Policy Management

Configuring Lawful Intercept Application Note

Release 12.6.1
F47286-03
October 2023

ORACLE

Policy Management Configuring Lawful Intercept Application Note, Release 12.6.1

F47286-03

Contents

About This User's Guide

This chapter describes the content and structure of the user's guide, indicates how to obtain help, details where to find related documentation, and provides other general information.

Introduction

This application note describes how to set up Oracle Communication Policy Management Lawful Intercept (LI) in the Oracle Communications Policy Management Configuration Management Platform (CMP) product.

Conventions

The following conventions are used throughout this application note:

- **Bold text** in procedures indicates icons, buttons, links, or menu items that you click on.
- *Italic text* indicates variables.
- `Monospace text` indicates text displayed on screen.
- **`Monospace bold text`** indicates text that you enter exactly as shown.

How This Application Note Is Organized

The information in this application note to set up LI is presented in one chapter, Setting Up Lawful Intercept.

Scope and Audience

This guide is intended for trained and qualified system administrators who are responsible for performing LI in a Policy Management network.

Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

Table 1 Admonishments

Icon	Description
	Danger: (This icon and text indicate the possibility of *personal injury*.)
	Warning: (This icon and text indicate the possibility of *equipment damage*.)
	Caution: (This icon and text indicate the possibility of *service interruption*.)
	Topple: (This icon and text indicate the possibility of *personal injury* and *equipment damage*.)

Related Publications

For information about additional publications related to this document, refer to the Oracle Help Center site. See Locate Product Documentation on the Oracle Help Center Site for more information on related product publications.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click `Industries`.
3. Under the Oracle Communications subheading, click the `Oracle Communications documentation` link.

   The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
4. Click on your Product and then the Release Number.

   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the `PDF` link, select `Save target as` (or similar command based on your browser), and save to a local folder.

Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training:

http://education.oracle.com/communication

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site:

www.oracle.com/education/contacts

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support can assist you with My Oracle Support registration.

Call the Customer Access Support main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

- For Technical issues such as creating a new Service Request (SR), select **1**.
- For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.
- For Hardware, Networking and Solaris Operating System Support, select **3**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support main number at 1-800-223-1711 (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions

- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

List of Figures

List of Tables

1

Setting Up Lawful Intercept

This application note provides an overview of Oracle Communications Policy Management Lawful Intercept (LI) and also describes how to set up LI by enabling the LI software and configuring the LI devices and connections.

Overview

The Communications Assistance for Law Enforcement Act (CALEA) enhances the ability of law enforcement and intelligence agencies to conduct electronic surveillance of telecom equipment and carriers through the use of LI.

This application note describes the configuration of Oracle Communications LI. Specifically, this document describes the internal network interface towards intercept access points in an IP multimedia subsystem packet data network. It specifies information relating to the provisioning of LI in an Intercept Access Point, the reporting of intercept identifying information by an intercept access point to the mediation function (MF), and describes other data necessary to satisfy LI requirements for IP multimedia subsystem packet data applications.

The LI 3GPP interface includes the following:

LI:
Lawful intercept. A mechanism that passes information between a network operator, access provider, or service provider and a handover interface; also, information passed between the handover interface and an internal network.

MF:
Mediation function. The LI handover interface device.

Handover Interface:
A physical and logical interface across which interception measures are requested from a network operator, access provider, or service provider. The results of interception are delivered to a law enforcement monitoring facility.

X1:
The X1 interface manages the provisioning, re-provisioning, de-provisioning, and querying of LI targets and modifies how and when the target activities on the network are monitored. You can determine which targets are to be provisioned or re-provisioned at a given time or have existing targets queried or de-provisioned.

X2:
The X2 interface receives the notification when the target's state changes.

X3:
The X3 interface delivers bulk content to the MF.

Figure 1-1 shows the architecture for LI within the IMS packet data network.

