 Patch Set 1 to ECE 11.3 Patch Set 2 Upgrading From ECE 11.3 Patch Set 2 to ECE 11.3 Patch Set 3 Upgrading From ECE 11.3 Patch Set 3 to ECE 11.3 Patch Set 4 Upgrading From ECE 11.3 Patch Set 4 to ECE 11.3 Patch Set 5 For ECE 11.3 upgrade instructions, see "Upgrading Existing ECE 11.3 Installation".

Version	Date	Description
E70767-09	July 2018	Documentation updates for ECE 11.3 Patch Set 8. ■ Added the following sections: Performing Zero Downtime Upgrade Configuring Persistence Environment Upgrading to ECE 11.3 Patch Set 7 Upgrading to ECE 11.3 Patch Set 8 ■ Updated the following sections: Software Requirements Overview of Upgrading Existing ECE 11.3 Installation Performing a Rolling Upgrade
E70767-10	November 2018	Documentation updates for ECE 11.3 Patch Set 9. ■ Updated the following sections: Software Requirements Overview of Upgrading Existing ECE 11.3 Installation Obtaining the ECE 11.3 Patch Set Software Loading Pricing Data From PDC into ECE

1

ECE Installation Overview

This chapter provides an overview of Oracle Communications Billing and Revenue Management Elastic Charging Engine (ECE) installed components and of the ECE installation process.

See the discussion about system architecture in *BRM Elastic Charging Engine Concepts* for information about ECE components.

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 your first installation, you typically install the ECE Server component only. This is called an ECE standalone installation. This is a test system only. Use this installation to get familiar with ECE and charge simulated usage by using sample data and sample programs provided with ECE. You use this installation before integrating ECE with other products.
- For your second or subsequent installation, you typically install the ECE Server component and the ECE integration packs. This is called an ECE integrated installation. Use this installation to integrate ECE with Oracle Communications Billing and Revenue Management (BRM), Pricing Design Center (PDC), and other products required for running ECE in an integrated end-to-end system. You use this installation for a test or production system.

Overview of ECE Installed Components

The installed components depend on whether you perform an ECE standalone installation or perform an ECE integrated installation. For information about installed components for each type of installation, see the following topics:

- Installed Components in an ECE Standalone Installation
- Installed Components in an ECE Integrated Installation

Installed Components in an ECE Standalone Installation

For an ECE standalone 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 integrated 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 an integrated test or production system, if they are not already installed:
  - PDC

    PDC requires that you also install Oracle WebLogic Server

    Oracle WebLogic Server is not part of the core ECE installation, but it is used by ECE when ECE is implemented in an integrated charging solution.
  - Oracle NoSQL Database
  - BRM
  - Online or offline network mediation software

    See "Software Requirements" for information about network mediation software that is designed to be used with ECE.

    Network mediation software is required for sending requests to ECE in an integrated 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 Diameter Gateway and 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 pre-installation tasks.

   See "ECE Pre-Installation Tasks".
4. If you are installing an ECE integrated installation:
   - Ensure you have installed and configured the following products:
     - PDC
     - Oracle NoSQL Database
     - BRM
   - Set up a JMS queue for ECE notification events
   - Create the required Oracle Advanced Queuing (AQ) database queues (DBMS AQs) for BRM update requests
5. Install ECE.
6. Perform post-installation tasks.

   If you are installing an ECE integrated installation, create required Oracle AQ database queues for ECE acknowledgment events (Acknowledgments Queue) and ECE suspense events (Suspense Queue).

   If you are using Diameter Gateway for network integration for online charging, add Diameter Gateway instances and configure each instance (Diameter Gateway was installed when you installed ECE Server software).
7. Verify the installation.
8. If you are installing an ECE integrated installation, install and configure your network mediation software.

   For example, for offline charging (and if you are using the product), install and configure Oracle Communications Offline Mediation Controller. For online charging (and if you are not using Diameter Gateway for network integration), install your third-party network mediation software for online charging.

If you install an ECE integrated installation, you need to perform some system administration tasks after ECE is installed; for example:

- Configure system security, including user names and passwords.

  Depending on the security mode in which you choose to run ECE, you may also need to set security-related system parameters in the JVM tuning file (**defaultTuningProfile.properties**).

  See *BRM Elastic Charging Engine Security Guide* for more information.

- Configure system-level configuration options such as logging and Coherence configurations.

  See the discussion about configuring ECE in *BRM Elastic Charging Engine System Administrator's Guide* for more information.

- Configure usage-charging business parameters and notifications.

  See the discussion about configuring charging in *BRM Elastic Charging Engine Implementation Guide* for more information.

Overview of the ECE Installation Procedure When Upgrading an ECE Installation

If you are upgrading ECE 11.3 or an ECE 11.3 Patch Set, see "Upgrading Existing ECE 11.3 Installation".

Overview of the ECE Installation Procedure When Creating A Disaster Recovery System

To create a disaster recovery system, you must install and configure ECE and other components required for the ECE integrated system at least at two different sites. This ensures that if one site fails, another one is available to process requests.

For more information, see the discussion about configuring ECE for disaster recovery in *BRM Elastic Charging Engine System Administrator's Guide*.

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.

Directory Placeholders Used in This Guide

Table 1–1 shows the placeholders that are used in this guide to refer to the directories that contain ECE system components.

Table 1–1 Directory Placeholders

Placeholder	Directory
ECE_home	The directory in which ECE is installed. This directory contains the ECE Server software directory (*ECE_home*) and the SDK directory (*ECE_home*/**ocecesdk**) and various installation-related files.

2

Planning Your ECE Installation

This chapter provides information about planning your Oracle Communications Billing and Revenue Management Elastic Charging Engine (ECE) installation.

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.

About Standalone Systems, Test Systems, and Production Systems

There are two types of ECE installations: a standalone installation, which you use to get familiar with ECE, and an integrated installation, which you use for test or production systems.

About Standalone Systems

An ECE standalone system consists only of the basic ECE components that enable you to process simulated usage from sample data provided with ECE. You use the sample data provided in the installation to verify that ECE can process requests when working with other applications such as Pricing Design Center (PDC) and BRM without having to connect to those applications.

For a standalone system, you typically install ECE on one machine. In this case, the ECE driver machine and the ECE server machine are the same machine.

To install a standalone system, you select the ECE Server component when you run the ECE installer.

About Test Systems and Production Systems

The difference between an ECE test system and an ECE production system is only the number of machines in the system. You install the same components in a test system that you install in a production system.

For an ECE integrated installation, you set up the ECE system on the driver machine and then later synchronize the setup to all other server machines in your cluster.

When you install an ECE integrated test or production system, you can select to install all ECE software components at once or install ECE software components individually.

A test system could focus on only one integration point at one time; for example, focus on the PDC integration point or the BRM integration point. In those cases, a test system could use the simulator rather than network mediation software during testing.

However, to test a production system, you must install network mediation software. The network mediation program must have a connection to ECE to send usage requests for processing. The network mediation program uses the Elastic Charging Client, included with the ECE SDK, to connect to ECE and build and send requests.

For online charging, you can use Diameter Gateway as your network integration. Diameter Gateway is installed as part of the ECE Server installation. Diameter Gateway uses Elastic Charging Client (which is integrated with it) to connect to ECE and build and send requests.

The ECE installer copies sample data files to your installation for use with the standalone installation.

See the discussion of system architecture in *BRM Elastic Charging Engine Concepts* for information about ECE components.

See "ECE System Requirements" for information about required hardware and software.

System Deployment Planning

When planning an ECE installation, you consider how many charging server nodes to include in your cluster. If you use Diameter Gateway as your network integration for online charging, you also consider how many Diameter Gateway nodes to include in your cluster.

When considering how many charging server nodes and Diameter 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 Diameter Gateway nodes is **2** to allow for failover plus additional nodes as needed to handle the expected throughput of the system.
- For a standalone installation (single machine) for a design or test environment, note the following guidelines:
  - Although you can use one charging server node in a design 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 Diameter 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, 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.

Oracle NoSQL Database Planning

After you install Oracle NoSQL Database, you can start the Oracle NoSQL data store with either a single-node or multiple-node configuration. A single-node data store configuration (KVLite) is included with the Oracle NoSQL Database installation and can be started in a non-production ECE environment. A multiple-node Oracle 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 cluster.

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

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. After you install ECE, you can enable SSL communication between ECE and BRM. For information about choices for installing a secure system, see *BRM Elastic Charging Engine Security Guide*. For information about setting up security in ECE after installation, see *BRM Elastic Charging Engine System Administrator's Guide*.

3

ECE System Requirements

This chapter describes the software, hardware, and information requirements for Oracle Communications Billing and Revenue Management Elastic Charging Engine (ECE).

Software Requirements

This section describes the supported and required software.

Table 3–1 lists operating systems that support ECE.

Table 3–1 Supported Operating Systems

Product	Version
Red Hat Enterprise Linux (64bit) **Important:** To protect from security vulnerabilities, ensure you apply the latest critical patch updates. See "About Critical Patch Updates". ECE is certified on Red Hat Enterprise Linux 5, 6, and 7; regularly apply the latest patch set for Red Hat Enterprise Linux 5, 6, and 7 to ensure that Red Hat Enterprise Linux has the latest security fixes.	5.0 (plus latest patch updates) 6.0 (plus latest patch updates) 7.0 (plus latest patch updates)
Oracle Linux (64bit) **Important:** To protect from security vulnerabilities, ensure you apply the latest critical patch updates. See "About Critical Patch Updates". ECE is certified on Oracle Linux 5, 6, 7 and you should regularly apply the latest patch set for Oracle Linux 5, 6, 7 to ensure that Oracle Linux has the latest security fixes.	5.0 (plus latest patch updates) 6.0 (plus latest patch updates) 7.0 (plus latest patch updates)
Oracle Solaris for SPARC (64bit)	10 From ECE 11.3 Patch Set 4: 11.*x*, where *x* is version 3 or later

Table 3–2 lists the required third-party software.

Table 3–2 Required Software

Product	Version
Groovy	■ For ECE 11.3: 2.3.9 ■ For ECE 11.3 Patch Set 1 through ECE 11.3 Patch Set 3: 2.4.7 ■ For ECE 11.3 Patch Set 4 through ECE 11.3 Patch Set 9: 2.4.11 **Note:** From ECE 11.3 Patch Set 3, Groovy is not provided as part of the ECE software package.
Java Platform, Standard Edition (Java SE), containing Java Development Kit (JDK) and Java Runtime Environment (JRE) (32bit or 64bit) **Important:** To protect from security vulnerabilities, ensure you apply the latest critical patch updates. See "About Critical Patch Updates". ECE is certified on JDK8 and you should regularly apply the latest patch set for JDK8 to ensure that JDK has the latest security fixes.	1.8.0_144
Oracle Coherence for Java libraries The ECE 11.3 and ECE 11.3 patch set packages include only those Oracle Coherence libraries that are required by ECE (not all Oracle Coherence libraries); these libraries are installed as part of the ECE installation.	■ For ECE 11.3, ECE 11.3 Patch Set 1 and ECE 11.3 Patch Set 2: 12.2.1.0.2 ■ For ECE 11.3 Patch Set 3: 12.2.1.0.3 ■ For ECE 11.3 Patch Set 4: 12.2.1.0.4 ■ For ECE 11.3 Patch Set 5 and ECE 11.3 Patch Set 6: 12.2.1.0.6 ■ For ECE 11.3 Patch Set 7: 12.2.1.2.2 ■ For ECE 11.3 Patch Set 8 and ECE 11.3 Patch Set 9: 12.2.1.0.7

Table 3–3 lists the additional products required for running ECE in an integrated, end-to-end test or production system. Network mediation software is required for ECE to communicate with network-facing applications of the charging system.

For a production system, Oracle recommends that you install the other products in the same system on which you install ECE and ensure that the other products use the same operating system as ECE. However, the other products can use different operating system for a test system.

