Hardware and Software
ORACLE
Engineered to Work Together

Oracle® Communications

Software Installation

Policy Management 12.6 Bare Metal Installation Guide

F45817-01

September 2021

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 (CAS) can assist you with My Oracle Support registration.

Call the CAS 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.

Oracle Communications Policy Management 12.6 Bare Metal Installation Guide
Copyright © 2017, 2021 Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services except as set forth in an applicable agreement between you and Oracle.

TABLE OF CONTENTS

1.1 Related documents 6
1.2 Acronyms 7
1.3 Terminology 8

2. INSTALLATION OVERVIEW 9
2.1 Overview of Installed Components 9
2.2 Overview of the Installation process 9

3. PLANNING YOUR INSTALLATION 11
3.1 About Planning Your Policy Management Installation 11
3.2 About Test Systems and Production Systems 11
3.3 System Deployment Planning 11
3.3.1 Networking (c-Class Hardware) 11
3.3.2 Networking (RMS Hardware) 11
3.4 About Installing and Maintaining a Secure System 12

4. SYSTEM REQUIREMENTS 13
4.1 Software Requirements 13
4.1.1 Operating Environment 13
4.1.2 Platform Management and Configuration (PMAC) 13
4.1.3 Policy Management Application 13
4.1.4 Acquiring Software 14
4.1.5 About Critical Patch Updates 16
4.1.6 Additional Software Requirements 17
4.2 Hardware Requirements 17
4.3 Acquiring Firmware 17
4.3.1 Acquiring Firmware for HP Hardware Purchased Through Oracle 17
4.3.2 Acquiring Firmware for HP Hardware Purchased Directly 18
4.4 Information Requirements 18
4.4.1 Logins/Passwords 18

5. PREPARING THE SYSTEM ENVIRONMENT 19
5.1 Preparing an HP RMS Environment 19
5.1.1 ILO Configuration Procedure 19
5.1.2 Updating DL380 Server Firmware 19
5.1.3 ILO Web GUI Settings 19
5.1.4 BIOS Configuration HP DL380 RMS Server 20

5.1.5 IPM of a HP DL380 RMS Server 20
5.1.6 Installing Policy Management Software 27
5.2 Preparing a c-Class Environment 35
5.2.1 Preparing the PM&C Management Server 35
5.2.2 HP C-7000 Enclosure Configuration 36
5.2.3 Adding the Cabinet and the Enclosure to the PM&C 37
5.2.4 Configure Blade Server iLO Password for Administrator Account 40
5.2.5 Configuring c-Class Aggregation and Enclosure Switches Using netConfig 41
5.2.6 Configuring the Application Blades 42
5.2.7 Updating Application Blade Firmware 42
5.2.8 Confirming and Updating Application Blade BIOS Settings 42
5.2.9 Loading Policy Management Software Images onto the PMAC 43
5.2.10 IPM Enclosure Blades Using the PMAC 43
5.2.11 Install Policy Management Software on Blades using PM&C 46

6. CONFIGURE POLICY APPLICATION SERVERS IN WIRELESS MODE 52
6.1 Perform Initial Server Configuration of Policy Servers—platcfg 52
6.2 Perform Initial Configuration of the Policy Servers—CMP GUI 62
6.3 CMP Site1 Cluster Configuration 67
6.4 Configuring Additional Clusters 77
6.4.1 Adding a CMP Site2 Cluster for CMP Geo-Redundancy 77
6.4.2 Setting Up a Non-CMP Cluster (MPE, MRA) 86
6.4.3 Setting Up a Geo-Redundant Site 95
6.4.4 Setting Up a Geo-Redundant Non-CMP Cluster (MPE, MRA) 99
6.5 Performing SSH Key Exchanges 112
6.6 Configure Routing on Your Servers 115
6.7 Configure Policy Components 116
6.7.1 Adding MPE and MRA to CMP Menu 116
6.7.2 Configure MPE Pool on MRA (Policy Front End) 122
6.7.3 Define and Add Network Elements 125
6.8 Load Policies and Related Policy Data 129
6.9 Add a Data Source 130
6.10 Perform Test Call 131
6.11 Pre-Production Configurations 132

7. SUPPORTING PROCEDURES 133
7.1 Accessing the iLO VGA Redirection Window 133

7.1.1 Accessing the iLO VGA Redirection Window for HP Servers 133
7.1.2 Accessing the Remote Console using the OA (c-Class) 137
7.2 Mounting Media (Image Files) 139
7.2.1 Mounting Virtual Media on HP Servers 140
7.3 Hardware Setup (Bios Configuration) 141
7.3.1 BIOS Settings for HP Gen 8 Blade 141
7.3.2 BIOS Settings for HP Gen 9 Blade and Rack Mount Servers 148
7.3.3 Using c-Class Enclosure OA to Update the BIOS Settings for the Application Blade 158
8. TROUBLESHOOTING THE INSTALLATION 161
8.1 Common Problems and Their Solutions 161
8.2 My Oracle Support 162

Preface

This guide provides instructions for installing Oracle Communications Policy Management (also referred to as Policy Management) software for Wireless on Bare Metal Hardware. Where specific procedures are described in related documents, you are referred to those documents.

1.1 Related documents

The following Tekelec Platform documents are available from the Oracle Help Center website at https://docs.oracle.com/en/industries/communications/tekelec/index.html

[1] F12269-01—HP Solutions Firmware Upgrade Pack, Software Centric Release Notes, Release 2.2.13 (see Note)
[2] E87833-01—Oracle Firmware Upgrade Pack, Release Notes, Release 3.1.8
[3] E87832-01—Oracle Firmware Upgrade Pack, Upgrade Guide, Release 3.1.8
[4] E53017-10—TPD Initial Product Manufacture, Release 6.7.2+
[5] F17461-01—PMAC 6.6 Configuration Reference Guide
[6] E93251-01—Tekelec Platform Distribution Licensing Information User Manual, Release 7.6
[7] E93258-02—Tekelec Virtualization Operating Environment (TVOE) Software Upgrade Procedure Release 3.6
[8] E93268-01—PMAC Incremental Upgrade Release 6.6

NOTE: The HP Solutions Firmware Upgrade Pack (HP FUP) is provided for HP hardware purchased through Oracle. If you need assistance, contact My Oracle Support.

The following Policy Management documents are available from the Oracle Help Center website at http://docs.oracle.com/en/industries/communications/policy-management/index.html Release 12.6

http://docs.oracle.com/cd/F45965-01/index.htm

[1] F46327-01—Release Notes
[2] F45402-01—Configuration Management Platform, Wireless User's Guide
[3] F45401-01—Platform Configuration User's Guide, Release
[4] F45503-01—Network Impact Report
[5] F45968-01—Policy Front End Wireless User's Guide
[6] F46325-01—Troubleshooting Reference
[7] F45967-01—SNMP User's Guide
[8] F46326-01—Analytics Data Stream Wireless Reference
[9] F44762-01—OSSI XML Interface Definitions Reference

The following documents are available from the Oracle Technology Network at http://www.oracle.com/technetwork/topics/security/alerts-086861.html:

- Critical patch update advisories
- Security alerts

1.2 Acronyms

Table 1. Acronyms

Term	Definition
CMP	Configuration Management Platform—component of a Policy Management system
ECO	Engineering Change Order
FUP	Firmware Upgrade Pack
iLO	Integrated Lights-Out—an HP embedded server remote management feature
ILOM	Integrated Lights Out Management. An Oracle embedded server remote management feature
IMI	Internal Management Interface
IPM	Initial Product Manufacture
MPE	Multimedia Policy Engine—component of a Policy Management System
MRA	Multiprotocol Routing Agent—also referred to as the Policy Front End (PFE)—component of a Policy Management System
NW-CMP	Network-Level CMP in a Multi-Level OAM Policy Deployment
OA	HP Onboard Administrator
OAM	The Operation, Administration, and Management network (The Platform documentation refers to this as the XMI network.)
UDR	User Data Repository
PCRF	Policy Charging and Rules Function
PFE	Policy Front End (also referred to as Multiprotocol Routing Agent)—component of a Policy Management System
PM&C	Platform Management and Configuration
REP	A replication network, to carry database replication traffic between servers in a cluster
RMS	Rack-Mounted Server
S-CMP	Site-Level CMP in a Multi-Level OAM Policy Deployment
SIG-A	The Signaling A network (The Platform documentation refers to this as the XSI-1 network)
SIG-B	The Signaling B network
SIG-C	The Signaling C network
SSH	Secure Shell
TPD	Tekelec Platform Distribution
TVOE	Tekelec Virtualization Operating Environment.
XMI	External Management Interface—see OAM
XSI-1	External Signaling Interface 1—see SIG-A

1.3 Terminology

Table 2. Terminology

Term	Description
Configuration Management Platform (CMP)	(CMP) A centralized management interface to create policies, maintain policy libraries, configure, provision, and manage multiple distributed MPE policy server devices, and deploy policy rules to MPE devices. The CMP has a web-based interface.
Multimedia Policy Engine (MPE)	A high-performance, high-availability platform for operators to deliver and manage differentiated services over high-speed data networks. The MPE includes a protocol-independent policy rules engine that provides authorization for services based on policy conditions such as subscriber information, application information, time of day, and edge resource utilization
Policy Front End (PFE) Previously known as Multi-Protocol Routing Agent (MRA)	Scales the Policy Management infrastructure by distributing the PCRF load across multiple Policy Server (MPE) devices
TPD	Oracle Communications: Tekelec Platform Distribution. A standard Linux-based operating system packaged and distributed by Oracle. TPD provides value-added features for managing installations and upgrades, diagnostics, integration of 3rd party software (open and closed source), build tools, and server management tools.
TVOE	A TPD-based virtualization host. TVOE allows for virtualization of servers so that multiple applications can reside on one physical machine while retaining dedicated resources. This means software solutions that include multiple applications and require several physical machines are installed on very few (possibly one) TVOE Hosts.
PMAC	Provides hardware and platform management capabilities at the site level for Tekelec platforms. The PM&C application manages and monitors the platform and installs the TPD operating system from a single interface
Perform initial configuration	The perform initial configuration is added to the policy server using the platcfg utility that brings the network interface for the server online and allows management and configuration from the CMP
Platcfg	The Oracle platform configuration utility used in TPD to configure IP and host values for a server.
Primary Site (Site1)	A site where the MPE, MRA primary cluster exists with co-located active and standby servers
Secondary Site (Site2	A site where the MPE, MRA secondary cluster exists with co-located active and standby servers for disaster recovery
HP c-Class	HP blade server system
Data Source	Interface that provides data to components

2. INSTALLATION OVERVIEW

This document describes how to install the 12.6 Policy Management applications on supported hardware platforms.

At the completion of installation, assuming that networking is correctly configured, you can do the following:

- Log in to the management interfaces for the Policy Management system from your network
- Access the management interfaces for the Policy Management system from a remote location (specifically, an Oracle support office)
- Verify that there are not any alarms for the Policy Management system
- Make a test call through the Policy Management system

2.1 Overview of Installed Components

This document describes methods utilized and procedures performed to configure hardware used with Policy Management software and to install Policy Management components on that hardware.

The Policy Management components are:

- Multimedia Policy Engine (MPE)—a required element that provides policy control decisions and charging control
- Policy Front End, also called the Multimedia Routing Agent (MRA)—an optional element that maintains bindings that link subscribers to MPE devices
- Configuration Management Platform (CMP)—a required element that provides element management functions

2.2 Overview of the Installation process

There are two starting points for installation:

- Equipment ordered from, pre-configured from, and installed by Oracle
- Equipment ordered and installed by the customer

In the first case, there is a known pre-configuration of the equipment that can reduce the installation time.

In the second case, you verify the hardware installation and cabling before starting. Also, additional steps are required for initial configuration of systems. In this case, it is possible that firmware revisions are newer than the qualified baseline. This document may not be enough to deal with all issues for your installation. At a minimum, the hardware configuration and cabling Technical References for the installation are needed. This document assumes that all hardware meets Oracle specifications.

You can configure the Policy Management software to operate in an environment of multiple internal and external networks, including the following:

- For HP hardware, the integrated Lights Out (iLO) feature, an independent subsystem inside an HP server which is used for out-of-band remote access
- For all configurations (c-Class and RMS), an administrative (OAM) network, to carry internal management traffic between Policy Management servers

- A signaling (SIG-A) network, to carry signaling traffic between Policy Management servers and an external network (a second signaling network, SIG-B or SIG-C, is also supported)
- A replication (REP) network, to carry database replication traffic between servers in a cluster

These networks must be cabled in a specific topology of internal cabinet cabling, switches, and external connections supported by the platform software. Different hardware requires different topologies. This document assumes that the specific topology appropriate for your hardware is installed and verified correct.

Installing Policy Management software involves a number of steps that you or others must complete in the following order:

1. Planning the installation. See Section 3, **Planning Your Installation.**
2. Reviewing and meeting system requirements. See Section 4, **System Requirements**.
3. Preparing the hardware and operating-system environment (including management servers if required). See Section 5, **Preparing the System Environment**.
4. Installing the Policy Management software. See Section 6, **Configure Policy Application Servers in Wireless Mode**

3. PLANNING YOUR INSTALLATION

This section provides a planning overview of the Installation activities.

3.1 About Planning Your Policy Management Installation

To install and use Policy Management software, you must plan your system by performing the following tasks:

- Determine the services and the mode you want to provide; for example, Wireless or Wireless-C (see note)
- Determine the names and addresses of network elements used in your network with which Policy Management interacts.
- Determine the names and addresses of external data sources used in your network with which the Policy Management software interacts; for example, subscriber profile repositories, on-line charging servers, and offline charging servers.
- Choose the Policy Management components you want to install.
- Install Policy Management software and any optional components.
- Configure each Policy Management component.

NOTE: Wireless-C supports a wireless system supporting SMS Notification Statistics and SCTP counters.

Oracle recommends contacting Oracle Consulting regarding your plans.

3.2 About Test Systems and Production Systems

Some prefer to test the Policy Management software in a separate environment to verify its functions, behavior, and performance before introducing it to their networks. Oracle recommends that a lab solution be installed that is a replica of the product environment. A lab solution is used to test and verify use cases before being implemented in a production environment, as well as test configurations or features ahead of implementation.

A test system focuses on only one integration point at one time; for example, throughput or connectivity. In some cases, a test system uses a traffic simulator instead of the actual subscriber data during testing.

For detailed information about Policy Management components, see the Configuration Management Platform Wireless User's Guide

See Section 4, **System Requirements**, for information about required hardware and software.

3.3 System Deployment Planning

The decision of what interconnect method to use depends on the server hardware and the implementation scale, and you decide before placing an equipment order.

3.3.1 Networking (c-Class Hardware)

HP c-Class systems are connected to your network using Ethernet uplinks directly from enclosure switches. The HP Proliant 6120XG or 6125XLG switches are supported with an uplink capacity of 10 GB or higher.

3.3.2 Networking (RMS Hardware)

HP RMS is connected individually to your network using IP networking switches. This includes installed interfaces NIC1, NIC2, and iLO.

3.4 About Installing and Maintaining a Secure System

The following principles are fundamental for establishing and maintaining a secure system:

- Change the factory default passwords immediately, but keep a secure record of your changes. This includes the root user passwords to servers as well as the passwords to the administrative accounts for HP OA, Platform Management and Configuration (PMAC), and the Policy Management CMP system.
- Keep software up-to-date. You must keep the product and the installed software dependencies up-to-date. This includes the latest product release and any patches that apply to it.
- Keep up-to-date on security information. Oracle regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible. See related *Oracle patch and security bulletins* for more information. See also Section 4.1.5, **About Critical Patch Updates**.

4. SYSTEM REQUIREMENTS

This chapter describes the hardware, firmware, operating system, and software requirements for installing software.

4.1 Software Requirements

The Policy Management software runs as a set of applications under an operating environment on server hardware (which can have its own management software). Later releases of software may be posted as per the latest Oracle engineering change order (ECO).

4.1.1 Operating Environment

Tekelec Platform (TPD)—ISO or USB image file:

- TPD.install-7.8.0.0.0_89.8.1-OracleLinux6.10-x86_64.iso
- TPD.install-7.8.0.0.0_89.8.1-OracleLinux6.10-x86_64.usb

Tekelec Virtual Operating Environment (TVOE)—ISO or USB image file:

- TVOE-3.8.0.0.0_89.5.0-x86_64.iso
- TVOE-3.8.0.0.0_89.5.0-x86_64.usb

NOTE: TVOE is used for the PMAC (Platform Management and Configuration) server

4.1.2 Platform Management and Configuration (PMAC)

For HP c-Class hardware, the Platform Management and Configuration (PMAC) server is required. PMAC is an Oracle application that provides tools to manage multiple enclosures and server software, as well as networking equipment (enclosure switches).

- PMAC-6.6.1.0.0-66.9.0-x86_64.iso

4.1.3 Policy Management Application

The Policy Management software consists of the following products:

- CMP: cmp-12.6.0.0.0_x.x.x-x86_64.iso
- MPE: mpe-12.6.0.0.0_ x.x.x-x86_64.iso
- MRA (PFE): mra-12.6.0.0.0_ x.x.x-x86_64.iso

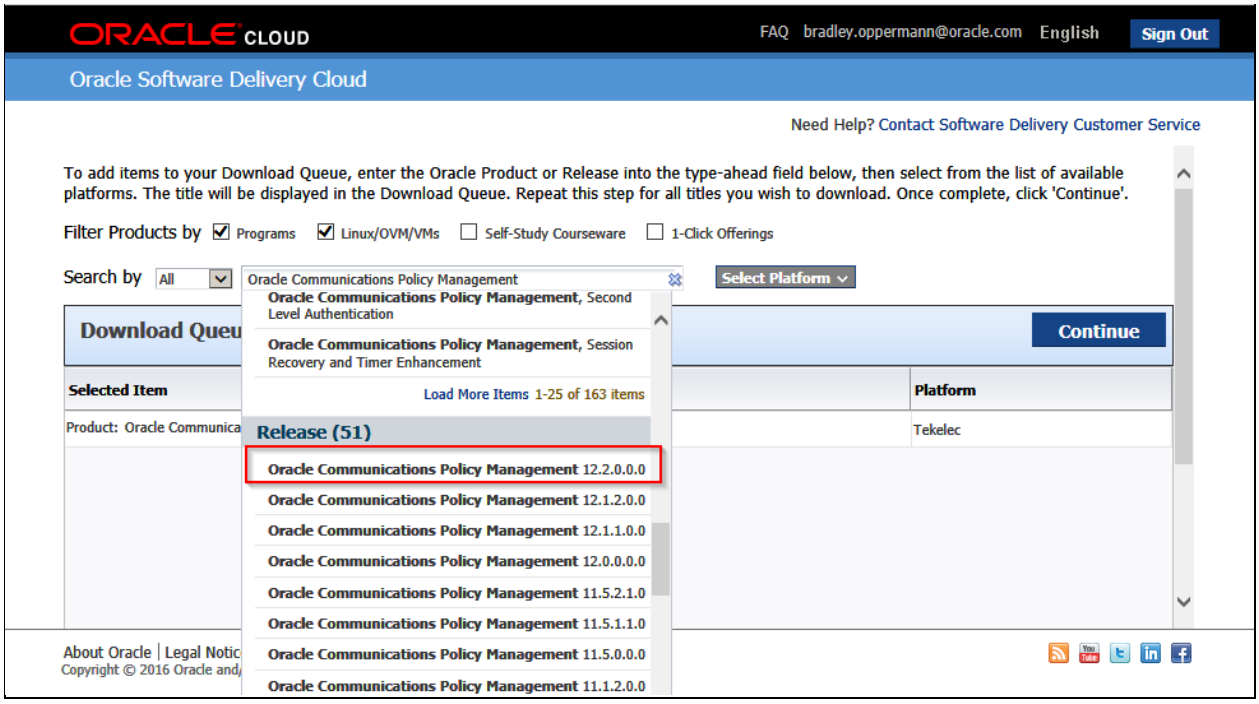
4.1.4 Acquiring Software

If you have a commercial license, you can download your software from the Oracle Software Delivery Cloud, which is specifically designed for software fulfillment.

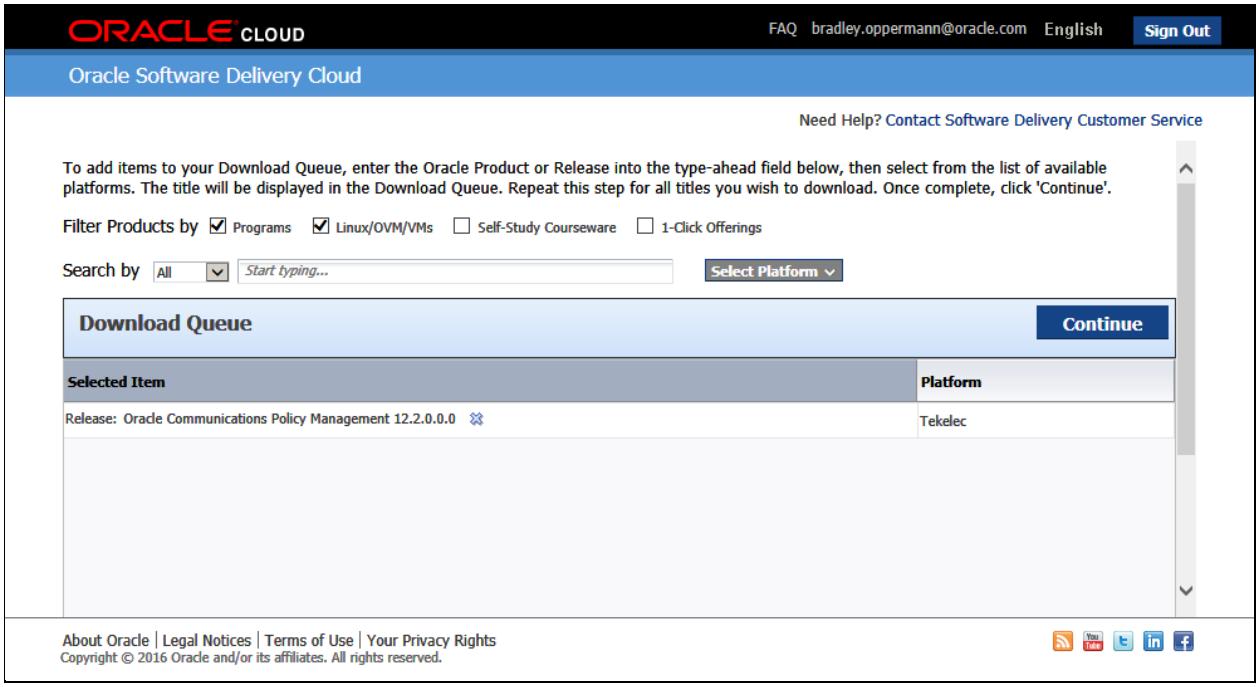
For patches, see My Oracle Support.

NOTE: The following is an example of downloading the Policy Management software.

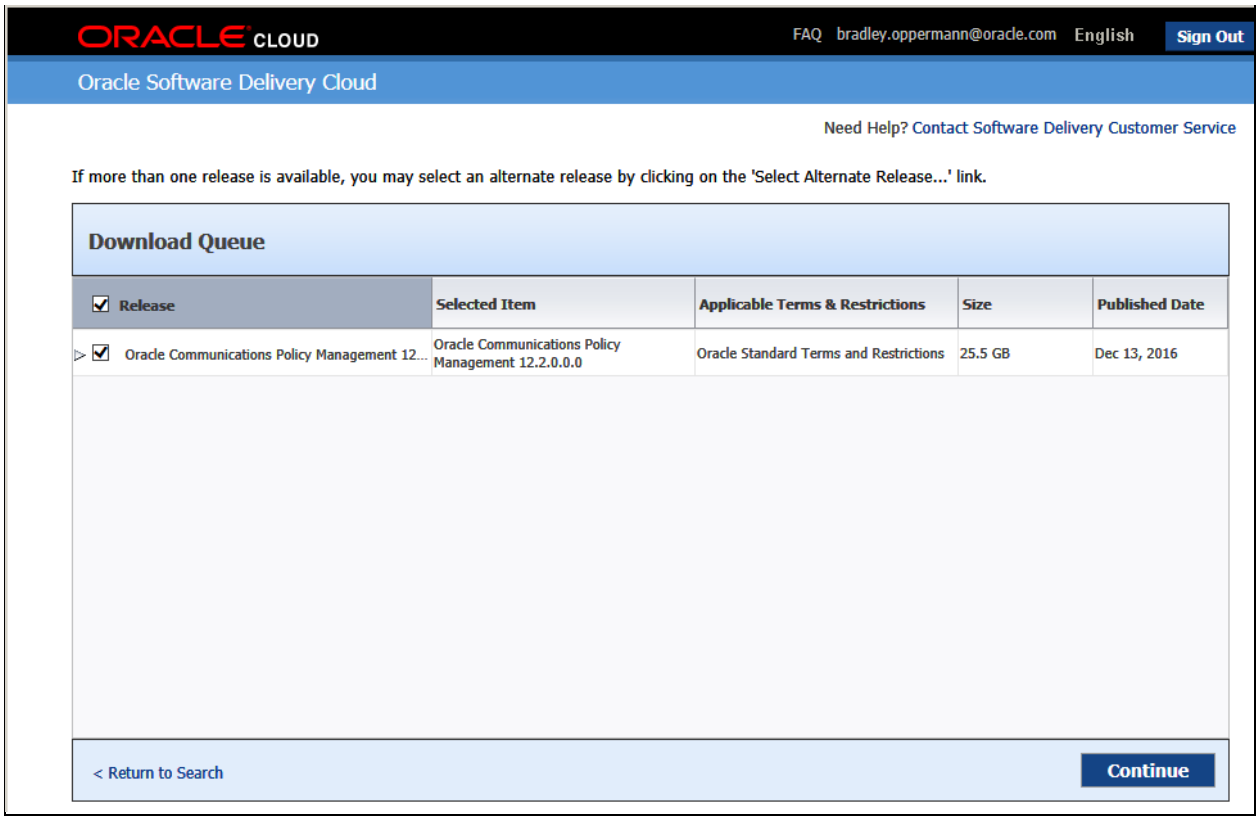
5. Set the Search by field to **Oracle Communications Policy Management** select **12.6.0.0.0**



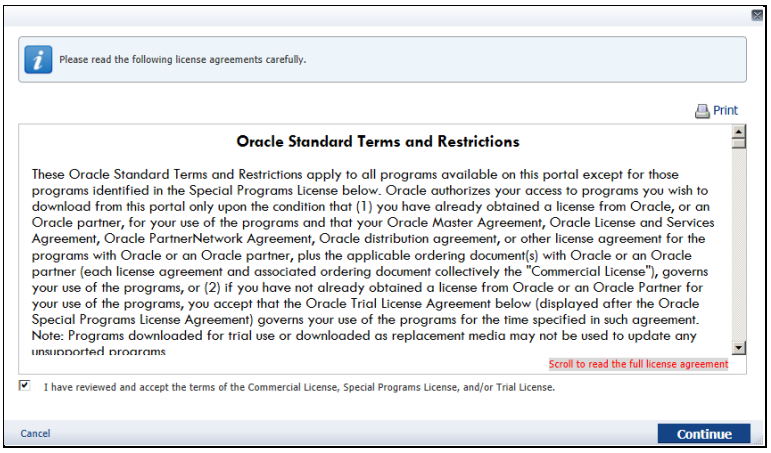
6. Click **Continue**.



7. Select the **Oracle Communications Policy Management 12.6.0.0.0** and click **Continue**.

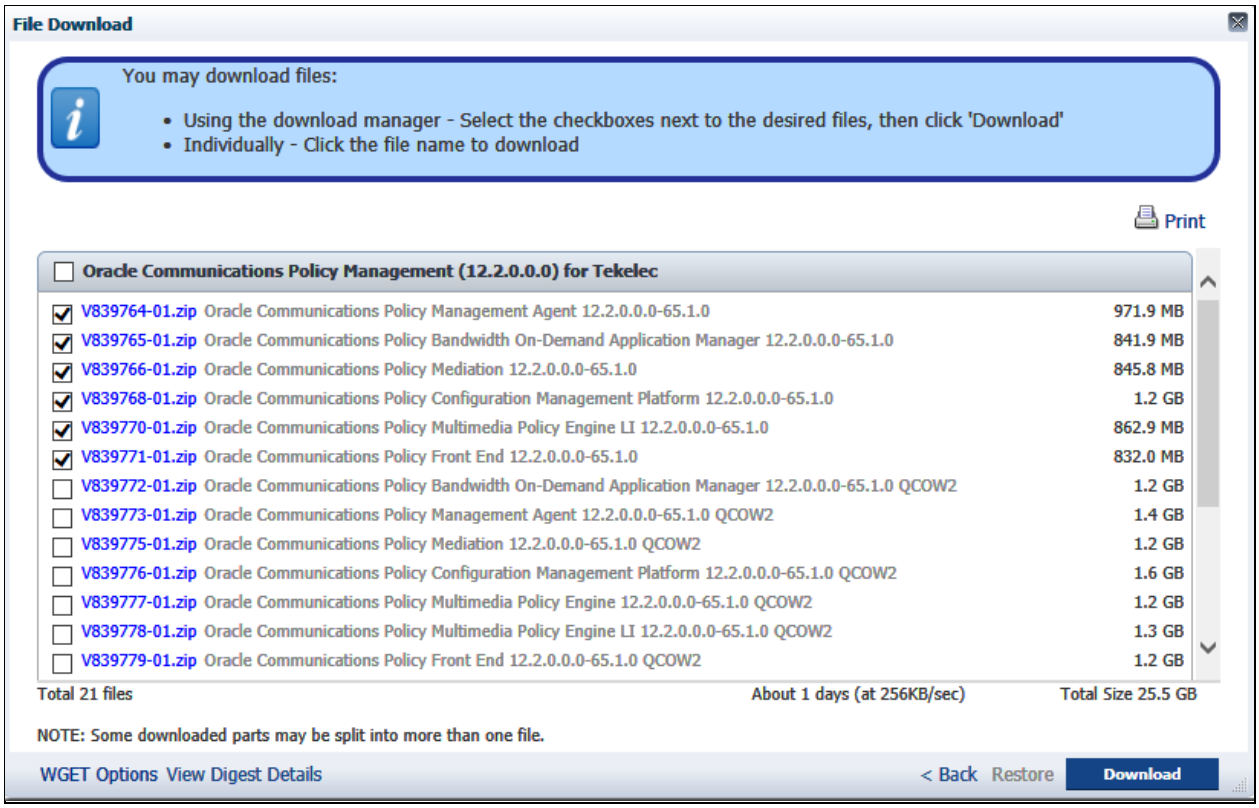


8. Confirm the License Agreement.



9. Select the required Software files in their .zip compressed format

   NOTE: Click **View Digest Details** in the lower left corner to see MD5sum and SHA-1 references



4.1.5 About Critical Patch Updates

Install all Oracle 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 **Oracle patch and security bulletins**.

4.1.6 Additional Software Requirements

For an HP c-Class hardware installation, the PMAC netConfig tool uses network configuration files to configure enclosure and aggregation switches. The Policy Management ISO image files include switch configuration template files. Edit these template files to make them specific for your installation and place them on the PMAC server after it is installed.

NOTE: These files may change from release to release.

4.2 Hardware Requirements

The following servers are supported:

- HP DL360/DL380 (G8/G9 RMS)
- HP c-Class server (BL460 G8/G9 Blade Server)

NOTE: A c-Class installation requires one dedicated management server running PMAC software for each site. For an RMS installation PM&C is optional.

Also have on hand:

- HP or Oracle firmware ISO or USB image files
- If you are installing USB files, USB flash drives (5GB or larger) for creating bootable USB media
- Laptop
- Console cable (to connect the laptop to switches in a c-Class environment)
- Category 5 Ethernet cable (to connect the laptop to the local switch, for serial over LAN console connections, and to access system GUIs)
- HP Blade Monitor/Keyboard/USB front handle cable (optional, for console and USB access directly to servers in a c-Class environment)

4.3 Acquiring Firmware

Several procedures in this document pertain to upgrading firmware on various servers and hardware devices. This process varies depending on from whom you purchased your hardware.

The following Policy Management 12.6 servers and devices may require firmware updates:

- HP DL360/DL380 RMS server
- HP c7000 Blade System Enclosure Components:
    - Onboard Administrator
    - HP 6125XLG blade switches
    - HP BL480c/BL460c blade servers

You must complete all firmware updates before putting the Policy Management system into service.

4.3.1 Acquiring Firmware for HP Hardware Purchased Through Oracle

The *HP Solutions Firmware Upgrade Pack, Software Centric Release Notes, Release 2.2.12* are provided for HP hardware purchased through Oracle. Each describes functionalities, fixed bugs, known bugs, and any additional installation and configuration instructions required, relative to this release.

For Policy Management 12.6, the minimum supported firmware is 2.2.12. Contact My Oracle Support for assistance if needed.

Firmware is available as:

- ISO or USB image files of HP Smart Update firmware:
  - FW2_SPP-2.2.12.0.0_x.x.x.iso
  - FW2_SPP-2.2.12.0.0_x.x.x.usb
- ISO image files of HP Misc firmware ISO:
  - FW2_MISC-2.2.12.0.0_x.x.x.iso

NOTE: Later releases may be posted as per the latest Oracle ECO.

4.3.2 Acquiring Firmware for HP Hardware Purchased Directly

If you have purchased your own HP hardware, Oracle does not directly provide you with firmware upgrade media. See HP Solutions Firmware Upgrade Pack, Software Centric Release Notes, Release 2.2.12

4.4 Information Requirements

You must determine and record the IP addresses that you need to configure the equipment. Record switch ports, cable drops, and IP network addresses for your network.

Be certain of the equipment location and the system identification method. Oracle recommends that you prepare, or have at hand, enclosure layout diagrams.

4.4.1 Logins/Passwords

The standard configuration steps configure standard passwords for root, admusr, configUser, pmacadmin, HP OA, and other standard accounts referenced in this procedure. These passwords are not included in this document. Contact Oracle Support for this information.

Initial login to an HP server/module is configured by HP at the factory. However, if you purchased your equipment from Oracle, then the HP passwords are replaced with the standard passwords.

When first logging in to the Configuration Management Platform (CMP), the management interface for the Policy Management product, three login IDs are available by default:

- admin

  This is the default administrator user with all privileges.
- operator

  This is the default operator user with all privileges except user administration.
- viewer

  This is the default read-only user.

IMPORTANT: The initial password for all three of these login IDs is policies. You are required to change the password the first time each login ID is used.

5. PREPARING THE SYSTEM ENVIRONMENT

To install the software, you first need to prepare the system environment with the following:

- Supported hardware servers (installed or racked), powered and cabled together
  - Each server includes the required firmware revision
  - Each server includes the required operating system software at the required revision level
- Supported interconnection switches, either enclosure switches or aggregation (network) switches

To prepare and configure servers, you need their login information.

5.1 Preparing an HP RMS Environment

The procedures listed in this section are specific to HP DL380 rack-mount servers.

5.1.1 ILO Configuration Procedure

You can configure the HP Integrated Lights-Out (iLO) remote management feature from the Console Boot menu. You can also configure iLO from the iLO GUI.

Prerequisites:

To complete this procedure, you need the following information and material:

- Static IP address, netmask, and default gateway of the server
- The current date and time
- The passwords you intend to define for the default Administrator account and the root user (root_password)
- Local console access (monitor/keyboard) or a laptop connected to the serial console for the server

The ILO configuration procedure is described in **TPD Initial Product Manufacture, Software Installation Procedure**. (Appendix F)

5.1.2 Updating DL380 Server Firmware

Each server must have the correct release of firmware.

The procedure for updating Oracle server firmware is described in the HP Solutions Firmware Upgrade Pack, Software Centric Release Notes, Release 2.2.12

5.1.3 ILO Web GUI Settings

After you have performed the ILO configuration procedure, ILO is accessible through its web GUI interface. Change the default password for the root account.

To complete this procedure, you need to record the password for the root account (root_password).

To change the password, while in the ILO web interface:

1. Navigate to **ILOM Administration → User Management → User Accounts**.
2. Click **Edit.**
3. Change the root account password.

4. Click **Save**.

The procedure to update ILOM web GUI settings is described in **TPD Initial Product Manufacture, Software Installation Procedure**. (Appendix F)

5.1.4 BIOS Configuration HP DL380 RMS Server

The procedure for BIOS configuration are located in section *7.3.1:BIOS Settings for HP Gen 8 Blade and Rackmount Servers* or *7.3.2:BIOS Settings for HP Gen 9 Blade and Rackmount Servers* of this document. BIOS configurations are also referenced in **TPD Initial Product Manufacture, Software Installation Procedure**. (Appendix E)

After completing ILOM and BIOS configuration the HP DL380 RMS server is ready to IPM

5.1.5 IPM of a HP DL380 RMS Server

Every HP DL380 RMS server must go through an initial product manufacturing (IPM) procedure to install software on it.