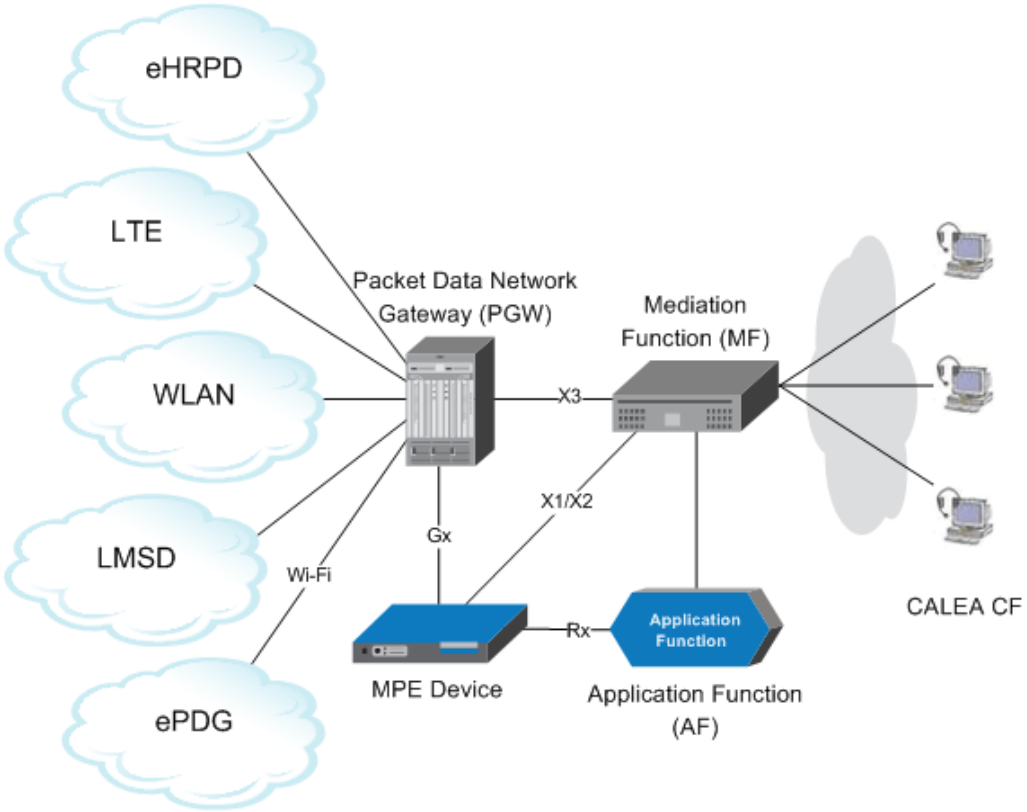
All of the Multimedia Policy Engine (MPE) devices making up a cluster must use the primary site virtual IP (VIP) address for generating the correlation ID, which is based on the policy

server ID. The single MPE server in the secondary site must be configured with a static IPv4 or IPv6 address, as described in Configuring a Static IP Address on an MPE Device. This IP address must be used for generating the correlation ID if the MPE device in the secondary site becomes active. Because the MPE device is a client to the X2 interface, only the active server initiates the X2 connections to the MF. If the server is reduced from active status, it disconnects from the MF.

You must synchronize the SSL certificates between the primary and secondary sites.

If georedundancy with state replication is enabled, the IPv4 or IPv6 address must also be configured on the X1 interfaces on the MF devices to allow them to connect to the MPE device in the secondary site through the X1 interface. When the MPE device in the secondary site is inactive, it uses its static IP address to indicate to the MF via X1 that it is not active and not servicing requests. Georedundancy and state replication are described in *CMP Wireless User's Guide*.

Figure 1-1 Lawful Intercept Architecture



To provide LI, the following occurs:

1. The MPE device receives information about an LI target that is to be provisioned on the network. The MPE device can process information sent from either of two sources:
   - an X1 message sent from an MF using HTTP 1.1
   - an Rx message sent from an application function (AF) containing an encrypted LI-indicator attribute-value pair (AVP)

2. The MPE device forwards the information about the target from either source to the policy and charging enforcement point (PCEF), in this example a packet data network gateway (PGW), using Diameter Gx, which provisions the target on the network and responds back to the MPE device with a Diameter Gx message.
3. The MPE device stores all the information about the provisioned target and sends an X2 message to the MF with the provisioned target information and status (active/inactive).