Table 3–3 Required Products in an Integrated System

Product	Version
Pricing Design Center (PDC)	■ For ECE 11.3: 11.1 with Patch Set 8 (23021246) ■ For ECE 11.3 Patch Set 1: 11.1 with Patch Set 8 (23021246) and the interim patch 24363238 ■ For ECE 11.3 Patch Set 2: 11.1 with Patch Set 8 (23021246) and the interim patch 25187795 ■ For ECE 11.3 Patch Set 3: 11.1 with Patch Set 9 (25655846) ■ For ECE 11.3 Patch Set 4: 11.1 with Patch Set 10 (26420729) 12.0 ■ For ECE 11.3 Patch Set 5: 11.1 with Patch Set 11 (27145305) 12.0 ■ For ECE 11.3 Patch Set 6: 11.1 with Patch Set 11 (27145305) 12.0 ■ For ECE 11.3 Patch Set 7: 11.1 with Patch Set 12 (27531591) 12.0 ■ For ECE 11.3 Patch Set 8: 11.1 with Patch Set 12 (27531591) 11.2 12.0 ■ For ECE 11.3 Patch Set 9: 11.1 with Patch Set 12 (27531591) 11.2 with Patch Set 1 (28738471) 12.0 with Patch Set 1 (28630301)
Oracle WebLogic Server 11*g* Enterprise Edition **Note:** Installing Oracle WebLogic Server 11*g* is a prerequisite for PDC 11.1. ECE also uses Oracle WebLogic Server in an integrated system.	10.3.6

Table 3–3 (Cont.) Required Products in an Integrated System

Product	Version
Oracle WebLogic Server 12*c* R2 Enterprise Edition **Note:** Installing Oracle WebLogic Server 12*c* R2 is a prerequisite for PDC 12.0. ECE also uses Oracle WebLogic Server in an integrated system.	12.2.1.2.0
Oracle Communications Billing and Revenue Management (BRM)	■ For ECE 11.3: 7.5 with Patch Set 15 (22738803) ■ For ECE 11.3 Patch Set 1 and ECE 11.3 Patch Set 2: 7.5 with Patch Set 16 (24383183) ■ For ECE 11.3 Patch Set 3: 7.5 with Patch Set 17 (25101805) and the interim patch 25839300 7.5 with Patch Set 18 (25596735) ■ For ECE 11.3 Patch Set 4: 7.5 with Patch Set 18 (25596735) 12.0 ■ For ECE 11.3 Patch Set 5 through ECE 11.3 Patch Set 7: 7.5 with Patch Set 20 (26940838) 12.0 ■ For ECE 11.3 Patch Set 8: 7.5 with Patch Set 20 (26940838) 7.5 with Patch Set 21 (27603295) 12.0 ■ For ECE 11.3 Patch Set 9: 7.5 with Patch Set 22 (28377280) 12.0 with Patch Set 1 (28630668)

Table 3–3 (Cont.) Required Products in an Integrated System

Product	Version
Oracle Communications Offline Mediation Controller ECE supports Offline Mediation Controller on Linux x86 or x86-64 or Solaris SPARC (64bit).	■ For ECE 11.3: 6.0.0.3.0 with 6.0.0.3.0 ECE distribution cartridge ■ For ECE 11.3 Patch Set 1 through ECE 11.3 Patch Set 3: 6.0.0.3.4 with 6.0.0.4.0 ECE distribution cartridge ■ For ECE 11.3 Patch Set 4 through ECE 11.3 Patch Set 8: 6.0.0.3.4 with 6.0.0.4.0 ECE distribution cartridge 12.0 with 12.0 ECE distribution cartridge ■ For ECE 11.3 Patch Set 9: 6.0.0.3.4 with 6.0.0.4.0 ECE distribution cartridge 12.0 Patch Set 1 with 12.0 Patch Set 1 ECE distribution cartridge
Oracle NoSQL Database Enterprise Edition	12*c*R1 (12.1.3.5.2)

Table 3–4 lists optional software products.

Table 3–4 Optional Products

Product	Version
Oracle Application Management Pack for Oracle Communications (for monitoring ECE nodes)	12.1.0.1

About Critical Patch Updates

You should install all critical patch updates as soon as possible. To download critical patch updates, find out about security alerts, and enable email notifications about critical patch updates, see the Security topic on Oracle Technology Network:

http://www.oracle.com/technetwork/topics/security/whatsnew/index.html

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.

For a standalone system, ECE requires:

- 4 GB of RAM (or more)
- 200 MB of disk space (or more)
- 2 x86 cores (or more)

Information Requirements

This section describes the information that you must provide during the ECE installation. You define some of these values when you install and configure BRM, PDC, Oracle NoSQL Database, and Oracle WebLogic Server for PDC.

Note: Oracle recommends that you print the tables in this section and record the values for future reference.

Certain information is required for both an ECE standalone installation and an ECE integrated installation. See "Information Requirements for Standalone and Integrated Installations".

Additional information is required for an integrated installation. See "Information Required Only for an ECE Integrated Installation".

For more information about standalone and integrated installations, see "Overview of ECE Installed Components".

Tip: This section describes information that you must provide during the ECE installation process for *predefined* values. For a preview of all required information, including values that you set *during* installation, see "Elastic Charging Engine Installer Screens".

Information Requirements for Standalone and Integrated Installations

This section describes the information requirements common to both an ECE standalone installation and an ECE integrated installation.

Persistence Data Details

During the installation, you must specify the path to the directory into which the ECE Rated Event Formatter Plug-in will write call detail record (CDR) files of rated events.

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

Required Information for Machines in the Coherence Cluster

Table 3–5 lists the information requirements for the machines in the Coherence cluster.

If convenient, you can use the **Value** column of the table to note the values for your specific installation so that you have them available when you run the ECE installer.

Table 3–5 Information for Machines in the Coherence Cluster

Information Type	Description	Value
User name	The user name for all machines in the cluster. You create this user and specify the user name as a pre-installation task. All machines must have the same user name. **Tip**: Along with same user name, all the servers must also allow password-less SSH login for the driver machine user.	-
Java heap settings	The memory to be allocated to each node in the Coherence cluster.	-

Table 3–5 (Cont.) Information for Machines in the Coherence Cluster

Information Type	Description	Value
Cluster name	The Coherence cluster name used by applications for identifying ECE in the cluster. The cluster name must be less than 32 characters.	-
Host names or IP addresses	The names or the IP addresses of all host machines on which ECE nodes will reside. This information is required only if you enable security-related configurations during the installation with or without Secure Sockets Layer (SSL). Include your computer name in this entry. Do not enter **localhost** or a loopback address.	-
IP address range	If you have multiple hosts in the same subnet, note the from and to IP addresses for the range of hosts in the same subnet. This information is required only if you enable security-related configurations during the installation with or without SSL.	-
Administrator alias name	The alias name that defines the administrator for securing the Coherence cluster. You define this value during installation. This is required only if you enable SSL and security-related configurations during the installation. This value cannot be changed after it is set.	-
Administrator alias password	The password for the administrator alias. You define this value during installation. This is required only if you enable SSL and security-related configurations during the installation. This value cannot be changed after it is set.	-

Required Oracle NoSQL Database Information

Table 3–6 lists the Oracle NoSQL database information required during the ECE installation.

If convenient, you can use the **Value** column of the table to note the values of the fields for your specific installation so that you have it available when you run the ECE installer.

Table 3–6 Oracle NoSQL Database Information

Information Type	Description	Value
Host name	The name of the machine on which Oracle NoSQL database is installed.	-
Port number	The port number assigned to the Oracle NoSQL Database service.	-

Table 3–6 (Cont.) Oracle NoSQL Database Information

Information Type	Description	Value
Data store name	The name of the data store in which you want ECE to persist rated event information. This must be the name that you defined during the installation of Oracle NoSQL database.	-

Keystore Credentials Information

ECE uses credential stores or *keystores* for cluster security. You will be asked to specify keystore credential values during the installation process.

ECE uses two keystore files:

- The **keystore.jks** file stores cipher keys used for encrypting the passwords used between ECE and BRM or PDC when required.
- The **server.jks** file is used for enabling Secure Sockets Layer (SSL) and stores cipher keys used for keeping the Coherence cluster secure.

During the ECE installation, you are asked to specify the following keystore credential information:

- The password ECE uses to access the boundary system alias key in the **keystore.jks** file. The boundary systems are BRM and PDC.
- The certificate store password used for accessing the **keystore.jks** and **server.jks** files.
- The authorization of users for what they can do regarding cluster security. You set this value in the **DName** field during installation.

  The DName (acronym for Distinguished Name) is similar to a group in UNIX.

  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.

For more information about the keystores and how they are used, see the discussion of setting up and managing Elastic Charging Engine security in *BRM Elastic Charging Engine System Administrator's Guide*.

Required Diameter Gateway Information

During installation, you must specify the following information that Diameter clients use to identify your Diameter Gateway server.

Table 3–7 Diameter Gateway Information

Information Type	Description	Value
Skip	During installation, you must specify whether Diameter Gateway is started when ECE is started.	-
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. This value 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.	-
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. This value 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-Host and Origin-Realm AVPs 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 screen apply to a single instance (node) of a Diameter Gateway server that the installer adds to your ECE topology. You must add more Diameter Gateway nodes to your topology after installation. See "Adding and Configuring Diameter Gateway Nodes for Online Charging" for more information.

Required RADIUS Gateway Information

During installation, you must specify the following information that RADIUS clients use to identify your RADIUS Gateway server.

Table 3–8 RADIUS Gateway Information

Information Type	Description	Value
Skip	If you do not want RADIUS Gateway to start when ECE starts, select this option.	-
Name	The name of the RADIUS Gateway instance.	-
Port	The port number assigned to RADIUS Gateway.	-
Shared Secret	The common password shared between your RADIUS Gateway server and Network Access Server (NAS). It is used by the RADIUS protocol for security. Each RADIUS Gateway instance must have a unique password in encrypted format.	-

Table 3–8 (Cont.) RADIUS Gateway Information

Information Type	Description	Value
Wallet Location	The path to the Oracle wallet file containing SSL trusted certificates and the BRM root key for RADIUS Gateway.	-

The RADIUS Gateway details you enter in this screen apply to a single instance (node) of a RADIUS Gateway server that the installer adds to your ECE topology. You must add more RADIUS Gateway nodes to your topology after installation. See "Adding and Configuring RADIUS Gateway Nodes for Authentication and Accounting" for more information.

Required Third-Party Library Information

During the installation, you need to know the directory where you saved the JAR files required for the ECE installation process.

For more information, see "Obtaining Required JAR Files."

Information Required Only for an ECE Integrated Installation

This section describes the additional information requirements for an ECE integrated installation.

Config Data Details

During the installation, you must specify the path to the directory that contains configuration data (mediation specifications).

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

For more information about configuration data, see the discussion about implementing ECE with BRM in *BRM Elastic Charging Engine Implementation Guide*.

Required WebLogic Server Information

You install WebLogic Server when you install PDC. You set up two JMS queues on a WebLogic server:

- A pricing data JMS queue that ECE listens on to consume pricing data that PDC publishes into the queue.
- A notification event queue (JMS topic) into which ECE publishes notification events that external systems, such as network mediation programs, can consume to obtain data for their own processing.

> **Note:** ECE provides a post-installation script that will create the notification event queue for you.

Table 3–9 lists the WebLogic Server information that is required during the ECE installation.

If convenient, you can use the **Value** column of the table to note the values of the fields for your specific installation so that you have it available when you run the ECE installer.

Table 3–9 WebLogic Server Information

Information Type	Description	Value
Host name	The host name of the server on which the JMS queues reside.	-
Port number	The port number of the server on which the JMS queues reside.	-
User name	The user name for logging in to the WebLogic server on which the JMS queues reside.	-
Password	The password for logging in to the WebLogic server on which the JMS queues reside.	-
Module name	The JMS system module name on the WebLogic server on which the JMS queues reside.	-
Subdeployment	The name of the subdeployment target in the JMS system module.	-
Connection Factory name	The connection factory name that is used to create connections to the JMS topic queue on the WebLogic Server to which ECE will publish notification events. After you install ECE, you will run an ECE post-installation script that will create the JMS topic queue on the WebLogic Server. The connection factory name is used by the script to create the connections to the JMS topic queue.	-
Topic Name	The JMS topic queue name of the JMS topic on the WebLogic Server to which ECE will publish notification events. After you install ECE, you will run a post-installation script that will create the JMS topic on the WebLogic Server. The topic name is the name the ECE post-installation script will use to create the JMS topic.	-
Suspense Queue Name	The BRM Gateway suspense queue is created as part of post-install script in case of full installation. In case of a patch-set release a new JMS suspense queue is configured manually in the WebLogic within the ECE JMS module.	
Disable SSL	During installation, you must specify whether SSL will be used to secure the ECE JMS queue connection.	-
Keystore password	The password used to access the SSL keystore file.	-
Keystore location	The full path to the SSL keystore file.	-

Required BRM Information

Table 3–10 lists the BRM information required during the ECE installation.