Prerequisites:

To complete this procedure, you need the following materials and to perform these installation steps:

- TPD ISO image file (Section 4.1 Software Requirements)

Additional information regarding the IPM install procedure is described in the **TPD Initial Product Manufacture, Software Installation Procedure** (Section 3.3)

This procedure installs system OS (IPM) of the server

Needed material:

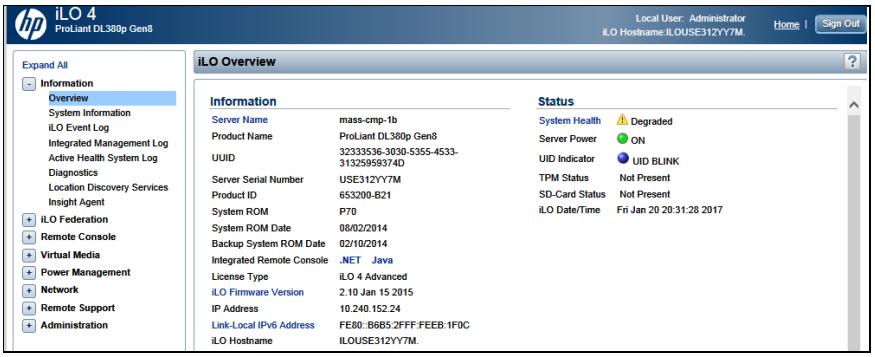
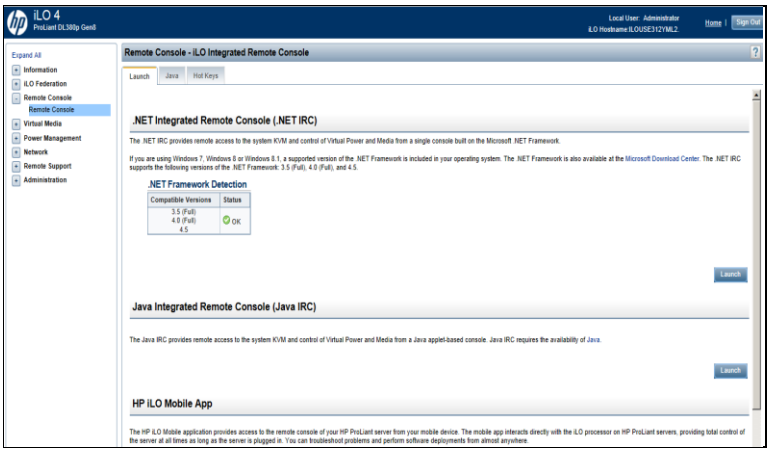
- TPD ISO image file used for virtual mount accessible on laptop
- USB device prepared with bootable version of TPD image

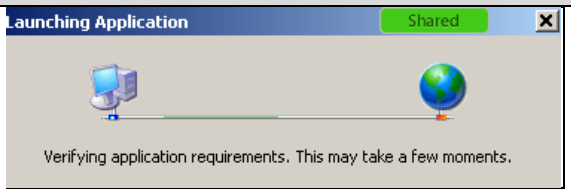
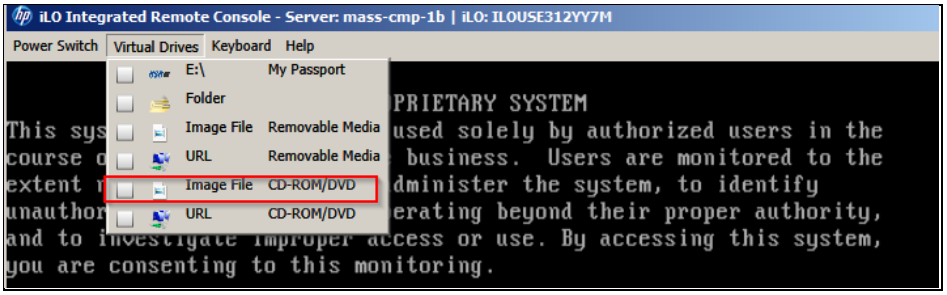
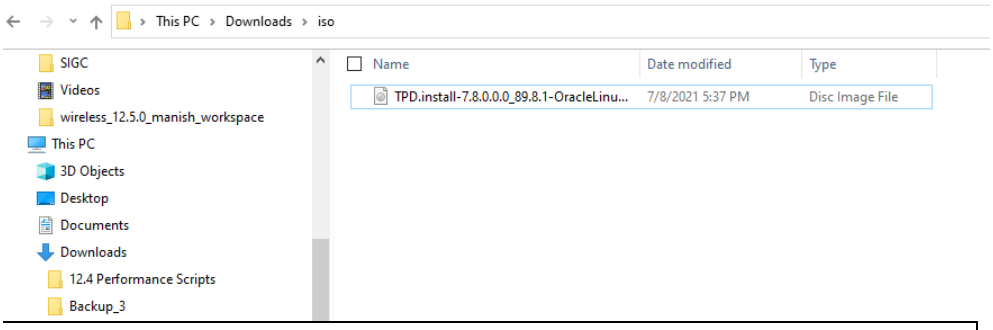
Check off (√) each step as it is completed. Check boxes are provided next to each step number.

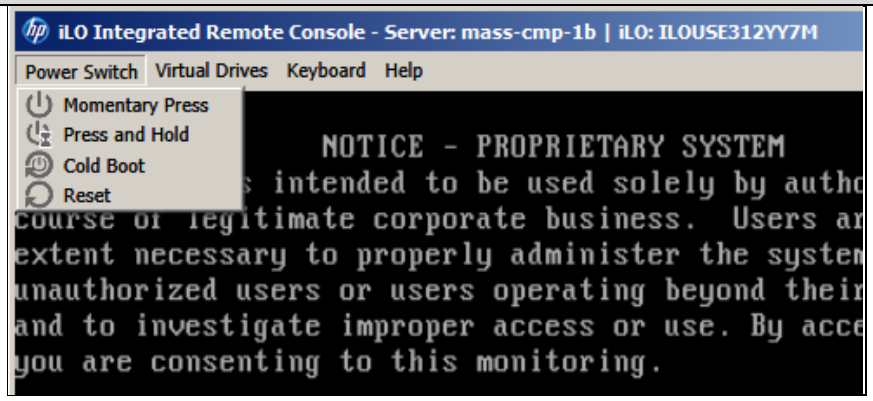
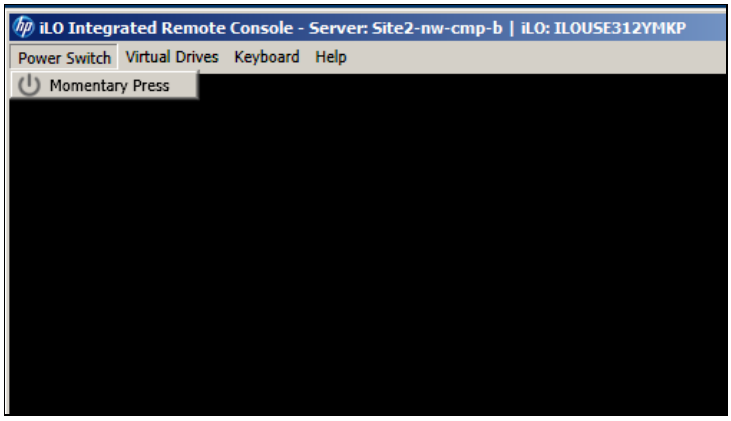
If this procedure fails, contact Oracle Technical Services and ask for assistance.

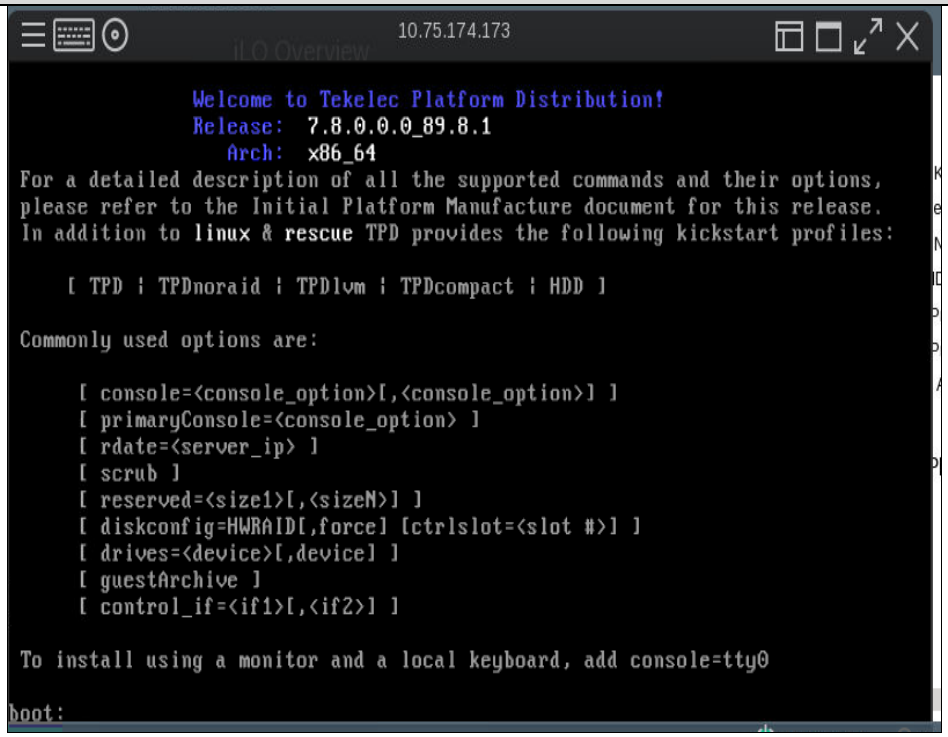
5.2.5: IPM of a HP DL380 RMS Server

Step	Procedure	Details
1. ☐	Insert Bootable USB Media/mount TPD ISO	Create a bootable USB drive with the TPD ISO image file. Use the method provided in the `README.txt` file that is included with the downloaded Policy Software or other suitable method for creating a bootable USB device. There are several readily available utilities to achieve this. Then insert the USB drive locally into the server and reboot the server to the bootable USB device. Then proceed to Step 3 of this procedure if using this method If local access to the server is not available and network access to the iLO of the server is enabled you can use the remote console capability of the HP iLO as per the following procedure See Section 7.1.2: Accessing the Remote Console using the OA (c-Class) If you are using the iLO remote console and have the TPD software as an ISO image file, do the following to restart the server to the ISO image file:

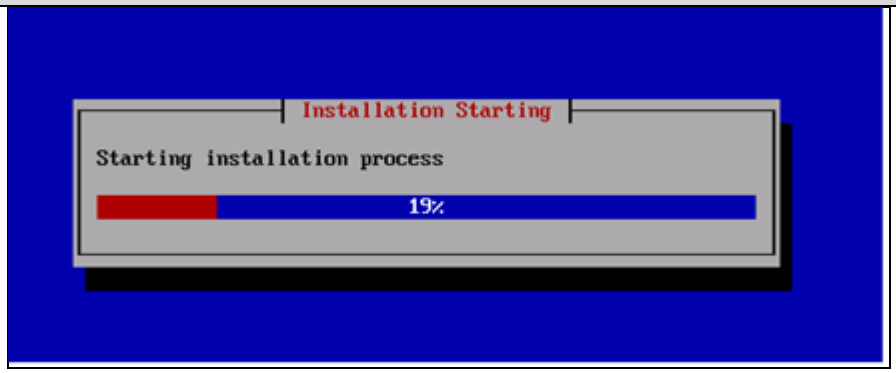
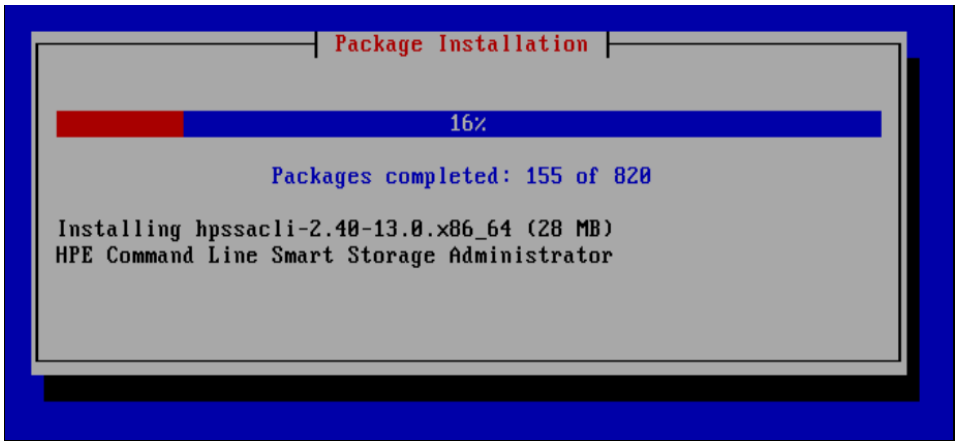
Step	Procedure	Details
		1. Open a browser, enter the URL of the iLO system (management_server_iLO_ip), and log in. For example:  2. On the home page, select **Remote Console → Remote Console**. The Remote Console page opens. For example:  **NOTE:** When launching a remote console, the .NET application is compatible with a Windows browser; Java is compatible with both Windows and Firefox browsers. 3. In the Java Integrated Remote Console section, click Launch. A security warning window opens, prompting for confirmation that you want to run the application. For example:

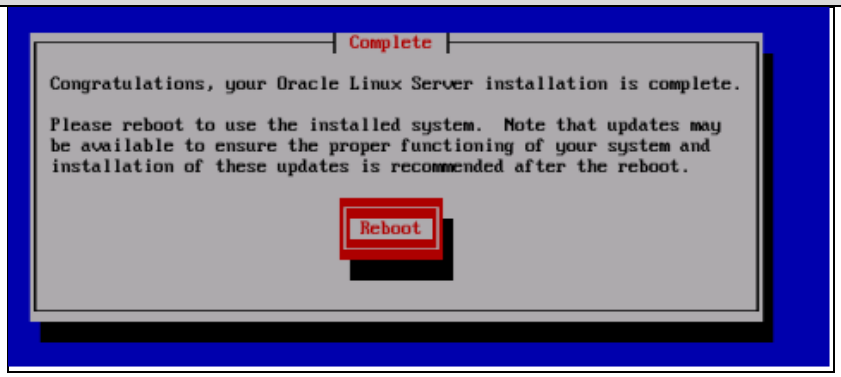
Step	Procedure	Details
		 4. Click **Run**. The Remote Console window opens. **5.** Select **Virtual Drives → Image File CD-ROM/DVD.** 6. Browse to the ISO image file location, and click **Open**. The ISO image file is mounted.  7. Select Image file CD-ROM/DVD and browse to the TPD ISO location then click **Open**:  8. Select **Power Switch → Momentary Press**. The server powers down.

Step	Procedure	Details
		 9. When the Power Switch options display the Momentary Press option, Click Momentary Press again.  10. The server starts and displays a screen similar to the following when the boot process is complete.

Step	Procedure	Details
		

2. ☐	**Console:** Enter TPD boot: command with correct options
	
	TPD install takes approximately 20 to 40 minutes to complete
		Enter the following command at the boot prompt to initiate the initial product manufacture (IPM) process.
		
		`TPDnoraid console=tty0 diskconfig=HWRAID,force`
		
		NOTE: If a direct connection to the serial console is being used for this step instead of the remote iLO console it is not necessary to include `console=tty0`
		
		NOTE: If a non Policy Management application was installed on the server, you may have to clean up logical disc partitions created by the application. Depending on the disc partitioning, this may add up to four hours to the installation process. Refer to **TPD Initial Product Manufacture, Software Installation Procedure** (Section 3.4)
		
		The TPD installation takes approximately 20 to 40 minutes to complete, starting with checks then installation starts:
		
		`boot: TPDnoraid diskconfig=HWRAID,force console=tty0`
		`Loading vmlinuz.....`
		`Loading initrd.img.....`

Step	Procedure	Details
		 Then you can able to monitor the packages installation progress:  Then post installation scripts kick off: After the IPM process is complete, you are prompted to press **Enter** to reboot the server. At this point the media used to install the OS must be removed or unmounted before selecting the Reboot option. Otherwise the server boots to the bootable media.

Step	Procedure	Details
		 When you see the Complete window, the IPM process is complete.
3. ☐	Remove or unmount the installation media.	• If installation is performed remotely unsing the remote console for iLO, unmount the image using the virtual drives menu (uncheck the image file option) then press **Enter** to reboot the server. • If a bootable USB device was used, remove the USB device. ***IMPORTANT: If you reboot the server without removing the installation media the server boot to the bootable media. If this happens, wait until you see the Complete window, remove the bootable image, and reboot again.***
4. ☐	**Console:** Press Enter to reboot	Ensure that the console window is selected. Press **Enter**. The server restarts and displays the login prompt
5. ☐	**Console:** Login prompt	After the server reboots, the login prompt displays. If the login prompt is not displayed after waiting 15 minutes, contact Oracle Customer Support for assistance.

Step	Procedure	Details

6. ☐	**Console:** Run syscheck	Log in as the root user and enter the following command to check the major components of the system:
		`# syscheck`
		The utility displays OK for each component that passes, or a descriptive error of the problem if a component fails. The following example shows a successful run where all subsystems pass, indicating that the post-installation process is complete:
		`[root@hostname483a475913f7 ~]# syscheck`
		`Running modules in class disk...`
		`OK`
		`Running modules in class hardware...`
		`OK`
		`Running modules in class net...`
		`OK`
		`Running modules in class proc...`
		`OK`
		`Running modules in class system...`
		`OK`
		`Running modules in class upgrade...`
		`OK`
		`LOG LOCATION: /var/TKLC/log/syscheck/fail_log`
		`[root@hostname483a475913f7 ~]#`
		If any of the modules return an error, do not continue; contact My Oracle Support and report the error condition.

7. ☐	**Console:** Verify Install success	Verify that IPM completed successfully using the following commands:
		`$ sudo verifyIPM` (use `-force` if needed)
		`$ sudo echo $?` (returns 0 errors)
		`$ sudo getPlatRev` (returns the current TPD version installed)
		The following example shows a successful installation:
		`[admusr@hostname6eb112f412bd ~]$ sudo verifyIPM`
		`Warnings were found in one of the /var/TKLC/log/ipm/boot.log* files.`
		`==== OUTPUT ====`
		`/var/TKLC/log/ipm/boot.log:Warning: There might not be enough space to save a vm core.`
		`== END OUTPUT ==`
		`Please examine log files for more details.`
		`[admusr@hostname6eb112f412bd ~]$ sudo echo $?`
		`0`
		`[admusr@hostname6eb112f412bd ~]$ sudo getPlatRev`
		`7.8.0.0.0-89.8.1`
		`[admusr@hostname6eb112f412bd ~]$`
		NOTE: If you see any errors, contact My Oracle Support.
		Repeat this procedure for every server.

—End of Procedure—		

5.1.6 Installing Policy Management Software

This procedure installs the Policy Management Software.

Prerequisites:

Before beginning this procedure, you must have the following material and information:

- The appropriate release and application packages of the Policy Management software, either on physical media to mount directly on the server or available as an ISO image file to mount virtually.
- Access to the server, either directly or through the ILO remote console.
- If you are using the ILO remote console, you need the IP address of the ILO system and the login information.

NOTE: Two methods for installing the Policy Application are listed.

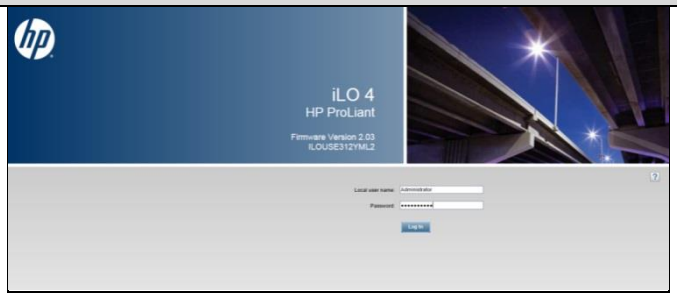
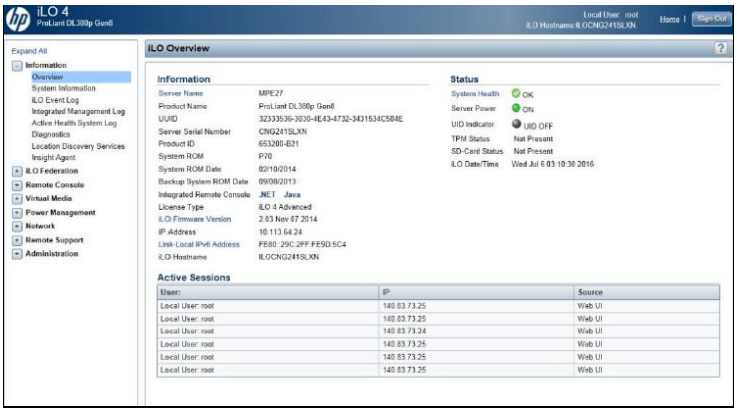
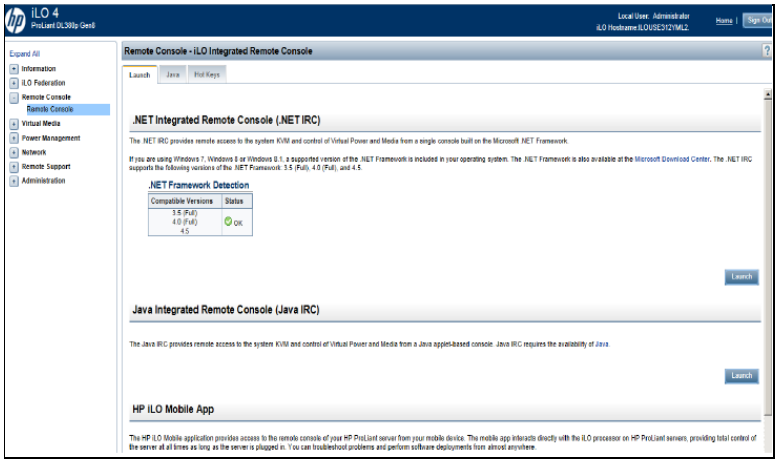
1. Use a USB drive inserted locally into the server. This is the preferred method.
2. Use the virtual mount capability of the iLO remote console over a network. This method is dependent on having a good network connection from the workstation where the ISO is located to the target server iLO. The browser used to attach the ISO and launch the server iLO remote console must be co-located with the ISO file repository. Additionally any method that places the Policy Application ISO image file in the `/var/TKLC/upgrade` directory of the target server is acceptable.

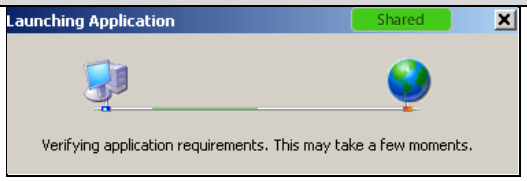
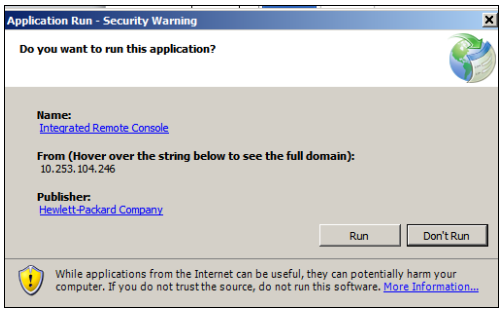
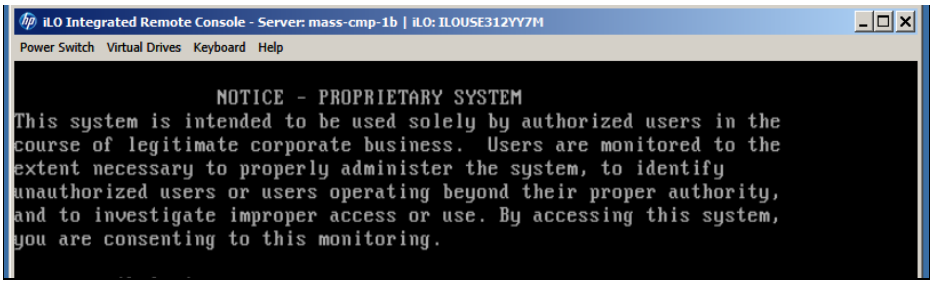
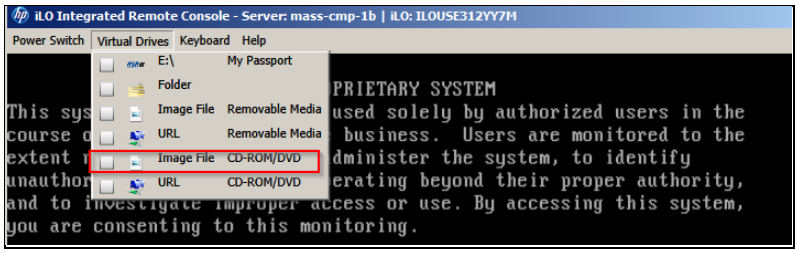
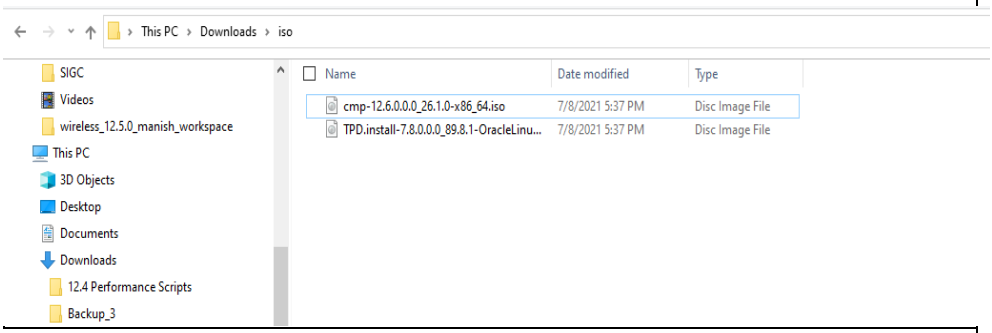
Check off (√) each step as it is completed. Check boxes are provided next to each step number.

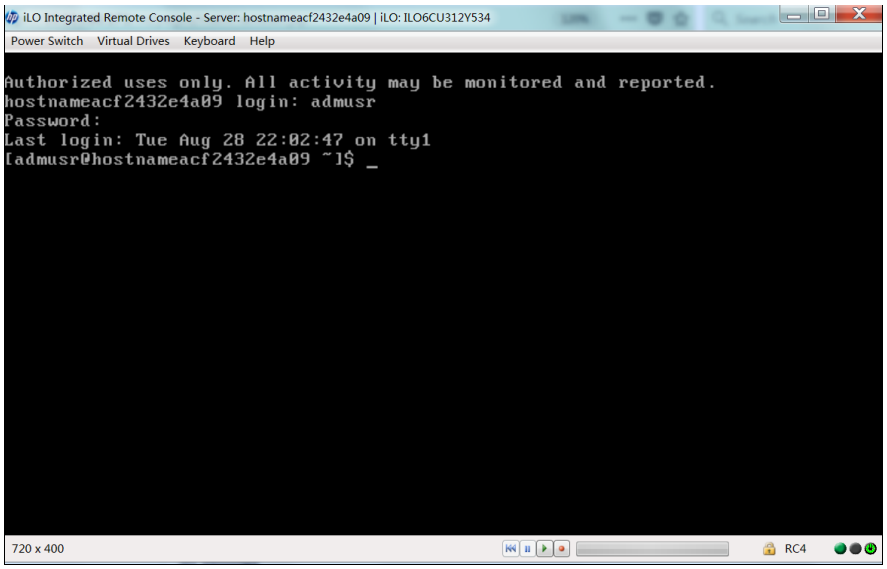
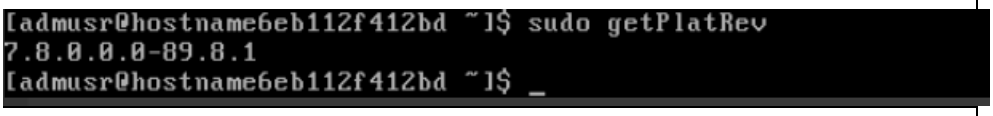
If this procedure fails, contact Oracle Technical Services and ask for assistance.

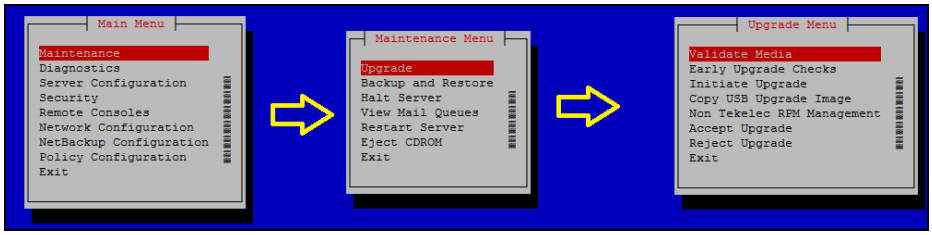
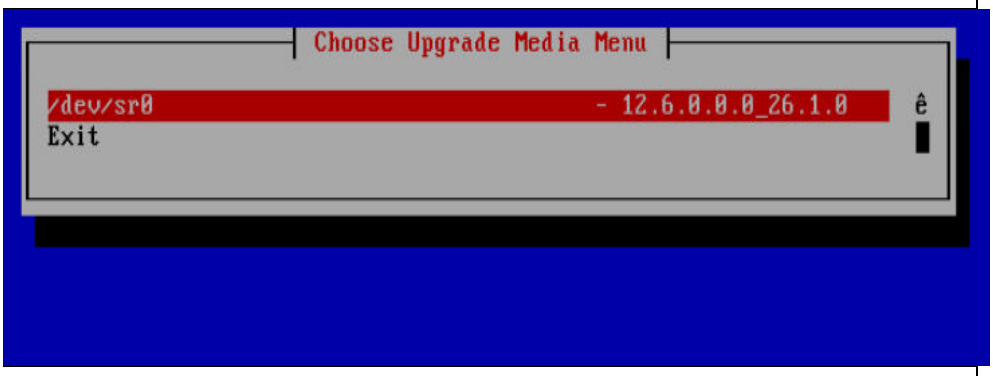
5.2.6: Installing Policy Management Software

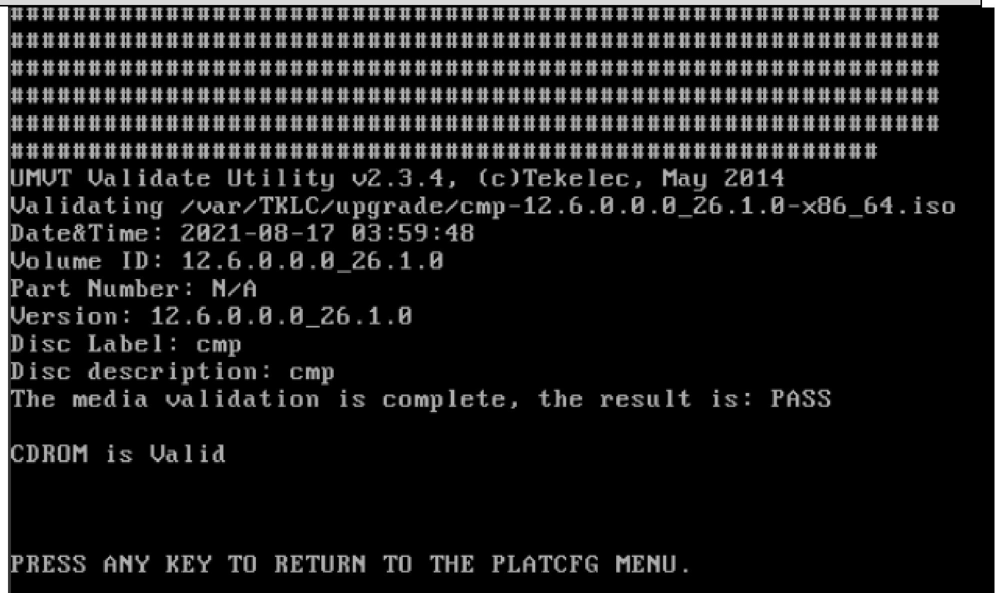
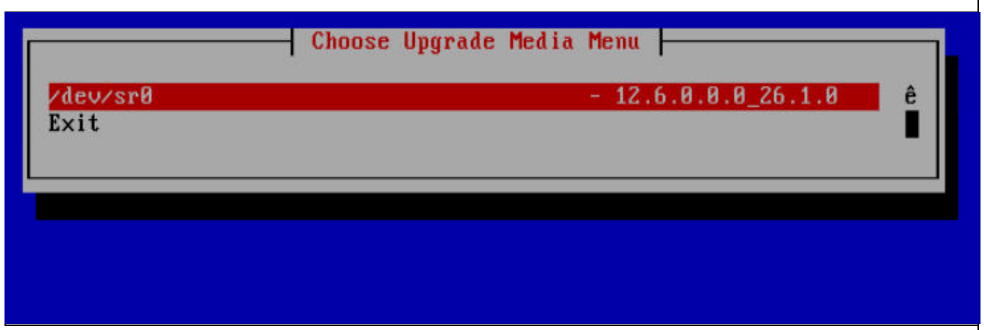
Step	Procedure	Details
1. ☐	Make the Policy Application ISO images available for installation	1. Copy the Policy Application ISO image file (CMP, MPE, MRA) onto a USB drive and insert the USB drive locally into the server. 2. Connect to the server console or remote console: - Uusing a VGA display and USB keyboard, or - Using the Server iLO port and iLO web interface (to access remote console) Proceed to step 2 of this procedure Or If you are using the iLO remote console and have the Policy Management software as an ISO image file, do the following to mount the ISO image file as a virtual drive: **NOTE:** This method is dependent on having a good network connection from the workstation where the ISO is located to the target server iLO. The browser used to attach the ISO and launch the server iLO remote console must be co-located with the ISO file repository. 3. Open a browser, enter the URL of the iLO system (management_server_iLO_ip), and log in. For example:

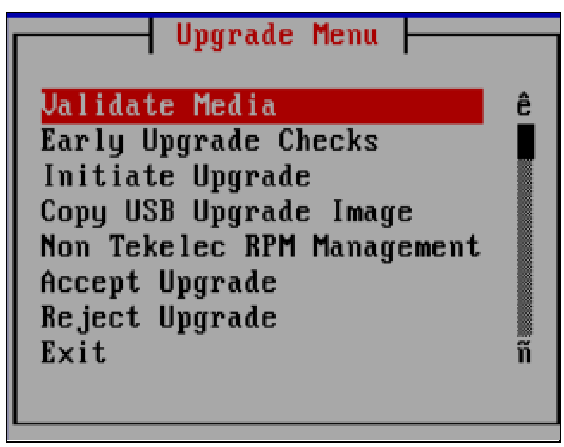
Step	Procedure	Details
		 After login the iLO home screen presents.  4. On the home page, select **Remote Console**. The Remote Console page opens. For example:  **NOTE:** When launching a remote console, the .NET application is compatible with a Windows browser; Java is compatible with both Windows and Firefox browsers. 5. In the Java Integrated Remote Console section, click **Launch**. A security warning window opens, asking for confirmation that you want to run the application. For example:

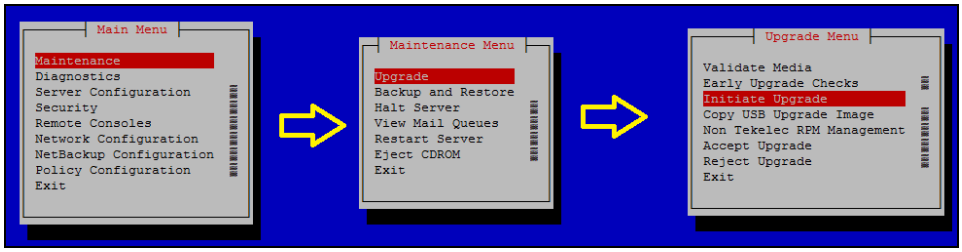
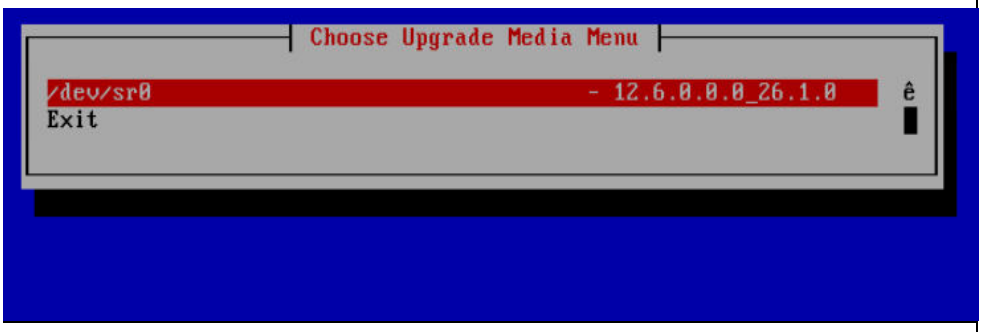
Step	Procedure	Details
		  6. Click Run. The Remote Console window opens.  7. Select **Virtual Drives → Image File CD-ROM/DVD**, browse to the ISO image file location, and click Open. The ISO image file is mounted.  **NOTE:** Verify that the ISO image file selected (CMP, MPE, MRA) is the correct one for the target server according to the Policy solution design. 

Step	Procedure	Details
		In this example the CMP ISO image is selected. Click open to mount the required ISO image file, the screen closes (the ISO has mounted) and you are returned to the CLI prompt of the remote console.
2. ☐	**Console**: Login as admusr	1. Connect to the server console, either directly or remotely: - Directly—using a display and keyboard - Remotely—using the iLO Remote Console and the server iLO port 2. Login as admusr if not logged in. 
3. ☐	**Console:** verify platform revision	You can verify the platform revision by logging in as the admusr user and entering the following command: $ sudo getPlatRev For example: `#sudo getPlatRev` 

4. ☐	**Console:** run platcfg and validate the media	1. Enter the following command to start the Platform Configuration utility: `#sudo su - platcfg` The Platform Configuration Main menu opens. 2. From the Main menu, navigate to **Maintenance → Upgrade → Validate Media**, select the ISO image file, and press **Enter**.  **NOTE:** Depending on the method used the platcfg utility searchs for any mounted ISOs and if successful displays the Policy Application ISO image file to install For example:  3. Select the ISO image and press **Enter**: The utility displays the message `Validating media or cdrom` and a series of hash marks (#). When it finishes, it displays information about the ISO image file and the message the CDROM or Media is Valid. The following example shows a successful validation:

<table>
<tr><th>Step</th><th>Procedure</th><th>Details</th></tr>
<tr><td></td><td></td><td> 
</td></tr>
<tr><td>5. ☐</td><td>Console: verify platform revision</td><td>1. Press Enter to return to the menu.
2. Scroll to select Exit.
3. Press Enter.
 