> **Note:**
>
> Intercept target messages sent over X2 only pertain to targets provisioned over X1. It does not apply to targets identified for intercept over Rx.

4. After the target is de-provisioned, the MPE device removes all the information about the target.

After an LI target is provisioned into the MPE device, and the intercepted subscriber establishes a data session, the MPE device provisions the PGW during real-time signaling interaction that occurs between these two nodes. Within this architecture, the MPE device is responsible for intercepting the packet data event (data session connected or disconnected, for example) and informing the MF.

The MPE device serves as the internet access point for the packet data event, but it is not received from the MF. It is received from the PGW and is triggered by the subscriber action (for example, call setup or termination). Information received from an AF is decrypted, translated into Gx protocol, reencrypted, and passed on to the PGW. The underlying PGW serves as the internet access point for data content. The MF directs, and interacts with, these network elements to obtain the necessary surveillance information and deliver the information to law enforcement CALEA collection functions (CF). All data-related information is delivered over a data channel, and data content is delivered over a data-content channel.

To obscure when a subscriber is being targeted, when the LI functionality is configured the MPE device randomly sends LI-indicator-Gx AVPs with phantom data on the Gx interface.

> **Note:**
>
> If the Policy Management software is rolled back to an earlier version while an LI target is being actively monitored, target data is not preserved. A subsequent audit can identify and correct any inconsistencies between the MF and the MPE device. Performing the audit is outside the scope of this document.

Enabling Lawful Intercept

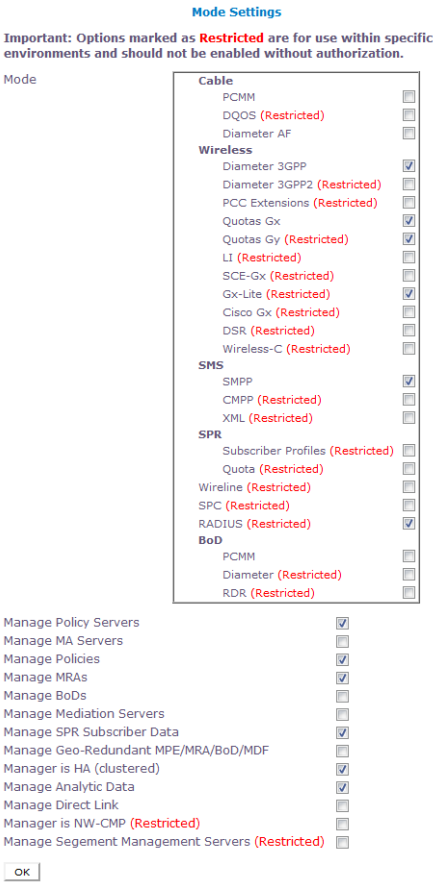
> **Note:**
>
> The procedures that follow assume that the CMP product and the LI software have been installed and are fully operational and that no one has yet logged on to the CMP system.

LI is enabled and configured using a dedicated administrative account, LIadmin. LI is only visible to, and can only be configured or modified by, the LIadmin user. LI user access cannot be added to another account.

To enable LI:

1. Open a web browser and enter the IP address or name assigned to the CMP system that contains the LI software.
2. Go to the Mode Settings page.