If convenient, you can use the **Value** column of the table to note the values of the fields for your specific installation so that you have it available when you run the ECE installer.

Table 3–10 BRM Information

Information type	Description	Value
BRM user name	The user name for logging in to BRM.	-
BRM password	The password for logging in to BRM.	-
Database user name	The BRM database schema user name.	-
Database password	The password for the BRM database user.	-
Database driver	The driver used to connect to the BRM database.	-
Database host name	The IP address or the host name of the computer on which the BRM database is configured.	-
Database port number	The port number assigned to the BRM database service.	-
Service name	The name of the BRM database service.	-
CM host name	The IP address or the host name of the computer on which the BRM Connection Manager (CM) is configured.	-
CM port number	The port number for the CM.	-
Disable SSL	During installation, you must specify whether SSL will be used to secure the BRM Gateway connection.	-
Wallet file absolute path	The default path to the Oracle wallet file containing the SSL trusted certificates for BRM Gateway: `/opt/wallet/client/cwallet.sso` If SSL is enabled for BRM Gateway but the wallet is in a different location, you must replace the default path with the full path to the actual location during installation.	-
Queue name	The name of the database queue that the BRM Account Synchronization DM uses to publish business events for ECE to consume.	-
Suspense queue name	The name of the database queue that ECE will use to move failed update requests (for business-event data that could not be consumed by ECE) so they can be retried later. An ECE post-installation script will create the queue itself. You only need to supply the name you want to use for the queue.	-
Acknowledgement queue name	The name of the database queue that ECE will use to publish acknowledgement events for BRM to consume (used for rerating). An ECE post-installation script will create the queue itself. You only need to supply the name you want to use for the queue.	-

Required External Manager Gateway Information

Table 3–11 lists the External Manager (EM) Gateway information required during the ECE installation.

If convenient, you can use the **Value** column of the table to note the values of the fields for your specific installation so that you have it available when you run the ECE installer.

Table 3–11 External Manager Gateway Information

Information type	Description	Value
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	During installation, you must specify whether SSL will be used to secure the EM Gateway connection.	-
Client Authentication Disabled	During installation, you must specify whether authentication is performed to check whether EM Gateway is allowed to communicate with ECE.	-
Wallet File Absolute Path	The default path to the Oracle wallet file containing the SSL trusted certificates for EM Gateway: `/opt/wallet/server/cwallet.sso` If SSL is enabled for EM Gateway but the wallet is in a different location, you must replace the default path with the full path to the actual location during installation.	-

Required PDC Pricing Components Queue Information

During the installation, you must specify the system connection information of the server on which the JMS queue for PDC pricing component data resides.

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

Field or Option	Description
Host Name	The IP address or the host name of the computer on which the PDC JMS queue resides.
Port Number	The port number of the computer on which the PDC JMS queue resides.

Field or Option	Description
User Name	The user for logging in to the server on which the PDC JMS queue resides.
Password	The password for logging in to the server on which the PDC JMS queue resides.
Disable SSL	During installation, you must specify whether SSL will be used to secure the PDC JMS queue connection.
PDC Keystore Password	The password used to access the SSL keystore file.
Keystore Path	The full path to the SSL keystore file.

4

ECE Pre-Installation Tasks

This chapter describes pre-installation tasks for Oracle Communications Billing and Revenue Management Elastic Charging Engine (ECE).

If you are upgrading ECE 11.3 or an ECE 11.3 patch set, see the following for information on pre-installation tasks:

- Upgrading Existing ECE 11.3 Installation

About Pre-Installation Tasks

You must perform certain tasks before installing ECE. Some tasks you only need to perform for an ECE integrated installation. See the following topics for the pre-installation tasks:

- Pre-Installation Tasks Common to All ECE Installations
- Pre-Installation Tasks for an ECE Integrated Installation

(Linux only) You can run the **ece_provision** script so that it automatically performs several ECE pre-installation tasks for you. This script also applies Oracle Linux network configuration changes on your environment to prepare machines in your topology for a distributed ECE installation. See "(Linux) Provisioning Your Environment for ECE Installations" for information.

Pre-Installation Tasks Common to All ECE Installations

This section describes the pre-installation tasks you must perform that are common to all ECE installations.

> **Note:** (Linux) If you use the **ece_provision** script, the script automates many of these tasks. See "(Linux) Provisioning Your Environment for ECE Installations".

Installing Groovy

Groovy is used for launching the Elastic Charging Controller (ECC), which is the ECE command line interface. The ECC is an extension of the Groovy Shell (**groovysh**) for ECE.

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

See the discussion in your Groovy documentation for instructions on installing and configuring Groovy.

Installing Java Development Kit

Install Oracle Java Development Kit (JDK) and set it in your PATH environment variable. The JRE is required for the installer process.

See the discussion in the Oracle JDK documentation for information about installing JDK.

Obtaining Required JAR Files

Obtain the following JAR files and save them in a directory of your choice on the driver machine. Note the location of the JAR files; you are required to specify this location during the ECE installation:

Table 4–1 Required JAR Files

File	Description
ojdbc7.jar	Download this file from the following page on Oracle Technology Network Web site in the "Oracle Database 12c Release 1 (12.1.0.1) JDBC Drivers & UCP" section: http://www.oracle.com/technetwork/database/features/jdbc/jdbc-drivers-12c-download-1958347.html
xdb6.jar	Download this file from the following page on Oracle Technology Network Web site in the "Oracle Database 12c Release 1 (12.1.0.1) JDBC Drivers & UCP" section: http://www.oracle.com/technetwork/database/features/jdbc/jdbc-drivers-12c-download-1958347.html
wlthint3client.jar	This file is available in the Oracle WebLogic Server client package. **Note:** If you choose to use two JMS providers, both WebLogic Server and another provider, ensure that you do the following after installation on the driver machine: ▪ Copy the other JMS provider's client JARs to the *ECE_home*/**oceceserver/lib** directory. ▪ Rename the other JMS provider JAR file **wlthint3client.jar**. ▪ (When using the other JMS provider to publish ECE notification events) Update the *ECE_home*/**oceceserver/JMSQueueConfiguration.xml** file to specify the InitialContextFactory and protocol information of the other JMS provider.
osdt_cert.jar	This file is available in the *BRM_Home*/**jars** directory, where *BRM_Home* is the directory in which you installed BRM.
osdt_core.jar	This file is available in the *BRM_Home*/**jars** directory.
oraclepki.jar	This file is available in the *BRM_Home*/**jars** directory.
httpclient-4.4.jar	This file is available in the *BRM_Home*/**jars** directory.
commons-logging-1.2.jar	This file is available in the *BRM_Home*/**jars** directory.
groovy-all-2.4.11.jar	Download this file from the following page on Apache Groovy Web site in the "Maven Repository" section: http://groovy-lang.org/install.html

(Solaris) Making the readlink Command Available to Your Environment

For deploying ECE on Solaris 10, you must have the **readlink** command available to your installation environment. The readlink command is included in the **SFWcoreu.pkg.bz2** package, an open source package you can download from the Internet.

To make the **readlink** command available to your environment, do the following:

1. Download the **SFWcoreu.pkg.bz2** package.
2. Execute the following commands:

   ```
   bunzip2 SFWcoreu.pkg.bz2
   pkgadd -d SFWcoreu.pkg
   ```

   The commands that are part of the **SFWcoreu.pkg.bz2** package are installed in **/opt/sfw/bin**.
3. Add **/opt/sfw/bin** to your PATH environment variable.

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 UNIX account used for password-less SSH.

You create the user account on the driver machine (the primary administrator machine). It is required that all machines have the same user name configured.

Note 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 about setting up and managing ECE security in *BRM Elastic Charging Engine System Administrator's Guide* for information about creating user accounts to manage ECE files.

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**.

See the discussion about setting up and managing ECE security in *BRM Elastic Charging Engine System Administrator's Guide* for more information.

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. For more information, see the discussion about starting and stopping ECE in *BRM Elastic Charging Engine System Administrator's Guide*.

Pre-Installation Tasks for an ECE Integrated Installation

For an ECE integrated installation, you perform the pre-installation tasks common to all ECE installations, (see "Pre-Installation Tasks Common to All ECE Installations") and also the tasks described in this section.

Installing and Configuring Pricing Design Center

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

ECE supports PDC on Linux x86 or x86-64 or Solaris SPARC (64bit).

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 dequeue and load the data into ECE.

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

Note 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. See "Required WebLogic Server Information" for details about the information you will need.

See the discussion in the Pricing Design Center documentation for information about installing and configuring PDC.

See the discussion in the Oracle WebLogic Server documentation for information about setting up JMS queues.

Installing and Configuring Oracle NoSQL Database

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

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. See "Required Oracle NoSQL Database Information".

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.

ECE supports BRM on Linux x86 or x86-64 or Solaris SPARC (64bit).

Take note 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 "Required External Manager Gateway Information" for details about the information you will need.

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 acknowledgement events for BRM to consume (used when processing rating requests from BRM, such as during rerating).

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

See the discussion in *Oracle Communications BRM Installation Guide* for information about installing BRM.

See the discussion about Customer Updater in the system architecture chapter of *BRM Elastic Charging Engine Concepts* for more information about how ECE interacts with the BRM Account Synchronization DM.

(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.

(Linux) Provisioning Your Environment for ECE Installations

You can provision machines on which you will install ECE by using the **ece_provision** script. The **ece_provision** script does the following to prepare machines for an ECE installation:

- Ensures that you install the recommended runtime environment.
- Ensures that the main Oracle Linux network configuration changes are applied.
- Ensures that ECE nodes can communicate with each other after going from a local installation of ECE to a distributed installation.

You can use **ece_provision** to prepare the network configuration of your local environment (single machine) or distributed environment (multiple machines). The script automates many manual steps, especially when deploying ECE in a distributed environment.

Important: The **ece_provision** script is intended as a quick-start solution for provisioning vanilla Oracle Linux installations. For customized Oracle Linux environments, use *only* the *instructions* in **ece_provision** as guidelines for performing configuration management on your existing provisioning framework.

Table 4–2 describes the variables of the **ece_provision** script configuration file (**ece_provision_config.sh**).

Table 4–2 Variables of the ece_provision Script Configuration File

Variable	Definition
HOSTS	The IP addresses of all machines in your ECE topology including the driver machine.
DRIVER_HOST	The IP address of the driver machine.
SUDO_USER	The user account that is to run the **ece_provision** script in your environment; this account must be **sudo** enabled. You must manually create this **sudo** enabled account on all machines in your topology.
SUDO_USER_HOME	The home directory of the **sudo** user.
ECE_PROVISION_HOME	The **ece_provision** root directory. This is the subdirectory of the **sudo** user home directory in which you unzip the ECE Oracle Universal Installer distribution file (zip file).
ECE_USER	The UNIX account used to run all ECE processes. The **ece_provision** script creates the ECE user account on all machines in your topology.
ECE_USER_HOME	The home directory of the ECE user.

To provision your local or distributed environment for ECE installations:

1. Enable **sudo** for your user account ($SUDO_USER) on all of the machines required to run ECE ($HOSTS).

   ece_provision requires a **sudo** enabled account.

2. On the driver machine ($DRIVER_HOST), log in as the **sudo** user.
3. Create a temporary directory (*temp_dir*).
4. Go to the My Oracle Support Web site:

   `http://support.oracle.com`

5. Sign in with your user name and password.
6. Click the **Patches & Updates** tab.
7. From the list, select **Patch Name or Number**.
8. In the text field, enter **28738541** and click **Search**.

   The Patch Search Results page appears.

9. Click the patch name.

   The patch details appear.

10. From the **Platform** list, select the platform and click **Download**.

    The File Download dialog box appears.

11. Download the **p28738541_113090**_*platform*.**zip** software pack to *temp_dir*, where *platform* is **linux** or **solaris**.
12. Unzip **p28738541_113090**_*platform*.**zip** and extract the contents to *temp_dir*:

    The extracted software pack has the following structure:

    ocece/Disk1/install

    ocece/Disk1/stage

13. In the **ocece/Disk1/install** directory, extract the **ece_provision** zip file.

```
$ unzip ocece/Disk1/install/ece_provision.zip
```

14. In the **ece_provision** root directory ($ECE_PROVISION_HOME), open the **ece_provision_config.sh** file.
15. Download the ECE required packages indicated in the file into the **ece_provision** root directory.