The Main menu opens.
 
</td></tr>
</table>

Step	Procedure	Details
6. ☐	**Console:** Select ISO to install, and confirm Application installation takes approximately 20 minutes—if installing with a virtual mount, it takes longer	1. From the Main menu, navigate to **Maintenance → Upgrade → Initiate Upgrade**. The Choose Upgrade Media Menu window opens. For example:  2. Select the ISO image as per the previous step, and press **Enter**  **NOTE:** The server reboots twice during the installation process, Do Not Remove the media at this time.

7. ☐	**Console:** Verify Policy install version	After the application has completed installation log back in to the command line as admusr and confirm the installed TPD platform version and the policy application version.
		
		`$appRev`
		
		`[root@CMP-1 ~]# appRev`
		`Install Time: Thu Aug 12 01:42:43 2021`
		`Product Name: cmp`
		`Product Release: 12.6.0.0.0_26.1.0`
		`Base Distro Product: TPD`
		`Base Distro Release: 7.8.0.0.0_89.8.1`
		`Base Distro ISO: TPD.install-7.8.0.0.0_89.8.1-OracleLinux6.10-x86_64.iso`
		`ISO name: cmp-12.6.0.0.0_26.1.0-x86_64.iso`
		`OS: OracleLinux 6.10`
		
		Verify:
		• TPD revision installed
		• Policy application installed and its revision

8. ☐	Console: Verify Install success	Inspect the `/var/TKLC/log/upgrade/upgrade.log` file to verify that the installation succeeded. Look for the line `Upgrade returned success!` near the end of the file. The following example shows a successful installation:

Step	Procedure	Details
		iLO Integrated Remote Console - Server: hostname483a475913f7 | iLO: ILO6CU312Y534 Power Switch Virtual Drives Keyboard Help 1531381069::Running postUpgradeBoot() for Upgrade::Policy::QPUpgradeCommon upgrade policy... 1531381069::Running postUpgradeBoot() for Upgrade::Policy::QPUpgradeProgress upgrade policy... 1531381069::Running postUpgradeBoot() for Upgrade::Policy::PlatformLast upgrade policy... 1531381069::Returning HIDS monitoring to its previous state... 1531381069::Returning HIDS monitoring to the CONFIGURED state... 1531381069::HIDS was successfully brought to the CONFIGURED state... 1531381069::Updating platform revision file... 1531381069::RCS_VERSION=1.1 1531381070::Upgrade returned success! 1531381070::Creating RC script to set alarm on next boot 1531381070::`/mnt/upgrade/upgrade/upgradeStatus' -> `/sysimage/etc/rc.d/rc4.d/S99TKLCupgradeStatus' 1531381070::Cleaning up chroot environment... 1531381070::Stopping remoteExec background process 1531381070::Shutting down /mnt/upgrade/upgrade/remoteExec... 1531381070:: 1531381277:: /etc/rc4.d/S99TKLCupgradeStatus - AlarmMgr daemon is not running, delaying by 1 minute 1531381320:: /etc/rc4.d/S99TKLCupgradeStatus - Not setting 'Upgrade Accept/Reject' alarm 1531381320:: /etc/rc4.d/S99TKLCupgradeStatus - **NOTE:** If the installation is not successful, inspect the following log files for more details and to see if errors occurred: • /var/TKLC/log/upgrade/upgrade.log • /var/TKLC/log/upgrade/ugwrap.log
9. ☐	**Remove Media**	Remove the installation media or dismount the virtually mounted ISO image file from the server. The Policy Management software is installed on the server.
10. ☐	**Policy Solution servers**	Repeat this procedure to install each Policy Management component (CMP, MPE, MRA) on each server. For Wireless mode, proceed to **Section 6: Configure Policy Application Servers in Wireless Mode**
—End of Procedure—		

5.2 Preparing a c-Class Environment

5.2.1 Preparing the PM&C Management Server

This section references the procedures used to install Policy Management software in a c-Class environment. A Platform Management and Configuration (PM&C) application on a Management Server is required for a c-Class installation. The Management Server is a rack mount server. PM&C provides tools to manage multiple enclosures and server software as well as networking equipment (enclosure switches).

Tekelec Virtual Operating Environment (TVOE) 4.1 Software Requirements is required for the Management Server installation. You must install TVOE first, then the PM&C application.

The procedure for installing and configuring the Management Server is described in the PMAC 6.6 Configuration Reference Guide.

It is necessary to IPM the Management Server and update the firmware according to the type of Hardware that is used for the Management Server.

Refer to Chapter 8 Management Server Procedures

- 8.1 IPM Management Server
- 8.2 Upgrade Management Server Firmware

To install the Platform Management and Configuration (PMAC) application on the Management Server refer to Chapter 9 PMAC Procedures

- 9.1 Installing TVOE on the Management Server
- 9.2 Configure TVOE Network
- 9.3 Deploy PMAC Guest

The procedures referenced in this section deploy PM&C on the management server. In Policy Management 12.6, the management server is used for installation, adding servers, field repairs, and deploying firmware upgrades. PM&C installation is not service-affecting for the Policy Management system; that is, Policy Management itself does not rely on PM&C to function.

5.2.2 HP C-7000 Enclosure Configuration

Procedures for Installing and configuring a HP C-7000 enclosures are found in PMAC 6.6 Configuration Reference Guide.

Refer to Chapter 7 C7000 Enclosure Procedures

PM&C can manage multiple enclosures. The following procedures are applied for each enclosure.

- Section 7.1 Configure Initial OA IP

You can configure the OA IP address using the enclosure front panel display.

- Section 7.2 Configure Initial OA Settings Using the Configuration Wizard

This procedure configures initial OA settings using a configuration wizard. This procedure is used for initial configuration only and is performed when the Onboard Administrator in OABay 1 (left as viewed from rear) is installed and active.

Prerequisites:

If the aggregation switches are supported by Oracle, then configure the Cisco 4948/4948E switches.

- Refer to Chapter 7 C7000 Enclosure Procedures
- Section 7.3 Configure OA Security

This procedure disables telnet access to OA.

- Section 7.4 Upgrade or Downgrade OA Firmware

This procedure updates the firmware on the OA.

- Section 7.5 Store OA Configuration on Management Server

  This procedure backs up OA settings on the management server.

- Section 7.8 Update IPv4 Address

  This procedure updates the IP addressing for a C7000 enclosure.

Or

- Section 7.9 Update IPv6 Address

This procedure updates the IP addressing for a C7000 enclosure. It may be used to add IPv6 addresses and/or to edit existing IPv6 addresses.

- Section 7.10 Add SNMP Trap Destination on OA

  An SNMP trap destination must be added and configured using the Onboard Administrator (OA), or SNMP must be disabled.

5.2.3 Adding the Cabinet and the Enclosure to the PM&C

This procedure provides instructions to add a cabinet and an enclosure to the PM&C system inventory.

Prerequisite:

Before beginning this procedure, you must have configured the PM&C application.

To complete this procedure, you need the following information:

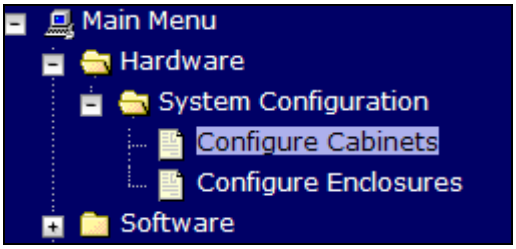
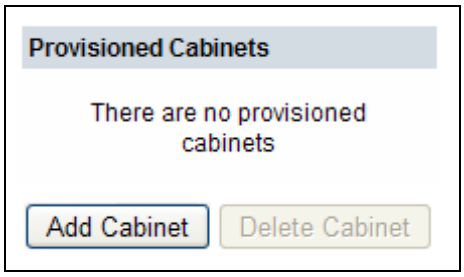
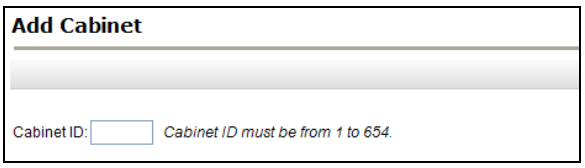
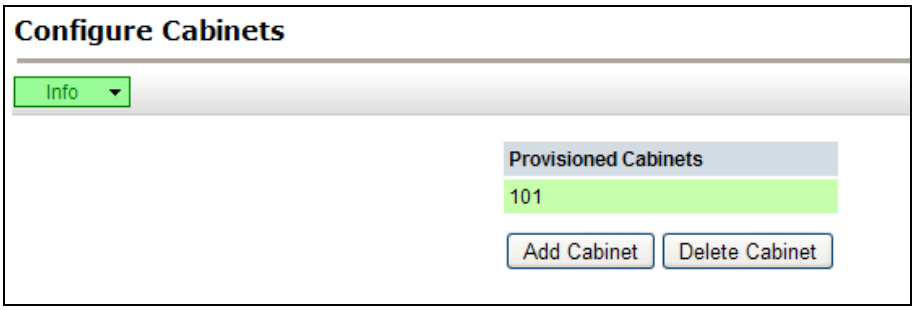
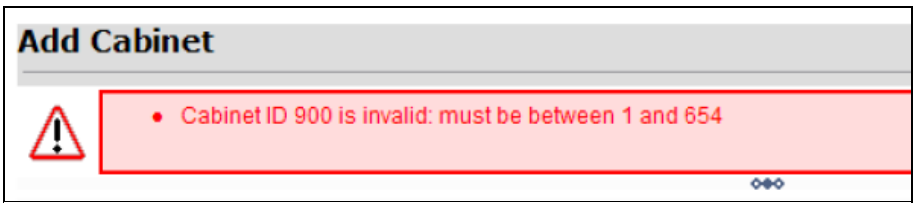
- The cabinet ID (cabinet_id), a number from 1 to 654.
- The Location ID (location_id), a number from 1 to 4, used to uniquely identify the enclosure in the cabinet. The cabinet ID and location ID are combined to create a globally unique ID for the enclosure (for example, an enclosure in cabinet 502 at location 1 has an enclosure ID of 50201). Enclosures are typically numbered from the bottom; that is, the enclosure in the bottom of the cabinet is location 1.

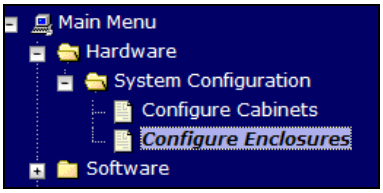
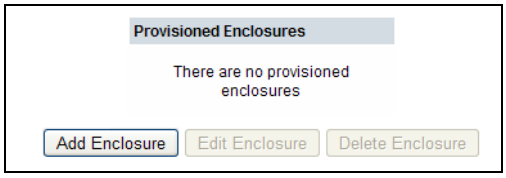
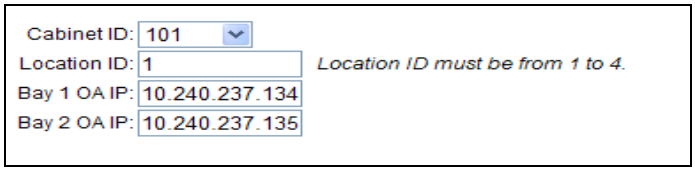
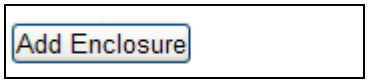
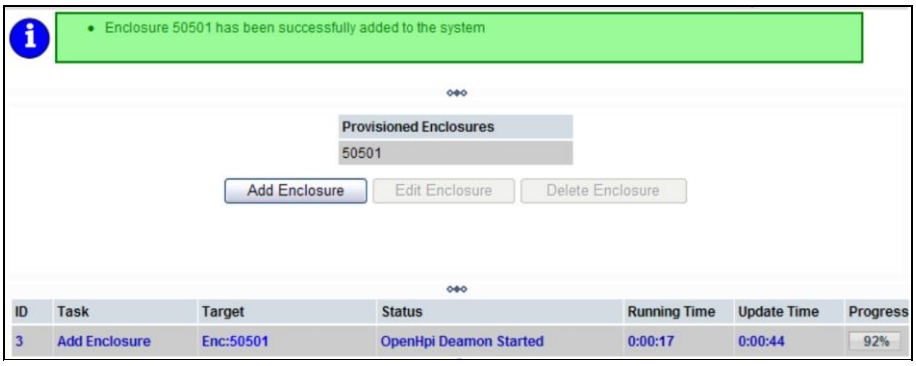
Check off (√) each step as it is completed. Check boxes are provided next to each step number.

If this procedure fails, contact Oracle Technical Services and ask for assistance.

5.3.3: Adding the Cabinet and the Enclosure to PM&C

Step	Procedure	Details
1. ☐	**PM&C GUI**: Login	1. Open web browser and enter: `https://<`*pmac_management_network_ip*`>` 2. Log in as the pmacadmin user.

Step	Procedure	Details
2. ☐	**PM&C GUI:** Configure Cabinets	Navigate to **Main Menu → Hardware → System Configuration → Configure Cabinets**. 
3. ☐	PM&C GUI: Add Cabinet	On the Configure Cabinets panel click **Add Cabinet** 
4. ☐	**PM&C GUI:** Enter Cabinet ID	Enter Cabinet ID and click **Add Cabinet**. 
5. ☐	**PM&C GUI:** Check errors	If errors are not reported, you see the following:  Or you see the Cabinet ID is invalid error message: 

Step	Procedure	Details
6. ☐	**PM&C GUI:** Go to Configure HPC Enclosures	Navigate to **Main Menu → Hardware → System Configuration → Configure Enclosures**. 
7. ☐	**PM&C GUI:** Go to Add Enclosure	On the Configure Enclosures panel, click **Add Enclosure** 
8. ☐	**PM&C GUI:** Add Enclosure	1. On the Add Enclosure panel, enter the Cabinet ID, Location ID, and two OA IP addresses (the active and standby OA for the enclosure). 2. Click **Add Enclosure**.   **Notes:** • Location ID is used to uniquely identify the enclosure in the cabinet. It can have a value of 1, 2, 3, or 4. The cabinet ID and location ID are combined to create a globally unique ID for the enclosure (for example, an enclosure in cabinet 502 at location 1 has an enclosure ID of 50201). • Enclosures are typically numbered from the bottom. That is, the enclosure in the bottom of the cabinet is location 1.
9. ☐	**PM&C GUI:** Monitor the Enclosure discovery status	When the task is complete, the text changes to green and the Progress bar indicates 100%. 

Step	Procedure	Details
10. ☐	**PM&C GUI:** Background Task monitoring	This page displays status updates. 3 | Add Enclosure | Enc:50202 | Enclosure added - starting monitoring | 0:01:13 | 2011-10-08 02:20:32 | 100% **NOTE:** Do not click the button, this button deletes the selected task from the Background Task Monitoring status screen.
11. ☐	**PM&C GUI:** Wait until the Add Enclosure task finishes	The color of the progress bar changes to green when complete: 3 | Add Enclosure | Enc:50202 | Enclosure added - starting monitoring | 0:01:13 | 2011-10-08 02:20:32 | 100% If the Add Enclosure task fails, the status displays information concerning the failed step and the color of the Progress bar changes to red.
12. ☐	**PM&C GUI:** Verify Software Inventory	Navigate to **Software → Software Inventory**. If the control network is configured correctly, the blades have TPD installed (at minimum), and the enclosure switches have a control network configured. The Software Inventory form shows blade server information. Example below: Main Menu: Software -> Software Inventory Tue Aug 17 10:12:04 2021 UTC Filter* **NOTE:** The procedure to configure the enclosure switches, if they not configured, is performed later.
—End of Procedure—		

Identity	IP Address	Hostname	Platform Name	Platform Version	Application Name	Application Version	Designat
Enc:12001 Bay:1F	...:b4ff:fe1e:95f0	g8-mra1-s2-a	TPD (x86_64)	7.8.0.0.0-89.4.0	MRA	12.6.0.0.0_16.1.0	
Enc:12001 Bay:2F	169.254.131.58	mpe5-s2-g8	TPD (x86_64)	7.8.0.0.0-89.5.0	MPE	12.6.0.0.0_23.1.0	
Enc:12001 Bay:3F	169.254.131.29	mpe1-s2-g8	TPD (x86_64)	7.8.0.0.0-89.8.1	MPE	12.6.0.0.0_26.1.0	
Enc:12001 Bay:4F	169.254.131.34	g8cmptest	TPD (x86_64)	7.8.0.0.0-89.8.1	CMP	12.6.0.0.0_26.1.0	
Enc:12001 Bay:5F	...:2fff:fe6f:fe8						
Enc:12001 Bay:6F	...:2fff:fe6f:cab0						
Enc:12001 Bay:7F	169.254.131.59	g8-MRA1-s2-b	TPD (x86_64)	7.8.0.0.0-89.8.1	MRA	12.6.0.0.0_26.1.0	
Enc:12001 Bay:8F	...:2fff:fe6f:4d70						
Enc:12001 Bay:9F	169.254.131.25	g8-MPE1-s1-c	TPD (x86_64)	7.8.0.0.0-89.8.1	MPE	12.6.0.0.0_26.1.0	
Enc:12001 Bay:10F	169.254.131.24	g8-MRA1-s1-c	TPD (x86_64)	7.8.0.0.0-89.8.1	MRA	12.6.0.0.0_26.1.0	

5.2.4 Configure Blade Server iLO Password for Administrator Account

The file `change_ilo_admin_password.xml` is provided on the Policy Management ISO image file and is used by the PM&C netConfig tool to push the configuration to the switches. The file may change from one release to the next. Edit this file for your installation and copy it to the PM&C server after it is installed.

Prerequisite:

Before beginning this procedure, you must configure the OA IP addresses.

Use this mandatory procedure to set iLO passwords for the Administrator and root accounts on all servers:

3. On the PM&C server, in the directory `/usr/TKLC/smac/html`, create the following subdirectory:

```
/ilo_passwd
```

4. Set the directory permissions to an appropriate level. For example:

```
$ sudo chmod go+x /usr/TKLC/smac/html/ilo_passwd
```

5. Locate the file `change_ilo_admin_password.xml` on the Policy Management ISO image file. For example:

```
$ sudo find . -name change_\* -print ./TPD/872-2544-102-9.1.0_28.1.0-cmp-
x86_64/upgrade/change_ilo_admin_passwd.xml
```

6. Copy the file to the following directory:

```
/usr/TKLC/smac/html/ilo_passwd
```

7. Set the file permissions to an appropriate level. For example:

```
$ sudo chmod 777 change_ilo_admin_passwd.xml
```

8. Edit the file to update the root password, iLO root password, and iLO Administrator password fields.
9. Make a temporary copy of the file in the following directory:

```
/usr/TKLC/smac/html/public-configs/
```

10. Log in to the active OA as the root user and enter the following command:

```
hponcfg all http://management_server_ip/public-configs/change_ilo_admin_passwd.xml
```

After the command finishes, verify that errors did not occurred.

1. Log out from the active OA.
2. Delete the temporary copy of the file.
3. (Optional) You can verify access to the server iLO by opening a browser, entering the IP address of the server iLO system (management_server_iLO_ip), and logging in using the values for Administrator and iLO Administrator password.
4. (Optional) You can verify root access to the server iLO using an SSH session. For example:

```
 # ssh root@ management_server_iLO_ip password: iLO_root_password
```

5.2.5 Configuring c-Class Aggregation and Enclosure Switches Using netConfig

The c-Class environment includes paired aggregation switches and enclosure switches. Prepare and verify network configuration files (used to configure the switches).

The Policy Management ISO image files include template configuration files in the `/upgrade/switchconfig/examples/netConfig/` directory. The templates include variables that you can replace with site- and customer-specific information. You can edit these template files to make them specific for your installation and place them on the PM&C server after it is installed. The PM&C netConfig tool uses these network configuration files to configure the switches. The following template files are provided:

- For 4948 aggregation enclosure switches:
  - 4948_cClass_init.xml
  - 4948_layer2_configure.xml
  - 4948_layer3_configure.xml
  - 4948_RMS_init.xml
- For 4948E aggregation enclosure switches:

  - 4948E_cClass_init.xml
  - 4948E_layer2_configure.xml
  - 4948E_layer3_configure.xml
  - 4948E_RMS_init.xml

- For 6120XG enclosure switches:
  - 6120XG_init.xml
  - 6120XG_Single_configure.xml (for connections using a single 10 Gb/s copper uplink)
  - 6120XG_LAG_Uplink_configure.xml (for connections using a bundle of four 1 Gb/s copper uplinks)
  - 6120XG_TagCtl_Uplink_configure.xml (if the Control network is VLAN tagged)

- For 6125XLG enclosure switches:
  - 6125XLG_init.xml
  - 6125XLG_Single_configure.xml (for connections using a single 10 Gb/s copper uplink)
  - 6125XLG_LAG_Uplink_configure.xml (for connections using a bundle of four 1 Gb/s copper uplinks)

Prerequisite:

Before beginning this procedure, you must have installed PM&C and configured the initial OA settings, the netConfig repository, and the initial OA IP address. To complete this procedure you need the following software and information:

- The appropriate netConfig XML files
- The HP miscellaneous firmware ISO image file
- The cabinet ID, a number from 1 to 654 (cabinet_id)

The procedures to configure aggregation switches and enclosure switches using netConfig are described in the PMAC 6.6 Configuration Reference Guide.

TIP: To minimize errors, after you prepare the files, review and verify them.

These templates cover the common configurations, but may not cover all possible configurations. You may need to change or add to these templates for specific requirements. To avoid potential support issues, do not deviate from Oracle standards.

5.2.6 Configuring the Application Blades

The following procedures are applied for each enclosure.

NOTE: during the following OA configuration steps, the IP addresses of the Enclosure switches are set. These IP addresses are then used to configure the Enclosure switches.

5.2.7 Updating Application Blade Firmware

Policy Management servers must have the correct release of firmware.

The procedure for updating Oracle server firmware is described in the HP Solutions Firmware Upgrade Pack, Software Centric Release Notes, Release 2.2.12

5.2.8 Confirming and Updating Application Blade BIOS Settings

You need to confirm and update the BIOS boot order on the Policy Management servers.

Prerequisites:

Before beginning this procedure, you must have updated the firmware on the Policy Management servers.

To complete this procedure, you need the following information:

- The root password *root_password* (use the root account instead of the Admin account)

BIOS configurations are also referenced in **TPD Initial Product Manufacture, Software Installation Procedure.** (Appendix E)

5.2.9 Loading Policy Management Software Images onto the PMAC

Prerequistes:

- Before beginning this procedure, you must have configured the PMAC application.
- To complete this procedure, you need the following:
  - TPD ISO image file.
  - Policy Management ISO image files (CMP, MPE, MRA).

See Section **4.1: Software Requirements**

The procedure for adding ISO Images to the PMAC Image Repository is described in the PMAC 6.6 Configuration Reference Guide Section 9.8. IPM Enclosure Blades Using the PMAC Application.

5.2.10 IPM Enclosure Blades Using the PMAC

This procedure provides the steps to install TPD on Blade servers from PMAC.

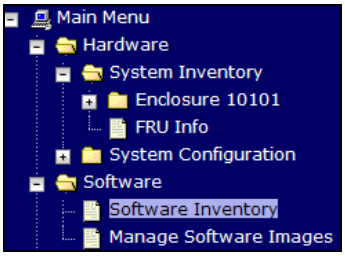
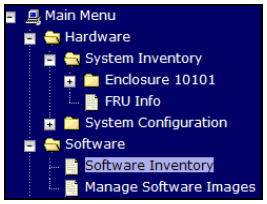
Prerequisites:

- Enclosures containing the blade servers targeted for IPM are configured.
- Appropriate version of TPD is added to the PMAC Software Image management.

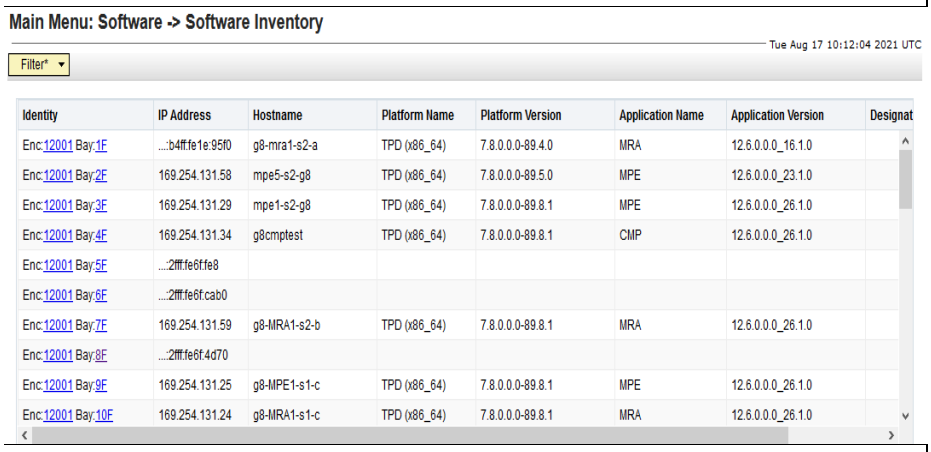
Check off (√) each step as it is completed. Check boxes are provided next to each step number.

If this procedure fails, contact Oracle Technical Services and ask for assistance.

5.3.10: IPM Enclosure Blades Using the PM&C

Step	Procedure	Details
1. ☐	**PM&C GUI:** Verify if PM&C Contol Network is established to the blades.	Navigate to Software → Software Inventory.  Ident | IP Address Enc:50301 Bay:1F | 192.168.1.6 Enc:50301 Bay:2F | 192.168.1.12 Enc:50301 Bay:3F | 192.168.1.8 Enc:50301 Bay:8F | 192.168.1.5 Enc:50301 Bay:9F | 192.168.1.11 Enc:50301 Bay:10F | 192.168.1.10 Enc:50301 Bay:11F | 192.168.1.9 Enc:50301 Bay:16F | 192.168.1.7 If the PM&C Control network is correctly configured, the PM&C acts as a DHCP server and provide control network addresses in the range of 192.168.1.3—254 to the blade servers in the managed cabinets/enclosures. PM&C takes the address of 192.168.1.1. If the server has requested an IP address from PM&C, the IP address is in the IP Address column. TPD always does this when a server blade is booted, and also periodically after this. If there are not any IP Addresses in this view, then either: • PM&C Control Network is not correctly configured (probably a switch config issue) • The Blades do not have an OS installed. Enc:801 Bay:14F Enc:801 Bay:16F Enc:802 Bay:1F If there are IP addresses in this view it means that an OS is installed. Enc:801 Bay:6F | 192.168.1.21 | hostnameb9d92a84cefe | TPD (x86_64) | 7.0.2.0.0-86.28.0 Enc:801 Bay:8F | 192.168.1.16 | hostname6de5d09f047e | TPD (x86_64) | 7.0.2.0.0-86.28.0 Porceed to the next step to IPM (install the OS) on the selected blade
2. ☐	**PM&C GUI**: Initiate OS Install	1. Navigate to **Software → Software Inventory**. 

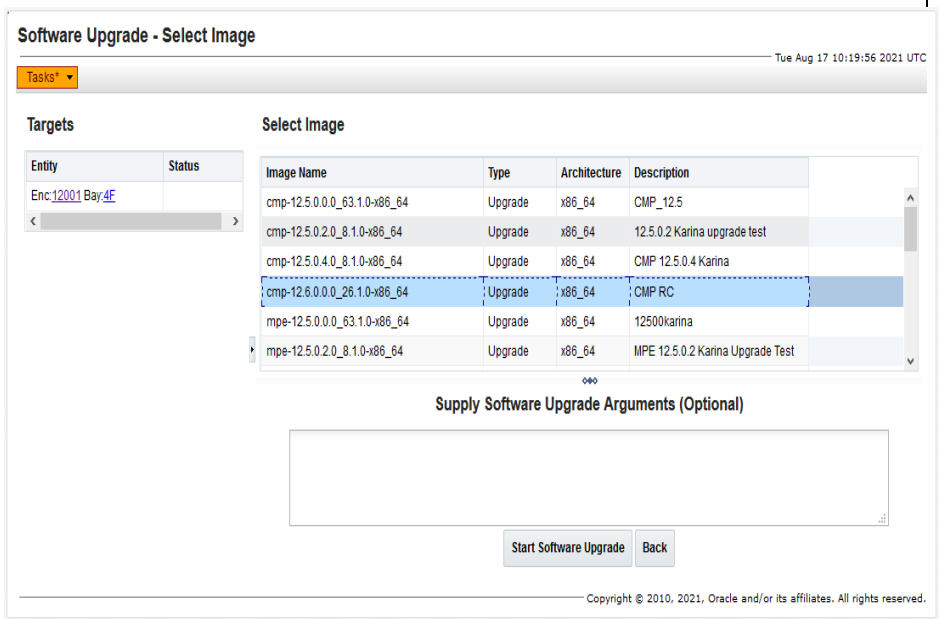
Step	Procedure	Details
		2. Select the servers you want to IPM with a bootable TPD ISO image file and click Install OS. If you want to install the same OS image to more than one server, you may select multiple servers by clicking multiple rows individually. Selected rows are highlighted.



Identity	IP Address	Hostname	Platform Name	Platform Version	Application Name	Application Version	Designat
Enc:12001 Bay:1F	...:b4ff:fe1e:95f0	g8-mra1-s2-a	TPD (x86_64)	7.8.0.0.0-89.4.0	MRA	12.6.0.0.0_16.1.0	
Enc:12001 Bay:2F	169.254.131.58	mpe5-s2-g8	TPD (x86_64)	7.8.0.0.0-89.5.0	MPE	12.6.0.0.0_23.1.0	
Enc:12001 Bay:3F	169.254.131.29	mpe1-s2-g8	TPD (x86_64)	7.8.0.0.0-89.8.1	MPE	12.6.0.0.0_26.1.0	
Enc:12001 Bay:4F	169.254.131.34	g8cmptest	TPD (x86_64)	7.8.0.0.0-89.8.1	CMP	12.6.0.0.0_26.1.0	
Enc:12001 Bay:5F	...:2fff:fe6f:fe8						
Enc:12001 Bay:6F	...:2fff:fe6f:cab0						
Enc:12001 Bay:7F	169.254.131.59	g8-MRA1-s2-b	TPD (x86_64)	7.8.0.0.0-89.8.1	MRA	12.6.0.0.0_26.1.0	
Enc:12001 Bay:8F	...:2fff:fe6f:4d70						
Enc:12001 Bay:9F	169.254.131.25	g8-MPE1-s1-c	TPD (x86_64)	7.8.0.0.0-89.8.1	MPE	12.6.0.0.0_26.1.0	
Enc:12001 Bay:10F	169.254.131.24	g8-MRA1-s1-c	TPD (x86_64)	7.8.0.0.0-89.8.1	MRA	12.6.0.0.0_26.1.0	

NOTE: IPM is also a useful recovery procedure if a server is in a bad or unknown condition, or was configured with a different application because the IPM cleans all the existing software and disk configurations off of the server, and returns the server to a clean state.

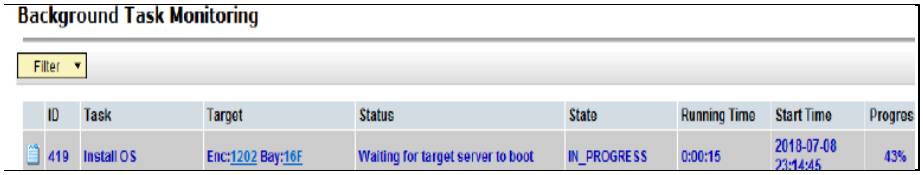
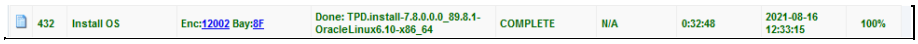
After selecting Install OS the Software Install, the Select Image screen opens:



Entity	Status
Enc:12001 Bay:4F	

Image Name	Type	Architecture	Description
cmp-12.5.0.0.0_63.1.0-x86_64	Upgrade	x86_64	CMP_12.5
cmp-12.5.0.2.0_8.1.0-x86_64	Upgrade	x86_64	12.5.0.2 Karina upgrade test
cmp-12.5.0.4.0_8.1.0-x86_64	Upgrade	x86_64	CMP 12.5.0.4 Karina
cmp-12.6.0.0.0_26.1.0-x86_64	Upgrade	x86_64	CMP RC
mpe-12.5.0.0.0_63.1.0-x86_64	Upgrade	x86_64	12500karina
mpe-12.5.0.2.0_8.1.0-x86_64	Upgrade	x86_64	MPE 12.5.0.2 Karina Upgrade Test

All bootable images in the PM&C repository are listed. Select the correct bootable image to proceed with the OS installation of the selected blade and click **Start Software Install**.

Step	Procedure	Details
3. ☐	**PM&C GUI:** Monitor OS Install	Navigate to **Main Menu → Task Monitoring** to monitor the progress of the OS Installation background task. A separate task displays for each blade affected.  Background Task Monitoring Filter ID Task Target Status State Running Time Start Time Progres 419 Install OS Enc:1202 Bay:16F Waiting for target server to boot IN_PROGRESS 0:00:15 2018-07-08 23:14:45 43% When the installation is complete, the task changes to green and the Progress bar indicates 100%.  432 Install OS Enc:12002 Bay:8F Done: TPD.install-7.8.0.0.0_89.8.1-OracleLinux6.10-x86_64 COMPLETE N/A 0:32:48 2021-08-16 12:33:15 100% **NOTE:** if the OS Install step fails, then it may be that the Control Network is not correctly established, and troubleshooting is required.
—End of Procedure—		

5.2.11 Install Policy Management Software on Blades using PM&C

This procedure installs the Policy Management software on HP c-Class servers using PM&C

CAUTION: Do not mix up the enclosures when deploying the applications. The bottom enclosure in a cabinet is identified in Oracle documentation as Enclosure 1. The enclosure above this is Enclosure 2. However, PM&C GUI forms may list the enclosures with Enclosure 1 listed first, and Enclosure 2 listed below this in the form lists.

PREREQUISITES:

Before beginning the procedure, complete hardware installation and verification as well as the IP networking plan and IP assignments.

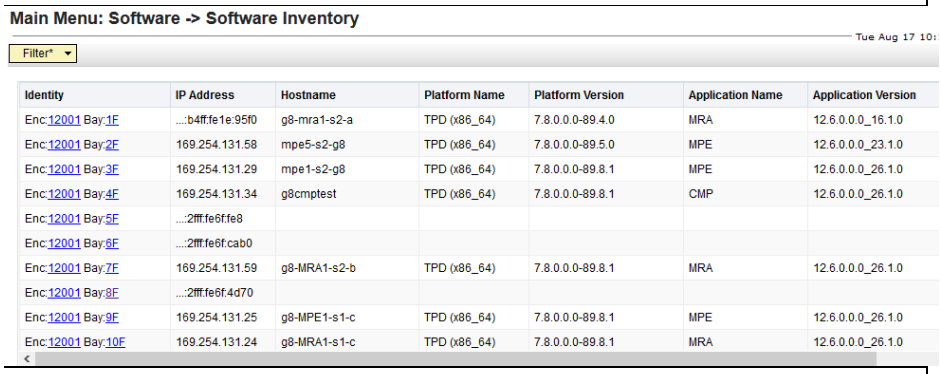
To complete the procedures in this section, you need the following material and information:

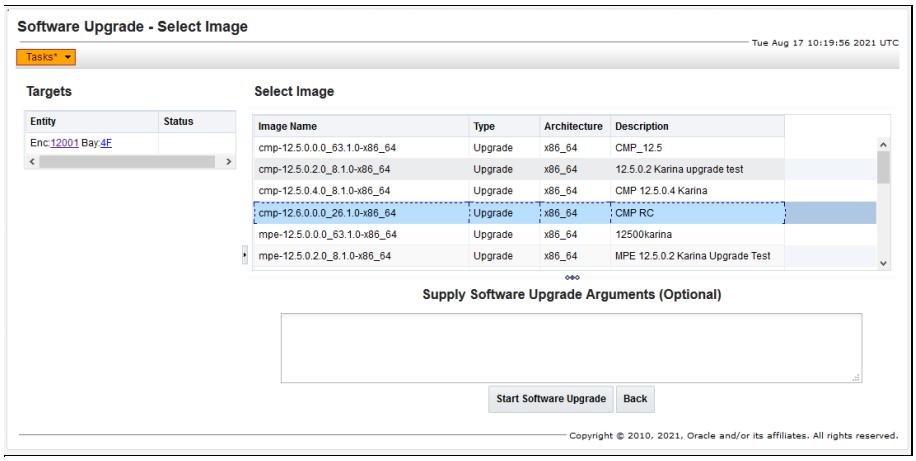
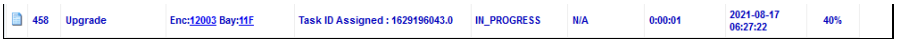
- The appropriate release and Policy Management Application iso images of the Policy Management software stored on the PM&C server.
- Layout diagram for c-Class enclosures, identifying which bays run which Policy Management application.

Check off (√) each step as it is completed. Check boxes are provided next to each step number.

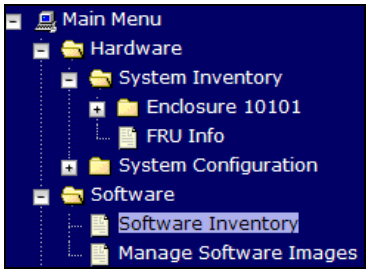
If this procedure fails, contact Oracle Technical Services and ask for assistance.