Figure 1-2 Mode Settings screen



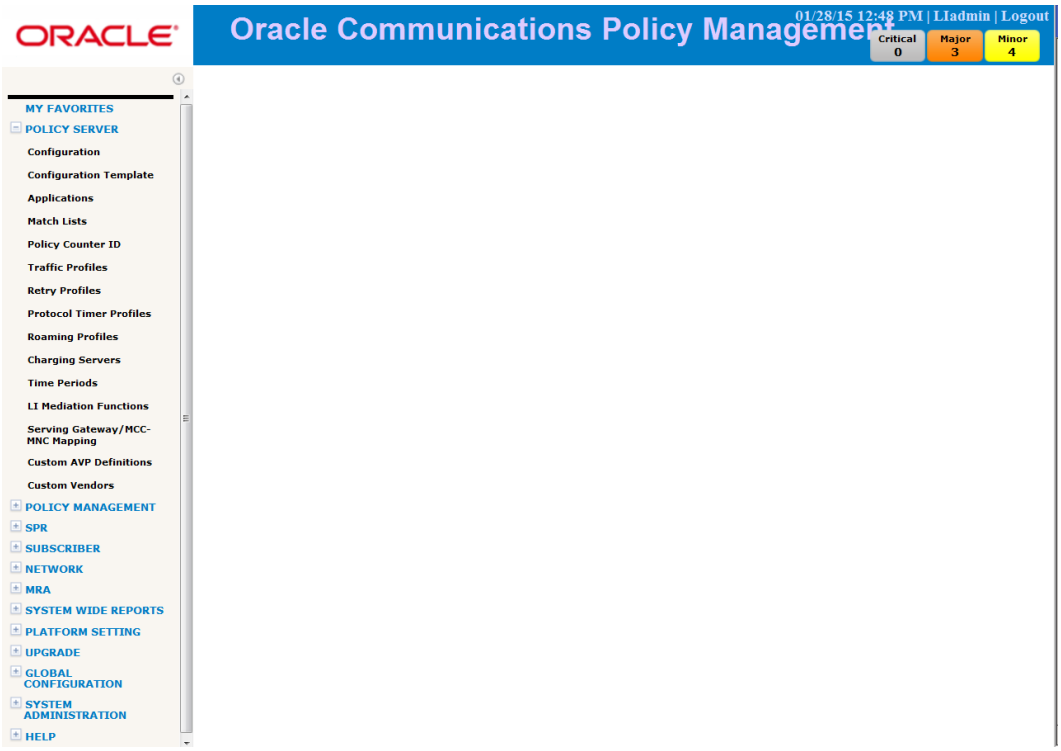
3. Under **Wireless**, select **LI** and **Diameter 3GPP** and click **OK**.

   You are logged out, and the login screen is displayed.
4. Enter **LIadmin** for the user name, **policies** for the password, and click **Login**.

   You are prompted to change the password.
5. Change the default password, confirm the password, and click **Change Password**.

   The **Policy Management** main page opens.

Figure 1-3 Policy Management main screen



Configuring Lawful Intercept

> **Note:**
>
> Configuring LI is possible in the CMP or Network Configuration Management Platform (NW-CMP) and is not enabled in the System Configuration Management Platform (S-CMP). The **Create LI-Mediation Function** option does not appear in the S-CMP, although LI that has been configured can be viewed in the S-CMP.

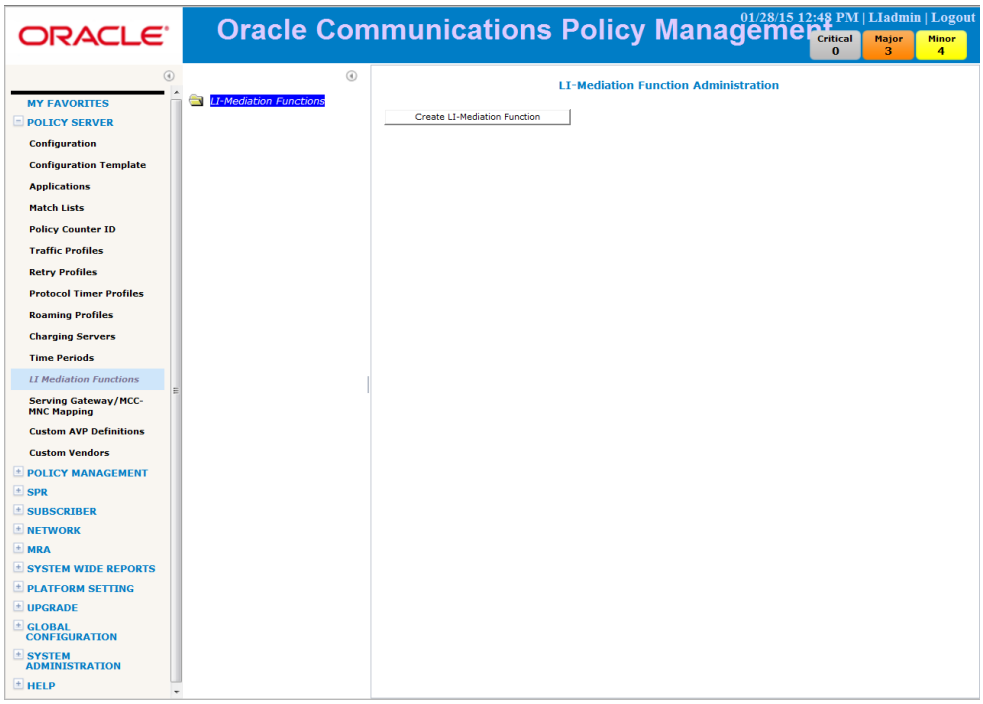
To configure LI:

1. From the **Policy Server** section of the navigation pane, select **LI-Mediation Functions**.

   The content tree displays the **LI-Mediation Functions** group.
2. From the content tree, select the **LI-Mediation Functions** group.

   The LI-Mediation Function Administration screen opens in the work area:

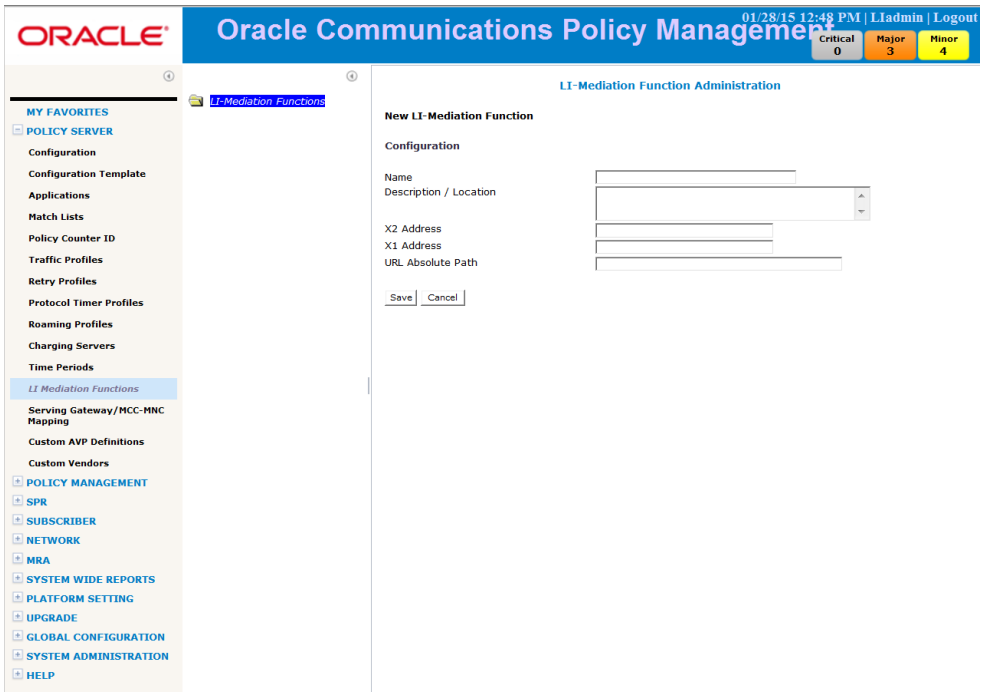
Figure 1-4 LI-Mediation Function Administration screen



3. In the work area, click **Create LI-Mediation Function**.

   The New LI-Mediation Function Administration Configuration screen opens:

Figure 1-5 New LI-Mediation Function Administration Configuration screen



> **Note:**
>
> Either IPv4 or IPv6 addresses can be used to configure the X2 interface of each MF on the LI-Mediation Function Administration screen.

> **Note:**
>
> The MPE device can support more than one MF.