    ```
    $ mv groovy-binary-2.4.11.zip jdk-8u141-linux-x64.tar.gz kv-ee-2.1.54.tar.gz
    ojdbc7.jar p14468425_371_Generic.zip wlthint3client.jar ece_provision
    ```

    This downloads files for the following software:

    - JDK
    - Groovy
    - Oracle NoSQL
    - Oracle Coherence
    - WebLogic Server client
    - JDBC client

16. In the **ece_provision_config.sh** file, edit the following configuration values. You must change the account names and directory locations shown in bold.
    - HOSTS="**192.168.1.10 192.168.1.11**"

      Under **HOSTS**, list the ECE driver machine first.
    - DRIVER_HOST="**192.168.1.10**"
    - SUDO_USER="**admin**"
    - SUDO_USER_HOME="/**home**/${SUDO_USER}"
    - ECE_USER="ece"
    - ECE_USER_HOME="/**home**/${ECE_USER}"
    - ECE_PROVISION_HOME=${SUDO_USER_HOME}**ece_install/ece_provision**
17. From the **ece_provision** root directory, run the **ece_provision.sh** script:

    ```
    $ cd $ECE_PROVISION_HOME; bash ./ece_provision.sh
    ```

    The script provisions all machines required to run ECE; it creates the ECE user and sets up two-way password-less SSH on all machines.

    After running **ece_provision**, proceed with the following steps to complete the provisioning of machines in your topology.
18. Still on the driver machine, switch to the newly created ECE user account ($ECE_USER).
19. Test to see if you have multicast configured in your network, by doing the following:

    Tip: Performing this test is only possible after running **ece_provision**.

    a. From your UNIX home directory, go to **/opt/coherence/bin**.
    b. Run the test according to the instructions at "Determining Whether Multicast Is Enabled".

If you have multicast configured in your network, you will configure ECE for multicast after installing ECE.

You have now provisioned your local or distributed environment for ECE installations. You can now install the ECE software (ECE Server or ECE Complete installation types). See "Installing ECE by Using the GUI Installation" for instructions for installing the ECE software.

5

Installing Elastic Charging Engine

This chapter describes how to install Oracle Communications Billing and Revenue Management Elastic Charging Engine (ECE). Before you install ECE, read these chapters:

- ECE Installation Overview
- Planning Your ECE Installation
- ECE System Requirements
- ECE Pre-Installation Tasks

About the GUI Installation and Silent Installation

You can install ECE by using the GUI installation or the silent installation. The silent installation procedure enables you to perform a noninteractive installation of ECE. You can use the silent installation to install ECE quickly on multiple systems.

The silent installer uses a response file in which you specify installation settings. To obtain the response file, you first run the GUI installation, which generates the response file. See "ECE Installation Options" and "Elastic Charging Engine Installer Screens" for more information.

For installation instructions, see the following sections:

- Installing ECE by Using the GUI Installation
- Installing ECE by Using the Silent Installation

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 standalone system, select the **Standalone** installation 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 stand-alone system for evaluation, demonstration, and functional testing.

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

- To install an ECE integrated system, do one of the following:
  - Select the **Complete** option to install all ECE software components, including all BRM and PDC integration packs.

  - Select the **Custom** option to choose one or more components to install each time you run the installer.

  See "Installing All ECE Components" and "Installing Individual ECE Components" for more information.

- To upgrade an existing ECE 11.3 installation, select the **Patchset** option.

  For more information, see "Upgrading Existing ECE 11.3 Installation".

Installing All ECE Components

To install all ECE components, select the **Complete** installation option, which installs ECE Server, ECE Diameter Gateway, and all ECE integration packs. Use this option for an ECE integrated installation.

During the installation, you will need the required information that you previously collected. See "Information Requirements."

To install all ECE components:

1. Create a temporary directory (*temp_dir*).
2. Go to the My Oracle Support Web site:

   `http://support.oracle.com`
3. Sign in with your user name and password.
4. Click the **Patches & Updates** tab.
5. From the list, select **Patch Name or Number**.
6. In the text field, enter **28738541** and click **Search**.

   The Patch Search Results page appears.
7. Click the patch name.

   The patch details appear.
8. From the **Platform** list, select the platform and click **Download**.

   The File Download dialog box appears.
9. Download the **p28738541_113090**_*platform*.**zip** software pack to *temp_dir*, where *platform* is **linux** or **solaris**.
10. Unzip **p28738541_113090**_*platform*.**zip** and extract the contents to *temp_dir*:

    The extracted software pack has the following structure:

    ocece/Disk1/install

    ocece/Disk1/stage
11. Go to the **ocece/Disk1/install/** directory, and run one of the following commands:

    - To start the GUI installer:

      `./runInstaller`

    - To start the GUI installer and create a silent installer response file during the installation:

      `./runInstaller -record -destinationFile` *`path`*

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

The Welcome screen appears.

12. Click **Next**.

    The Specify Inventory Directory and Credentials screen appears.

    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.

    In this screen, enter the following if you do not want to accept the defaults:

    - Full path of the inventory directory
    - Name of the operating system group that has write permission to the inventory directory

13. Click **Next**.

    The Select Installation Type screen appears.

14. Select **Complete**, and click **Next**.

    The Specify Home Details screen appears.

15. Enter the following information:

    a. In the **Name** field, enter a name for the installation, or select a name from the list.

    b. In the **Path** field, enter the full path or browse to the directory in which to install ECE.

16. Click **Next**.

    The Select ECE Security Options screen appears.

17. Select one of the ECE security options described in the following table.

    For more information, see *BRM Elastic Charging Engine Security Guide*.

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 ■ BRM SSL security authentication ■ PDC SSL security authentication ■ EM Gateway SSL security authentication

18. Click **Next**.

    The Config Data Details screen appears.

19. In the **Directory** field, enter the path or browse to the directory where ECE gets the XML files that contain configuration data (mediation specifications).

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

    For more information about configuration data, see the discussion about implementing ECE with BRM in *BRM Elastic Charging Engine Implementation Guide*.

20. Click **Next**.

    The Persistence Data Details screen appears.

21. In the **Directory** field, 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.

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

22. Click **Next**.

    The ECE Cluster Details screen appears.

23. Enter information about the ECE cluster:

    Note: (Linux) If you used the **ece_provision** script to provision your environment for an ECE installation, the user name for host machines you enter in the ECE Cluster Details screen must be the same user name you entered for the ECE_USER field in the **ece_provision_config.sh** file.

    a. In the **User Name for Host Machines** field, enter 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 user name is used by the Elastic Charging Controller to identify the remote machines on which to deploy ECE.

    b. In the **Java Heap Settings** field, specify 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.

    c. In the **Cluster Name** field, enter 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.

24. Click **Next**.

    The Coherence Grid Security screen appears.

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

Note: (Linux) If you used the **ece_provision** script to provision your environment for an ECE installation, authorized host list information you enter in the Coherence Grid Security screen must be the same host information you entered for the HOST field in the **ece_provision_config.sh** file.

25. Specify the machines allowed to be part of the Coherence cluster and the credentials required for accessing the cluster.

    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.

      See the discussion about Coherence cluster security in *BRM Elastic Charging Engine Security Guide*.

26. Click **Next**.

    The Oracle NoSQL Database Details screen appears.

27. Specify the NoSQL database connection information:

    a. In the **Host Name** field, enter the host name or IP address of the machine on which the Oracle NoSQL database is installed.

    b. In the **Port Number** field, enter the port number assigned to the NoSQL database service.

    c. In the **NoSQL Datastore Name (database name)** field, enter the name of the NoSQL data store into which ECE will publish rated events.

       This is where Rated Event Publisher writes rated events generated by the ECE server.

28. Click **Next**.

The KeyStore Credentials screen appears.

29. Specify the keystore credential information required for the ECE installation.

    For information about keystore credentials, see *BRM Elastic Charging Engine Security Guide* and the discussion about setting up and managing ECE security in *BRM Elastic Charging Engine System Administrator's Guide*.

    a. In the **Key Password for Boundary System Alias** field, enter the password ECE uses to access the boundary system alias key in the keystore JKS file (*ECE_home***/oceceserver/config/keystore.jks**).

    b. In the **Certificate store password** field, enter the password used to access the server JKS file and the keystore JKS file:

       *ECE_home***/oceceserver/config/keystore.jks**

       Stores symmetric keys for boundary system password encryption.

       *ECE_home***/oceceserver/config/server.jks**

       Stores credentials for cluster node authentication details. This file is also used for encrypting intra-cluster communication over SSL.

       These files share the same key and store password.

    c. In the **DName** (Distinguished Name) field, specify 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 UNIX.

       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 and the **keystore.jks** keystore.

30. Click **Next**.

    The ECE Notification Queue Details screen appears.

31. Enter the Java Message Service (JMS) credentials for the JMS server on which the ECE notification queue (JMS topic) is to reside.

    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 post-installation script that creates the JMS queue (JMS topic) on the server.

a. In the **Host Name** field, enter the host name of the server. on which the JMS queue (JMS topic) resides.

b. In the **Port Number** field, enter the port number of the server.on which the JMS queue (JMS topic) resides.

c. In the **User Name** field, enter the user name for logging in to the server. on which the JMS queue (JMS topic) resides.

d. In the **Password** field, enter the password for logging in to the server. on which the JMS queue (JMS topic) resides.

e. In the **Connection Factory Name** field, enter the connection factory name used to create connections to the JMS queue (JMS topic) queue.

   After installing ECE, you run an ECE post-installation 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 (JMS topic).

f. In the **Topic Name** field, enter the name of the JMS queue (JMS topic) on the server, to which ECE publishes notification events.

   After installing ECE, you run a post-installation script that creates the JMS queue (JMS topic) on the server. The topic name entered here is the name the ECE post-installation script uses to create the JMS queue (JMS topic).

g. In the **Suspense Queue Name** field, enter the name for the suspense queue, to which ECE pushes the failed notifications.

32. Click **Next**.

    The ECE Notification Queue SSL Details screen appears.

33. Enter secure socket layer (SSL) information required to connect to the Java Message Service (JMS) queue to which ECE publishes notification events:

    a. If you will *not* 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.

    b. In the **Keystore password** field, enter the password used to access the SSL keystore file.

    c. In the **Keystore location** field, enter the full path to the SSL keystore file.

34. Click **Next**.

    The BRM Gateway Details screen appears.

35. Enter the BRM Gateway connection details:

    a. In the **Host Name** field, enter the IP address or the host name of the computer on which BRM is configured.

    b. In the **CM Port** field, enter the port number assigned to the CM.

    c. In the **User Name** field, enter the BRM user name.

    d. In the **Password** field, enter the password for logging in to BRM.

    e. 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.

f. 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.

36. Click **Next**.

    The External Manager (EM) Gateway Details screen appears.

37. Specify the EM Gateway information:

    a. In the **Number EM Gateways** field, enter the number of EM Gateway instances you want ECE to run automatically when you start EM Gateway.

    b. In the **Starting Port Number** field, enter 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.

    c. If you will *not* 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.

    d. 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.

    e. 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.

38. Click **Next**.

    The PDC Pricing Components Queue Details screen appears.

39. Enter the system connection information of the server on which the JMS queue for PDC pricing component data resides.

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

    a. In the **Host Name** field, enter the IP address or the host name of the computer on which the PDC JMS queue to which PDC publishes the pricing data resides.

    b. In the **Port Number** field, enter the port number of the computer on which the PDC JMS queue resides.

    c. In the **User Name** field, enter the user name for logging in to the server on which the PDC JMS queue resides.

    d. In the **Password** field, enter the password for logging in to the server on which the PDC JMS queue resides.

e. 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.

f. In the **PDC Keystore Password** field, enter the password used to access the SSL keystore file.

g. In the **Keystore Path** field, enter the full path to the SSL keystore file.

40. Click **Next**.

    The BRM Database Connection Details screen appears.

41. Specify the BRM database connection information:

    a. In the **JDBC URL** field, enter 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`

    b. In the **User Name** field, enter the BRM database schema user name.

    c. In the **Password** field, enter the password for the BRM database user.

    d. In the **Queue Name** field, enter 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.

    e. In the **Suspense Queue Name** field, enter 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 post-installation script to create this queue. When prompted by the script, enter the queue name you entered here.

    f. In the **Acknowledgement Queue Name** field, enter 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 post-installation script to create this queue. When prompted by the script, enter the queue name you entered here.

42. Click **Next**.

    The Diameter Gateway Details screen appears.