5.3.11: Install the Policy Management Application Software on Blades using PM&C

Step	Procedure	Details
1. ☐	**PM&C GUI:** Login	1. Open web browser and enter: `http://<management_network_ip>` 2. Login as PM&C admin user.
2. ☐	**PM&C GUI:** Select Servers for Application install	1. Navigate to **Software → Software Inventory**.  Identity | IP Address | Hostname | Platform Name | Platform Version | Application Name | Application Version Enc:12001 Bay:1F | ...:b4ff:fe1e:95f0 | g8-mra1-s2-a | TPD (x86_64) | 7.8.0.0.0-89.4.0 | MRA | 12.6.0.0.0_16.1.0 Enc:12001 Bay:2F | 169.254.131.58 | mpe5-s2-g8 | TPD (x86_64) | 7.8.0.0.0-89.5.0 | MPE | 12.6.0.0.0_23.1.0 Enc:12001 Bay:3F | 169.254.131.29 | mpe1-s2-g8 | TPD (x86_64) | 7.8.0.0.0-89.8.1 | MPE | 12.6.0.0.0_26.1.0 Enc:12001 Bay:4F | 169.254.131.34 | g8cmptest | TPD (x86_64) | 7.8.0.0.0-89.8.1 | CMP | 12.6.0.0.0_26.1.0 Enc:12001 Bay:5F | ...:2fff:fe6f:fe8 Enc:12001 Bay:6F | ...:2fff:fe6f:cab0 Enc:12001 Bay:7F | 169.254.131.59 | g8-MRA1-s2-b | TPD (x86_64) | 7.8.0.0.0-89.8.1 | MRA | 12.6.0.0.0_26.1.0 Enc:12001 Bay:8F | ...:2fff:fe6f:4d70 Enc:12001 Bay:9F | 169.254.131.25 | g8-MPE1-s1-c | TPD (x86_64) | 7.8.0.0.0-89.8.1 | MPE | 12.6.0.0.0_26.1.0 Enc:12001 Bay:10F | 169.254.131.24 | g8-MRA1-s1-c | TPD (x86_64) | 7.8.0.0.0-89.8.1 | MRA | 12.6.0.0.0_26.1.0 2. Select the servers where the application is installed. If you want to install the same application image to more than one server, you may select multiple servers by clicking multiple rows individually. Selected rows are highlighted. **NOTES:** - After the TPD OS is installed the system assigns a host name. - 8 is the maximum number selected at one time. 3. Click **Upgrade**

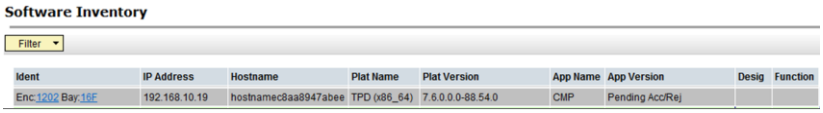
Step	Procedure	Details
3. ☐	**PM&C GUI:** Initiate Application Install	The Software Upgrade page opens. The left side of this screen shows the servers where the Application Software is applied. 1. From the list of available images, select the version and Application Software Package (CMP, MRA, MPE) according to the system design.  2. Click **Start Software Upgrade.** A confirmation window opens. 3. Click **OK** to proceed with the install.
4. ☐	**PM&C GUI:** Monitor the installation status	Navigate to **Main Menu → Task Monitoring** to monitor the progress of the Application Installation task, a separate task displays for each blade affected.  When the installation is complete, the task changes to green and the Progress bar indicates 100%.
5. ☐	REPEAT the above steps for each Application	**Repeat steps 3 and 4 for each Application beings installed at the site.**

<table>
<tr><th>Step</th><th>Procedure</th><th>Details</th></tr>
<tr><td>6. ☐</td><td>Verify Application installations-accept upgrade</td><td>
1. Navigate to **Software → Software Inventory**.



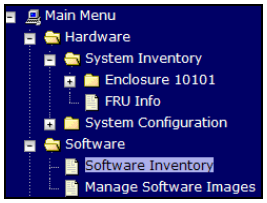
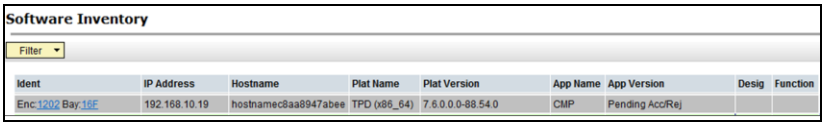
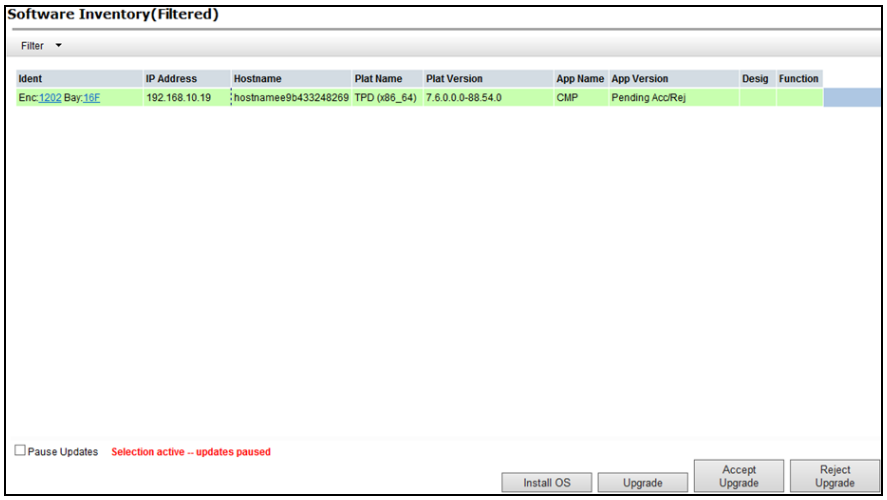
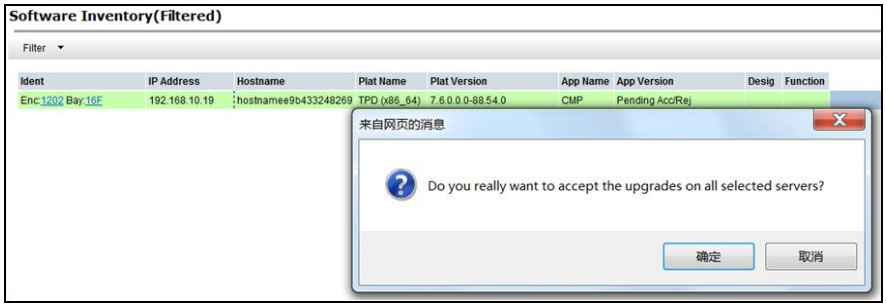
At this point, all the target servers have had their applications installed and the AppVersion displays the latest application version.

Note: The option to Accept/ Reject upgrade is not available on the latest versions of PMAC.



Ident	IP Address	Hostname	Plat Name	Plat Version	App Name	App Version	Desig	Function
Enc:1202 Bay:16F	192.168.10.19	hostnamec8aa8947abee	TPD (x86_64)	7.6.0.0.0-88.54.0	CMP	Pending Acc/Rej		

2. Verify the App Name shows the correct name (CMP, MPE, MRA) for each server where the Applications are installed. Also, confirm the Enclosure and Bay position. Confirm all assignments are per the design.
3. Select the servers to upgrade. The **Accept Upgrade** option is available.
4. Click **Accept Upgrade** to confirm the upgrade.
</td></tr>
</table>

Step	Procedure	Details
7. ☐	Verify application installations-accept upgrade	Navigate to **Software → Software Inventory**.  At this point, all the target servers have their applications installed and the AppVersion displays the latest application version. Note: The option to Accept/ Reject upgrade is not available on the latest versions of PMAC.  Software Inventory Filter Ident: Enc:1202 Bay:16F IP Address: 192.168.10.19 Hostname: hostnamec8aa8947abee Plat Name: TPD (x86_64) Plat Version: 7.6.0.0.0-88.54.0 App Name: CMP App Version: Pending Acc/Rej Desig Function 1. Verify the App Name shows the correct name (CMP, MPE, MRA or Medition) for each server where the Applications are installed. 2. Confirm the Enclosure and Bay position. 3. Confirm all assignments are per the design. 4. Select the servers you wish to upgrade. 5. Click **Accept Upgrade**.  Software Inventory(Filtered) Filter Ident: Enc:1202 Bay:16F IP Address: 192.168.10.19 Hostname: hostnamee9b433248269 Plat Name: TPD (x86_64) Plat Version: 7.6.0.0.0-88.54.0 App Name: CMP App Version: Pending Acc/Rej Desig Function Pause Updates Selection active -- updates paused Install OS Upgrade Accept Upgrade Reject Upgrade  Software Inventory(Filtered) Filter Ident: Enc:1202 Bay:16F IP Address: 192.168.10.19 Hostname: hostnamee9b433248269 Plat Name: TPD (x86_64) Plat Version: 7.6.0.0.0-88.54.0 App Name: CMP App Version: Pending Acc/Rej Desig Function 来自网页的消息 Do you really want to accept the upgrades on all selected servers? 确定 取消

Step	Procedure	Details
8. ☐	Verify Application Installations	1. Navigate to **Software → Software Inventory**. Enc:12001 Bay:4F | 169.254.131.34 | g8cmptest | TPD (x86_64) | 7.8.0.0.0-89.8.1 | CMP | 12.6.0.0.0_26.1.0 a. Confirm that the App Version column does not display the Pending Acc/Rej status but shows the correct Application Version.
—End of Procedure—		

6. CONFIGURE POLICY APPLICATION SERVERS IN WIRELESS MODE

The following procedures configure the Policy Management Application and establish the network relationships, to a level that allows a basic test call though the system.

The following procedures are common to c-Class and RMS environments, except for small differences noted in the procedures.

It is assumed that the Installation tasks associated with preparing the appropriate Installation Environment in Section 5 are completed before proceeding with the following tasks.

The post-installation tasks consist of the following:

1. Establishing network addresses and connections for every Policy Management server
2. Configuring the first CMP server
3. Configuring the CMP Site 1 cluster to manage the Policy Management network
4. Configuring a CMP Site 2 cluster for Geo-Reundancy (optional)
5. Configuring Policy Management clusters
6. Exchanging SSH keys between Policy Management servers
7. Configuring routing on servers

Configuration Management Platform Wireless User's Guide

Platform Configuration User's Guide

6.1 Perform Initial Server Configuration of Policy Servers—platcfg

You must configure the operation, administration, and management (OAM) network address of the server, as well as related networking. Perform the referenced procedure on every server in the Policy Management network.

Prerequisites:

To complete this procedure, you need the following information:

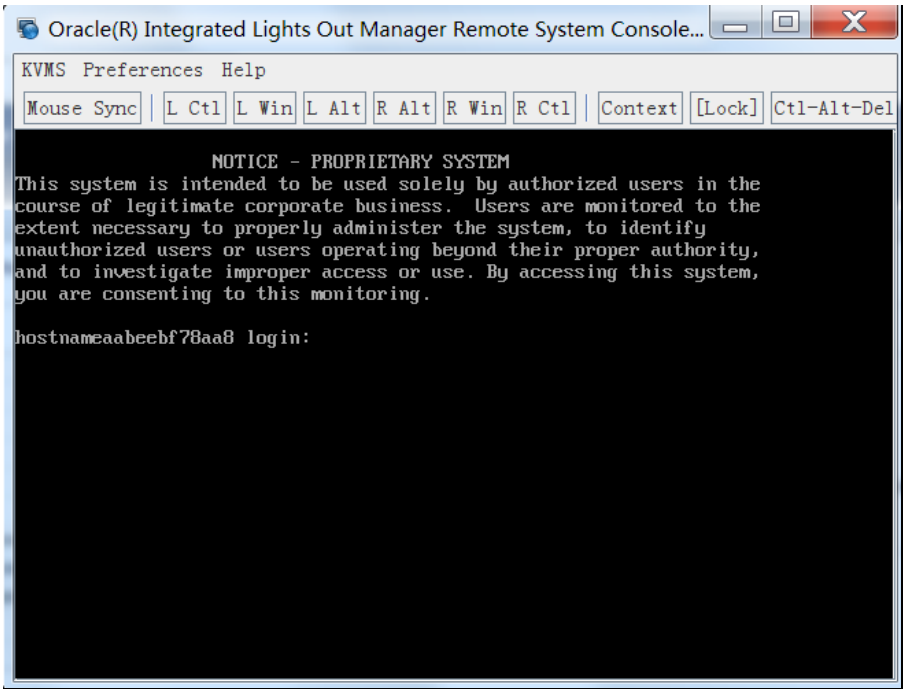
- This procedure assumes that you are using Policy Management in a Wireless or Wireless-C.
- You need to know whether or not the server has an optional Ethernet Mezzanine card installed.
- Hostname—The unique hostname for the device being configured.
- OAM Real IP IPv4 Address—The IP address that is permanently assigned to this device.
- OAM Default IPv4 Route—The default route of the OAM network. The MPE and MRA system may move the default route to the SIG-A interface after the topology configuration is complete. The default route remains on the OAM interface for the CMP system.
- OAM Real IP IPv6 Address (optional)—The IP address that is permanently assigned to this device.
- OAM Default IPv6 Route (optional)—The default route of the OAM network. Note the MPE and MRA system may move the default route to the SIG-A interface after the topology configuration is complete. The default route remains on the OAM interface for the CMP system.
- NTP Servers—Reachable NTP server) (ntp_address).
- DNS Server A (optional)—A reachable DNS server.
- DNS Server B (optional)—A reachable DNS server.
- DNS Search—The domain name appended to a DNS query.

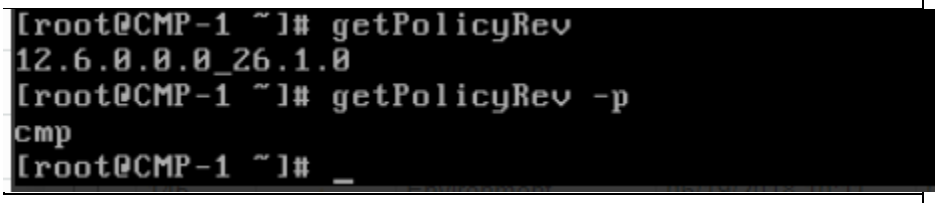
- Device—The bond interface of the OAM device. Use the default value, as changing this value is not supported.
- OAM VLAN ID—The OAM network VLAN ID.
- SIG A VLAN ID—The Signaling-A network VLAN ID.
- SIG B VLAN ID (optional)—The Signaling-B network VLAN ID.
- SIG C VLAN ID (optional)—The Signaling-C network VLAN ID.

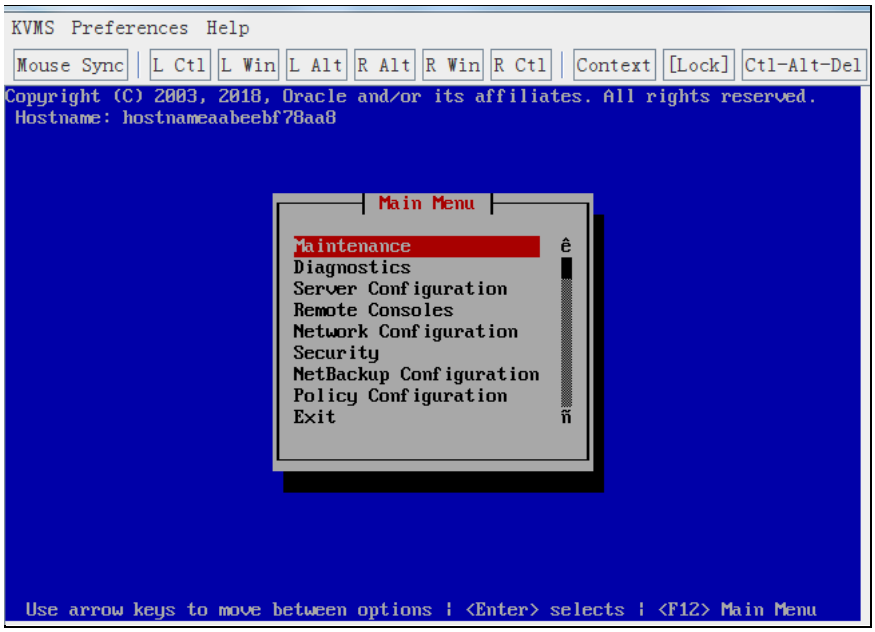
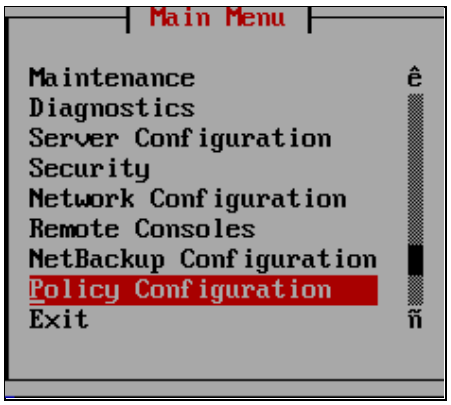
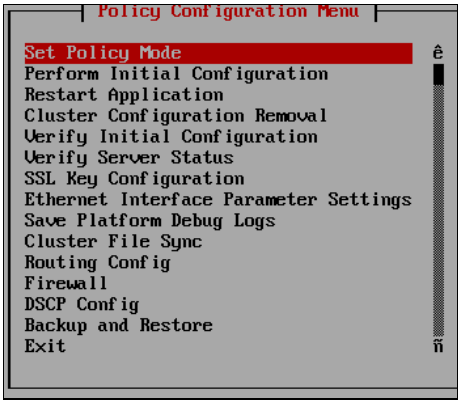
Check off (√) each step as it is completed. Check boxes are provided next to each step number.

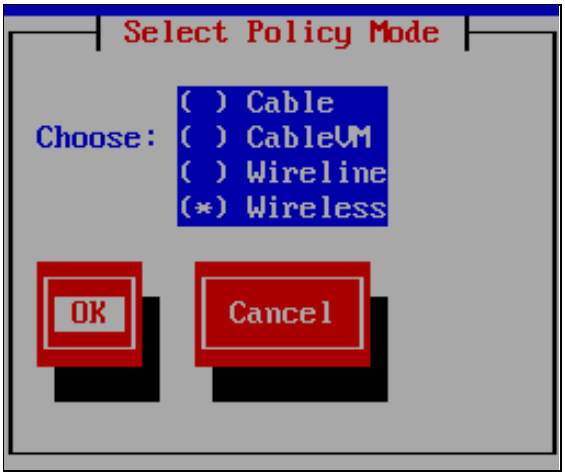
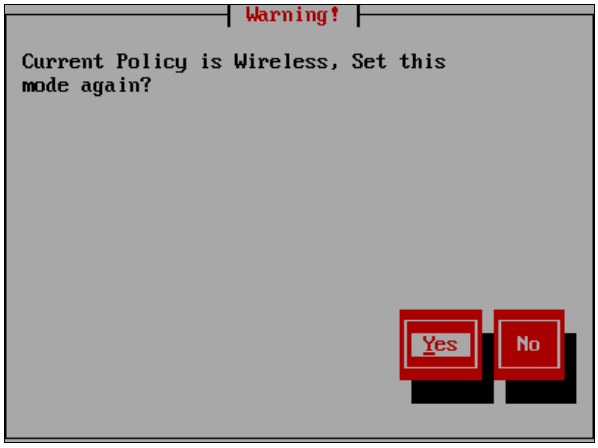
If this procedure fails, contact Oracle Technical Services and ask for assistance.

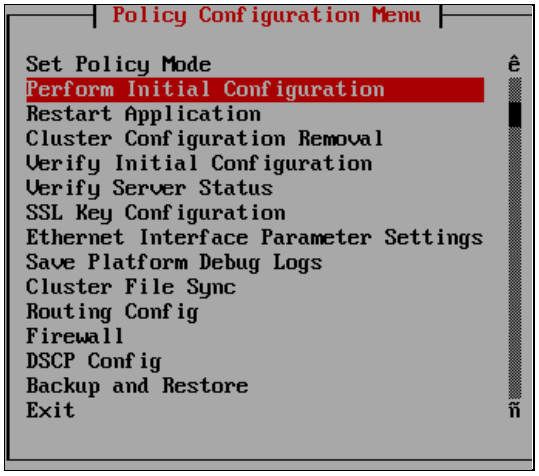
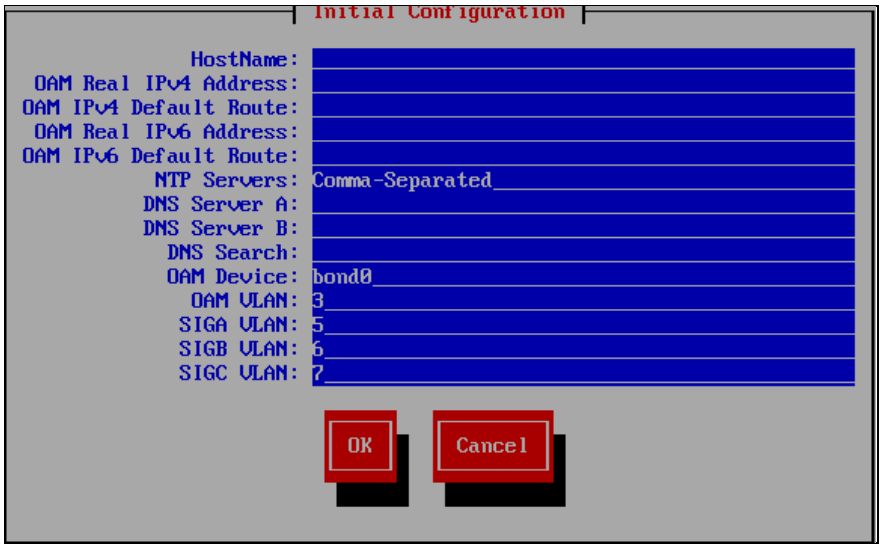
6.1: Perform Initial Server Configuration of Policy Servers—platcfg

Step	Procedure	Details
1. ☐	Login to server as root via Console	Access the iLO GUI, and open a Remote Console session then login as root **NOTE:** iLO procedures are found in section 7:Accessing the iLO VGA Redirection Window 

2. ☐	**Remote Console:** Verify the server type	Login as root, via the Remote Console, and confirm the installed Policy Management software version and server profile
		
		`# getPolicyRev`
		`# getPolicyRev -p`
		
		 
		
		The server profile is either cmp, mpe, mra

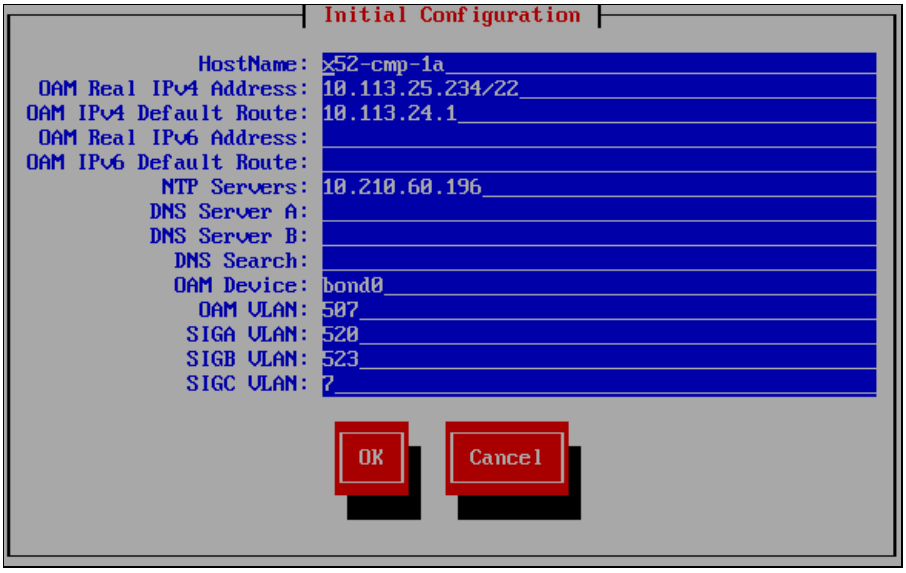
3. ☐	**Remote Console:** Login to platcfg	1. Open the platcfg utility by running the following command `# su -platcfg`  The platcfg tool opens 2. Select **Policy Configuration**  The Policy Configuration Menu opens 

Step	Procedure	Details
4. ☐	**Remote Console**: Set Policy Mode	1. Go to the **Select Policy Mode** menu 2. Select **Wireless** from the options.  3. Click **OK** Wireless is the default configuration. If the current policy mode is Wireless, this prompt is not displayed and Wireless mode is set. 4. Click **Yes**  Depending on the hardware configuration, a Select Network Layout screen may open. Refer to Configuration Management Platform Wireless User's Guide (Setting Policy Management Mode) for further detail. If the Select Network Layout screen does not display, you are returned to the Policy Configuration Menu.

Step	Procedure	Details
5. ☐	**Remote Console:** Perform Initial Configuration	From the Policy Configuration Menu, select **Perform Initial Configuration**  The initial configuration form opens 

Step	Procedure	Details
6. ☐	**Remote Console:** Perform Initial Configuration	Enter the configuration values and then click **OK**, where: • **HostName**—The unique name of the host for the device being configured. • **OAM Real IPv4 Address**—The IPv4 address that is permanently assigned to this device. • **OAM IPv4 Default Route**—The IPv4 default route of the OAM network. • **OAM Real IPv6 Address**—The IPv6 address that is permanently assigned to this device. • **OAM IPv6 Default Route**—The IPv6 default route of the OAM network. • **NTP Server** (required)—A reachable NTP server on the OAM network. • **DNS Server A** (optional)—A reachable DNS server on the OAM network. • **DNS Server B** (optional)—A second reachable DNS server on the OAM network. • **DNS Search**—the domain name appended to a DNS query • **OAM Device**—The bond interface of the OAM device. Note that the default value must be used because changing this value is not supported. • **OAM VLAN**—The OAM network VLAN ID (only applies to c-Class servers; field does not display otherwise). • **SIG A VLAN—**The Signaling-A network VLAN ID (only applies to c-Class servers; field does not display otherwise). • **SIG B VLAN** (optional)—The Signaling-B network VLAN ID (only applies to c-Class servers; field does not display otherwise). • **SIG C VLAN** (optional)—The Signaling-C network VLAN ID (only applies to c-Class servers; field does not display otherwise). **NOTE:** All of the fields listed above are required, except for fields DNS Server and DNS Search, which are optional but recommended. **NOTE:** Every network service and IP flow that is supported by IPv4 is supported by IPv6. Either interface or a combination of the two is configured.

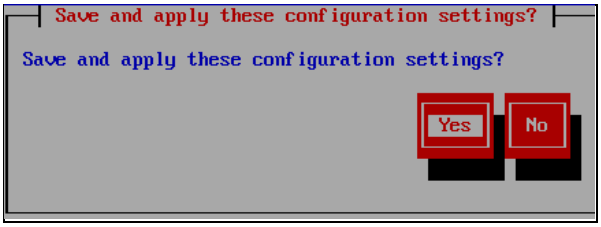
Step	Procedure	Details
7. ☐	**Remote Console:** Perform Initial Configuration	**For example:**



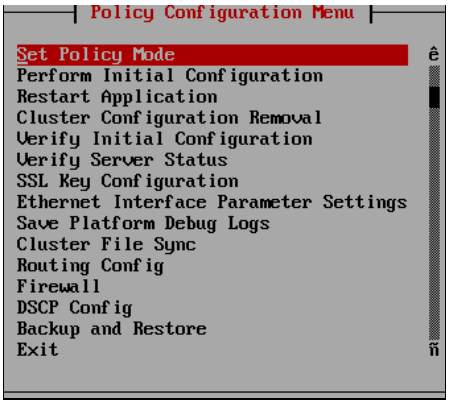
1. Enter the configuration information.
2. Click **OK** to save and apply the configuration.

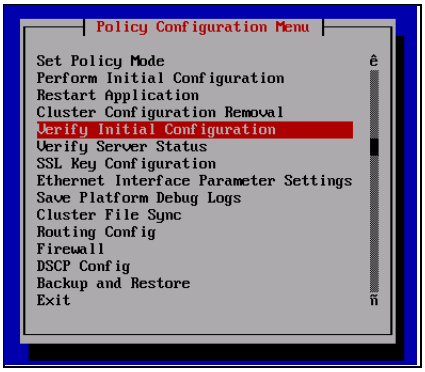
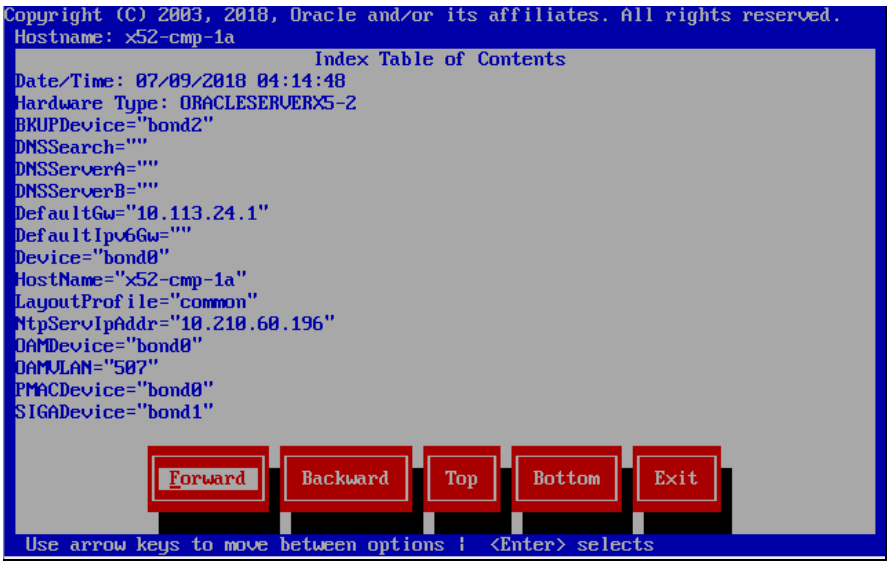
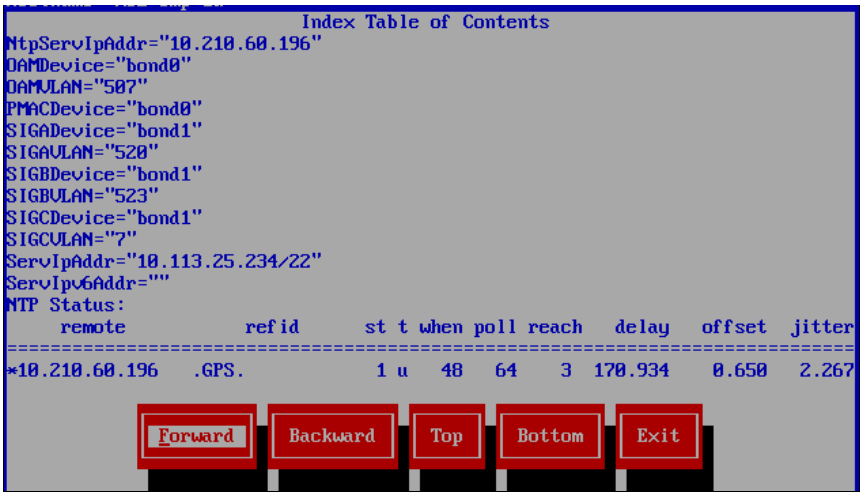
   At this point the screen pauses for approximately a minute. This is normal behavior.

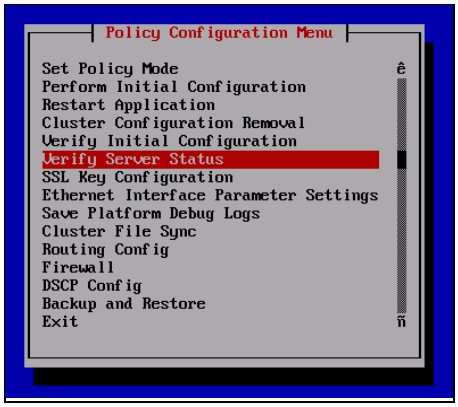
3. A confirmation message displays, click **YES** to save and apply the configurations.



The platcfg form processes the configuration of the server, and then it returns to the platcfg menu.



Step	Procedure	Details
8. ☐	**Remote Console:** Verify Initial Configuration	From the main menu navigate to **Policy Configuration → Verify Initial Configuration** from the platcfg utility.  A display similar to the following displays.  **NOTE:** The NTP status may not have updated. This is normal behavior. You may need to click **Forward** to view the NTP status. 

Step	Procedure	Details
9. ☐	**Remote Console:** Verify Server Status	Exit from this screen and select Verify Server Status:  The server must be in a running state. For example: **NOTES:** • At this point in the installation procedure, the Server Role is Unknown. Unknown is a valid state during initial configuration because the cluster is not formed. • If the product is MPE,the Policy Process Management Status is Not Running. Not Running is a valid state for MPE in this step. Cick **Exit** until you exit the platcfg utility. You are returned back to Linux prompt screen.

Step	Procedure	Details
10. ☐	Ping the OAM default gateway to verify server is available on the network	From the Linux command prompt ping the OAM gateway (default Gateway from the initial config procedure) to verify that the gateway is reachable. Ping the OAM gateway to verify that it is reachable: NOTICE - PROPRIETARY SYSTEM This system is intended to be used solely by authorized users in the course of legitimate corporate business. Users are monitored to the extent necessary to properly administer the system, to identify unauthorized users or users operating beyond their proper authority, and to investigate improper access or use. By accessing this system, you are consenting to this monitoring. x52-cmp-1a login: admusr Password: Last login: Sun Jul 8 22:19:39 on tty1 [admusr@x52-cmp-1a ~]$ ping 10.113.24.1 PING 10.113.24.1 (10.113.24.1) 56(84) bytes of data. 64 bytes from 10.113.24.1: icmp_seq=1 ttl=255 time=0.888 ms 64 bytes from 10.113.24.1: icmp_seq=2 ttl=255 time=0.744 ms 64 bytes from 10.113.24.1: icmp_seq=3 ttl=255 time=0.747 ms ^C --- 10.113.24.1 ping statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 2285ms rtt min/avg/max/mdev = 0.744/0.793/0.888/0.067 ms [admusr@x52-cmp-1a ~]$ If the gateway is reachable it is possible to SSH to the server IP and login as admusr If you cannot SSH to the configured server or cannot reach the OAM gateway, review the initial configurations and review the network setup to ensure there are not any connectivity issues. Run `ip -4 addr` (IPv4) or `ip -6 addr` (IPv6) to confirm the IP addresses configured during the initialization are present.

Step	Procedure	Details

11. ☐	Verify NTP connectivity	**NOTE:** Server sync to Network Time Protocol (NTP) is very important to the later steps in this install.
		
		4. To sync and verify NTP server connectivity, perform these steps:
		
		`# ntpq -pn`
		
		`[admusr@x52-cmp-1a ~]$ ntpq -pn`
		`  remote  refid  st t when poll reach  delay  offset  jitter`
		`==========`
		`*10.210.60.196  .GPS.  1 u  40  64  377  171.111  23.933  14.560`
		`[admusr@x52-cmp-1a ~]$`
		
		The * (asterisk) next to the NTP server IP indicates the NTP server is in sync.
		
		If the asterisk is not there, you can manually sync with NTP server:
		
		`# service ntpd stop`
		`# ntpdate <ntpserver address>`
		
		Bad response: 26 Jun 16:47:25 ntpdate[16364]: no server suitable for synchronization found
		
		Good response:
		
		`[root@x52-cmp-1a ~]#`
		`[root@x52-cmp-1a ~]# service ntpd stop`
		`Shutting down ntpd:  [ OK ]`
		`[root@x52-cmp-1a ~]# ntpdate 10.210.60.196`
		`9 Jul 04:31:43 ntpdate[10282]: adjust time server 10.210.60.196 offset 0.097114 sec`
		`[root@x52-cmp-1a ~]#`
		
		`# service ntpd start`
		
		If `ntpdate` has a bad response, follow up to get the needed networking, firewalls and permissions to solve this connectivity issue with the NTP server.
		
		NOTE: `ntpdate` is an emergency utility; use only when you see significant time difference between system and the actual time.

12. ☐	Repeat on remaining servers	Repeat this procedure on all Policy component servers that are planned for service. If your system is georedundant, repeat this procedure for site1 and site2 Policy servers
—End of Procedure—		

6.2 Perform Initial Configuration of the Policy Servers—CMP GUI

This procedure performs initial configuration of the CMP GUI on the installed environment.

NOTE: In a deployment that has Geo-Redundant CMP servers (that is, CMP servers at two different sites), the other pair of CMP servers are added to the network topology using the CMP server at Site 1. The CMP Site 1 cluster pushes the configuration to the Site 2 (Geo-Redundant) CMP servers later.

This procedure configures the CMP at the active site (CMP Site 1).