4. Configure the following fields:
   a. **Name**—Name of the MF.
   b. **Description / Location** (optional)—Provides a description of the MF.
   c. **X2 Address**—IP address or FQDN of the MF that receives messages over X2 interfaces about changes in the states of provisioned targets.
   d. **X1 Address**—IP address or FQDN of the MF that sends requests over X1 interface for managing the life cycles of targets of lawful intercept.
   e. **URL Absolute Path** (optional)—Absolute URL for the MF X2 interface. This field is only required if the MF requires a specific URL path for processing X2 messages. For example, if the MF IP address is 11.*xx.xx.xx*, and the URL for processing X2 messages is https://11.*xx.xx.xx*/X2, the URL absolute path should be /X2.
5. When you finish, click **Save**.

   The MF definition is added to the CMP database.

You are now ready to associate the MF with an MPE device.

Configuring LI on an MPE Device

You must configure MPE devices before you can associate MF devices with them. For information, see *CMP Wireless User's Guide*.

To configure LI on an MPE device:

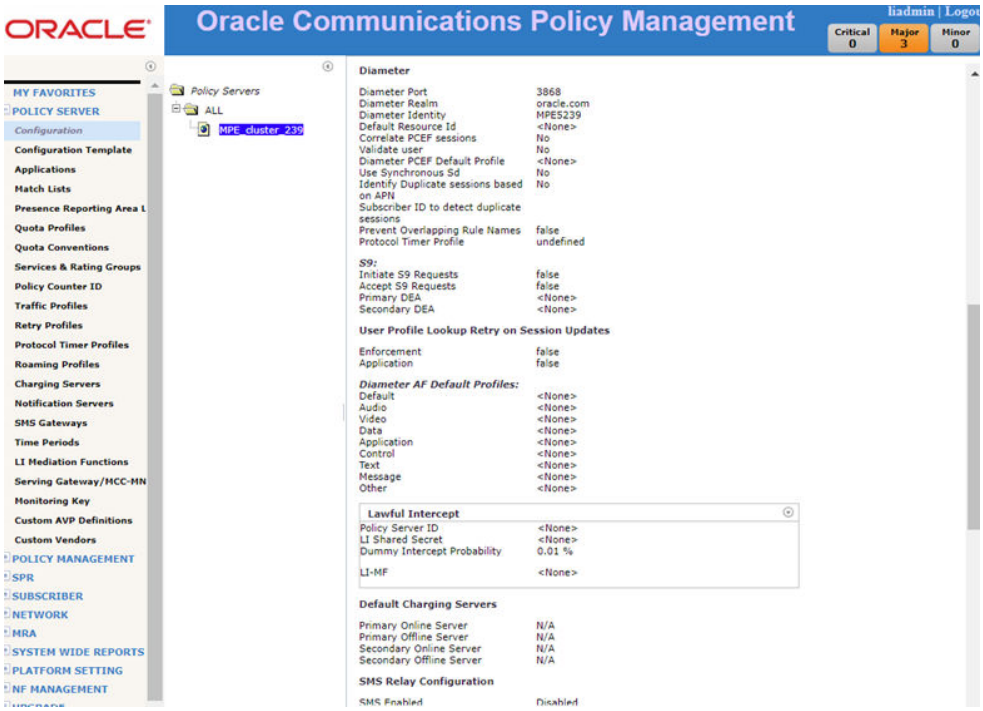
1. From the **Policy Server** section of the navigation pane, click **Configuration**.

   The content tree displays a list of policy server groups; the initial group is **All**.
2. From the content tree, select the MPE device where LI is to be configured .

   The Policy Server Administration screen opens.
3. Click the **Policy Server** tab.

   The current configuration options are displayed:

Figure 1-6 Policy Server Administration screen



4. Click **Modify**.

   The configuration fields become editable.