43. Enter information that Diameter clients use to identify your Diameter Gateway server:

a. 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.

b. In the **Origin Host** field, enter 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).

c. In the **Origin Realm** field, enter 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 screen 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 Post-Installation Tasks".

44. Click **Next**.

    The RADIUS Gateway Details screen appears.

45. Enter information that RADIUS clients use to identify your RADIUS Gateway server:

    a. 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.

    b. In the **Name** field, enter the name of the RADIUS Gateway instance.

    c. In the **Port** field, enter the port number assigned to RADIUS Gateway.

    d. In the **Shared Secret** field, enter the common password shared between the RADIUS Gateway server and Network Access Server (NAS). It is used by the RADIUS protocol for security.

    e. In the **Wallet Location** field, enter 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 screen 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 Post-Installation Tasks".

46. Click **Next**.

    The Third-Party Library Details screen appears.

47. In the **Directory** field, enter the patch or browse to the directory that contains the JAR files required by ECE, which you copied to this directory before running the installer.

48. Click **Next**.

    The Summary screen appears.

49. Review your selections, and click **Install**.

    The Install screen appears, and the installation begins.

    Note: If you click **Cancel** after the installation begins, the installation stops, but files already copied are not removed.

    When the installation is done, the End of Installation screen appears.

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

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 stand-alone system for evaluation, demonstration, and functional testing.

During the installation, refer to the required information that you previously collected. See "Information Requirements".

To install a standalone ECE system:

1. Create a temporary directory (*temp_dir*).
2. Go to the My Oracle Support Web site:

   `http://support.oracle.com`
3. Sign in with your user name and password.
4. Click the **Patches & Updates** tab.
5. From the list, select **Patch Name or Number**.
6. In the text field, enter **TBD** and click **Search**.

   The Patch Search Results page appears.

7. Click the patch name.

   The patch details appear.

8. From the **Platform** list, select the platform and click **Download**.

   The File Download dialog box appears.

9. Download the **pTBD_113090**_*platform*.**zip** software pack to *temp_dir*, where *platform* is **linux** or **solaris**.

10. Unzip **pTBD_113090**_*platform*.**zip** and extract the contents to *temp_dir*:

    The extracted software pack has the following structure:

    ocece/Disk1/install

    ocece/Disk1/stage

11. Go to the **ocece/Disk1/install/** directory, and run one of the following commands:

    - To start the GUI installer:

      ```
      ./runInstaller
      ```

    - To start the GUI installer and create a silent installer response file during the installation:

      ```
      ./runInstaller -record -destinationFile path
      ```

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

    The Welcome screen appears.

12. Click **Next**.

    The Specify Inventory Directory and Credentials screen appears.

    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.

    In this screen, enter the following if you do not want to accept the defaults:

    - Full path of the inventory directory
    - Name of the operating system group that has write permission to the inventory directory

13. Click **Next**.

    The Select Installation Type screen appears.

14. Select **Standalone**, and click **Next**.

    The Specify Home Details screen appears.

15. (Optional) Enter the following information if you do not want to accept the default values:

    a. In the **Name** field, enter a name for the standalone ECE installation, or select a name from the list.

    b. In the **Path** field, enter the full path or browse to the directory in which to install the standalone ECE software.

16. Click **Next**.

The Select ECE Security Options screen appears.

17. Select one of the ECE security options described in the following table.

    For more information, see *BRM Elastic Charging Engine Security Guide*.

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

18. Click **Next**.

    The Persistence Data Details screen appears.

19. In the **Directory** field, 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.

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

20. Click **Next**.

    The ECE Cluster Details screen appears.

21. Enter information about the ECE cluster:

    Note: (Linux) If you used the **ece_provision** script to provision your environment for an ECE installation, the user name for host machines you enter in the ECE Cluster Details screen must be the same user name you entered for the ECE_USER field in the **ece_provision_config.sh** file.

    a. In the **User Name for Host Machines** field, enter 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 user name is used by the Elastic Charging Controller for identifying the remote machines on which to deploy ECE.

    b. In the **Java Heap Settings** field, specify 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.

c. In the **Cluster Name** field, enter 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.

22. Click **Next**.

    The Coherence Grid Security screen appears.

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

    Note: (Linux) If you used the **ece_provision** script to provision your environment for an ECE installation, authorized host list information you enter in the Coherence Grid Security screen must be the same host information you entered for the HOST field in the **ece_provision_config.sh** file.

23. Specify the machines allowed to be part of the Coherence cluster and the credentials required for accessing the cluster.

    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.

      See the discussion about Coherence cluster security in *BRM Elastic Charging Engine Security Guide*.

24. Click **Next**.

    The Oracle NoSQL Database Details screen appears.

25. Specify the NoSQL database connection information:

    a. In the **Host Name** field, enter the host name or IP address of the machine on which the Oracle NoSQL database is installed.

    b. In the **Port Number** field, enter the port number assigned to the NoSQL database service.

    c. In the **NoSQL Datastore Name (database name)** field, enter the name of the NoSQL data store into which ECE will publish rated events.

       This is where Rated Event Publisher writes rated events generated by the ECE server.

26. Click **Next**.

    The KeyStore Credentials screen appears.

27. Specify the keystore credential information required for the ECE installation.

    For information about keystore credentials, see *BRM Elastic Charging Engine Security Guide* and the discussion about setting up and managing ECE security in *BRM Elastic Charging Engine System Administrator's Guide*.

    a. In the **Key Password for Boundary System Alias** field, enter the password ECE uses to access the boundary system alias key in the keystore JKS file (*ECE_home***/oceceserver/config/keystore.jks**).

    b. In the **Certificate store password** field, enter the password used to access the server JKS file and the keystore JKS file:

       *ECE_home***/oceceserver/config/keystore.jks**

       Stores symmetric keys for boundary system password encryption.

       *ECE_home***/oceceserver/config/server.jks**

       Stores credentials for cluster node authentication details. This file is also used for encrypting intra-cluster communication over SSL.

       These files share the same key and store password.

    c. In the **DName** (Distinguished Name) field, specify 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 UNIX.

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 and the **keystore.jks** keystore.

28. Click **Next**.

    The ECE Notification Queue Details screen appears.

29. Enter the Java Message Service (JMS) credentials for the JMS server on which the ECE notification queue (JMS topic) is to reside.

    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 post-installation script that creates the JMS queue (JMS topic) on the server.

    a. In the **Host Name** field, enter the host name of the server on which the JMS queue (JMS topic) resides.

    b. In the **Port Number** field, enter the port number of the server on which the JMS topic resides.

    c. In the **User Name** field, enter the user name for logging in to the server on which the JMS queue (JMS topic) resides.

    d. In the **Password** field, enter the password for logging in to the server on which the JMS queue (JMS topic) resides.

    e. In the **Connection Factory Name** field, enter the connection factory name used to create connections to the JMS queue (JMS topic) queue.

       After installing ECE, you run an ECE post-installation 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 (JMS topic).

    f. In the **Topic Name** field, enter the name of the JMS queue (JMS topic) on the server to which ECE publishes notification events.

       After installing ECE, you run a post-installation script that creates the JMS queue (JMS topic) on the server. The topic name entered here is the name the ECE post-installation script uses to create the JMS queue (JMS topic).

30. Click **Next**.

    The ECE Notification Queue SSL Details screen appears.

31. Enter secure socket layer (SSL) information required to connect to the Java Message Service (JMS) queue to which ECE publishes notification events:

    a. If you will *not* 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.

    b. In the **Keystore password** field, enter the password used to access the SSL keystore file.

    c. In the **Keystore location** field, enter the full path to the SSL keystore file.

32. Click **Next**.

    The Diameter Gateway Details screen appears.

33. Enter information that Diameter clients use to identify your Diameter Gateway server:

    a. 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.

    b. In the **Origin Host** field, enter 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).

    c. In the **Origin Realm** field, enter 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 screen 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 Post-Installation Tasks".

34. Click **Next**.

    The RADIUS Gateway Details screen appears.

35. Enter information that RADIUS clients use to identify your RADIUS Gateway server:

    a. 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.

    b. In the **Name** field, enter the name of the RADIUS Gateway instance.

    c. In the **Port** field, enter the port number assigned to RADIUS Gateway.

d. In the **Shared Secret** field, enter the common password shared between the RADIUS Gateway server and Network Access Server (NAS). It is used by the RADIUS protocol for security.

e. In the **Wallet Location** field, enter 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 screen 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 Post-Installation Tasks".

36. Click **Next**.

The Third-Party Library Details screen appears.

37. In the **Directory** field, enter the patch or browse to the directory that contains the JAR files required by ECE, which you copied to this directory before running the installer.

38. Click **Next**.

The Summary screen appears.

39. Review your selections, and click **Install**.

The Install screen appears, and the installation begins.

Note: If you click **Cancel** after the installation begins, the installation stops, but files already copied are not removed.

When the installation is done, the End of Installation screen appears.

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 Individual ECE Components

The ECE installer enables you to install one or more of the following individual ECE components:

- **ECE Server.** This option is equivalent to the ECE Complete installation. See "Installing All ECE Components."
- **ECE Third-Party Dependent JARs.** This option installs the **ojdbc7.jar** and **wlthint3client.jar** files, which enable the ECE installer to connect ECE to BRM if BRM is in a secure mode. To obtain the JAR files required to install *ECE* in a secure mode, see "Obtaining Required JAR Files."
- **ECE SDK.** This option installs the ECE software development kit. See the discussion about the ECE SDK in *BRM Elastic Charging Engine Implementation Guide* for more information.

During the installation of these components, refer to the required information that you previously collected. See "Information Requirements".

To install an individual ECE component:

1. Create a temporary directory (*temp_dir*).
2. Go to the My Oracle Support Web site:

   http://support.oracle.com
3. Sign in with your user name and password.
4. Click the **Patches & Updates** tab.
5. From the list, select **Patch Name or Number**.
6. In the text field, enter **28738541** and click **Search**.

   The Patch Search Results page appears.
7. Click the patch name.

   The patch details appear.
8. From the **Platform** list, select the platform and click **Download**.

   The File Download dialog box appears.
9. Download the **p28738541_113090**_*platform*.**zip** software pack to *temp_dir*, where *platform* is **linux** or **solaris**.
10. Unzip **p28738541_113090**_*platform*.**zip** and extract the contents to *temp_dir*:

    The extracted software pack has the following structure:

    ocece/Disk1/install

    ocece/Disk1/stage
11. Go to the **ocece/Disk1/install/** directory, and run one of the following commands:
    - To start the GUI installer:

      ```
      ./runInstaller
      ```
    - To start the GUI installer and create a silent installer response file during the installation:

      ```
      ./runInstaller -record -destinationFile path
      ```

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

    The Welcome screen appears.
12. Click **Next**.

    The Specify Inventory Directory and Credentials screen appears.

    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.

    In this screen, enter the following if you do not want to accept the defaults:

    - Full path of the inventory directory

- Name of the operating system group that has write permission to the inventory directory

13. Click **Next**.

    The Select Installation Type screen appears.

14. Select **Custom**, and click **Next**.

    The Specify Home Details screen appears.

15. (Optional) Enter the following information if you do not want to accept the default values:

    a. In the **Name** field, enter a name for the component installation, or select a name from the list.

    b. In the **Path** field, enter the full path or browse to the directory in which to install the component.

16. Click **Next**.

    The Available Product Components screen appears.

17. In the **Components** list, select the components to install, and deselect any other selected components.

18. Click **Next**.

19. Do one of the following:

    - If a screen other than the Summary screen appears, provide the requested information, and click **Next**.

      Continue moving through the screens until the Summary screen appears.

    - If the Summary screen appears, review your selections, and click **Install**.

      The Install screen appears, and the installation begins.

      Note: If you click **Cancel** after the installation begins, the installation stops, but files already copied are not removed.

When the installation is done, the End of Installation screen appears.

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 uses a response file in which you have set installation information. To obtain the response file, you run the GUI installer for the first install. The GUI installer generates a response file that contains the key-value pairs based on the values that you specify during the GUI installation. You can then copy and edit the response file to create additional response files for installing ECE on different machines.

Creating a Response File

The response file must contain the key-value pairs for the mandatory installation parameters used for the ECE software component you install. All information requested in the GUI installation is associated with mandatory parameters.

The parameters in the response file can also be specified on the command line, although specifying all of them on the command line is not recommended. You could, however, have a standard file with set options and then specify, for example, the log locations on the command line. If an option is specified both in the file and on the command line, the command-line option takes precedence over the value in the file.