Prerequisites:

- Network access to the CMP OAM REAL IP address, to open a web browser (HTTP)
- If network access to the CMP is not available and the installation has an Aggregation switch, then a laptop is configured to use a port on the Aggregation switch to access the CMP GUI. If an

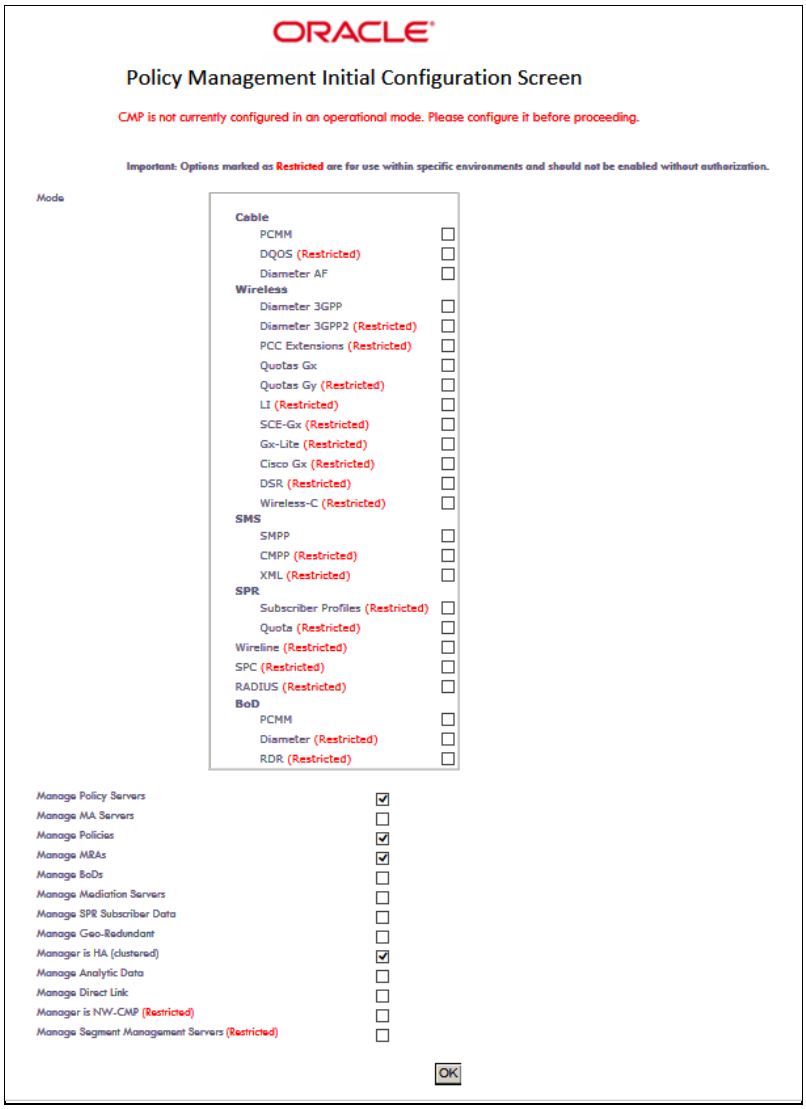
Aggregation switch is not available, a temporary switch may be used to provide network access to the CMP GUI.

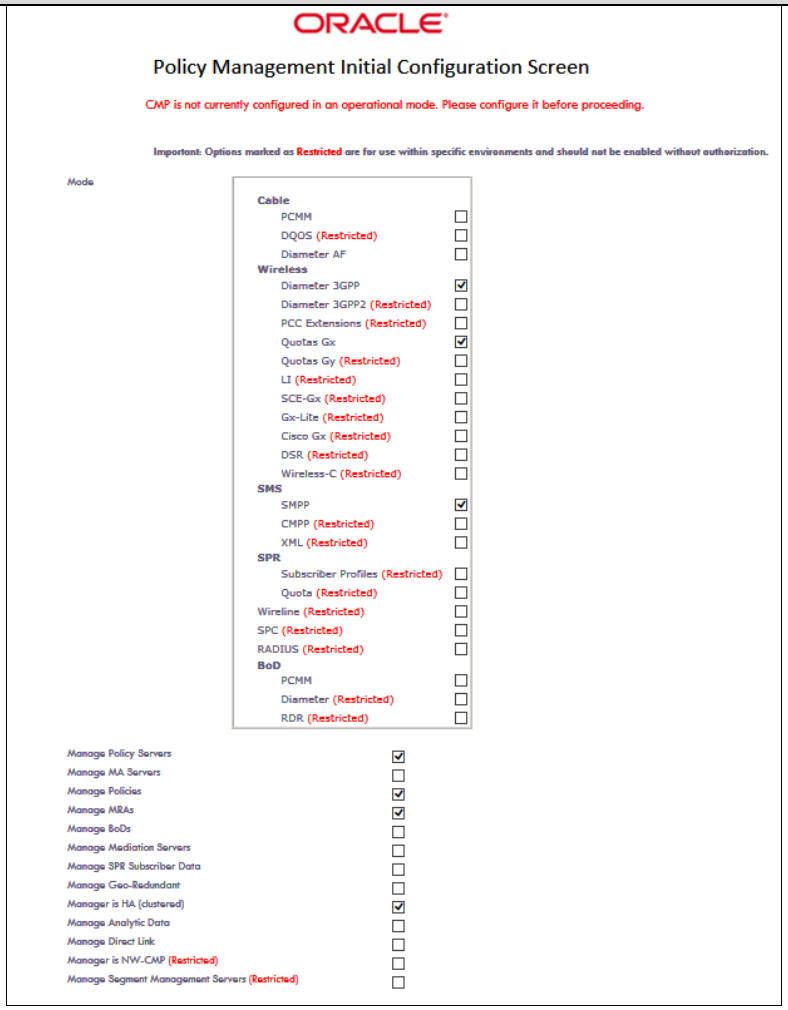
Check off (√) each step as it is completed. Check boxes are provided next to each step number.

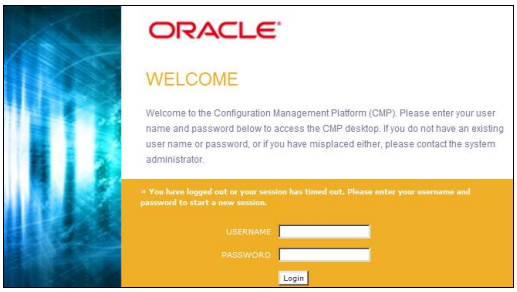
If this procedure fails, contact Oracle Technical Services and ask for assistance.

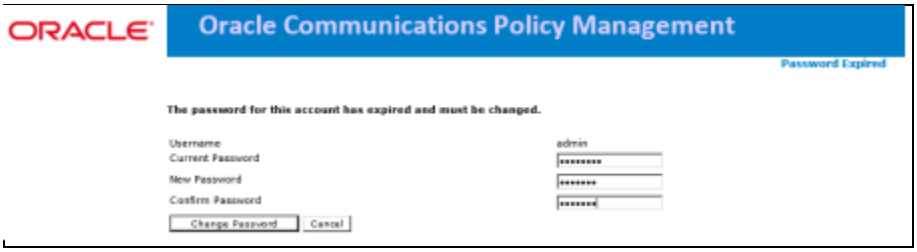
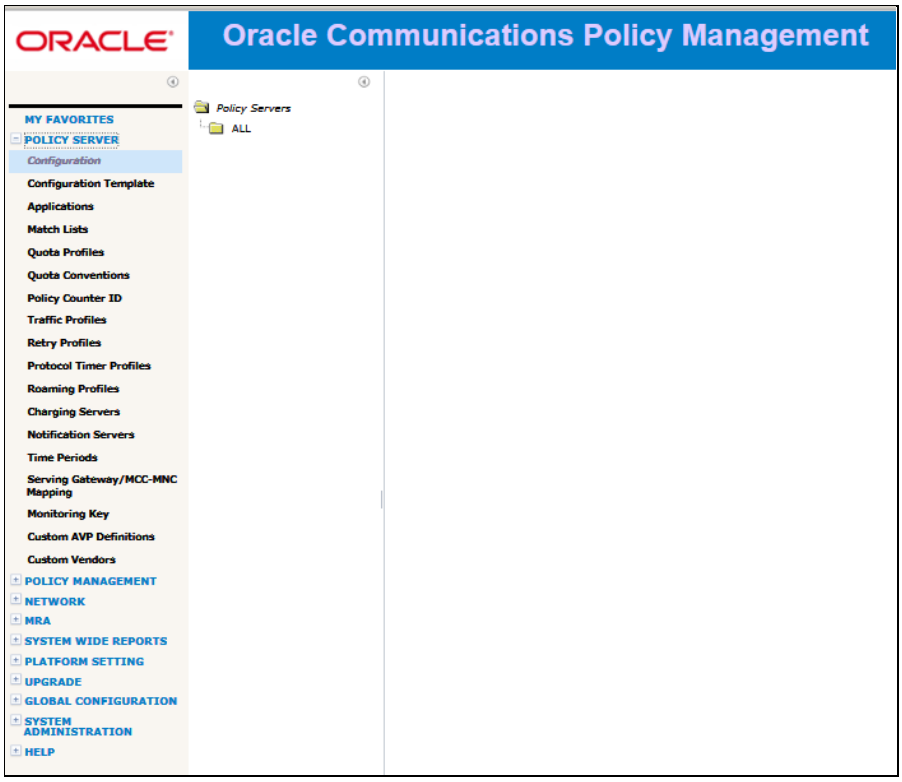
6.2: Perform Initial Configuration of the Policy Servers—CMP GUI

Step	Procedure	Details
1. ☐	CMP GUI	Open CMP GUI for the first time by opening the CMP OAM IP address in a supported browser: `http://<cmp_real_OAM_ip>` **NOTE:** The initial GUI configuration is performed on either CMP that is located at Site1. If this is not a geo-redundant solution, there is not a Site 2 location. If Network access is not enabled and the Installation has an Aggregation switch, then a laptop is configured to use a port on the Aggregation switch to access the CMP GUI. Alternately, if an Aggregation switch is not available, a temporary Aggregation switch may be needed during installation.

Step	Procedure	Details
2. ☐	**CMP GUI**: Set CMP Mode in 1st selected CMP	After you are connected to the CMP GUI for the first time, you are prompted to configure operation mode settings for the system, which define what functionality is configurable from the CMP GUI. The selection depends on the deployment. The Policy Management Initial Configuration Screen presents as follows:  **NOTE:** Modes are changed at a later time if needed, but the method to access to this mode selection is not documented.] Contact Oracle Support if Mode selection is changed after the initial configuration.
3. ☐	**CMP GUI:** Set CMP Mode in 1st selected CMP	This configuration example provides basic functionality for a Policy Wireless solution. The wireless mode of operation was confirmed in earlier procedures. (Selections are for example only). For more detail, refer to the CMP Modes section of the [Configuration Management Platform Wireless User's Guide]

Step	Procedure	Details
		 **NOTE:** Restricted mode options are only selected with the advice of an Oracle Support representative. The following examples are for reference only. The particular requirements for any given configuration may be specific a customer. **For a Wireless network:** • Wireless: Diameter 3GPP • Quotas Gx • Manage Policy Servers • Manage Policies • Manage MRAs • Manage Geo-Redundant • Manager is HA (clustered) **For a Wireless-C network:** • Wireless: Diameter 3GPP, Quotas Gx, DSR, Wireless-C; SMS: CMPP • Manage Policy Servers • Manage Policies • Manage MRAs • Manage SPR Subscriber Data

Step	Procedure	Details
		• Manager is HA (clustered) **About using Wireless-C Mode:** Wireless-C supports a wireless system supporting SMS Notification Statistics and SCTP counters **Additional Information:** **Diameter 3GPP, 3GPP2**(Restricted) and **Gx-Lite** (Restricted) enable the functionality required to support these protocols in a Policy Management solution **LI** (Restricted) is used if the MPE installation uses LI (Lawful Intercept) functions. To use this option, the LI version of the MPE ISO image must be installed on the MPEs in the Policy Management solution. Contact Oracle Support for additional Information. **Manage Policy Servers** and **Manage Policies** are basic functions of the Policy Management solution **Manage MRAs** is only needed if MRAs, which are optional, are planned in the deployment **Manager is HA (clustered)** provides High Availability functionality for a clustered pair of servers. **Manager is NW CMP** and **Manager is S-CMP** are specific to a Tiered CMP System deployment. Refer to Configuration Management Platform Wireless User's Guide for the procedure to deploy a Tiered CMP System. **NOTE:** The mode selections on this form depend on the deployment. Conform the selections with the engineering team responsible for the planned Policy Management solution deployment.
4. ☐	**CMP GUI:** Login to CMP GUI	After finishing the policy mode selection and clicking **OK**, login screen displays. 

Step	Procedure	Details
5. ☐	**CMP GUI:** Set admin password	**Initial, default login is admin/policies** After login, the system prompts you to change the admin password.  Enter the default password then the new password twice and click **Change Password**.
6. ☐	**CMP GUI:** Verify that the CMP GUI is displayed, with expected menus.	
—End of Procedure—		

6.3 CMP Site1 Cluster Configuration

This procedure performs the initial configuration of the CMP GUI, CMP Site 1 cluster

You must configure the active site (Site 1) CMP cluster.

NOTE: In a deployment that has Geo-Redundant CMP servers (that is, CMP servers at two different sites), the other pair of CMP servers are added to the network topology using the CMP server at Site 1. The CMP Site 1 cluster pushes the configuration to the Site 2 (Geo-Redundant) CMP servers later.

Prerequisites:

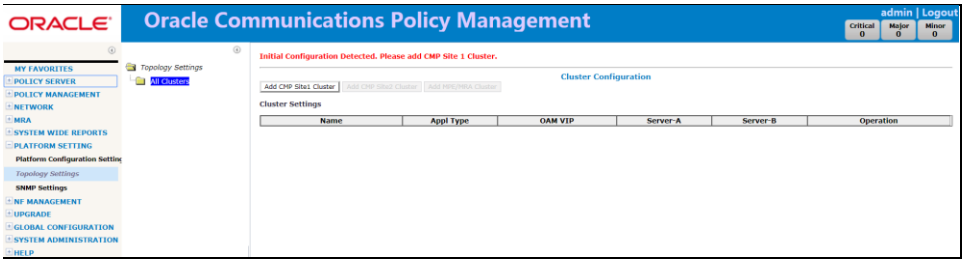
To complete this procedure, you need the following information:

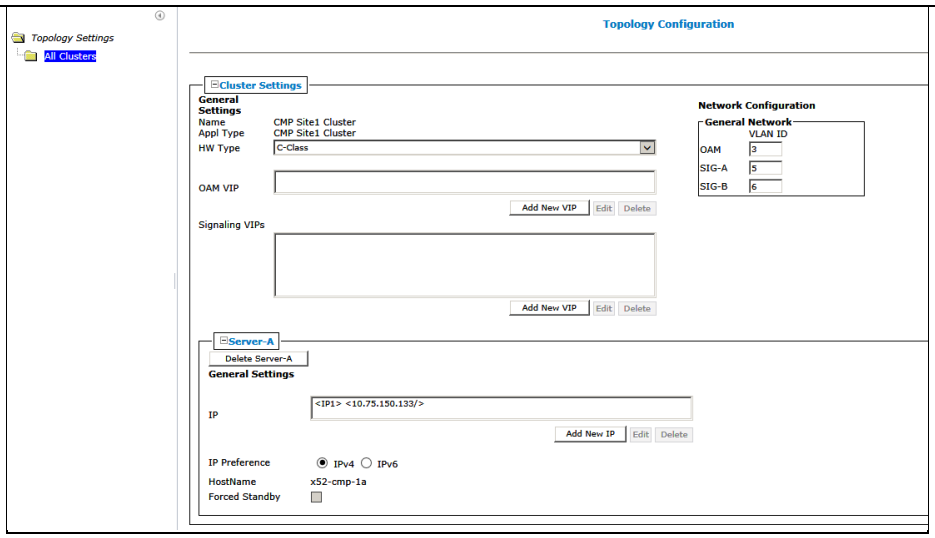
- OAM VIP—IP address and netmask for the cluster VIP address on the OAM network.
- Hostname—The names you choose for each server in the cluster.
- Signaling VIPs (optional)—Up to four IPv4 or IPv6 addresses and netmasks of the signaling VIP addresses. For each, select None, SIG-A, SIG-B, or SIG-C to indicate whether the cluster uses an external signaling network. If you specify either SIG-A, SIG-B, or SIG-C you must enter a Signaling VIP value.
- The admin password (cmp_password) you defined.
- Cluster Name—The name you choose for the CMP cluster (the default is CMP Site 1 cluster).
- HW Type—Determines whether VLANs are required. If you select c-Class, c-Class (segregated traffic), or VLANs are required.
- Network VLAN IDs—The values designated during the Initial Configuration done with placfg.
- SNMP configuration (optional)—snmp_sys_location (the enclosure name), snmp_community_string (the community string), and snmp_trap_destination (the trap destination), which you defined.
- Network access to the CMP OAM IP address, to open a web browser (HTTP)

Check off (√) each step as it is completed. Check boxes are provided next to each step number.

If this procedure fails, contact Oracle Technical Services and ask for assistance.

6.3: CMP Site1 Cluster Topology Configuration

Step	Procedure	Details
1. ☐	**CMP GUI**: View Topology Settings	**NOTE:** Only the following Web Browsers are supported in Oracle Communications Policy Management 12.6 • Mozilla Firefox® release 81.0 or later • Google Chrome version 86.0 or later *Internet Explorer in not supported for this procedure Navigate to **Platform Settings → Topology Settings → All Clusters** The initial form opens, and display a message that initial configuration detected and CMP Site 1 cluster is added. 
2. ☐	**CMP GUI:** Add CMP Site 1 cluster—Server A	1. Click **Add CMP Site 1 Cluster**. The Topology Configuration form is displayed.



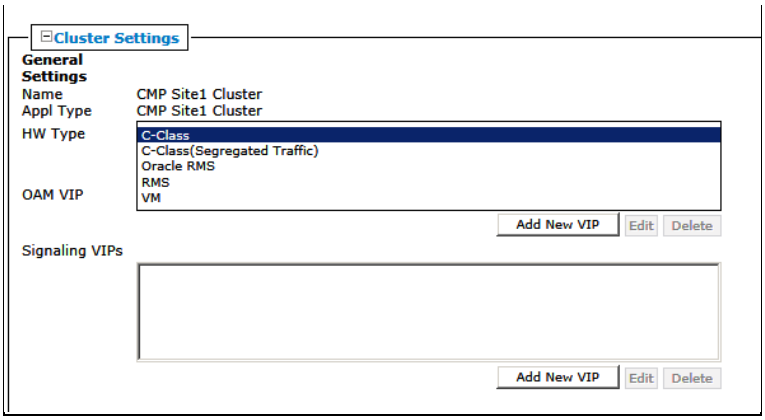
In this form, the CMP cluster is given a name, and certain characteristics of the cluster are defined.

This form defines a VIP address assigned to the active server in the cluster.

Complete the form according to the system design.

Define the Cluster Settings

2. Select the HW Type from the list



Available options are:

- C-Class (default)—HP Enterprise ProLiant BL460 Gen8/Gen9 server
- C-Class (segregated traffic) (a configuration where Signaling and other networks are separated onto physically separate equipment)—HP Enterprise ProLiant BL460 Gen8/Gen9
- RMS (for a rack-mounted server not using VLANs)

If you selected C-Class, C-Class (segregated traffic), enter the General Network—VLAN IDs.

3. Enter the OAM, SIG-A, and SIG-B (optional) virtual LAN (VLAN) IDs.

   VLAN IDs are in the range 1 through 4095. The default values are:

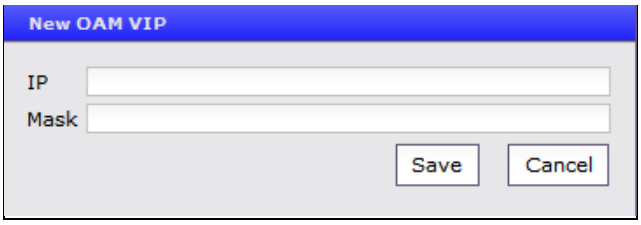
   - OAM—3
   - SIG-A—5

- SIG-B—6

4. Click **Add New VIP**.

   The New OAM VIP window opens.

5. Enter the OAM VIP and the mask.



   This is the IP address the CMP server uses to communicate with a Policy Management cluster.

   NOTE: Enter the IPv4 address in standard dot format and its subnet mask in CIDR notation from 0 to 32, or the IPv6 address in standard 8-part colon-separated hexadecimal string format and its subnet mask in CIDR notation from 0 to 128.

6. Click **Save**.

   The OAM VIP and mask are saved. Repeat this step for a second OAM VIP, if needed.

   NOTE: Typically Signaling VIPs are not added to the CMP

Define the settings for Server-A in the Server-A section of the page

The IP address and hostname of Server-A are the IP address and hostname configured during the Initial Configuration of the server in section 6.1 of this document. The IP address and hostname must match exactly. If Server-A is network reachable from the CMP it is recommended to click **Load** after the IP address and IP preference are defined. The CMP attempts to load the hostname from the IP reachable server. This confirms network connectivity and minimizes the possibility of incorrectly defining the hostname.

To configure Server-A, in the Server-A section of the page:

7. (Required) Click **Add New IP** to enter the IP address.

   The Add New IP window opens.

8. Enter the IP address in either IPv4 or IPv6 format.

   This is the IP address of the server. For an IPv4 address, enter it in the standard IP dot-format.

   For an IPv6 address, enter it in the standard 8-part colon-separated hexadecimal string format.

9. Select the IP Preference: IPv4 or IPV6.

   The server uses the IP address in the specified format for communication.

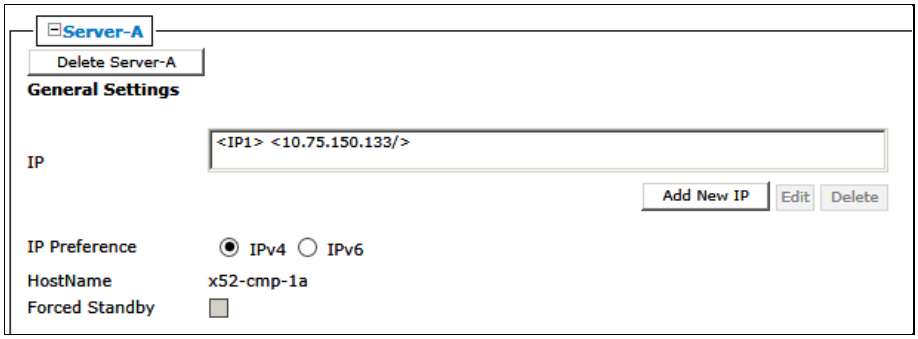
   - If neither an IPv6 OAM IP nor a static IP address is defined, IPv6 cannot be selected.
   - If neither an IPv4 OAM IP nor a static IP address is defined, IPv4 cannot be selected.

10. Enter the HostName of the server.

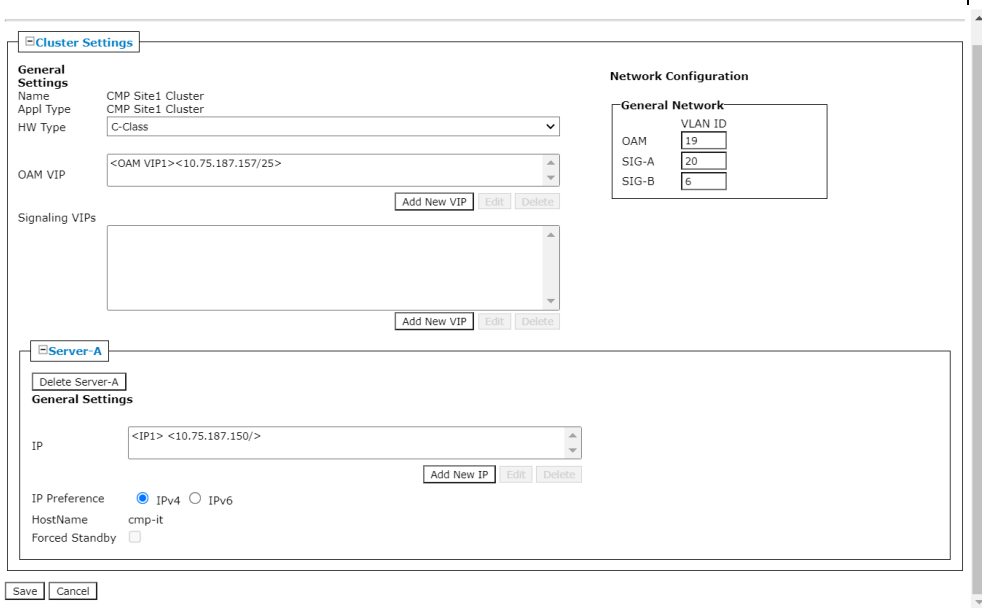
This must exactly match the host name provisioned for this server (the output of the `uname -n` Linux command).

NOTE: If the server has a configured server IP, you can click Load to retrieve the remote server host name. If the retrieve fails, this a sign that the ip address configured is not accessible across the network. Alternately, you may enter the host name manually but it is recommeneded to do any network troubleshooting that may be required.

Server-A example:

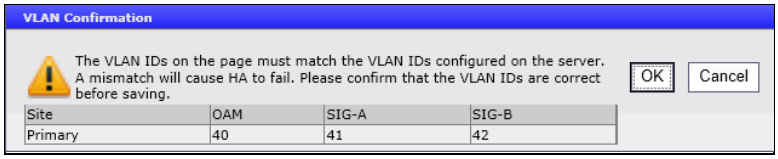


Topology Configuration of the HW Type C-Class example:



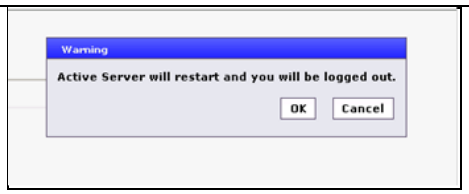
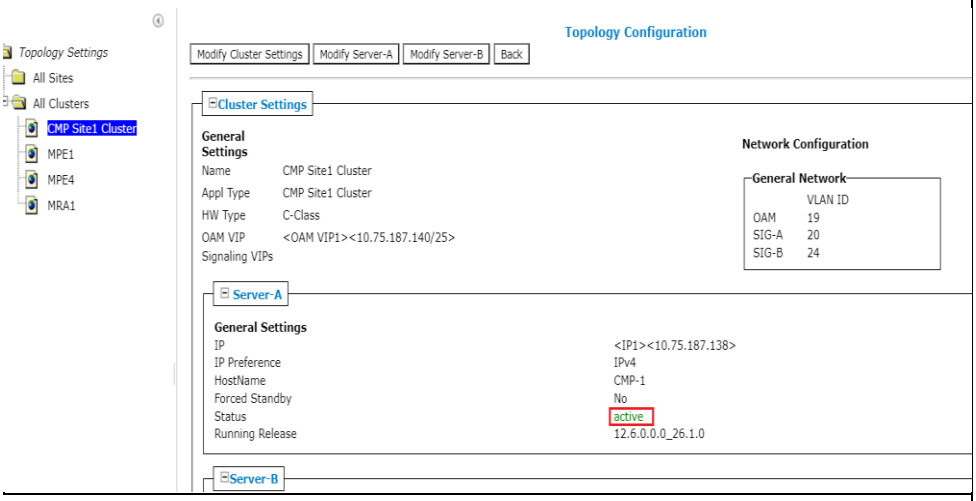
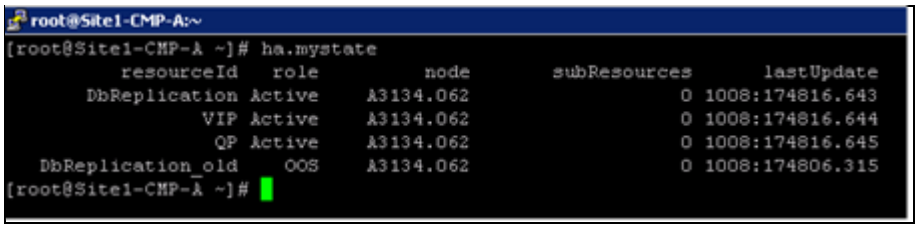
11. When done, click **Save** and the click **OK**.

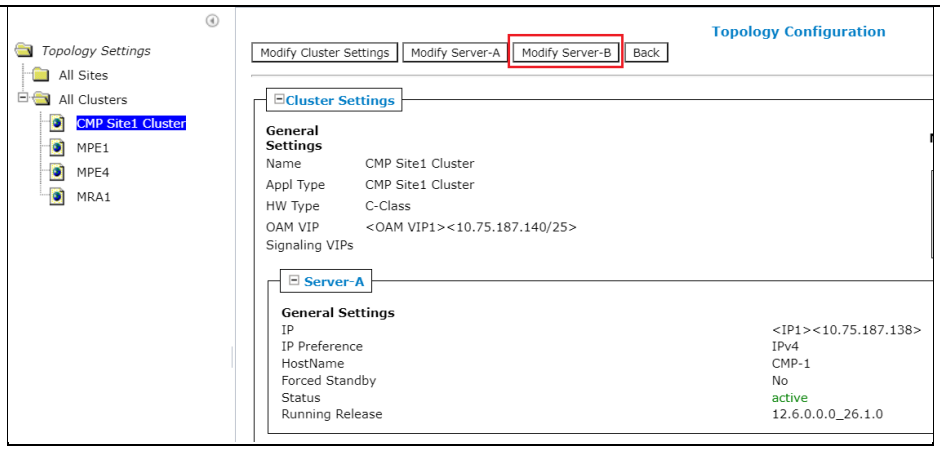
    If the configuration contains VLAN IDs, you are prompted to confirm the VLAN IDs.



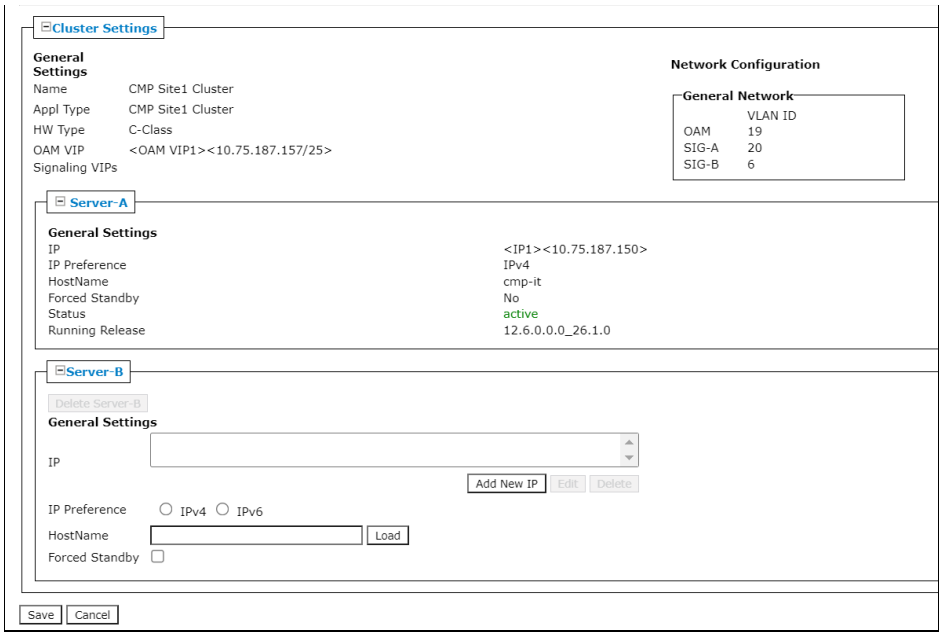
    Then the following confirmation prompt displays.

12. Click **OK**

		 At this point you are logged out of CMP GUI.
3. ☐	**CMP GUI**: Login using the CMP cluster VIP.	After the Topology Configuration is saved, the CMP VIP address is taken by the active CMP server of the cluster. This may take a minute. 1. Login to the CMP GUI using the VIP address. 2. Navigate to **Platform Settings →Topology Settings → All Clusters → CMP Site1 Cluster**  3. Verify the configured CMP server is in Active state
4. ☐	**SSH to CLI**: If the CMP VIP is not available	SSH to the CMP real IP address of the CMP server to confirm the server role is active. `# ha.mystate`  **NOTE:** DbReplication_old with role OOS is not an indication of a problem and is ignored. It is still possible to login to the CMP server with its Real IP address, if needed, to verify that the Topology Configuration.
5. ☐	**CMP GUI:** Modify CMP Site 1 cluster—add Server B	**Modify CMP Site 1 Cluster—add Server B** 1. Navigate to **Menu →Platform Settings → Topology Settings** 2. Click **View** for CMP Site 1 cluster 3. Click **Modify Server B**



The Topology Configuration opens the Server-B for configuration.



Define the settings for Server-B in the Server-B section of the page

To configure Server-B, in the Server-B section of the page:

4. (Required) Click **Add New IP** to enter the IP address.

   The Add New IP window opens.

5. Enter the IP address in either IPv4 or IPv6 format.

   This is the IP address of the server. For an IPv4 address, enter it in the standard IP dot-format.

   For an IPv6 address, enter it in the standard 8-part colon-separated hexadecimal string format.

6. Select the IP Preference: IPv4 or IPV6.

   The server uses the IP address in the specified format for communication.

   - If neither an IPv6 OAM IP nor a static IP address is defined, IPv6 cannot be selected.

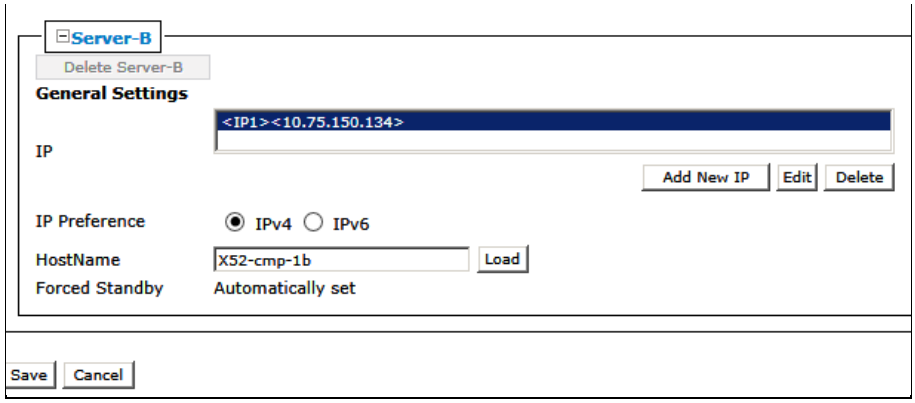
- If neither an IPv4 OAM IP nor a static IP address is defined, IPv4 cannot be selected.

7. Enter the HostName of the server.

   This must exactly match the host name provisioned for this server (the output of the `uname -n` Linux command).

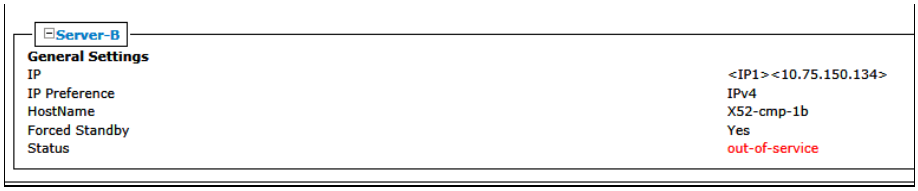
   NOTE: If the server has a configured server IP, you can select the server IP and click Load to retrieve the remote server host name. If the retrieve fails, this a sign that the ip address configured is not accessible across the network. Alternately, you may enter the host name manually but it is recommeneded to do any network troubleshooting that may be required.

Example of Site1 CMP Cluster Server B Topology Configuration



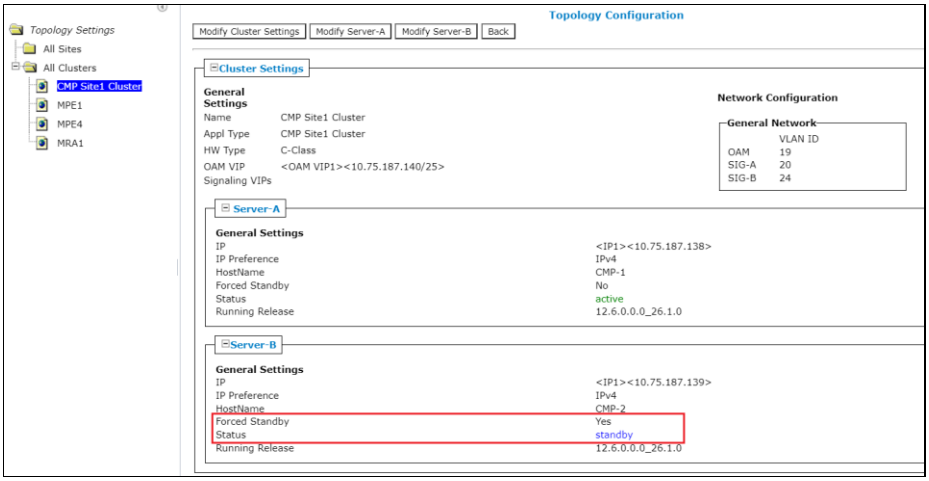
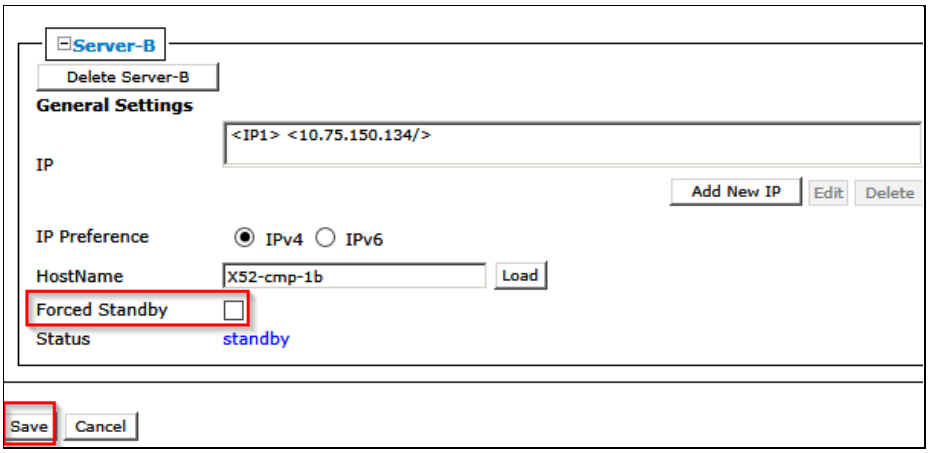
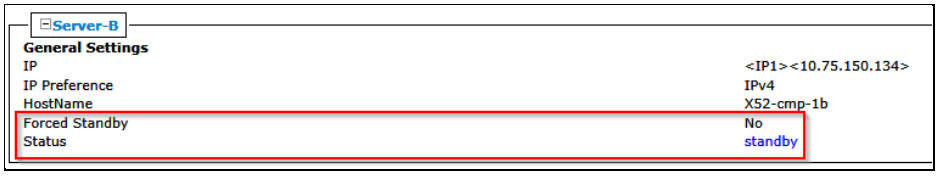
8. Click **Save** and then click **OK** on the confirmation message.