5. Scroll down to the Lawful Intercept section of the work area and expand it.

6. Enter the following:

   - **Policy Server ID**—Enter a unique 24-bit identifier for each PCRF cluster within a given CMP cluster. Initially input as a number less than 8388608, the MPE then internally sets the two most significant bytes to make the identifier 32 bit, resulting in a number less than 2147483648. This identifier is used to generate the appropriate 64-bit correlation identifier for each target MF.
   - **LI Shared Secret**—Enter the LI shared secret used for encrypting/decrypting LI-related AVPs over the Gx and Rx interfaces.
   - **Dummy Intercept Probability**—Enter the probability, expressed as a percentage, of injecting dummy LI AVPs into the Gx messages sent from the MPE device to the PCEF to mask real LI provisioning from users who might be monitoring traffic between the MPE device and the PCEF. The default is 0.01%.
   - **LI-MF**— Select the MF devices that the MPE device communicates with from the available list. A maximum of 10 MF devices are supported per MPE.

7. Click **Save**.

The MPE device is now configured for LI.

Configuring a Static IP Address on an MPE Device

You must configure the static IP address, which is used only by the single MPE server at the secondary site before the server can communicate with an MF device. For more information, see *CMP Wireless User's Guide*.

To configure a static IP address on an MPE device:

1. From the **Platform Setting** section of the navigation pane, click **Topology Settings**.

   The content tree displays the Topology Settings group.

2. From the content tree, click the **All Clusters** group.

   The Cluster Configuration screen opens, displaying information about clusters.

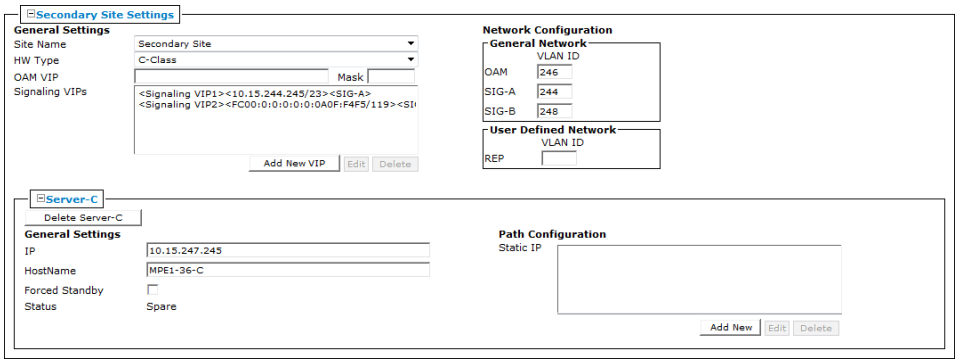
3. Click the **View** link to the right of the MPE cluster you want to modify.

   The Topology Configuration screen opens, displaying information about the cluster.

4. On the Topology Configuration screen, click **Modify Secondary Site**.

   The Secondary Site Settings section (at the bottom of the work area) become editable; for example:

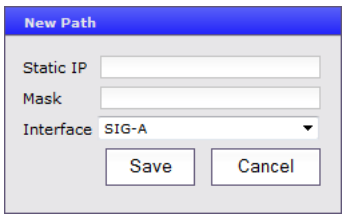
Figure 1-7 Secondary Site Settings screen



5. Scroll down to the Server-C section of the work area; in the **Path Configuration** element, click **Add New**.

   The New Path window opens:

Figure 1-8 New Path window



6. Enter the following:

- **Static IP**— The IPv4 or IPv6 address for the spare MPE device.
- **Mask** — Subnet mask, in CIDR notation: from 0 to 32 for an IPv4 address, from 0 to128 for an IPv6 address.
- **Interface** — Select the signaling interface in use from the list.

7. Click **Save**.
8. From the **Policy Server** section of the navigation pane, select **Configuration**.

   The content tree displays a list of policy server groups; the initial group is **All**.
9. From the content tree, select the same MPE device.

   The Policy Server Administration screen opens.
10. On the Policy Server Administration screen, click the **Policy Server** tab.

    The current configuration options are displayed.
11. Click **Reapply Configuration**.

    An in-progress message displays. When the operation is complete you are prompted, “The configuration was applied successfully.”

The MPE device is configured with a static IP address.