To create a response file:

1. Run the GUI installation for the ECE software component you want to install. Use the command that generates a response file. See "Installing ECE by Using the GUI Installation."

   A response file containing the required parameters is generated in the *ECE_home*/**Disk1/stage/Response** directory.

2. Copy the response file, and give the copy a different file name.

   You can create as many response files as needed.

3. Modify the response file you copied by specifying the key-value information for the parameters you want in your installation.

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. Create a temporary directory (*temp_dir*).
3. Go to the My Oracle Support Web site:

   `http://support.oracle.com`

4. Sign in with your user name and password.
5. Click the **Patches & Updates** tab.
6. From the list, select **Patch Name or Number**.
7. In the text field, enter **28738541** and click **Search**.

   The Patch Search Results page appears.

8. Click the patch name.

   The patch details appear.

9. From the **Platform** list, select the platform and click **Download**.

   The File Download dialog box appears.

10. Download the **p28738541_113090**_*platform*.**zip** software pack to *temp_dir*, where *platform* is **linux** or **solaris**.
11. Unzip **p28738541_113090**_*platform*.**zip** and extract the contents to *temp_dir*:

    The extracted software pack has the following structure:

    ocece/Disk1/install

ocece/Disk1/stage

12. Copy the response file you created to the machine on which you will run the silent installation.
13. On the machine on which you will run the silent installation, go to the **ocece/Disk1/install/** directory, and run the following command:

    ```
    ./runInstaller.sh [parameter=value] -responseFile path -silent
    ```

    where:

    - *path* is the location and name of your response file.
    - *parameter* is the name of an installation parameter.
    - *value* is the value of the installation parameter.

    For example:

    ```
    ./runInstaller.sh INSTALL_TYPE=Complete -responseFile /tmp/ece_complete.rsp
    -silent
    ```

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."

Next Steps

After you install ECE, perform the post-installation tasks. See "ECE Post-Installation Tasks."

> **Note:** To uninstall ECE, you run the GUI installation and click **Next** until you reach the Specify Home Details screen. In the Specify Home Details screen, click **Installed Products**. In the Inventory screen, select the ECE components to uninstall, and then click **Remove**.

6

Upgrading Existing ECE 11.3 Installation

This chapter describes how to upgrade the existing Oracle Communications Billing and Revenue Management Elastic Charging Engine (ECE) 11.3 installation.

In this chapter, the current ECE 11.3 patch set release running on your system is called the *old* release. The ECE patch set you are upgrading to is called the *new* release.

When upgrading the existing ECE installation, note the following:

- A direct upgrade from the ECE 11.1 or ECE 11.2 release is not supported.
- If you are upgrading to the latest patch set from an earlier ECE 11.2 patch-set release, ECE 11.3, or an ECE 11.3 patch-set release, you must upgrade your system to all prior patch set releases first. For example, if you are running ECE 11.3, you must upgrade to ECE 11.3 Patch Set 8 in the following order:
  - ECE 11.3 Patch Set 1
  - ECE 11.3 Patch Set 2
  - ECE 11.3 Patch Set 3
  - ECE 11.3 Patch Set 4
  - ECE 11.3 Patch Set 5
  - ECE 11.3 Patch Set 6
  - ECE 11.3 Patch Set 7
  - ECE 11.3 Patch Set 8
  - ECE 11.3 Patch Set 9
- The ECE Installer installs the complete ECE software and copies the configuration files to the new complete installation to match your existing ECE 11.3 patch set settings.

Overview of Upgrading Existing ECE 11.3 Installation

Important: To upgrade the existing ECE installation by using the zero downtime upgrade method, see "Performing Zero Downtime Upgrade".

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

Important: Ensure that you install the following in the following order:

1. The ECE patch set.
2. A compatible version of BRM. See the corresponding *BRM 7.5 Patch Set Installation Guide* for installing BRM.
3. A compatible version of PDC. See *PDC Installation and System Administration Guide* for installing PDC.

See "ECE System Requirements" for the compatible version of BRM and PDC.

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

Caution: If you are upgrading to ECE 11.3 Patch Set 7 or later releases, you must install ECE 11.3 Patch Set 7 interim patch 27976672 (IP2) and update the Coherence libraries before performing the rolling upgrade. Otherwise, the rolling upgrade for ECE 11.3 Patch Set 8 will not work. In such a case, you must stop all ECE nodes of your existing installation, restore your ECE system, and then start all ECE nodes of your existing installation. See "Stopping and Restoring Your ECE System".

See the following for more information:

- To upgrade to ECE 11.3 Patch Set 7, see "Upgrading to ECE 11.3 Patch Set 7".
- To upgrade to ECE 11.3 Patch Set 8 from any release prior to ECE 11.3 Patch Set 7, see "Upgrading to ECE 11.3 Patch Set 8".

5. Perform the post-upgrade tasks. See "Performing the Post-Upgrade Tasks".

Upgrading to ECE 11.3 Patch Set 7

To upgrade to ECE 11.3 Patch Set 7:

1. Upgrade your system to all prior patch set releases until ECE 11.3 Patch Set 6.
2. Install ECE 11.3 Patch Set 7.
3. Install the ECE 11.3 Patch Set 7 interim patch 27976672 (IP2).
4. Delete the Coherence libraries in the *ECE_11.3_PS7_IP2_home*/**oceceserver/lib** directory.
5. Copy the Coherence 12.2.1.0.6 libraries manually from the *ECE_11.3_PS6_home*/**oceceserver/lib** directory to the *ECE_11.3_PS7_IP2_home*/**oceceserver/lib** directory.
6. Perform the rolling upgrade for ECE 11.3 Patch Set 7 IP2.

You can later upgrade to ECE 11.3 Patch Set 8 and then ECE 11.3 Patch Set 9 by following the standard instructions in "Performing the Upgrade Tasks" and "Performing the Post-Upgrade Tasks".

Upgrading to ECE 11.3 Patch Set 8

To upgrade to ECE 11.3 Patch Set 8 from any release prior to ECE 11.3 Patch Set 7:

1. Upgrade your system to all prior patch set releases until ECE 11.3 Patch Set 6.
2. Install ECE 11.3 Patch Set 7.
3. Install the ECE 11.3 Patch Set 7 interim patch 27976672 (IP2).
4. Install ECE 11.3 Patch Set 8.
5. Delete the Coherence libraries in the *ECE_11.3_PS7_IP2_home*/**oceceserver/lib** directory.
6. Copy the Coherence 12.2.1.0.7 libraries manually from the *ECE_11.3_PS8_home*/**oceceserver/lib** directory to the *ECE_11.3_PS7_IP2_home*/**oceceserver/lib** directory.
7. Perform the rolling upgrade for ECE 11.3 Patch Set 7 IP2.
8. Perform the rolling upgrade for ECE 11.3 Patch Set 8.

You can later upgrade to ECE 11.3 Patch Set 9 by following the standard instructions in "Performing the Upgrade Tasks" and "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.

For more information on creating an active-hot standby disaster recovery system, see the discussion about configuring ECE for disaster recovery in *BRM Elastic Charging Engine System Administrator's Guide*.

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

- You have the same instances of ECE 11.3 or an ECE 11.3 patch set, BRM 7.5 patch set, and PDC 11.1 patch set 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.

      See "ECE System Requirements" for the compatible BRM version and the corresponding *BRM 7.5 Patch Set Installation Guide* for installing BRM using the zero downtime upgrade method.

c. Upgrade the PDC instance to the version compatible with your *new* release.

   See "ECE System Requirements" for the compatible PDC version and *PDC Installation and System Administration Guide* for installing PDC.

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 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 need not upgrade to all prior patch set releases. You can also skip the "Performing a Rolling Upgrade" task.

   c. Start ECE. See the discussion about starting and stopping ECE in *BRM Elastic Charging Engine 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. In your production site, do the following:

   a. Stop the BRM and PDC instances.

   b. Upgrade ECE to the *new* release. You must upgrade to all prior patch set releases first before upgrading to the *new* release. Perform all the tasks described in "Overview of Upgrading Existing ECE 11.3 Installation".

   c. Upgrade the BRM instance to the version compatible with your *new* release.

      See "ECE System Requirements" for the compatible BRM version and the corresponding *BRM 7.5 Patch Set Installation Guide* for installing BRM using the zero downtime upgrade method.

   d. Upgrade the PDC instance to the version compatible with your *new* release.

      See "ECE System Requirements" for the compatible PDC version and *PDC Installation and System Administration Guide* for installing PDC.

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

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

```
gridSync start
gridSync replicate
```

6. In your backup site, start replicating the ECE cache data to your production site by running the following commands:

```
gridSync start
gridSync replicate
```

7. Verify that the ECE data is automatically replicated to both sites.

Performing the Pre-Upgrade Tasks

This section provides instructions for ECE pre-upgrade tasks.

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.

Important: 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 11.3 patch set home directory, *ECE_New_home*; for example, ECE_113PS9. 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 11.3 patch set 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

This section provides instructions for ECE upgrade tasks.

Obtaining the ECE 11.3 Patch Set Software

To obtain ECE 11.3 Patch Set software:

1. Create a temporary directory (*temp_dir*).
2. Go to the My Oracle Support Web site:

   http://support.oracle.com

3. Sign in with your user name and password.
4. Click the **Patches & Updates** tab.
5. From the list, select **Patch Name or Number**.

6. In the text field, enter the *PatchNumber* and click **Search**.

   where *PatchNumber*:

   - For ECE 11.3 Patch Set 1 is **24489027**
   - For ECE 11.3 Patch Set 2 is **24708603**
   - For ECE 11.3 Patch Set 3 is **25655714**
   - For ECE 11.3 Patch Set 4 is **26420699**
   - For ECE 11.3 Patch Set 5 is **27145275**
   - For ECE 11.3 Patch Set 6 is **27406358**
   - For ECE 11.3 Patch Set 7 is **27531574**
   - For ECE 11.3 Patch Set 8 is **28133198**
   - For ECE 11.3 Patch Set 9 is **28738541**

   The Patch Search Results page appears.

7. Click the patch name.

   The patch details appear.

8. From the **Platform** list, select the platform and click **Download**.

   The File Download dialog box appears.

9. Download the **p***PatchNumber_PatchSet_platform***.zip** software pack to *temp_dir*.

   where:

   - *PatchSet*:
     - For ECE 11.3 Patch Set 1 is **113010**
     - For ECE 11.3 Patch Set 2 is **113020**
     - For ECE 11.3 Patch Set 3 is **113030**
     - For ECE 11.3 Patch Set 4 is **113040**
     - For ECE 11.3 Patch Set 5 is **113050**
     - For ECE 11.3 Patch Set 6 is **113060**
     - For ECE 11.3 Patch Set 7 is **113070**
     - For ECE 11.3 Patch Set 8 is **113080**
     - For ECE 11.3 Patch Set 9 is **113090**
   - *platform* is **linux** or **solaris**.

10. Unzip **p***PatchNumber_PatchSet_platform***.zip** and extract the contents to *temp_dir*:

    The extracted software pack has the following structure:

    ocece/Disk1/install

    ocece/Disk1/stage

Installing the ECE 11.3 Patch Set for Your Upgrade

Install the ECE 11.3 patch set using the **Patchset** installer type into *ECE_New_home*.

Follow the instructions in "Installing Elastic Charging Engine" to install ECE using the **Patchset** installer type.

In the Existing ocece Installation Details screen, 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 patch set, 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.

> **Important:** 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**.

   > **Important:** 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.

For information about the mediation specification file, see *BRM Elastic Charging Engine Implementation Guide*.

Reconfiguring Log4j2 Configuration File Settings to Match Your Old Settings

Note: Perform this step only if you are upgrading from ECE 11.3 Patch Set 3 to ECE 11.3 Patch Set 4.

In ECE 11.3 Patch Set 4, the **Log4j.properties** file is replaced with the **log4j2.xml** file. After installing ECE 11.3 Patch Set 4, reconfigure all the default settings in the *ECE_home***/oceceserver/config/log4j2.xml** file to match your customized settings in the **Log4j.properties** file in your old release.

From ECE 11.3 Patch set 4, use the **log4j2.xml** file to configure logging in the XML format for the entire cluster.

Important: The existing **log4j.properties** configuration is supported only for backward compatibility.

For information about Log4j settings and configuring logging, see *BRM Elastic Charging Engine System Administrator's Guide*.

Configuring Persistence Environment

Important: Perform this step only in the test environment.