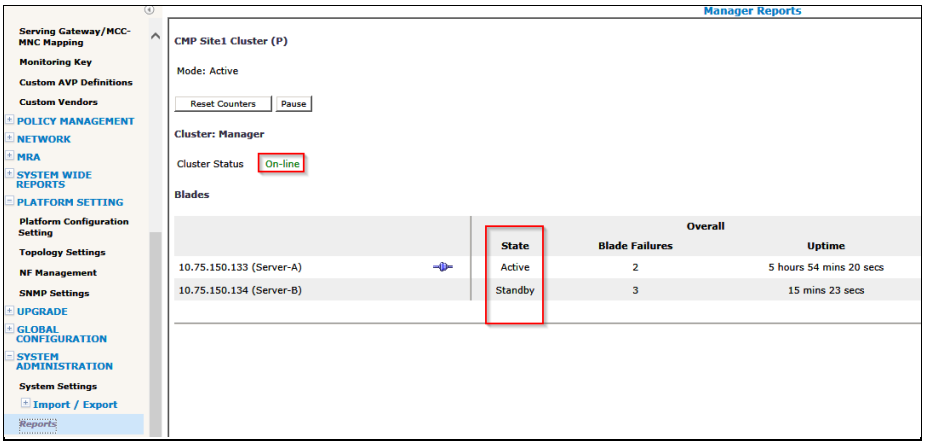
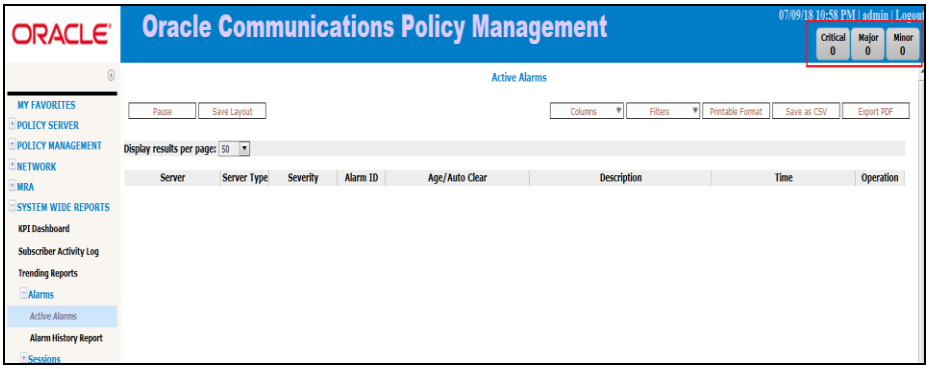
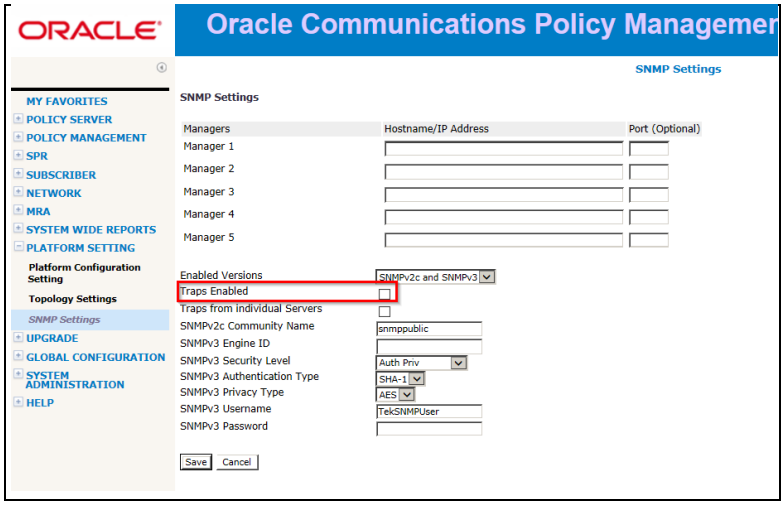
The server statusis out-of-service for few minutes and that is expected until the cluster forms.



NOTE: Wait for any alarms to clear. This takes approximately 5 minutes

31282	The HA manager (cmha) is impaired by a s/w fault

6. ☐	**CMP GUI:** Verify Server B is added	1. Refresh the CMP GUI screen: **Topology Settings → CMP Site 1 Cluster**  2. Verify status is: Forced Standby is set to `Yes` (automatically set when entering CMP Server-B information). 3. Status si `standby` (after refreshing the page).
7. ☐	**CMP GUI:** Remove force standby on Server B	1. Click **Modify Server-B** 2. Clear **Force Standby**.  3. Click **Save** and then click **OK** to the confirmation message. Verify status in the General Setting is: • Forced Standby is set to No • Status is set to standby 

8. ☐	**CMP GUI:** Verify CMP cluster	1. Navigate to **SYSTEM ADMINISTRATION → Reports**. 2. Verify both CMP servers are present , with one in the Active state and the other in the Standby state. Also the status of the cluster is On-line. 
9. ☐	**CMP GUI:** Verify CMP cluster	1. Navigate to **SYSTEM WIDE REPORTS → Active Alarms** 2. Verify that there are not any active alarms on CMPs. 
10. ☐	**CMP GUI:** Add SNMP Servers	1. Navigate to **PLATFORM SETTING → SNMP Settings** 2. Enter the configuration information for the SNMP destination, version, and community string. 3. Click **Save**. 

		NOTE: Clear **Traps Enabled** until you are ready to go live.
—End of Procedure—		

6.4 Configuring Additional Clusters

You must configure the management relationships between the active-site CMP cluster and the other servers and the cluster assignments. After you complete these procedures, the status of the servers is available from the CMP system.

You can configure clusters at remote sites even if those sites are not fully networked or configured. In this case the CMP system reports alarms and continues to try to establish the management services to the clusters until it can reach them. When the clusters become available, the CMP system updates status and the alarms clear.

NOTE: For the full management relationships established, certain IP network services are allowed between the CMP Site 1 cluster and the other clusters in the network. Incorrectly configured firewalls in the network cause the management relationships to fail and alarms are raised at the CMP system.

6.4.1 Adding a CMP Site2 Cluster for CMP Geo-Redundancy

This procedure configures a Geo-Redundant CMP Site2 cluster. After this procedure a Site2 CMP cluster is visible on the CMP GUI: **Platform Setting → Topology Settings**

IMPORTANT: Certain IP network services must be allowed between the CMP Site1 cluster and the CMP Site2 cluster in the network in order to establish the geo-redundant CMP relationship. Incorrectly configured firewalls in the network can cause issues. It is recommended that any network issues are resolved before performing this procedure.

Prerequisites:

Before beginning this procedure, verify that you have HTTP access to the CMP server. The Policy Management CMP software must be installed on the target servers which form the CMP Site2 cluster and they are configured with network time protocol (NTP), IP routing, and OAM IP addresses. See Section 5:Preparing the System Environment in this document.

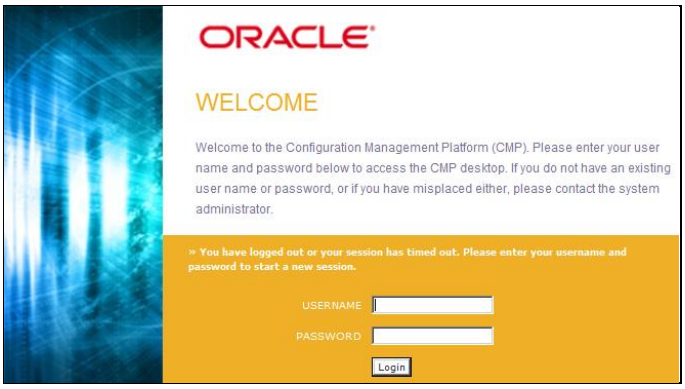
To complete this procedure, you need the following:

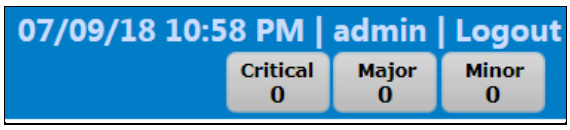
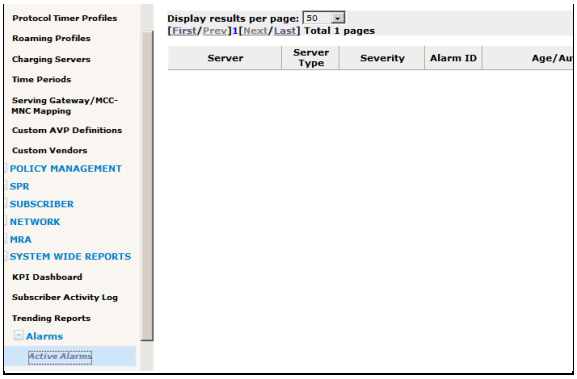
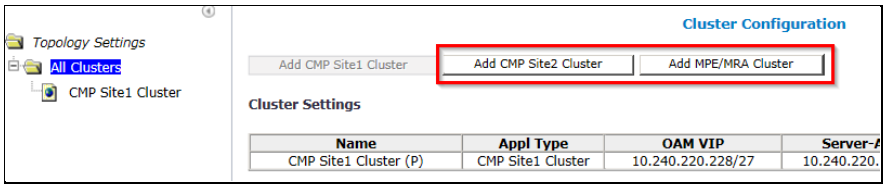
- HW Type—Determines whether VLANs are required. If you select c-Class, c-Class (segregated traffic), or VLANs are required.
- OAM VIP—The IP address and netmask the CMP cluster uses to communicate with an MPE or MRA cluster.
- Network VLAN IDs (depends on HW Type)—The values designated during the Initial Configuration done with placfg.
- The information that you configured for the CMP Site 1 cluster.

Check off (√) each step as it is completed. Check boxes are provided next to each step number.

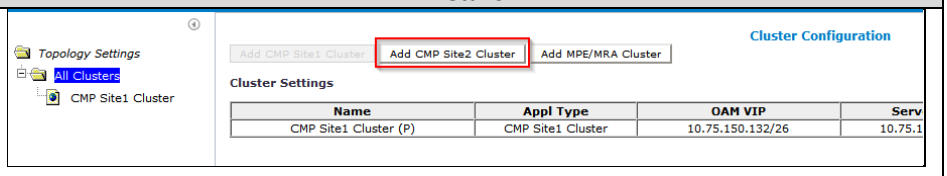
If this procedure fails, contact Oracle Technical Services and ask for assistance.

6.4.1: Adding a CMP Site2 Cluster for CMP Geo-Redundancy

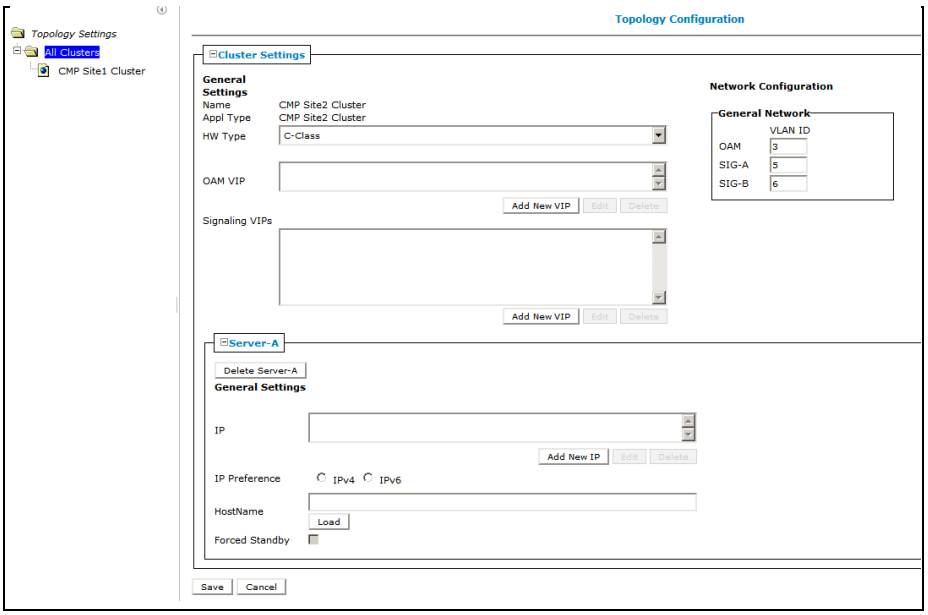
Step	Procedure	Details
1. ☐	**CMP GUI:** Login to CMP Server GUIs (using VIP)	1. Open a browser. 2. Enter the CMP server VIP for the navigation string. **NOTE:** Only the following Web Browsers are supported in OCPM 12.6 - Mozilla Firefox® release 81.0 or later - Google Chrome version 86.0 or later *Internet Explorer in not supported for this procedure  Login as admin (or a user with administrative privileges).

Step	Procedure	Details
2. ☐	**CMP GUI**: View active alarms	It is recommended to View the active alarms in the system before performing Configuration work. Check the alarm information and determine if any alarms are present that may affect configuration activies. You can view the alarms by: • Using the CMP GUI upper right banner  • Navigating to **System Wide Reports → Active Alarms**.  *IMPORTANT:* ***In Policy 12.6, there is help provided for alarm descriptions.*** - In the Alarm views, click the alarm ID to open the alarm description help page. – Alternatively, from the menu select **On-Line Help**, and select Troubleshooting Guide. Search this for the alarm ID.
3. ☐	**CMP:** View topology settings	Navigate to **PLATFORM SETTINGS → Topology Settings**  The Topology Settings screen allows for the selection of adding a CMP Site2 cluster (used for CMP cluster georedundancy) or adding an (MPE/MRA) cluster. **Note:** Adding a CMP Site2 cluster does not require that the Manage Geo-Redundant option is selected. This option is for adding Geo-Redundant MPE, MRA clusters.
4. ☐	**CMP GUI:** Add Site 2 CMP cluster	**Adding a CMP Site2 CMP cluster is optional.** If the Policy Management solution design calls for georedundant CMP clusters, the Site 2 CMP cluster must be configured from the CMP Site1 cluster GUI. 1. Navigate to **PLATFORM SETTINGS →Topology Settings**

Step	Procedure	Details



2. Click **Add CMP Site2 Cluster** and the Topology Configuration from presents



Complete the form according to the system design.

Define the Cluster Settings

3. Select the HW Type from the list

   Available options are:

   - C-Class (default)—HP Enterprise ProLiant BL460 Gen8/Gen9 server
   - C-Class (segregated traffic) (a configuration where Signaling and other networks are separated onto physically separate equipment)—HP Enterprise ProLiant BL460 Gen8/Gen9
   - RMS (for a rack-mounted server not using VLANs)

   If you selected C-Class, C-Class (segregated traffic), enter the General Network—VLAN IDs.

4. Enter the OAM, SIG-A, and SIG-B (optional) virtual LAN (VLAN) IDs.

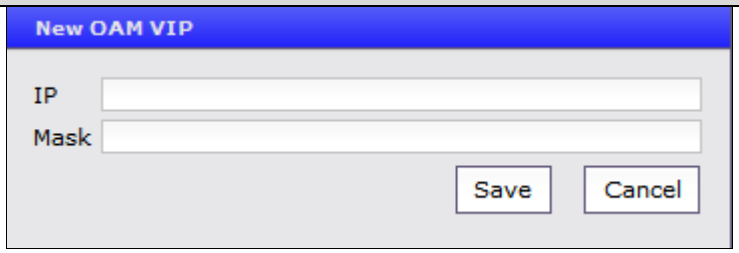
   VLAN IDs are in the range 1 through 4095. The default values are:

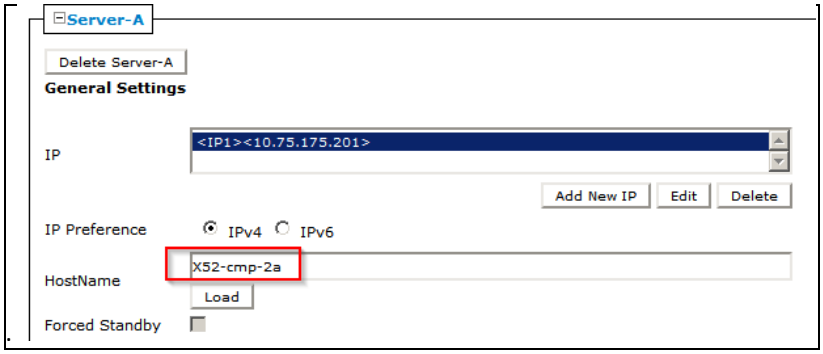
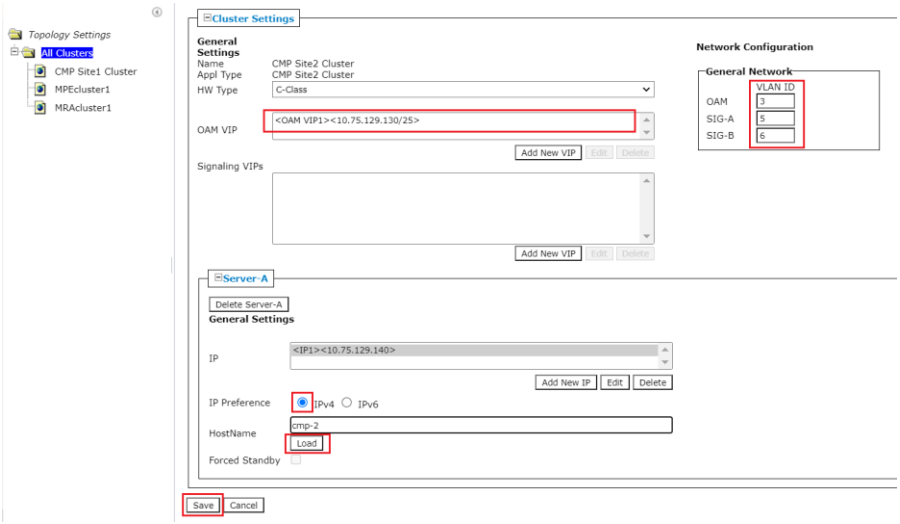
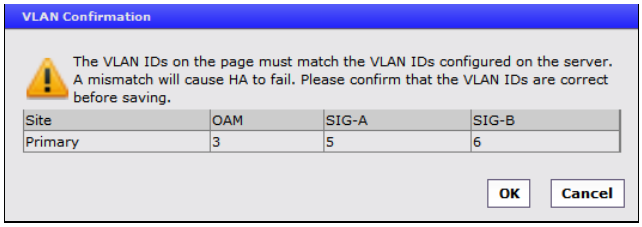
   - OAM—3
   - SIG-A—5
   - SIG-B—6

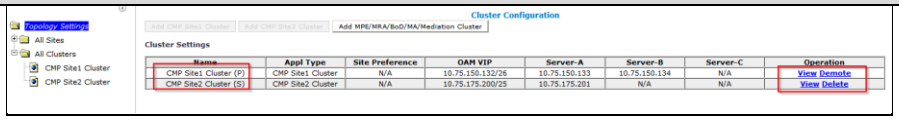
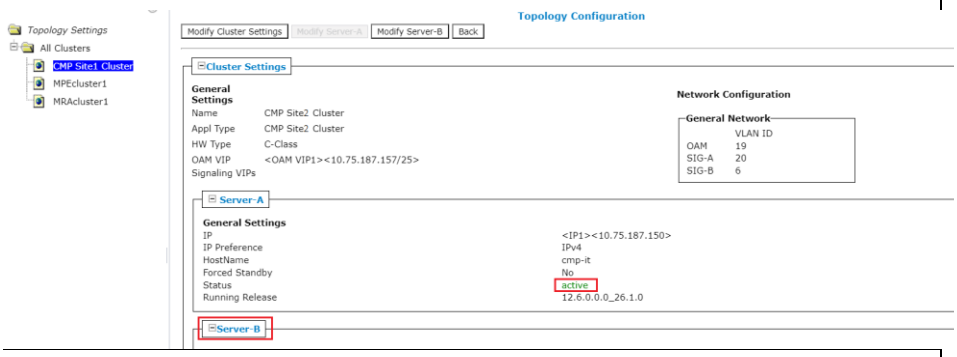
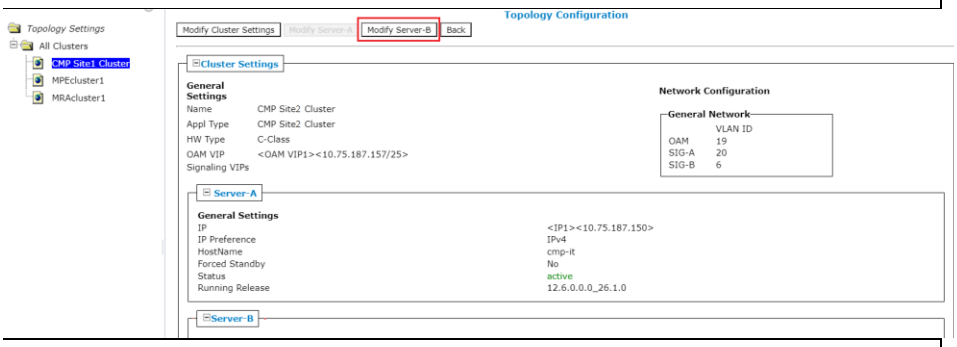
5. Select OAM VIP **Add New VIP**.

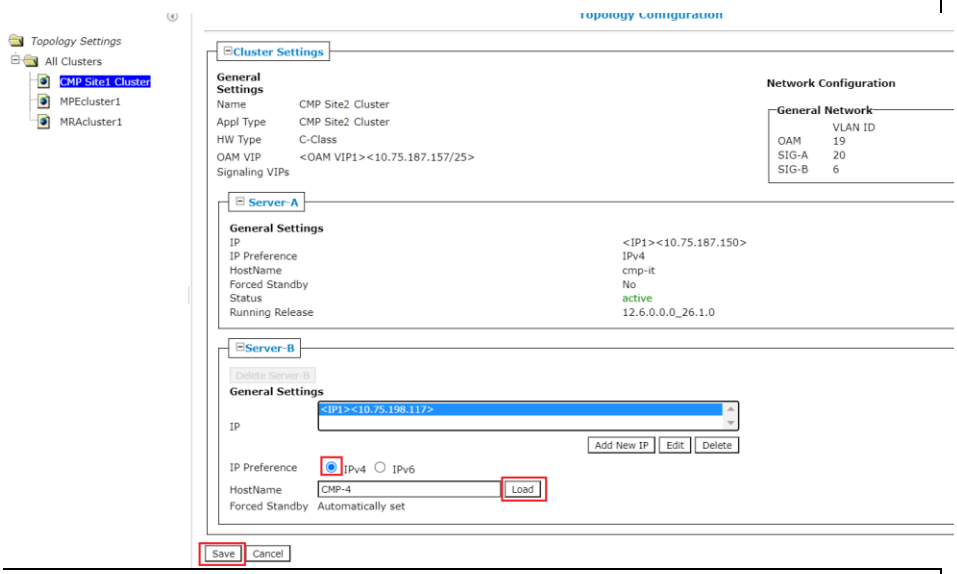
   The New OAM VIP window opens.

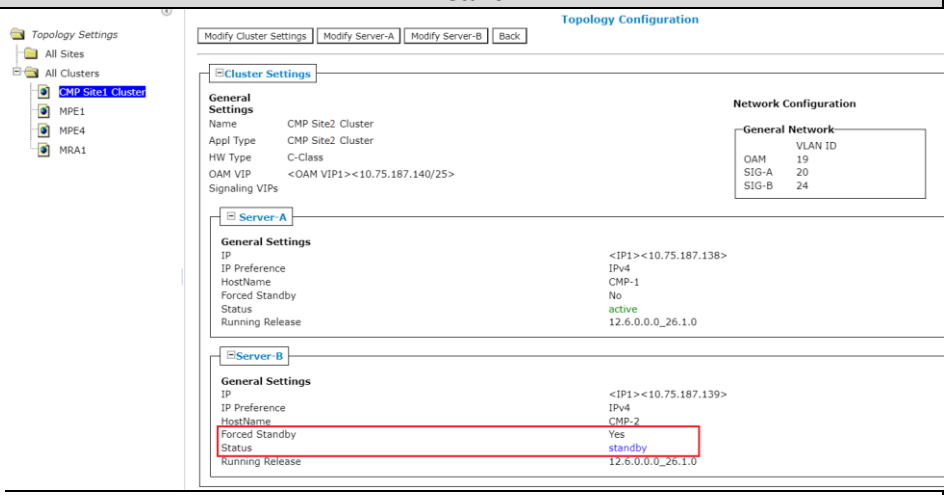
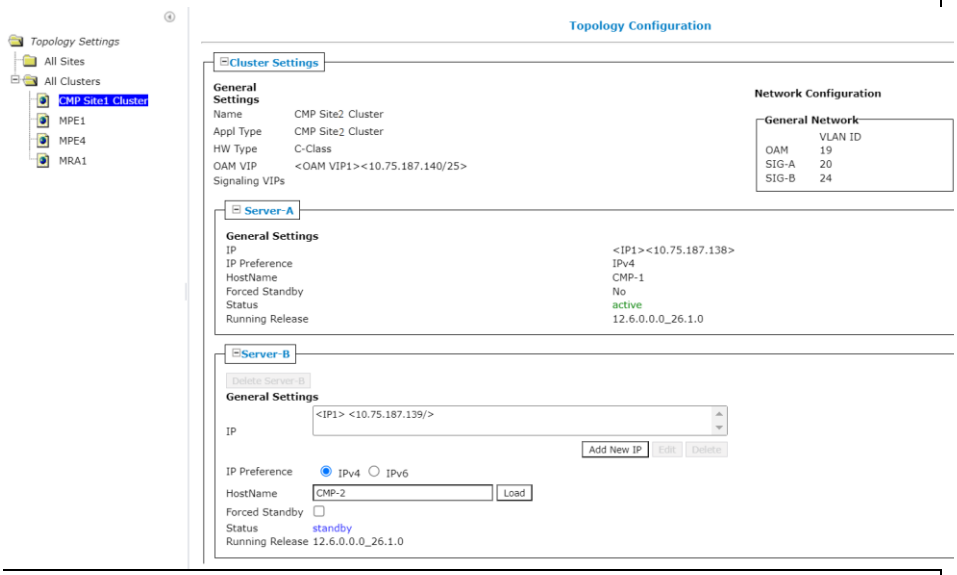
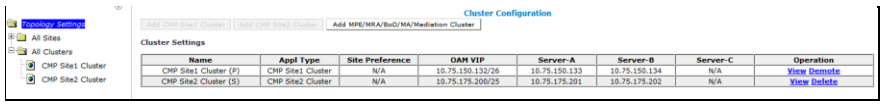
6. Enter the OAM VIP and the mask.

Step	Procedure	Details
		 This is the IP address the CMP server uses to communicate with a Policy Management cluster. **NOTE:** Enter the IPv4 address in standard dot format and its subnet mask in CIDR notation from 0 to 32, or the IPv6 address in standard 8-part colon-separated hexadecimal string format and its subnet mask in CIDR notation from 0 to 128. 7. Click **Save**. The OAM VIP and mask are saved. Repeat this step for a second OAM VIP, if needed. **NOTE:** Typically Signaling VIPs are not added to the CMP **Define the settings for Server-A in the Server-A section of the page** The IP address and hostname of Server-A are the IP address and hostname configured during the Initial Configuration of the server in section 6.1 of this document. The IP address and hostname must match exactly. If Server-A is network reachable from the CMP it is recommended to click **Load** after the IP address and IP preference are defined. The CMP attempts to load the hostname from the IP reachable server. This confirms network connectivity and minimizes the possibility of incorrectly defining the hostname. **To configure Server-A, in the Server-A section of the page:** 8. (Required) Click **Add New IP** to enter the IP address. The Add New IP window opens. 9. Enter the IP address in either IPv4 or IPv6 format. This is the IP address of the server. For an IPv4 address, enter it in the standard IP dot-format. For an IPv6 address, enter it in the standard 8-part colon-separated hexadecimal string format. 10. Select the IP Preference: IPv4 or IPV6. The server uses the IP address in the specified format for communication. - If neither an IPv6 OAM IP nor a static IP address is defined, IPv6 cannot be selected. - If neither an IPv4 OAM IP nor a static IP address is defined, IPv4 cannot be selected. 11. Enter the HostName of the server. This must exactly match the host name provisioned for this server (the output of the `uname -n` Linux command).

Step	Procedure	Details
		NOTE: If the server has a configured server IP, you can click Load to retrieve the remote server host name. If the retrieve fails, this a sign that the ip address configured is not accessible across the network. Alternately, you may enter the host name manually but it is recommeneded to do any network troubleshooting that may be required. For example: Here the HostName is populated by clicking **Load**  An example of the completed form for HW Type C-Class  Save the completed form and confirm the VLAN IDs, if needed  There is a transition period and alarms clear after a few minutes while the Site1 CMP cluster configures the georedundant CMP Site2 server-A. When complete, the georedundant CMP Site2 cluster is visible in **PLATFORM SETTINGS →Topology Settings**

Step	Procedure	Details
		 **NOTE:** For further detail of how this relationship between the Primary Site1 CMP cluster (P) and the Site2 CMP cluster (S) refer to [Configuration Management Platform Wireless User's Guide] Confirm that the Site2 CMP cluster server-A is active. Navigate to **PLATFORM SETTINGS →Topology Settings→CMP Site2 Cluster**  **NOTE:** Server-B is visible and is used for the next step
5. ☐	**CMP GUI:** Add site 2 CMP cluster	CMP-site 2 cluster must have server-B added to complete the cluster configuration. 1. From the Topology Setting menu, select CMP site 2 cluster. 2. Click **Modify server-B**.  **Define the settings for Server-B in the Server-B section of the page** To configure server-B, in the server-B section of the page: 3. (Required) Click Add **New IP** to enter the IP address. The Add New IP window opens. 4. Enter the IP address in either IPv4 or IPv6 format. This is the IP address of the server. For an IPv4 address, enter it in the standard IP dot-format. For an IPv6 address, enter it in the standard 8-part colon-separated hexadecimal string format.

Step	Procedure	Details
		5. Select the IP Preference: IPv4 or IPV6. The server uses the IP address in the specified format for communication. - If neither an IPv6 OAM IP nor a static IP address is defined, IPv6 cannot be selected. - If neither an IPv4 OAM IP nor a static IP address is defined, IPv4 cannot be selected. 6. Enter the HostName of the server. This must exactly match the host name provisioned for this server (the output of the `uname -n` Linux command). **NOTE:** If the server has a configured server IP, you can click Load to retrieve the remote server host name. If the retrieve fails, this a sign that the ip address configured is not accessible across the network. Alternately, you may enter the host name manually but it is recommended to do any network troubleshooting that may be required. For example:  There is a transition period and several alarms that clear after a few minutes while the site 1 CMP cluster configures the georedundant CMP site 2 server-B. Wait for all alarms to clear and then then confirm that server B in the CMP Site 2 cluster is in standby. Navigate to **PLATFORM SETTINGS →Topology Settings→CMP Site2 Cluster**

Step	Procedure	Details
		 **Note:** Forced Standby of Server-B status is Yes.
6. ☐	**CMP GUI:** Clear Forced Standby setting for server-B	1. From the Topology Settings menu, select the CMP site 2 cluster. 2. Click **Modify Server-B**. 3. Clear the Forced Standby state of Server-B. 4. Click **Save**.  The Geo-Redundant Site2 cluster confugration is completed. The CMP Site1 cluster is marked with a (P) for primary and the CMP Site2 cluster is marked with an (S) for secondary. **PLATFORM SETTINGS →Topology Settings→** 
—End of Procedure—		

6.4.2 Setting Up a Non-CMP Cluster (MPE, MRA)

This procedure configures the management relationships between the CMP and other Non-CMP clusters in Wireless Mode.

A non-CMP cluster includes one of the following server types:

- MPE
- MRA

IMPORTANT: Certain IP network services must be allowed between the CMP Site 1 cluster and the other clusters in the network, in order to establish the full management relationships. Incorrectly configured firewalls in the network can cause the management relations to fail, and alarms are raised at the CMP.

Prerequisites:

Before beginning this procedure, verify that you have HTTP access to the CMP server.

Before defining a non-CMP cluster, ensure the following:

- The server software is installed on all servers in the cluster.
- The servers are configured with network time protocol (NTP), IP Routing, and OAM IP addresses.
- The server IP connection is active.

See **Section 5:Preparing the System Environment** in this document.

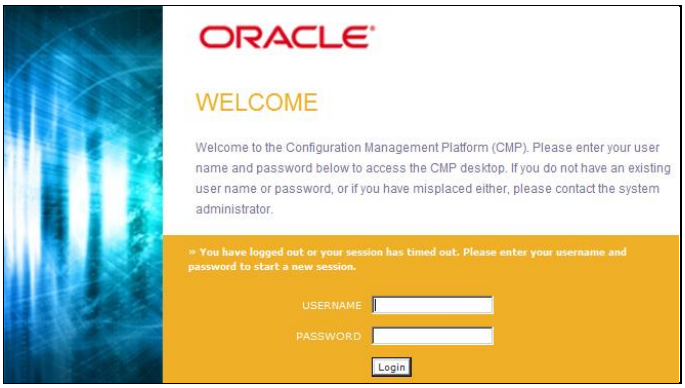
To complete this procedure, you need the following:

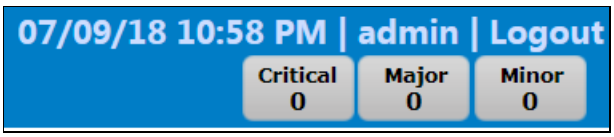
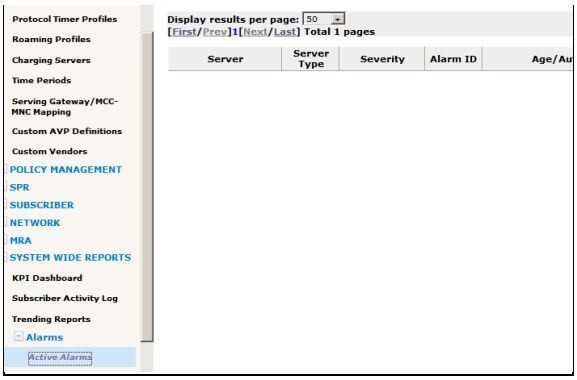
- HW Type—Determines whether VLANs are required. If you select c-Class, c-Class (segregated traffic), VLANs are required. For RMS hardware, VLANs are not required.
- OAM VIP (optional)—The IP address and netmask a CMP cluster uses to communicate with an MPE or MRA cluster.
- Signaling VIPs (required)—The IP address a policy charging and enforcement function (PCEF) uses to communicate with a cluster. At least one signaling VIP is required. Define up to four IPv4 or IPv6 addresses and netmasks of the signaling VIP addresses. For each, select None, SIG-A, SIG-B, or SIG-C to indicate whether the cluster uses an external signaling network. You must enter a Signaling VIP value if you specify either SIG-A, SIG-B, or SIG-C.
- Network VLAN IDs—The values designated during the Initial Configuration done with placfg.

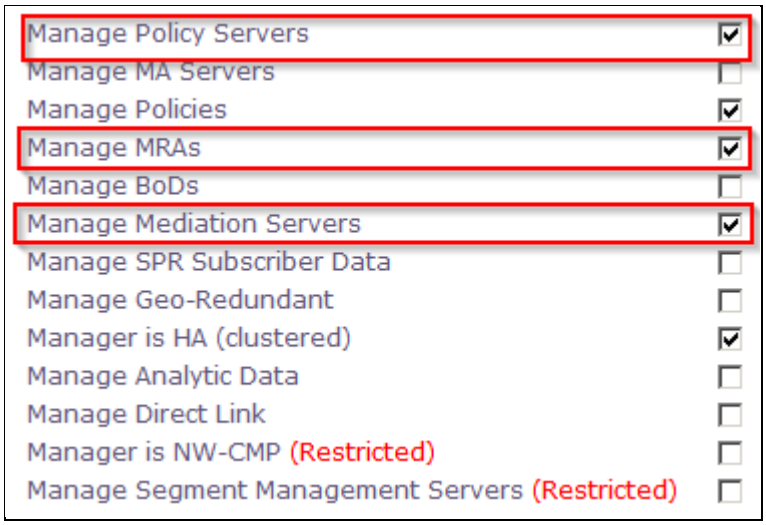
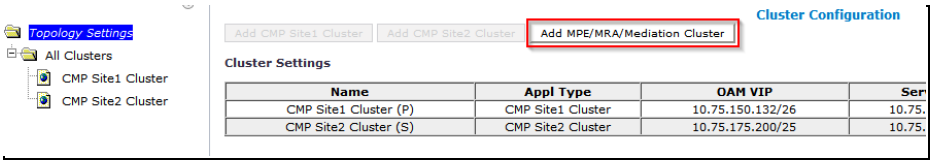
Check off (√) each step as it is completed. Check boxes are provided next to each step number.