In the test environment, you can configure the persistence if you are upgrading from ECE 11.3 Patch Set 4 to ECE 11.3 Patch Set 5.

To configure the persistence environment:

1. On the driver machine, open the *ECE_home***/oceceserver/config/ece.properties** file.
2. Ensure that the **java.property.ece.persistence.mode** and **java.property.coherence.distributed.persistence.base.dir** entries are set:

   ```
   java.property.ece.persistence.mode=on-demand
   java.property.coherence.distributed.persistence.base.dir= ECE_home/persistence/
   ```

   If you want to persist the pricing and configuration data in the active persistence mode, set the **java.property.ece.persistence.mode** entry to **active**. For more information, see the discussion about active persistence of ECE caches in *ECE Release Notes*.
3. Save and close the file.
4. Open the ECE Coherence override file your ECE system uses (for example, *ECE_home***/oceceserver/config/charging-coherence-override-secure-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.
5. Add the following entries:

   ```
   <!-- ECE persistence environment -->
          <persistence-environments>
              <persistence-environment id="ece-environment">
                  <persistence-mode
   system-property="ece.persistence.mode">persistence_mode</persistence-mode>
              </persistence-environment>
          </persistence-environments>
   ```

   where *persistence_mode* is **active** or **on-demand**. If you have set **java.property.ece.persistence.mode** to **active** in step 2, set *persistence_mode* to **active**.
6. Save and close the file.

Upgrading Extension Code

If you customized 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 screen, 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 screen, 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 the discussion about encrypting new passwords in *BRM Elastic Charging Engine System Administrator'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. For more information, see the discussion about configuring a WebLogic Server connection factory for a JMS topic.

- *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 the discussion about configuring JMS credentials for publishing external notifications in the *ECE Implementation Guide*.

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 screen, 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 screen, 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

This section provides instructions for ECE post-upgrade tasks.

Deploying the Patch Set Onto Server Machines

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

Deploying the patch set 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 patch set 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.

Performing a Rolling Upgrade

Caution: If you are upgrading to ECE 11.3 Patch Set 7 or ECE 11.3 Patch Set 8, you must install ECE 11.3 Patch Set 7 interim patch 27976672 (IP2) and update the Coherence libraries before performing the rolling upgrade. Otherwise, the rolling upgrade for ECE 11.3 Patch Set 8 will not work. In such a case, you must stop all ECE nodes of your existing installation, restore your ECE system, and then start all ECE nodes of your existing installation. See "Stopping and Restoring Your ECE System".

See the following for more information:

- To upgrade to ECE 11.3 Patch Set 7, see "Upgrading to ECE 11.3 Patch Set 7".
- To upgrade to ECE 11.3 Patch Set 8 from any release prior to ECE 11.3 Patch Set 7, see "Upgrading to ECE 11.3 Patch Set 8".

Note: You can skip this step if you are upgrading from ECE 11.3 to ECE 11.3 Patch Set 1.

Rolling upgrade does not work for upgrading to ECE 11.3 Patch Set 1. You must stop all ECE nodes of your existing installation, restore your ECE system, and then start all ECE nodes of your existing installation. For more information, see "Stopping and Restoring Your ECE System".

Rolling upgrades will gracefully shut down processes of the old ECE installation and start up the processes of the new installation while maintaining operation of the overall ECE system.

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.

To perform a rolling upgrade:

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 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.

Tip: Before performing the rolling upgrade, the new release must be installed in a different directory. After launching ECC using the new installation, the **rollingUpgrade** command is called to upgrade the system to the new release.

1. Ensure that you deploy the new release onto server machines. See "Deploying the Patch Set Onto Server Machines".
2. Run the following command to start the rolling upgrade in the new release while ECE is still operating on the old release:

   ```
   groovy:000> rollingUpgrade
   ```

   One by one, each node on the old location is brought down, upgraded, and joined back to the cluster.

   When you run the **rollingUpgrade** command with no parameters specified, all running nodes are upgraded (charging server nodes, data-loading utility nodes, data updating nodes, and so on) except for simulator nodes.

   The order in which the nodes are restarted adheres to the order in which the nodes are listed in the *ECE_New_home***/config/eceTopology.conf** file.

   You can choose to upgrade nodes (bring them down, upgrade them, and join them back to the cluster) by node *role*. It is recommended to first upgrade all the nodes of role **ratedEventFormatter**, followed by all the nodes of role **server**, followed by all the nodes of role **updater**, and then followed lastly by all the nodes of role **diametergateway**; for example:

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

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

When 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 by doing the following:

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).

Loading Pricing Data From PDC into ECE

After you perform the rolling upgrade, load all the pricing data (the metadata, setup, pricing, and profile data) from the PDC database into ECE.

To load the pricing data from PDC into ECE:

1. 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.
2. Log on to the driver machine.
3. Go to the *ECE_New_home*/**bin** directory.
4. Start ECC:

   ```
   ./ecc
   ```

5. Run the following commands in this order:

   ```
   start
   start configLoader
   start pricingUpdater
   ```

   All the pricing data from the PDC database is loaded into ECE.

Stopping and Restoring Your ECE System

> **Caution:** 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.
>
> Restarts of the ECE system are done for test systems only when it is intended to remove 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. 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 the discussion about configuring ECE for synchronizing BRM and ECE customer data in real time in *BRM Elastic Charging Engine Implementation Guide* for more information.
7. Start ECE processes and gateways in the following order:

   > **Important:** 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.

Verifying the Installation After the Upgrade

Note: Test the patch set 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 Post-Installation Tasks

This chapter provides instructions for Oracle Communications Billing and Revenue Management Elastic Charging Engine (ECE) post-installation tasks. You must install ECE before following these procedures. See "Installing Elastic Charging Engine".

If you are upgrading ECE 11.3 or an ECE 11.3 patch set, see the following for information on post-installation tasks:

- Upgrading Existing ECE 11.3 Installation

Overview of ECE Post-Installation Tasks

After installing ECE, you must perform certain tasks. Some tasks you only need to perform for an ECE integrated installation. See the following topics for the post-installation tasks:

- Post-Installation Tasks Common to All ECE Installations
- Post-Installation Tasks for an ECE Integrated Installation

Post-Installation Tasks Common to All ECE Installations

This section describes the post-installation tasks you must perform that are common to all ECE installations.

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.

> **Note:** (Linux) If you used the **ece_provision** script to provision your environment for an ECE installation, verify that the **rootDir**, **user**, and **driverIP** parameters match the corresponding parameters that you defined in the **ece_provision_config.sh** script.

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 pre-configured 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*/**oceceserver/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*/**oceceserver/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*/**oceceserver/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

This section describes how to configure ECE for multicast or unicast. 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 pre-existing 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 the discussion about 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:

http://docs.oracle.com/cd/E18686_01/coh.37/e18679/tune_multigramtest.htm

To determine whether multicast is enabled in the operating system, go to the directory where the **multicast-test.sh** script is located and use the following test.

> **Note:** If you used the **ece_provision** script, run the test from your UNIX home directory in **/opt/coherence/bin**.

```
$ ./multicast-test.sh -ttl 0
```

You can use the following tests to determine if multicast is enabled in the network. Start the test on Machine A and Machine B by entering the following command into the respective command window of each and pressing ENTER:

```
Machine A $ ./multicast-test.sh -ttl 1
Machine B $ ./multicast-test.sh -ttl 1
```

If multicast across Machine A and Machine B is not working with a TTL (time to live) setting of **1**, repeat this test with the default TTL setting of **4**. A TTL setting of **4** is required when the machines are not on the same subnet. If all participating machines are connected to the same switch, and therefore in the same subnet, use the TTL setting of **1**.

If Machine A and Machine B both have multicast enabled in the environment, the test output for each machine will show the machine issuing multicast packets and seeing both its own packets as well as the packets of the other machine. This indicates that multicast is functioning properly between the machines.

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*/**ocecerver/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*/**ocecerver/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 on adding and configuring Diameter Gateway nodes, see *BRM Elastic Charging Engine System Administrator's Guide*.

Important: When configuring additional Diameter Gateway nodes, ensure that you configure the Diameter peers and alternative peers for routing notifications. See the discussion about configuring alternative Diameter peers for notifications in *BRM Elastic Charging Engine Implementation Guide* 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 on adding and configuring RADIUS Gateway nodes, see *BRM Elastic Charging Engine 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 the discussion about configuring default system currency in *BRM Elastic Charging Engine System Administrator's Guide*.

Configuring Headers for External Notifications

To identify and process external notifications, you must configure a header for each external notification. See the discussion about configuring headers for external notifications in *BRM Elastic Charging Engine Implementation Guide* for more information.

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.

Post-Installation Tasks for an ECE Integrated Installation

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

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

1. Create the following required queues for BRM and Pricing Design Center (PDC):
   - Suspense queue

     See the *BRM Elastic Charging Engine System Administrator's Guide* for the discussion on configuring the suspense queue and troubleshooting update request failures.
   - Acknowledgement queue

     See the discussion about implementing ECE with BRM in *BRM Elastic Charging Engine Implementation Guide* for information about the acknowledgement queue.
   - 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.

     See the discussion in the Oracle WebLogic Server documentation for information about setting up JMS queues.

     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 the discussion about configuring notifications for charging in *BRM Elastic Charging Engine Implementation Guide* for more information about configuring the ECE notification queue.

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

2. 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 *Oracle Communications Offline Mediation Controller Elastic Charging Engine Cartridge Pack User Guide* for instructions on installing and configuring Offline Mediation Controller to access ECE SDK libraries and send usage requests for offline CDRs.
3. 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 Required Queues for BRM

Use the **post_Install.pl** script to create the required BRM queues: suspense queue, acknowledgement queue, and JMS notification queue.

Location

ECE_home/**oceceserver/post_installation/**

Syntax

```
perl post_Install.pl
```

You are prompted to install the BRM suspense and acknowledgement queues and the JMS notification queue. You can choose to install one, two, or all the queues.

The queue names are specified during the ECE installation process and are used by the post installation 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 acknowledgement queues are already created, a note will be logged in **brm_queue.log**. If the JMS notification queue is already created, a note will be logged in **output.log**.

Parameters

For the BRM suspense and acknowledgement 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 database schema user name.
- **BRM_DB_PASSWORD**: The password for the BRM database user.

For the JMS 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 the WebLogic server:

1. Log on to the WebLogic Server on which the JMS topic for the ECE notification queue resides.
2. In the WebLogic Server Administration Console, from the JMS modules list, select the connection factory that applies to the JMS topic.
3. In the **Client** tab, do the following:
   a. Set **Reconnect Policy** to **None**.
   b. Set **Client ID Policy** to **Unrestricted**.
   c. Set **Subscription Sharing Policy** to **shareable**.
4. In the **Transactions** tab, set **Transaction Timeout** to **2147483647**.

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 (see "ECE Notification Queue Details."). If your ECE system includes multiple ECE notification queue hosts for failover, you must specify connection information for *all* the hosts.