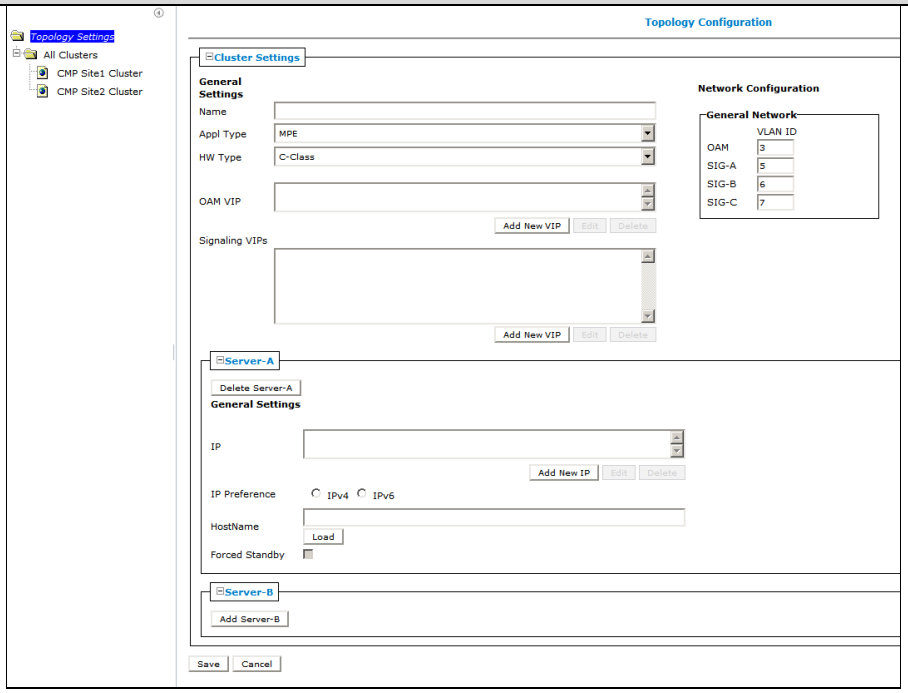
If this procedure fails, contact Oracle Technical Services and ask for assistance.

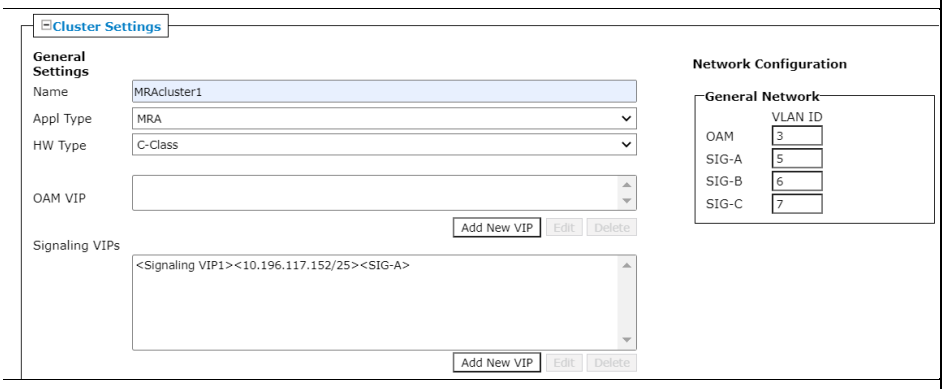
6.4.2: Setting Up a Non-CMP Cluster (MPE, MRA)

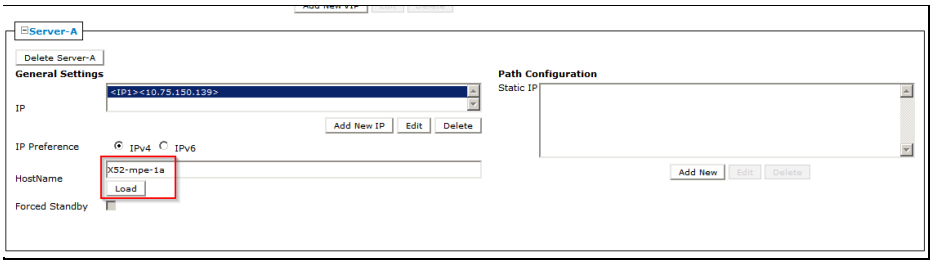
Step	Procedure	Details
1. ☐	**CMP GUI:** Login to CMP Server GUIs (using VIP)	1. From Browser, enter CMP Server VIP in Navigation string. **NOTE:** Only the following Web Browsers are supported in OCPM 12.6 - Mozilla Firefox® release 81.0 or later - Google Chrome version 86.0 or later *Internet Explorer in not supported.  2. Login as admin (or a user with administrative privileges).

Step	Procedure	Details
2. ☐	**CMP GUI**: View active alarms	It is recommended to View the active alarms in the system before performing Configuration work. Check the alarm information and determine if any alarms are present that may affect configuration activies. You can view the alarms by: • Using the CMP GUI upper right banner  • Navigating to **System Wide Reports → Active Alarms**.  *IMPORTANT:* ***In Policy 12.6, there is help provided for alarm descriptions.*** - In the Alarm views, click the alarm ID to open the alarm description help page. – Alternatively, from the menu select **On-Line Help**, and select **Troubleshooting Guide**. Search this for the alarm ID.
3. ☐	Mode configuration considerations	The Modes must be selected during the initial GUI configuration for all the options in this procedure to be available for configuration on the CMP. To add a Non-CMP cluster the following Mode Options must be selected on the CMP: • MPE (Manage Policy Servers) • MRA (Manage MRAs)

Step	Procedure	Details
		 **Note:** • If the **Manage Geo-Redundant** is selected go to the next procedure. (6.4.4: Setting Up a Non-CMP cluster (MPE, MRA) Modes are changed at a later time if needed, but the method to access this mode selection is not documented. Contact Oracle Support if Mode selection is required to changed after the initial configuration.
4. ☐	**CMP GUI:** Add MPE, MRA clusters	1. Navigate to **PLATFORM SETTINGS → Topology Settings**  2. On the cluster Configuration page, click **Add MPE/MRA Cluster** The procedure for adding an MPE, MRA cluster is the same except for selecting the Appl Type which is MPE, MRA respectively. The Topology Configuration page opens.

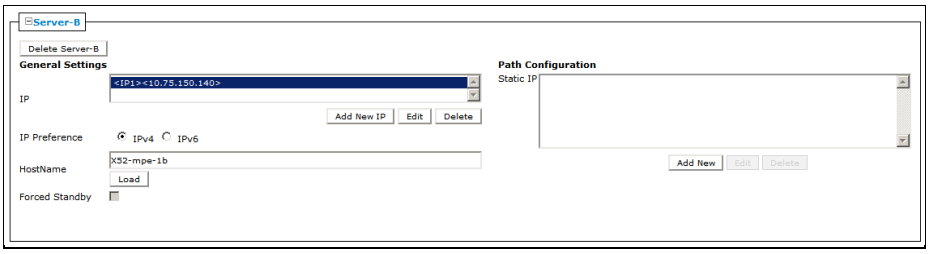
Step	Procedure	Details
		
5. ☐	**CMP GUI:** Add MPE, MRA clusters	Complete the form according to the system design. You can add both Server-A and Server-B at the same time. **Notes:** - It is possible to come back at a later time and modify any settings made at this time. - The procedure for adding an MPE, MRA cluster is the same except for selecting Appl Type which is MPE, MRA respectively. **Define the Cluster Settings** **Name** (required)—Name of the cluster. Enter up to 250 characters, excluding quotation marks(") and commas (,). **Appl Type**—Select the type of server: MPE (default), MRA **HW Type**—Select the type of hardware: - C-Class (default)—HP ProLiant BL460 Gen8 server - C-Class (segregated traffic) (a configuration where Signaling and other networks are separated onto physically separate equipment)—HP ProLiant BL460Gen8 - RMS (for a rack-mounted server not using VLANs) If you selected C-Class, C-Class (segregated traffic), enter the General Network—VLAN IDs. 1. Enter the OAM, SIG-A, SIG-B (optional),and SIG-C (optional) virtual LAN (VLAN) IDs. VLAN IDs are in the range 1 through 4095. The default values are: - OAM—3 - SIG-A—5

Step	Procedure	Details
		- SIG-B—6 **OAM VIP**—The OAM VIP is not typically used for Non-CMP clusters. The Real IP address is used by the CMP to communicate with the Non-CMP cluster. **Signaling VIPs** (required)—The signaling VIP is the IP address a PCEF (or Gateway) device uses to communicate with a cluster. Click **Add New VIP** to add a VIP to the system. A cluster supports the following redundant communication channels for carriers that use redundant signaling channels. - SIG-A - SIG-B - SIG-C At least one signaling VIP is required. For Example:  **Define the settings for Server-A in the Server-A section of the page** The IP address and hostname of Server-A are the IP address and hostname configured during the Initial Configuration of the server in section 6.1 of this document. The IP address and hostname must match exactly. If Server-A is network reachable from the CMP it is recommended to click **Load** after the IP address and IP preference are defined. The CMP attempts to load the hostname from the IP reachable server. This confirms network connectivity and minimizes the possibility of incorrectly defining the hostname. To configure Server-A, in the Server-A section of the page: 2. (Required) To enter the IP address, click **Add New IP**. The Add New IP window opens. 3. Enter the IP address in either IPv4 or IPv6 format. This is the IP address of the server. For an IPv4 address, enter it in the standard IP dot-format. 4. For an IPv6 address, enter it in the standard 8-part colon-separated hexadecimal string format. - For an IPv6 address, enter it in the standard 8-part colon-separated hexadecimal string format. - Select the IP Preference: IPv4 or IPV6.

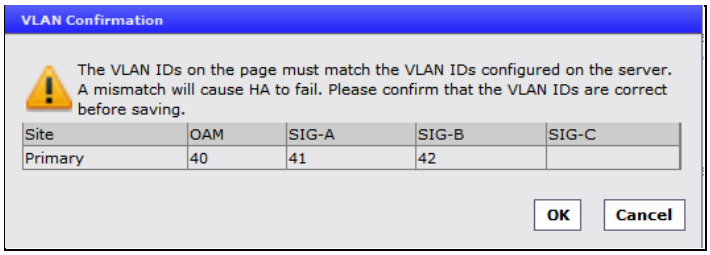
Step	Procedure	Details
		The server uses the IP address in the specified format for communication. - If neither an IPv6 OAM IP nor a static IP address is defined, IPv6 cannot be selected. - If neither an IPv4 OAM IP nor a static IP address is defined, IPv4 cannot be selected. 5. Enter the HostName of the server. This must exactly match the host name provisioned for this server (the output of the `uname -n` Linux command). **NOTE:** If the server has a configured server IP, you can click Load to retrieve the remote server host name. If the retrieve fails, this a sign that the ip address configured is not accessible across the network. Alternately, you may enter the host name manually but it is recommeneded to do any network troubleshooting that may be required. For example:  **Define the settings for Server-B in the Server-B section of the page** To configure Server-B, in the Server-B section of the page: 6. (Required) Click **Add New IP** to enter the IP address. The Add New IP window opens. 7. Enter the IP address in either IPv4 or IPv6 format. This is the IP address of the server. For an IPv4 address, enter it in the standard IP dot-format. For an IPv6 address, enter it in the standard 8-part colon-separated hexadecimal string format. 8. Select the IP Preference: IPv4 or IPV6. The server uses the IP address in the specified format for communication. - If neither an IPv6 OAM IP nor a static IP address is defined, IPv6 cannot be selected. - If neither an IPv4 OAM IP nor a static IP address is defined, IPv4 cannot be selected. 9. Enter the HostName of the server. This must exactly match the host name provisioned for this server (the output of the `uname -n` Linux command). **NOTE:** If the server has a configured server IP, you can click Load to retrieve the remote server host name. If the retrieve fails, this a sign that the ip address

<table>
<tr><th>Step</th><th>Procedure</th><th>Details</th></tr>
<tr><td></td><td></td><td>configured is not accessible across the network. Alternately, you may enter the host name manually but it is recommeneded to do any network troubleshooting that may be required.

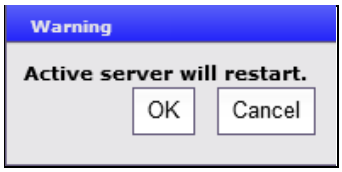
For example:

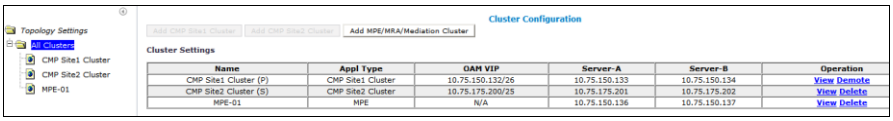
NOTE: These settings are only an example of a likely configuration. An actual deployment is specific to your requirements.</td></tr>
<tr><td>6. ☐</td><td>CMP GUI: Add MPE, MRA clusters</td><td>1. Save the Topology Configuration at the bottom of the Topology Configuration page.
2. Confirm the VLAN configuration if the hardware type requires VLANs

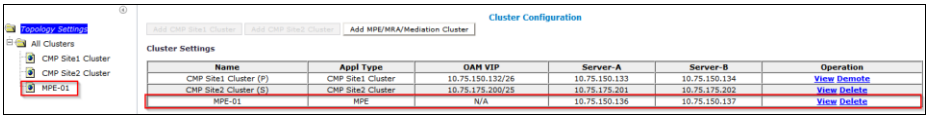
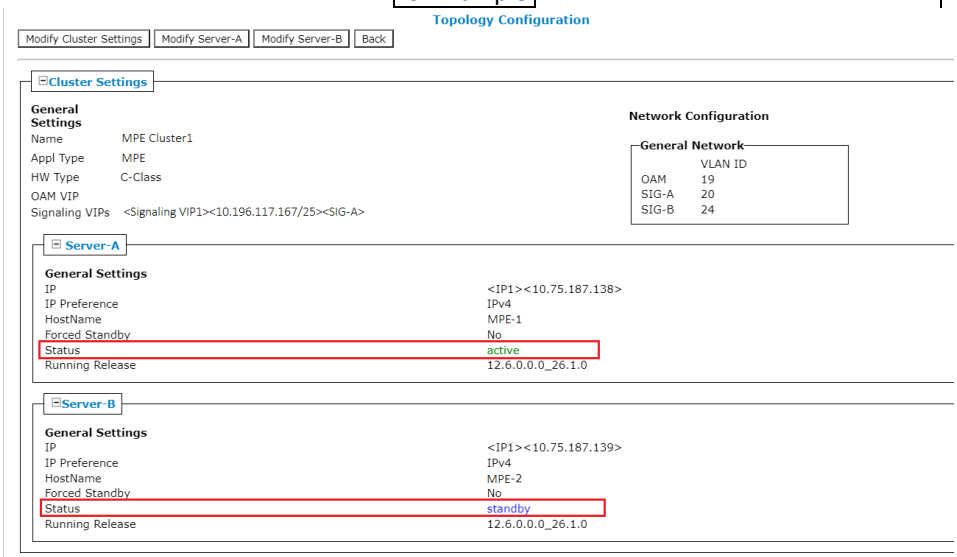
 

3. Click OK to confirm

If the cluster added successfully, it is visible on the Cluster Configuration page. The Cluster Configuration page displays:

 
</td></tr>
</table>

Step	Procedure	Details
7. ☐	**CMP GUI:** Add MPE, MRA clusters	Confirm the cluster added successfully. The following shows an example of adding a non-CMP cluster of Appl Type MPE Check that all alarms have cleared and then click **View** for the cluster that was added  The Topology Configuration opens for the added non CMP cluster. There is an active and a standby server. It does not matter which server is active. If this is the case, and there are not any alarms, then the cluster is added successfully. For Example:  **NOTE:** If the topology configuration is performed at a time when there is not a network connection between the CMP and the MRA, MPE servers being added to the topology, the status of the servers is offline and alarms are generated because of the offline state. These alarms persist until the servers become reachable from the CMP. The CMP continually retries connecting to the servers that are added in the topology. In this case, no further configuration is performed until the network connectivty between the CMP and the target servers is available. Do not proceed. Return to this step when the network connectivty from the CMP to the target servers is available. If the servers are reachable then proceed to the next step. The cluster is successfully added.
8. ☐	Repeat the previous step for additional clusters	A list of clusters configured are added to this step as a reminder. The procedure for adding an MPE, MRA cluster is the same except for selecting the Appl Type which is MPE, MRA respectively.
9. ☐	If the CMP manages remote sites, and these are not available.	If the CMP manages remote sites and the sites are not available, you can either: • Configure the clusters and return to the verify steps after the connectivity is established. • Configure the clusters at a later time when connectivity is established.

Step	Procedure	Details
		—End of Procedure—

6.4.3 Setting Up a Geo-Redundant Site

This procedure creates sites that are used if Geo-Redundant clusters are added to the CMP Topology. A Geo-Redundant cluster is associated with these sites in the next procedure. If Geo-Redundant clusters are not needed, than skip this procedure.

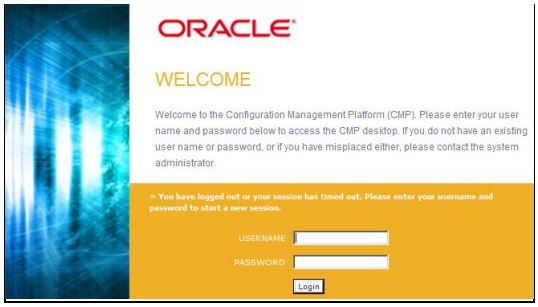
Prerequisites:

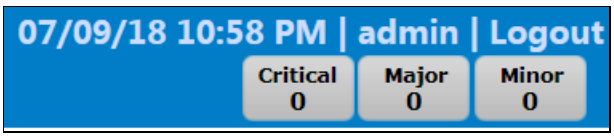
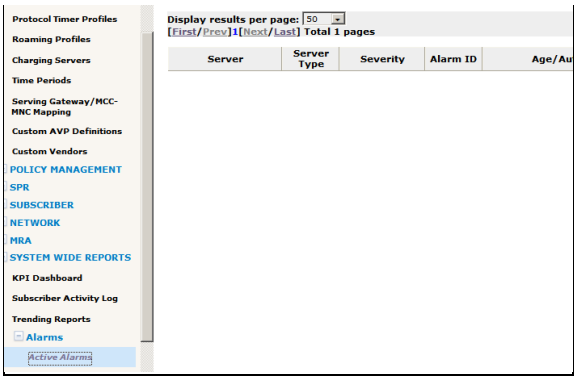
- Before beginning this procedure, verify that you have HTTP access to the CMP server.
- Names of Sites created

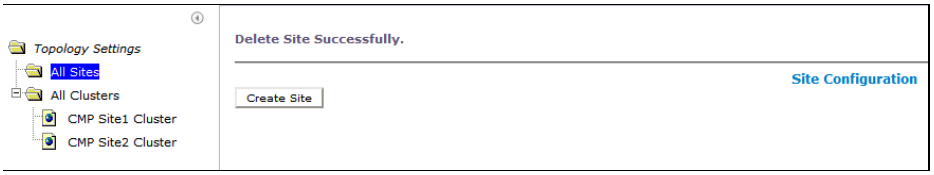
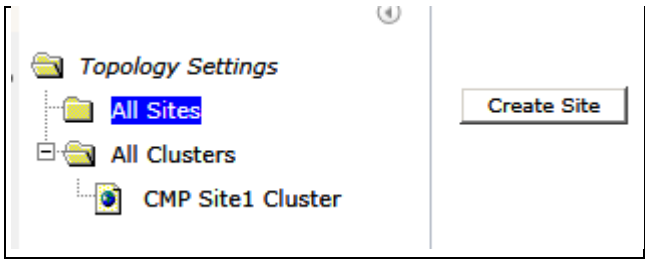
Check off (√) each step as it is completed. Check boxes are provided next to each step number.

If this procedure fails, contact Oracle Technical Services and ask for assistance.

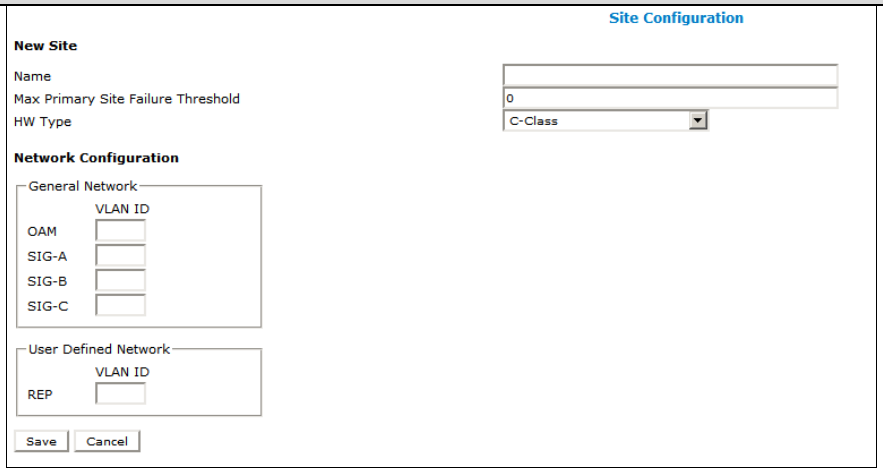
6.4.3: Setting Up a Geo-Redundant Site

Step	Procedure	Details
1. ☐	**CMP GUI:** Login to CMP Server GUIs (using VIP)	1. From Browser, enter CMP Server VIP in Navigation string. **NOTE:** Only the following Web Browsers are supported in OCPM 12.6 - Mozilla Firefox® release 81.0 or later - Google Chrome version 86.0 or later *Internet Explorer in not supported for this procedure  2. Login as admin (or a user with administrative privileges)

Step	Procedure	Details
2. ☐	**CMP GUI**: View active alarms	It is recommended to View the active alarms in the system before performing Configuration work. Check the alarm information and determine if any alarms are present that may affect configuration activies. You can view the alarms by: • Using the CMP GUI upper right banner  • Navigating to **System Wide Reports → Active Alarms**.  *IMPORTANT:* ***In Policy 12.6, there is help provided for alarm descriptions.*** - In the Alarm views, click the alarm ID to open the alarm description help page. – Alternatively, from the menu select **On-Line Help**, and select **Troubleshooting Guide**. Search this for the larm ID.

Step	Procedure	Details
3. ☐	**CMP:** View Topology Settings	1. Navigate to **PLATFORM SETTINGS → Topology Settings**. 2. Confirm that All Sites is listed in the Topology Settings menu.  **NOTE:** Sites may only be created when Manage Geo-Redundant mode is enabled. **NOTE:** If Manage Geo-Redundant mode was not selected during initial configuration of the Site1 CMP cluster, the CMP modes are changed if needed, but the method to access this mode selection is not documented. Contact Oracle Support if Mode selection is required to be changed after the initial configuration.
4. ☐	**CMP GUI:** Create sites for georedundant configuration	For a georedundant configuration at least 2 Sites must be created before proceeding with this procedure. This step is preparation for adding georedundant MPE, MRA clusters and is not needed to add a georedundant CMP cluster. If georedundancy is not going to be used, this step may be skipped. 1. Navigate to **PLATFORM SETTINGS →Topology Settings→All Sites** 2. Click **Create Site**.  The Site Configuration form opens.

Step	Procedure	Details



3. Select the HW Type from the list.

   The available options are:

   - C-Class (default)
   - C-Class(segregated traffic) (for a configuration where Signaling and other networks are separated onto physically separate equipment)
   - RMS (for a rack-mounted server)

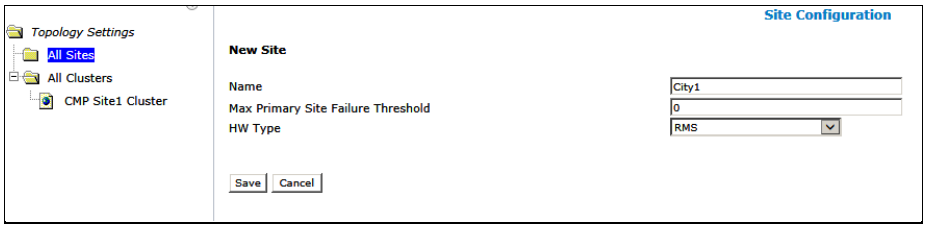
   If you selected C-Class, C-Class(segregated traffic), enter the General Network - VLAN IDs.

4. Enter the OAM, SIG-A, SIG-B (optional), and SIG-c (optional) virtual LAN (VLAN) IDs.

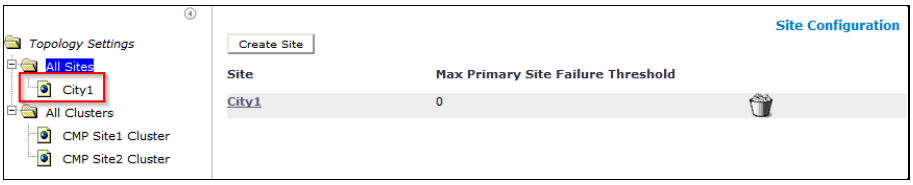
   VLAN IDs are in the range 1 through 4095. The default values are:

   - OAM—3
   - SIG-A—5
   - SIG-B—6
   - SIG-C—7

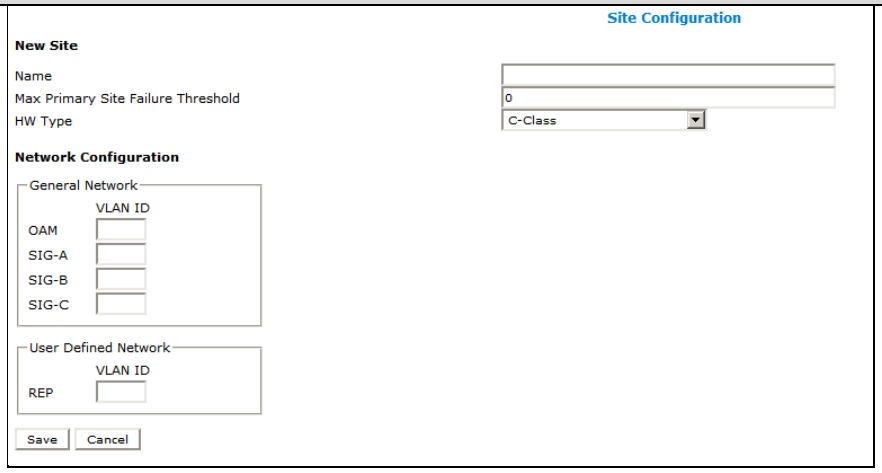
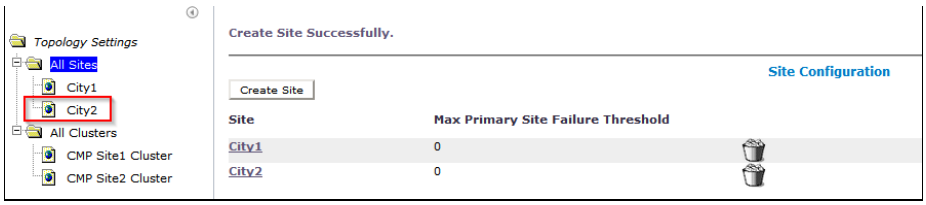
5. Name the site and click **Save**.



   The site is listed in the Topology Settings menu



6. Create a 2nd Site and click **Save**.

Step	Procedure	Details
		 The site is listed in the Topology Settings menu. 
—End of Procedure—		

6.4.4 Setting Up a Geo-Redundant Non-CMP Cluster (MPE, MRA)

This procedure configures the management relationships between the CMP and other Geo-Redundant Non-CMP in Wireless Mode.

A non-CMP cluster includes one of the following server types:

- MPE
- MRA

IMPORTANT: Certain IP network services must be allowed between the CMP Site 1 cluster and the other clusters in the network, in order for the full management relationships to be established. Incorrectly configured Firewalls in the network can cause the Management relations to fail, and alarms to be raised at the CMP.

Prerequisites:

Before beginning this procedure, verify that you have HTTP access to the CMP server.

Before defining a non-CMP cluster, ensure the following:

- The server software is installed on all servers in the cluster.
- The servers are configured with network time protocol (NTP), IP Routing, and OAM IP addresses.
- The server IP connection is active.

  See Section 5:Preparing the System Environment in this document

- Procedure 6.4.3: Setting Up a GeoRedundant Site is completed

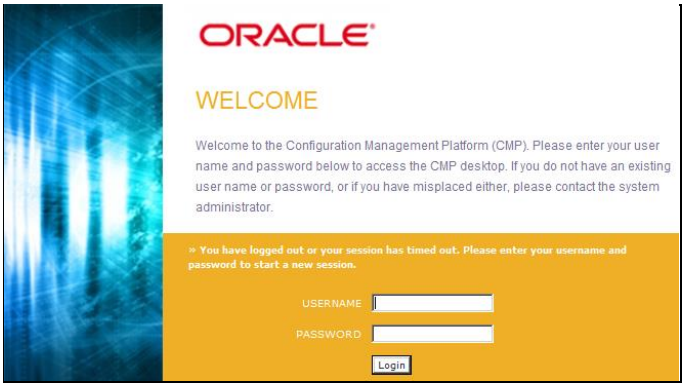
To complete this procedure, you need the following:

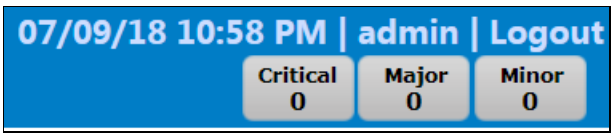
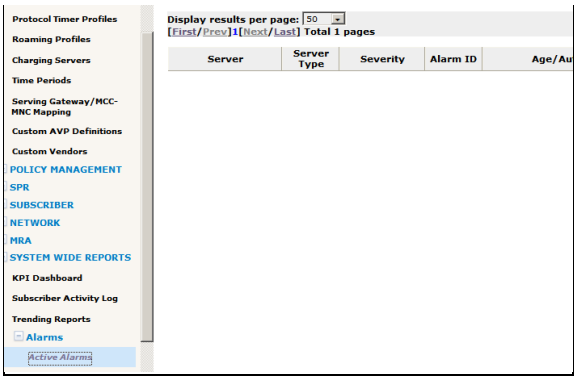
- HW Type—Determines whether VLANs are required. If you select c-Class, c-Class (segregated traffic), VLANs are required.
- OAM VIP (optional)—The IP address and netmask a CMP cluster uses to communicate with an MPE or MRA cluster.
- Signaling VIPs (required)—The IP address a policy charging and enforcement function (PCEF) uses to communicate with a cluster. At least one signaling VIP is required. Define up to four IPv4 or IPv6 addresses and netmasks of the signaling VIP addresses. For each, select None, SIG-A, SIG-B, or SIG-C to indicate whether the cluster uses an external signaling network. You must enter a Signaling VIP value if you specify either SIG-A, SIG-B, or SIG-C.
- Network VLAN IDs—The values designated during the Initial Configuration done with placfg.

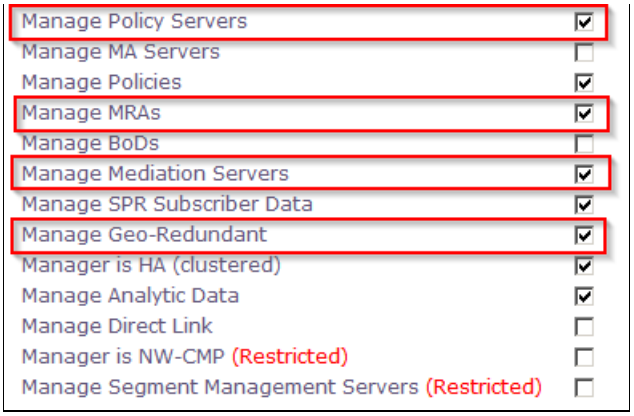
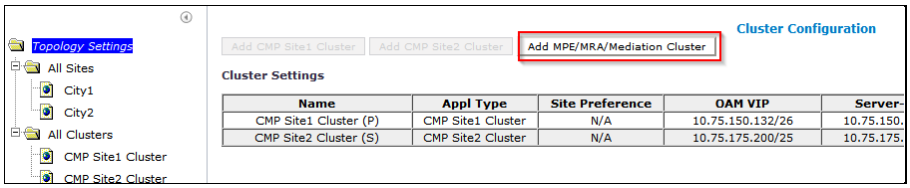
Check off (√) each step as it is completed. Check boxes are provided next to each step number.

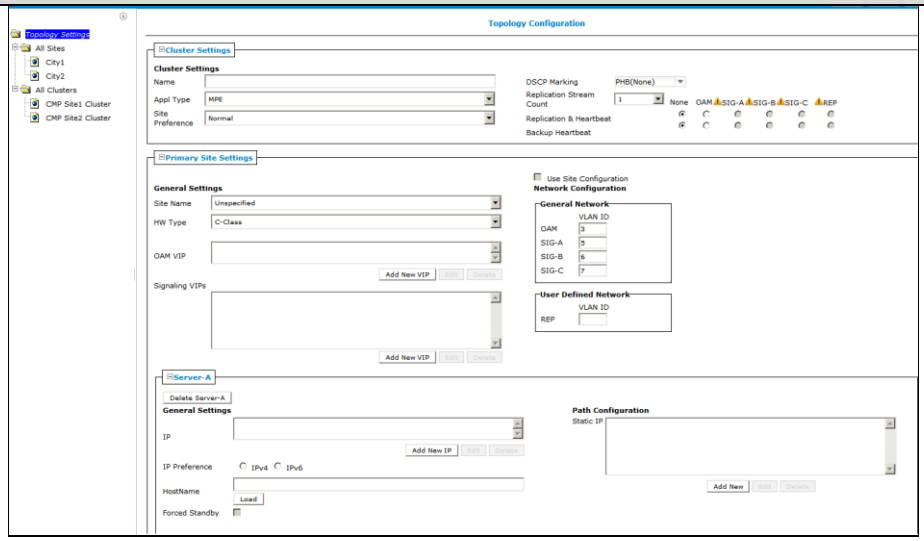
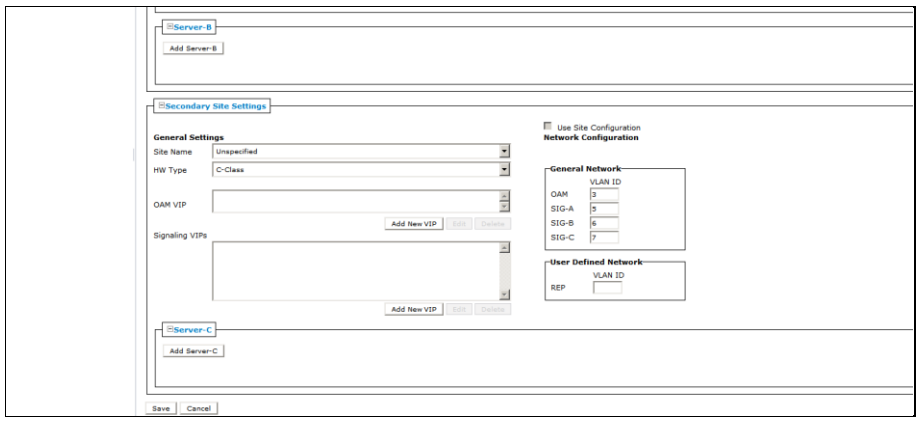
If this procedure fails, contact Oracle Technical Services and ask for assistance.

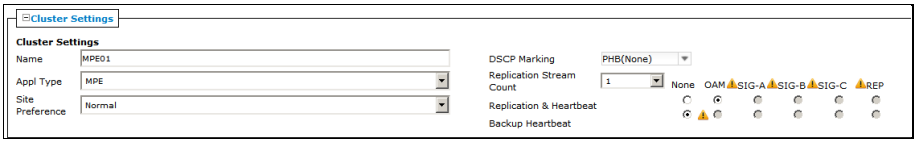
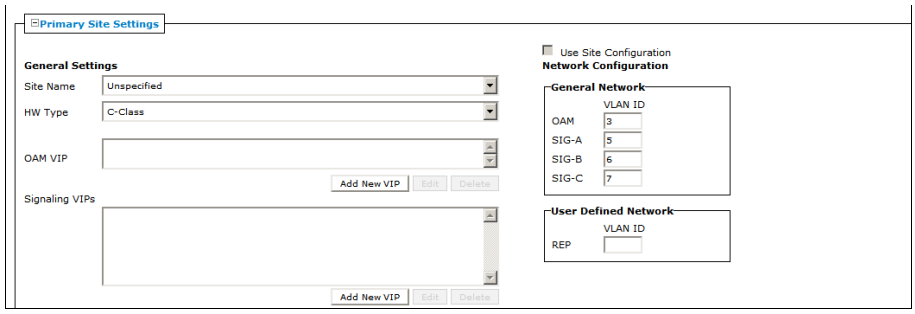
6.4.4: Setting Up a Geo-Redundant Non-CMP Cluster (MPE, MRA)

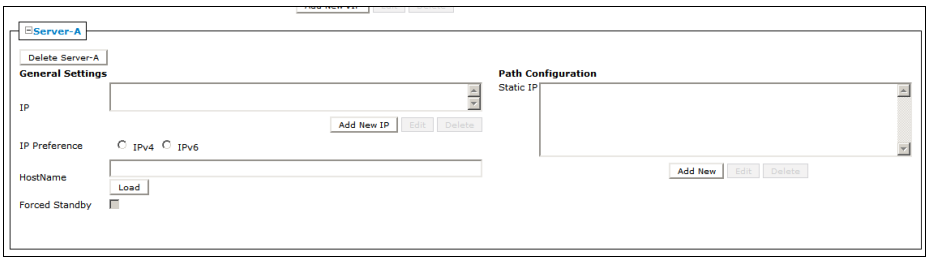
Step	Procedure	Details
1. ☐	**CMP GUI:** Login to CMP Server GUIs (using VIP)	1. Open a browser and enter the CMP server VIP as the navigation string. **NOTE:** Only the following Web Browsers are supported in OCPM 12.6 - Mozilla Firefox® release 81.0 or later - Google Chrome version 86.0 or later *Internet Explorer in not supported.  2. Login as admin (or a user with administrative privileges)

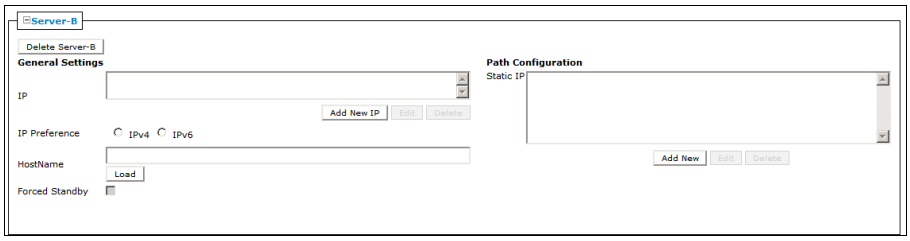
Step	Procedure	Details
2. ☐	**CMP GUI**: View active alarms	It is recommended to View the active alarms in the system before performing Configuration work. Check the alarm information and determine if any alarms are present that may affect configuration activies. You can view the alarms by: • Using the CMP GUI upper right banner  • Navigating to **System Wide Reports → Active Alarms**.  *IMPORTANT:* ***In Policy 12.6, there is help provided for alarm descriptions.*** - In the Alarm views, click the alarm ID to open the alarm description help page. – Alternatively, from the menu select **On-Line Help**, and select **Troubleshooting Guide**. Search this for the alarm ID.