To configure credentials for multiple JMS WebLogic servers:

1. Open the *ECE_home***/oceceserver/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 screen, 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 screen, 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 the discussion about encrypting new passwords in *BRM Elastic Charging Engine 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 configuring a WebLogic Server connection factory for a JMS topic in *BRM Elastic Charging Engine Implementation Guide* for more information.
   - **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, and BRM:

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
```

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
```

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 for the Weblogic server, PDC, and BRM 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
```

where:

- *certificatename* is the name of the certificate file in which the Java keystore certificates for connecting to the Weblogic server, PDC, and BRM are stored.
- *mykeystore* is the keystore.
- *mystorepass* is the keystore password.

The Java keystore certificates are imported into the default Java ketstore.

Next Steps

For a standalone installation, verify the installation. See "Verifying the ECE Installation" for instructions.

For an integrated installation, you are ready to implement ECE with the required software products in the charging system. See *BRM Elastic Charging Engine Implementation Guide* for complete instructions.

8

Verifying the ECE Installation

This chapter describes how to verify that Oracle Communications Billing and Revenue Management Elastic Charging Engine (ECE) was installed correctly. If you cannot verify the installation, see "Troubleshooting the ECE Installation".

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; see the discussion about verifying an ECE integrated installation in *BRM Elastic Charging Engine Implementation Guide* for information about the specific tasks.

- 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.

See *BRM Elastic Charging Engine Implementation Guide* for instructions on implementing ECE with each product in an integration installation (configuring the integration points) and verifying that the integrated installation is working.

Verifying an ECE Standalone Installation

This section describes how to verify an ECE 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*/**ocecesever/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 JConosle, that enables you to edit MBean attributes.
   d. Connect to the ECE charging server node set to **start CohMgt = true** in the *ECE_home*/**ocecesever/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*/**oceceserver/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 pricingLoader
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*/**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 **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 the discussion about using the simulator in *BRM Elastic Charging Engine Implementation Guide* for more information about using the simulator.

This procedure assumes you are in the *ECE_home*/**oceceserver/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

See *BRM Elastic Charging Engine Implementation Guide* for instructions on implementing ECE with each product in an integrated installation and verifying that the integrated installation is working.

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.

If you cannot verify the ECE installation, see the discussion about troubleshooting ECE in *BRM Elastic Charging Engine System Administrator's Guide*.

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 post-installations:

- **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.

  See *BRM Elastic Charging Engine Implementation Guide* for information about the tasks required to implement ECE with BRM and PDC.
- Set up ECE system security.

See the discussion about setting up and managing ECE security in *BRM Elastic Charging Engine System Administrator's Guide* and *BRM Elastic Charging Engine Security Guide*.

- Configure the ECE system.

  See *BRM Elastic Charging Engine System Administrator's Guide*.

- 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.

  For information about purging rated events, see the discussion about managing persisted data in the Oracle NoSQL Database in *BRM Elastic Charging Engine System Administrator's Guide*.

- If you installed the optional product Oracle Application Management Pack for Oracle Communications, see Oracle Application Management Pack for Oracle Communications System Administrator's Guide for information about monitoring ECE nodes and clusters.

A

Elastic Charging Engine Installer Screens

This appendix describes the information you need to provide for each screen when you install Oracle Communications Billing and Revenue Management Elastic Charging Engine (ECE) in interactive mode for a complete installation type. You can also access the information in this appendix by clicking **Help** during installation.

> **Note:** This document does not substitute for ECE installation instructions. You should read all chapters in *ECE Installation Guide* in preparation for installing ECE, including "ECE System Requirements" for information you need to collect in preparation for installation, and "Installing Elastic Charging Engine" for installation procedures.

Select Installation Type

Select the installation type.

Option	Description
Complete	Installs Oracle Communications Billing and Revenue Management (BRM) Elastic Charging Engine (ECE) server, ECE SDK, and all BRM and Pricing Design Center (PDC) integration packs.
Standalone	Installs a self-contained, nonproduction version of ECE that is not integrated with BRM or PDC. Use the stand-alone system for evaluation, demonstration, and functional testing.
Patchset	Upgrades an existing system to the current version of ECE.
Custom	Enables you to choose multiple components for installation.

Specify Home Details

Specify the name and location of the directory in which to install ECE.

Field	Description
Name	The name of the directory in which to install ECE. If the directory exists, it should be empty. If it does not exist, the installer creates it.
Path	The full path to the directory in which to install ECE.

Select ECE Security Options

Select your preferred security configuration, such as whether to enable secure socket layer (SSL) configuration.

Based on the security configuration you select, ECE sets parameters in the relevant Oracle Coherence and ECE configuration files to enable the security levels specified.

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 ■ BRM SSL security authentication ■ PDC SSL security authentication ■ EM Gateway SSL security authentication

See *BRM Elastic Charging Engine Security Guide* for more information about each security option that can be enabled.

Config Data Details

Enter the path to the directory that contains configuration data (mediation specifications).

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

For more information about configuration data, see the discussion about implementing ECE with BRM in *BRM Elastic Charging Engine Implementation Guide*.

Persistence Data Details

Enter the path to the directory into which the BrmCdrPluginDirect Plug-in will write call detail record (CDR) files of rated events.

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

ECE Cluster Details

Enter information about the ECE cluster.

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. **Note:** If you used the **ece_provision** script to provision your environment for an ECE installation, the user name for host machines you enter in the ECE Cluster Details screen must be the same user name you entered for the ECE_USER field in the **ece_provision_config.sh** file.
Java Heap Settings	The memory to be allocated to each node in the ECE cluster.
Cluster Name	The cluster name used by applications to identify ECE in the cluster. The cluster name must be less than 32 characters.

Coherence Grid Security

Enter information about the machines allowed to be part of the Coherence cluster and the account alias information for Coherence cluster security.

For specifying trusted machines, you can enter a range of IP addresses, a list of IP addresses separated with a comma, or both.

Field	Description
Host Details in Comma Separated Format	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. **Note:** (Linux) If you used the **ece_provision** script to provision your environment for an ECE installation, authorized host list information you enter in the Coherence Grid Security screen must be the same host information you entered for the HOST field in the **ece_provision_config.sh** file.
Host Details Range from IP Address	The valid from address for the range of IP addresses in the subnet. The from-to format of entering IP addresses is typically used for hosts that are in the same subnet.
Host Details Range to IP Address	The valid to address for the range of IP addresses in the subnet.
Alias Name for Coherence Grid Security	The account alias that defines the administrator for securing the Coherence cluster.
Password for the Alias	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.

See the discussion about Coherence cluster security in *BRM Elastic Charging Engine Security Guide* for more information.

Oracle NoSQL Database Details

Enter the Oracle NoSQL database connection information, including the name of the NoSQL data store in which you want to persist ECE rated events.

Field	Description
Host Name	The host name or IP address of the Oracle NoSQL database.
Port Number	The port of the Oracle NoSQL database service.
NoSQL Datastore Name (database name)	The name of the Oracle NoSQL data store into which ECE will publish rated events.

Keystore Credentials

Enter the keystore credential information required for the ECE installation.

Field	Description
Key Password for Boundary System Alias	The password ECE uses to access the boundary system alias key in the (*ECE_home*/**oceceserver/config/keystore.jks**) file. The boundary systems are BRM and PDC. ECE uses a file-based keystore for encrypting passwords when required. The **keystore.jks** file stores cipher keys and is used for encrypting and managing the credentials of BRM and PDC (and other client applications), allowing them to access the cluster using encrypted passwords.
Certificate Store Password	The password used to access the keystores. This password is used to access both the Coherence grid security keystore and the boundary system keystore JKS files: ■ *ECE_home*/**oceceserver/config/keystore.jks** ■ *ECE_home*/**oceceserver/config/server.jks** The **server.jks** file stores cipher keys used for Oracle Coherence cluster security (securing ECE cluster processes) and for enabling Secure Socket Layer (SSL). The **server.jks** file is a storage where cluster node credentials are stored and credentials are authenticated against. The **keystore.jks** and **server.jks** files share the same key and store password.

Field	Description

DName	The DName (Distinguished Name) is similar to a group in UNIX.
	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 value set here (in creating the certificate) is used for authentication in the cluster and must be the same 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 and the **keystore.jks** keystore.

See the discussion about keystores in *BRM Elastic Charging Engine Security Guide* for more information about keystore credentials information.

ECE Notification Queue Details

Enter the Java Message Service (JMS) credentials for the JMS server on which the ECE notification queue (JMS topic) is to reside.

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 post-installation script that creates the JMS queue (JMS topic) on the server.

Field	Description
Host Name	The host name of the server on which the JMS queue (JMS topic) resides.
Port Number	The port number on which the server resides.
User Name	The user for logging in to the server.
Password	The password for logging in to the server.
Connection Factory Name	The connection factory name used to create connections to the JMS queue (JMS topic) on the server to which ECE publishes notification events. After installing ECE, you run an ECE post-installation 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 (JMS topic).

Field	Description
Topic Name	The name of the JMS topic on the server to which ECE publishes notification events. After installing ECE, you run a post-installation script that creates the JMS queue (JMS topic) on the server. The topic name entered here is the name the ECE post-installation script uses to create the JMS queue (JMS topic).
Suspense Queue Name	The BRM Gateway suspense queue is created as part of post-install script in case of full installation. In case of a patch-set release a new JMS suspense queue is configured manually in the WebLogic within the ECE JMS module.

ECE Notification Queue SSL Details

Enter secure socket layer (SSL) information required to connect to the Java Message Service (JMS) queue to which ECE publishes notification events.

Field or Option	Description
Disable SSL	When selected, specifies that SSL is not used to secure the ECE JMS queue connection. 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.

BRM Gateway Details

Enter the BRM Gateway connection details.

Field or Option	Description
Host Name	The IP address or the host name of the computer on which BRM is configured.
CM Port	The port number for the BRM Connection Manager.
User Name	The user name for logging in to BRM.
Password	The password for logging in to BRM.
Disable SSL	When selected, specifies that secure socket layer (SSL) is not used to encrypt communication between ECE and BRM through BRM Gateway. If you select this option, do not change the value in the following field.
Wallet File Absolute Path	The default path to the Oracle wallet file containing the SSL trusted certificates for BRM Gateway: `/opt/wallet/client/cwallet.sso` If SSL is enabled for BRM Gateway but the wallet is in a different location, replace the default path with the full path to the actual location.

External Manager (EM) Gateway Details

Enter the External Manager (EM) Gateway connection details.

Field or Option	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	When selected, specifies that secure socket layer (SSL) is not used to encrypt communication between BRM and ECE through EM Gateway. If you select this option, do not enter or change values in the following fields.
Client Authentication Disabled	When selected, specifies that no authentication is performed to check whether EM Gateway is allowed to communicate with ECE.
Client wallet	The default path to the Oracle wallet file containing the SSL trusted certificates for EM Gateway: `/opt/wallet/server/cwallet.sso` If SSL is enabled for EM Gateway but the wallet is in a different location, replace the default path with the full path to the actual location.

PDC Pricing Components Queue Details

Enter the system connection information of the server on which the JMS queue for PDC pricing component data resides.

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

Field or Option	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 for logging in to the server on which the PDC JMS queue resides.
Password	The password for logging in to the server on which the PDC JMS queue resides.
Disable SSL	When selected, specifies that secure socket layer (SSL) is not used to encrypt communication between BRM and PDC. If you select this option, do not enter values in the following fields.

Field or Option	Description
PDC Keystore Password	The password used to access the SSL keystore file.
Keystore Path	The full path to the SSL keystore file.

BRM Database Connection Details

Enter the 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 you created in the BRM system for the BRM Account Synchronization Data Manager (DM) to publish business events for ECE to consume. ECE listens on this queue for loading update requests from BRM.
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 post-installation script to create this queue. When prompted by the script, enter the queue name you entered here.
Acknowledgement 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 post-installation script to create this queue. When prompted by the script, enter the queue name you entered here.

Diameter Gateway Details

Enter information that Diameter clients use to identify your Diameter Gateway server.

Field or Option	Description
Skip	When selected, specifies that Diameter Gateway is not started when ECE is started. 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. This value 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.
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. This value is used by Diameter clients to identify your Diameter Gateway server as the source of the Diameter message. The Diameter Gateway details you enter in this screen 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.

For more information about how the Origin-Host and Origin-Realm AVPs can be specified, see Internet Engineering Task Force (IETF) Network Working Group RFC 3588 (Diameter Base Protocol).

The Diameter Gateway details you enter in this screen apply to a single instance (node) of a Diameter Gateway server that the installer adds to your ECE topology. You must add more Diameter Gateway nodes to your topology after installation. See the discussion about adding and configuring Diameter Gateway nodes for online charging in *BRM Elastic Charging Engine Installation Guide* for more information.

RADIUS Gateway Details

Enter information that RADIUS clients use to identify your RADIUS Gateway server.

Field or Option	Description
Skip	Specify whether RADIUS Gateway is started when ECE is started.
Name	The name of the RADIUS Gateway instance.
Port	The port number assigned to RADIUS Gateway.
Shared Secret	The common password shared between your RADIUS Gateway server and Network Access Server (NAS). It is used by the RADIUS protocol for security. Each RADIUS Gateway instance must have a unique password in encrypted format.
Wallet Location	The path to the Oracle wallet file containing SSL trusted certificates and the BRM root key for RADIUS Gateway.

The RADIUS Gateway details you enter in this screen apply to a single instance (node) of a RADIUS Gateway server that the installer adds to your ECE topology. You must add more RADIUS Gateway nodes to your topology after installation. See the discussion about adding and configuring RADIUS Gateway nodes for Authentication and Accounting in *BRM Elastic Charging Engine Installation Guide* for more information.

Third-Party Library Details

Enter the directory where you saved the JAR files required during the ECE installation process.

See the discussion about pre-installation tasks in *BRM Elastic Charging Engine Installation Guide* for information about required JAR files.

Existing ECE Installation Details

Enter the full path to the directory in which your current version of ECE is installed.