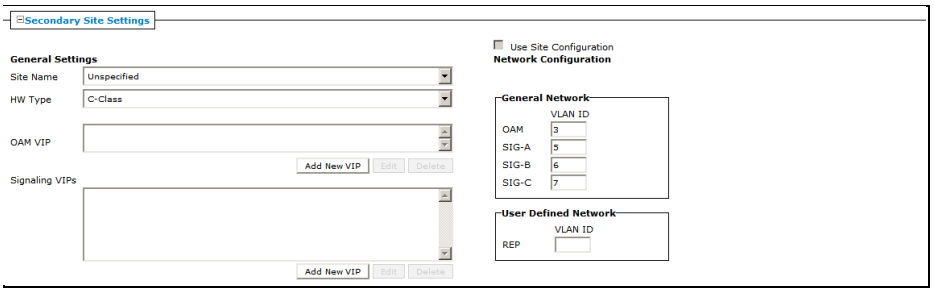
Step	Procedure	Details
3. ☐	Mode Configuration Considerations	The Modes must be selected during the initial GUI configuration for all the options in this procedure to be available for configuration on the CMP. To add a Non-CMP cluster the following Mode Options must be selected on the CMP: • MPE (Manage Policy Servers) • MRA (Manage MRAs) • Manage Geo-Redundant  **Note:** • Manage Geo-Redundant mode enables you to configure Primary and Secondary sites as well as adding a Server-C (spare) to each non-CMP cluster in the Topology. Modes are changed at a later time if needed, but the method to access this mode selection is not documented. Contact Oracle Support if Mode selection is required to be changed after the initial configuration.
4. ☐	**CMP GUI:** Add MPE, MRA clusters	1. Navigate to **PLATFORM SETTINGS → Topology Settings**  2. On the cluster Configuration page, click **Add MPE/MRA** The procedure for adding an MPE or MRA cluster is the same except for selecting the Appl Type which is MPE or MRA respectively. The Topology Configuration page opens:

Step	Procedure	Details
		  **Notes:** • All Sites is available in the Topology Settings menu. • Primary Site Settings and Secondary Site Settings is available on the Topology Configuration page. • Server-C is available in the Secondary Site Settings sections.
5. ☐	**CMP GUI:** Add MPE/MRA clusters	Complete the form according to the system design. You can add Server-A, Server-B and Server-C at the same time. To add Server-C expand the Server-C option by clicking on the + (plus) sign for Server-C. **Notes:** - It is possible to come back at a later time and modify any settings made at this time. - The procedure for adding an MPE/MRA cluster is the same except for selecting Appl Type which is MPE, MRA respectively. **Define the Cluster Settings** **Name** (required)—Name of the cluster. Enter up to 250 characters, excluding quotation marks(") and commas (,). **Appl Type**—Select the type of server: **MPE** (default) or **MRA** **Site Preference**—NORMAL (default)

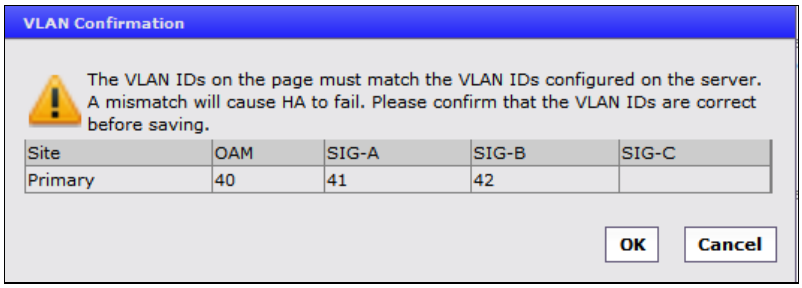
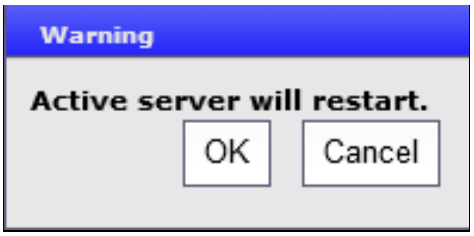
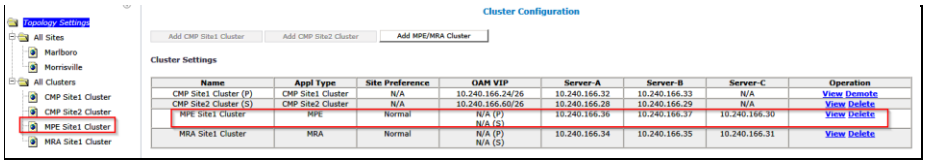
Step	Procedure	Details
		DSCP Marking—PHB(None)is the default **Replication Stream Count**—1 through 8. 1 is the default. **Replication and Heartbeat**—None is the default. OAM is typically preferred. **Backup Heartbeat**—None (default) or OAM For Example:  **NOTE:** A warning icon ( ) indicates that you cannot select a network until you define a static IP address on all servers of both sites. **Define the Primary Site Settings (General Settings)**  **Site Name**—Here the added server is associated with a configured site in the drop down tab if this is a Geo-Redundant topology **HW Type**—Select the type of hardware: - C-Class (default)—HP ProLiant BL460 Gen8 server - C-Class (segregated traffic) (a configuration where Signaling and other networks are separated onto physically separate equipment)—HP ProLiant BL460 Gen8 - RMS (for a rack-mounted server not using VLANs) **Define the Network Configuration.** - if you selected C-Class, C-Class(segregated traffic), enter the General Network—VLAN IDs. - Enter the OAM, SIG-A, SIG-B (optional), and SIG-C (optional) virtual LAN (VLAN) IDs. VLAN IDs are in the range 1 through 4095. The default values are: - OAM—3 - SIG-A—5 - SIG-B—6 - SIG-C—7 If the hardware type is C-Class or C-Class(segregated traffic), for the user defined network, enter the REP VLAN ID. **NOTE:** Virtual LAN (VLAN) IDs are in the range of 1 to 4095.

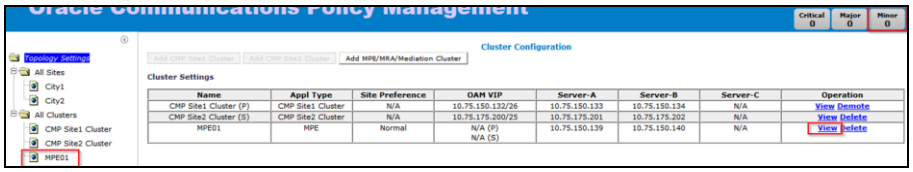
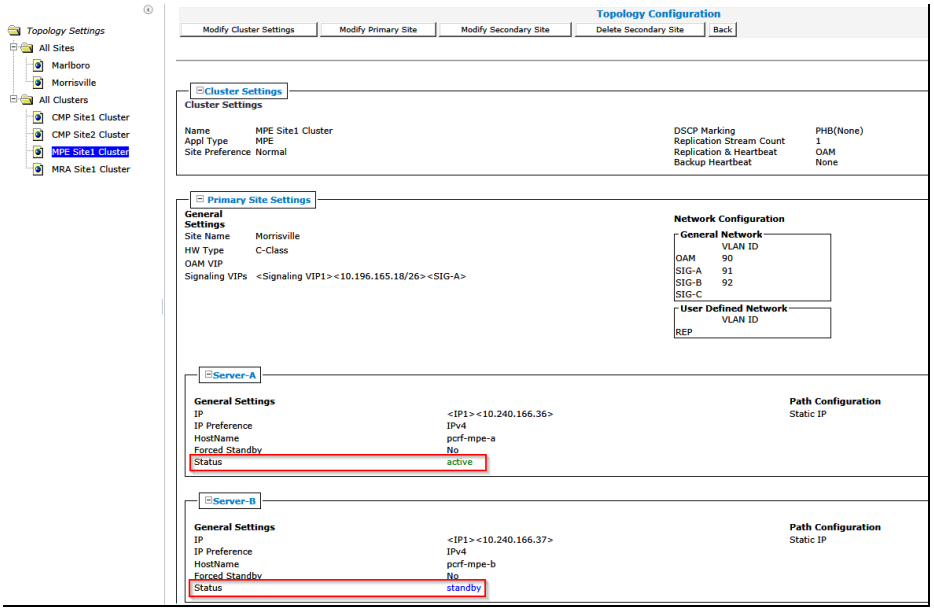
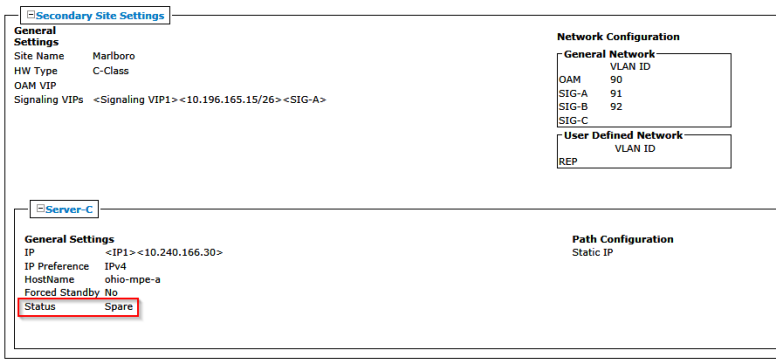
Step	Procedure	Details
		OAM VIP—The OAM VIP is not typically used for Non-CMP clusters. The Real IP address is used by the CMP to communicate with the Non-CMP cluster. **Signaling VIPs** (required)—The signaling VIP is the IP address a PCEF (or Gateway) device uses to communicate with a cluster. Click **Add New VIP** to add a VIP to the system. A cluster supports the following redundant communication channels for carriers that use redundant signaling channels. - SIG-A - SIG-B - SIG-C At least one signaling VIP is required. - Define the settings for Server-A in the Primary Site Settings section of the page The IP address and hostname of Server-A are the IP address and hostname configured during the Initial Configuration of the server in section 6.1 of this document. The IP address and hostname must match exactly. If Server-A is network reachable from the CMP it is recommended to click **Load** after the IP address and IP preference are defined. The CMP attempts to load the hostname from the IP reachable server. This confirms network connectivity and minimizes the possibility of incorrectly defining the hostname.  To configure Server-A, in the Server-A section of the page: - (Required) Click **Add New IP** to enter the IP address. The Add New IP window opens. - Enter the IP address in either IPv4 or IPv6 format. This is the IP address of the server. For an IPv4 address, enter it in the standard IP dot-format. For an IPv6 address, enter it in the standard 8-part colon-separated hexadecimal string format. - Select the IP Preference: IPv4 or IPV6. The server uses the IP address in the specified format for communication. - If neither an IPv6 OAM IP nor a static IP address is defined, IPv6 cannot be selected. - If neither an IPv4 OAM IP nor a static IP address is defined, IPv4 cannot be selected. - Enter the HostName of the server. This must exactly match the host name provisioned for this server (the output of the `uname -n` Linux command).

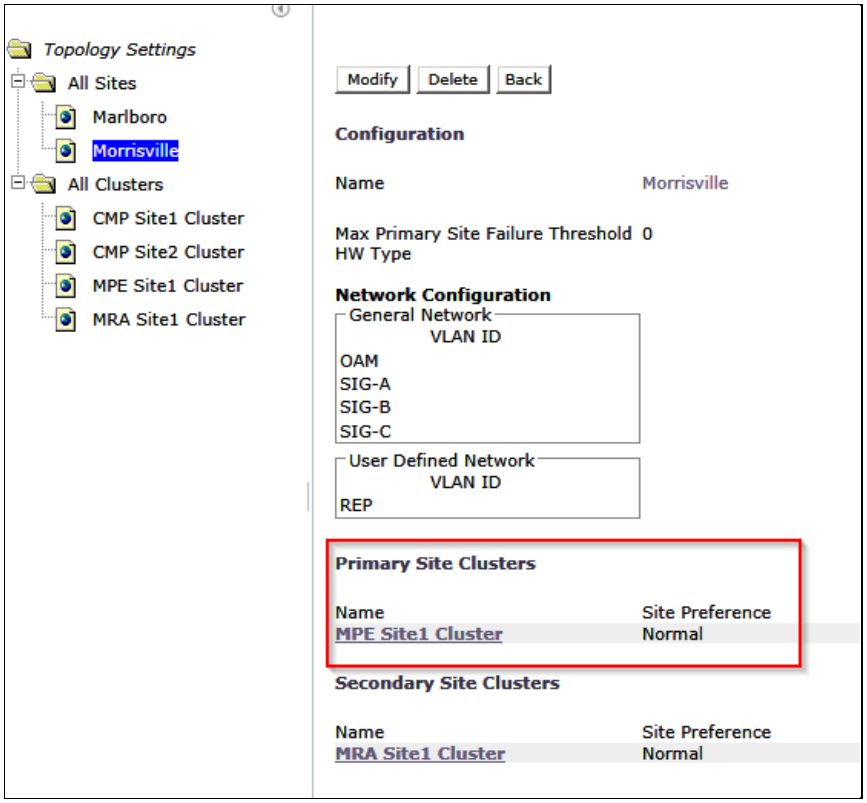
Step	Procedure	Details
		NOTE: If the server has a configured server IP, you can click Load to retrieve the remote server host name. If the retrieve fails, this a sign that the ip address configured is not accessible across the network. Alternately, you may enter the host name manually but it is recommended to do any network troubleshooting that may be required. - In the Path Configuration section, click **Add New** to add a Static IP. The New Path window opens. **NOTE:** If an alternate replication path and secondary HA heartbeat path is used, a server Static IP address must be entered in this field. - Enter a Static IP address and Mask. - Select the Interface: - SIG-A - SIG-B - SIG-C - REP - BKUP **Define the settings for Server-B in the Server-B section of the page** - Click **Add Server-B** on the Topology Configuration page The Server-B configuration form opens  To configure Server-B, in the Server-B section of the page: - (Required) Click **Add New IP** to enter the IP address. The Add New IP window opens. - Enter the IP address in either IPv4 or IPv6 format. This is the IP address of the server. For an IPv4 address, enter it in the standard IP dot-format. For an IPv6 address, enter the address in the standard 8-part colon-separated hexadecimal string format. - Select the IP Preference: IPv4 or IPV6. The server uses the IP address in the specified format for communication. - If neither an IPv6 OAM IP nor a static IP address is defined, IPv6 cannot be selected.

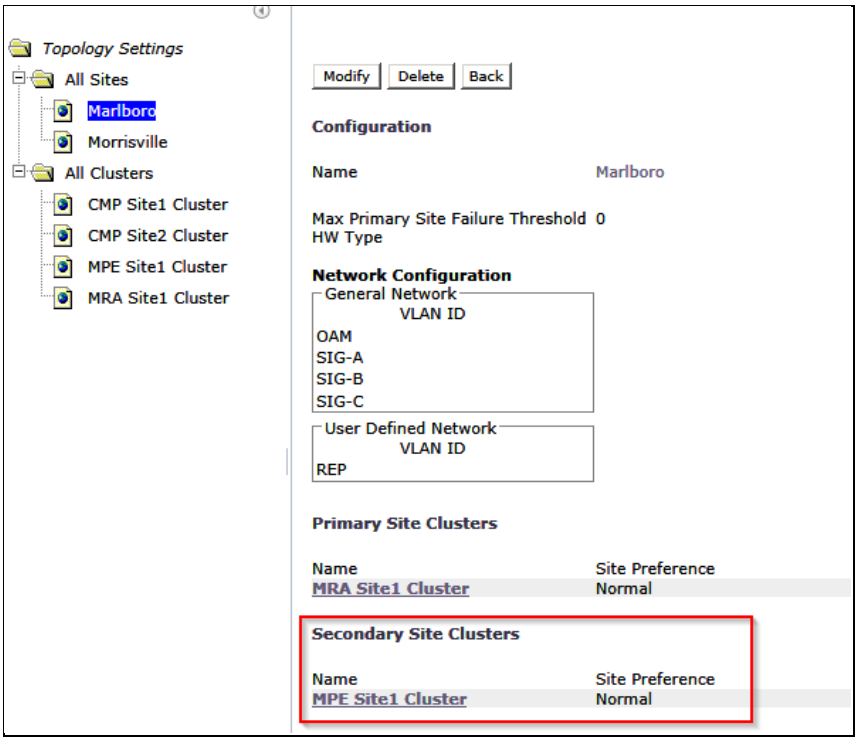
Step	Procedure	Details
		- If neither an IPv4 OAM IP nor a static IP address is defined, IPv4 cannot be selected. - Enter the HostName of the server. This must exactly match the host name provisioned for this server (the output of the `uname -n` Linux command). **NOTE:** If the server has a configured server IP, you can click Load to retrieve the remote server host name. If the retrieve fails, this a sign that the ip address configured is not accessible across the network. Alternately, you may enter the host name manually but it is recommended to do any network troubleshooting that may be required. - In the Path Configuration section, click **Add New** to add a Static IP. The New Path window opens. **NOTE:** If an alternate replication path and secondary HA heartbeat path is used, a server Static IP address must be entered in this field. - Enter a Static IP address and Mask. - Select the Interface: - SIG-A - SIG-B - SIG-C - REP - BKUP - Define the Secondary Site Settings  **Site Name**—Here the added server is associated with a configured site in the drop down tab if this is a geo-redundant topology **HW Type**—Select the type of hardware: - C-Class (default)—HP ProLiant BL460 Gen8 server - C-Class (segregated traffic) (a configuration where Signaling and other networks are separated onto physically separate equipment)—HP ProLiant BL460 Gen8 **Define the Network Configuration.** - if you selected C-Class, C-Class(segregated traffic), enter the general network—VLAN IDs. - Enter the OAM, SIG-A, and SIG-B (optional) virtual LAN (VLAN) IDs. VLAN IDs are in the range 1 through 4095. The default values are:

Step	Procedure	Details
		- OAM—3 - SIG-A—5 - SIG-B—6 - If the hardware type is C-Class or C-Class(segregated traffic), for the user defined network, enter the REP VLAN ID. **NOTE:** Virtual LAN (VLAN) IDs are in the range of 1 to 4095. **OAM VIP**—The OAM VIP is not typically used for Non-CMP clusters. The Real IP address is used by the CMP to communicate with the Non-CMP cluster. **Signaling VIPs** (required)—The signaling VIP is the IP address a PCEF (or Gateway) device uses to communicate with a cluster. Click **Add New VIP** to add a VIP to the system. A cluster supports the following redundant communication channels for carriers that use redundant signaling channels. - SIG-A - SIG-B - SIG-C At least one signaling VIP is required. - Define the settings for Server-C in the Secondary Site Settings section of the page - Click **Add Server-C** on the Topology Configuration page The Server-C configuration form opens - (Required) To enter the IP address, click Add New IP. The Add New IP window opens. - Enter the IP address in either IPv4 or IPv6 format. This is the IP address of the server. For an IPv4 address, enter it in the standard IP dot-format. For an IPv6 address, enter it in the standard 8-part colon-separated hexadecimal string format. - Select the IP Preference: IPv4 or IPV6. The server preferentially uses the IP address in the specified format for communication. - If neither an IPv6 OAM IP nor a static IP address is defined, IPv6 cannot be selected. - If neither an IPv4 OAM IP nor a static IP address is defined, IPv4 cannot be selected. - Enter the HostName of the server. This must exactly match the host name provisioned for this server (the output of the `uname -n` Linux command). **NOTE:** If the server has a configured server IP, you can click Load to retrieve the remote server host name. If the retrieve fails, this a sign that the ip address configured is not accessible across the network. Alternately, you may enter the

Step	Procedure	Details
		host name manually but it is recommeneded to do any network troubleshooting that may be required. - In the Path Configuration section, click **Add New** to add a Static IP. The New Path window opens. **NOTE:** If an alternate replication path and secondary HA heartbeat path is used, a server is Static IP address must be entered in this field. - Enter a Static IP address and Mask. - Select the Interface: - SIG-A - SIG-B - SIG-C - REP - BKUP **NOTE: NOTE:** These settings are only an example of a likely configuration. An actual deployment is specific to your requirements.
6. ☐	**CMP GUI:** Add MPE/MRA clusters	1. Save the Topology Configuration from the bottom of the Topology Configuration page. 2. Confirm the VLAN configuration if the hardware type requires VLANs  3. Click **OK** to confirm.  If the cluster added successfully, it is visible on the Cluster Configuration page. The Cluster Configuration page opens: 
7. ☐	**CMP GUI:** Add MPE, MRA clusters	Confirm the cluster is added successfully.

Step	Procedure	Details
		The following shows an example of adding of a non-CMP cluster that is MPE Appl Type cluster. Check that all alarms have cleared and then click **View** for the cluster that is added  Server-A and Server-B is in active and standby. It does not matter which server is active. Spare-Server-C shows a staus of Spare. If this is the case, and there are not any alarms, then the Geo-Redundant cluster was added successfully. **NOTE:** If the Forced Standby for Server-B is selected, clear the selection. For Example:   **NOTE:** If the topology configuration is performed at a time when the network connectivity between the CMP and the MRA/MPE servers being added to the topology is not available, the status of the added servers is offline and alarms are

Step	Procedure	Details
		generated due the offline state. These alarms persist until the servers become reachable from the CMP. The CMP continually retries connecting to the servers that are added in the topology. In this case, no further configuration is performed until the network connectivity between the CMP and the target servers is available. Do not proceed further but return to this step when the network connectivity from the CMP to the target servers is available. If the servers are reachable then proceed to the next step. Confirm that the non-CMP clusters are associated with the correct site. **Topology Settings→All Sites→<*Site Name*>** **Examples** • MPE Site1 cluster is associated with the Morrisville Site as a Primary Site cluster. This is Server-A and Server-B.  • MPE Site1 cluster is associated with the Marlboro Site as a Secondary Site cluster. This is Server-C.

Step	Procedure	Details
		 The cluster is successfully added.
8. ☐	Repeat the previous step for additional clusters	A list of clusters for configuration is added to this step as a reminder. The procedure for adding an MPE/MRA cluster is the same except for selecting the Appl Type which specify either MPE/MRA respectively.
9. ☐	If the CMP manages remote sites, and the sites are not available.	If the CMP manage remote sites, and the stes are not available. • Configure these clusters, but Return to the verify steps above after the connectivity is established. • Configure these clusters at a later time when the connectivity is established.
—End of Procedure—		

6.5 Performing SSH Key Exchanges

You must exchange SSH keys between the CMP, MPE, MRA servers. Perform this procedure whenever you add additional servers to the Policy Management topology. You can run the command multiple times, even if keys were exchanged

NOTE: After the topology is set up and SSH keys are exchanged, it is possible that a server in the topology changes its keys. This happens when:

- A server is added to the topology
- A server is re-installed
- A server is replaced by another server
- A server has its SSH keys recreated manually

In any of the above scenarios, rerun this procedure. The SSH provisioning utility rechecks the existing SSH key exchanges in the topology and provisions any key exchanges not performed. You can run the command multiple times, even if keys were exchanged.

Prerequisite:

- CMP Site 1 cluster is configured and GUI available
- Before beginning this procedure, the systems that are exchanging keys must be configured and reachable.

Check off (√) each step as it is completed. Check boxes are provided next to each step number.

If this procedure fails, contact Oracle Technical Services and ask for assistance.

6.5 Performing SSH Key Exchanges

Step	Procedure	Details

1. ☐	**Ssh to CMP Site 1 active server:** Run Key Exchanges on all servers	1. Use SSH to connect to the active server at the CMP Site 1 cluster as the admusr user.
		2. Enter the command `sudo ha.mystate` to confirm that the server is the active server in the HA cluster. The following example shows an active server:
		`login as: admusr`
		`Using keyboard-interactive authentication.`
		`Password:`
		`[admusr@cmp236 ~]$ sudo ha.mystate`
		`resourceId role node subResources lastUpdate`
		`DbReplication Active A0582.070 0 0425:164256.062`
		`VIP Active A0582.070 0 0425:164256.064`
		`QP Active A0582.070 0 0425:164256.104`
		`DbReplication_old OOS A0582.070 0 0425:164245.744`
		`[admusr@cmp236 ~]$`

2. ☐	**Ssh to CMP Site 1 active server:** Run Key Exchanges on all servers	1. Enter the following command: `$ sudo qpSSHKeyProv.pl—prov (double dash)` You are prompted: `The password of admusr in topology` 2. Enter the admusr password (*admusr_password*). The procedure exchanges keys with the rest of the servers in the Policy Management topology. If the key exchange is successful, the procedure displays the message SSH keys are OK. The following example shows a successful key exchange:

		``
^C[admusr@x52cmp-1a ~]$ sudo qpSSHKeyProv.pl --prov The password of admusr in topology: Connecting to admusr@x52mpe-1b ... Connecting to admusr@x52mra-1b ... Connecting to admusr@x52mpe-1a ... Connecting to admusr@x52mra-1a ... Connecting to admusr@x52cmp-1a ... Connecting to admusr@x52cmp-1b ... [1/6] Provisioning SSH keys on x52mpe-1b ... [2/6] Provisioning SSH keys on x52mra-1b ... [3/6] Provisioning SSH keys on x52mra-1a ... [4/6] Provisioning SSH keys on x52mpe-1a ... [5/6] Provisioning SSH keys on x52cmp-1a ... [6/6] Provisioning SSH keys on x52cmp-1b ...   SSH keys are OK. ```

3. ☐	**SSH to CMP Site 1 active server:** Verify Key Exchanges on all servers	1. Enter the following command to verify that the keys are successfully exchanged:
		`$sudo qpSSHKeyProv.pl—check—verbose`
		You are prompted for the password of admusr in topology.
		2. Enter the admusr password (admusr_password).
		The procedure verifies keys with the rest of the servers in the Policy Management topology and displays the results of each exchange. The following example shows all keys are checked and exchanged successfully:
		`[admusr@x52cmp-1a ~]$ sudo qpSSHKeyProv.pl --check --verbose`
		`The password of admusr in topology:`
		`Connecting to admusr@x52mpe-1b ...`
		`Connecting to admusr@x52mra-1b ...`
		`Connecting to admusr@x52mpe-1a ...`
		`Connecting to admusr@x52mra-1a ...`
		`Connecting to admusr@x52cmp-1a ...`
		`Connecting to admusr@x52cmp-1b ...`
		`[1/6] Checking SSH keys on x52mpe-1b ...`
		`[2/6] Checking SSH keys on x52mra-1b ...`
		`[3/6] Checking SSH keys on x52mra-1a ...`
		`[4/6] Checking SSH keys on x52mpe-1a ...`
		`[5/6] Checking SSH keys on x52cmp-1a ...`
		`[6/6] Checking SSH keys on x52cmp-1b ...`
		`From root@x52cmp-1b (10.240.220.230):`
		`to root@x52cmp-1b (10.240.220.230): OK`
		`to root@x52mra-1a (10.240.220.232): OK`
		`to root@x52cmp-1a (10.240.220.229): OK`
		`to root@x52mpe-1b (10.240.220.236): OK`
		`to root@x52mpe-1a (10.240.220.235): OK`
		`to root@x52mra-1b (10.240.220.233): OK`
		`From root@x52mra-1a (10.240.220.232):`
		`to root@x52mra-1b (10.240.220.233): OK`
		`From root@x52cmp-1a (10.240.220.229):`
		`to root@x52cmp-1b (10.240.220.230): OK`
		`to root@x52mra-1a (10.240.220.232): OK`
		`to root@x52cmp-1a (10.240.220.229): OK`
		`to root@x52mpe-1b (10.240.220.236): OK`
		`to root@x52mpe-1a (10.240.220.235): OK`
		`to root@x52mra-1b (10.240.220.233): OK`
		`From root@x52mpe-1b (10.240.220.236):`
		`to root@x52mpe-1a (10.240.220.235): OK`
		`From root@x52mpe-1a (10.240.220.235):`
		`to root@x52mpe-1b (10.240.220.236): OK`
		`From root@x52mra-1b (10.240.220.233):`
		`to root@x52mra-1a (10.240.220.232): OK`
		`SSH keys are OK.`
		`[admusr@x52cmp-1a ~]$`

—End of Procedure—		

6.6 Configure Routing on Your Servers

On the MPE and MRA servers, the default route is initially configured to route all traffic via the OAM interface for remote servers. This facilitates clustering and topology configurations. However, in many networking environments, it is desirable to route signaling traffic (that is, Diameter messages) using the

Signaling interfaces of the servers and switches, and OAM traffic (that is, replication, configuration, alarms, and reports) using the OAM interface. This requires configuring routing on the servers.

If you are using the Signaling interfaces, you must configure the required static routes on the MPE and MRA servers to separate OAM and Signaling traffic. The recommended method to provide separation is:

- Add static routes on the OAM network to management servers (CMP, NTP, SNMP, PM&C).

  NOTE: Administration of the MPE and MRA servers that require SSH access may be impacted by moving the default gateway and may need static routes as well.

- Change the default route on the servers to the Sig-A network.

In this way, traffic to other signaling points in the network follows the default route over the Sig-A network.

Other routing configurations may be required, depending on your needs.

Prerequisite:

Before beginning this procedure, verify that you have SSH access to the MPE and MRA servers.

You need the following information to complete this procedure:

- The root account password (root_password)
- At a minimum, the following static routes:
  - Site 1 and 2 CMP OAM network (if not co-located)
  - Server C for georedundant MPE and MRA clusters
  - NTP server
  - DNS server
  - snmp_trap_destination (SNMP trap destination)
  - Remote backup archives
  - External syslog servers
  - Any host you wish the MPE or MRA server to access over the OAM network (that is, routes to mates in georedundant networks)

The procedure for configuring routing on your servers is described in the Platform Configuration User's Guide

TIP: During this procedure, ensure that access to the server ILOM or iLO remote console is always available if a route change impacts remote access to get back into the server. Using SSH from the CMP system to connect to the MRA or MPE servers is recommended to minimize such impacts.

NOTE: You must perform this procedure for every MPE and MRA server. Perform this procedure only for the MPE and MRA servers, as the CMP system retains the default route on the OAM interface.

6.7 Configure Policy Components

This section covers procedures to configure the Policy Servers to a minimum level to perform a test call.

6.7.1 Adding MPE and MRA to CMP Menu

This procedure configures the Policy Server (MPE) and MRA applications.

Prerequisite:

- Network access to the CMP OAM IP address, to open a web browser (HTTP)

- MRA and MPE clusters are added to the CMP Topology

  NOTE: Only the following Web Browsers are supported in OCPM 12.6

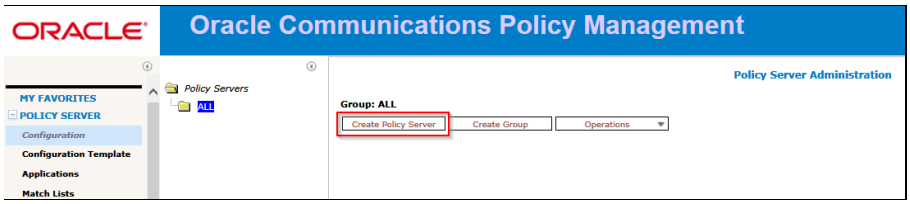
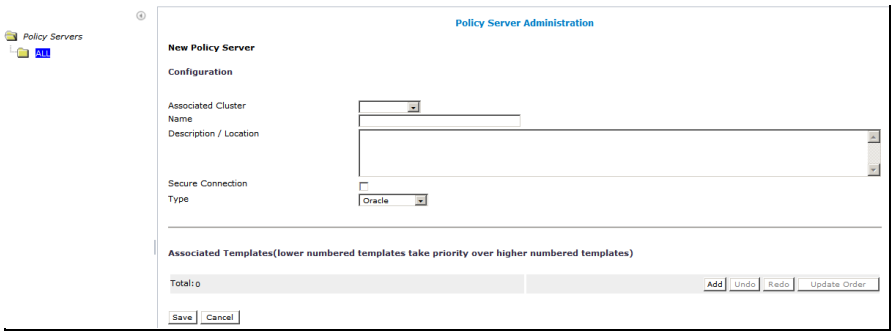
  - Mozilla Firefox® release 81.0 or later
  - Google Chrome version 86.0 or later

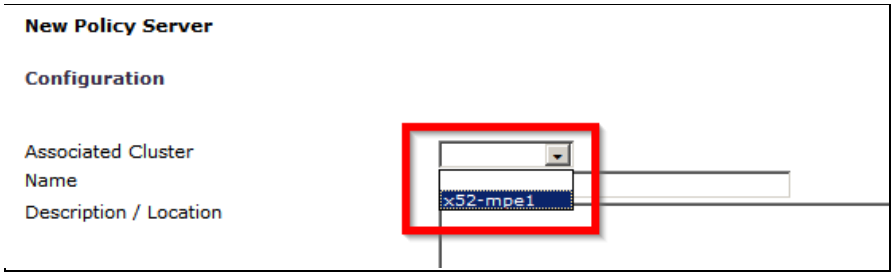
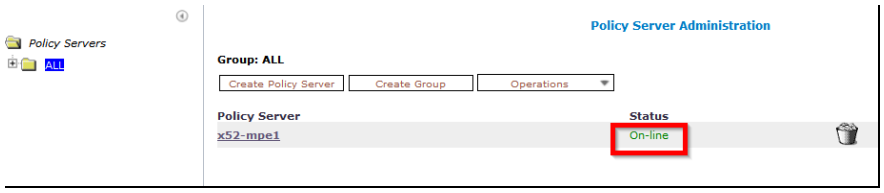
  *Internet Explorer in not supported for this procedure

Check off (√) each step as it is completed. Check boxes are provided next to each step number.

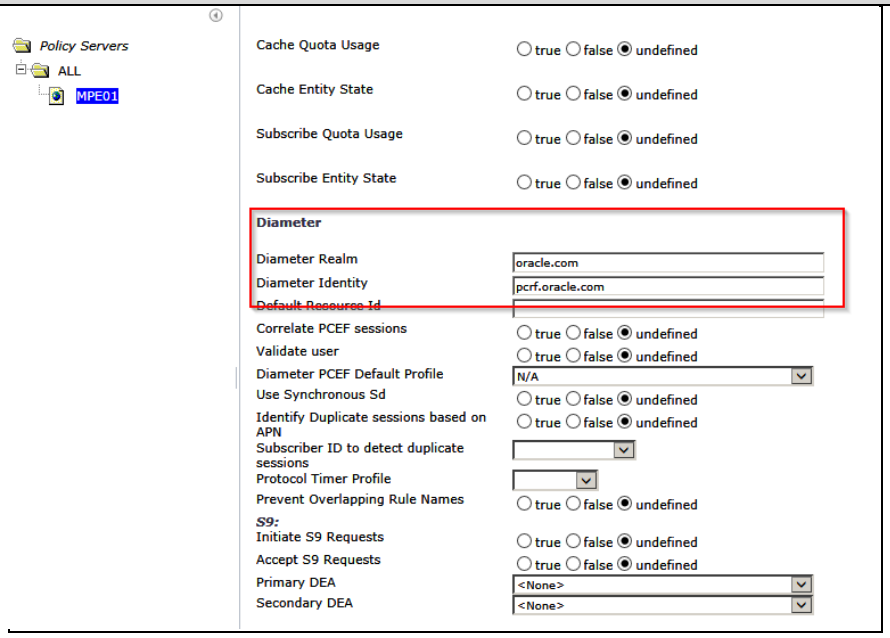
If this procedure fails, contact Oracle Technical Services and ask for assistance.

6.7.1: Adding MPE and MRA to the CMP Menu

Step	Procedure	Details
1. ☐	**Create Policy Server in CMP GUI**	1. Navigate to **Policy Server→ Configuration→ Policy Servers**  2. Click **Create Policy Server** in the Policy Server Administration screen:  3. Enter values for the configuration attributes: a. **Associated Cluster** (required)—Select the cluster with which to associate this MPE device. MPE clusters configured in Topology Settings are listed. b. **Name—**Name of this MPE device. The default is the associated cluster name. c. **Description/Location** (optional)—Information that defines the function or location of this MPE device. d. **Secure Connection—**Designates whether or not to use the HTTPS protocol for communication (certifcates must be configured to use this option) between Policy Management devices. If selected, devices communicate over port 8443. e. **Type—**Defines the policy server type: ▫ **Oracle** (default)—The policy server is an MPE device and is managed by the CMP. ▫ **Unmanaged—**The policy server is not an MPE device and therefore cannot be actively managed by the CMP. This selection is useful when an MPE device is routing traffic to a non-Oracle policy server.

Step	Procedure	Details
		NOTE: When configuring an associated cluster, the menu is populated with MPE clusters that are configured in the CMP Topology from previous steps.  4. Click **Save** and confirm Configured Policy Server status is On-line. 
2. ☐	Check MPE cluster in Reports tab	1. Navigate to **Policy Server→Configuration →** <*MPE*>**→ Reports** tab 2. Validate that MPE cluster status is On-line and that both active and standby servers displayed correctly.
3. ☐	Diameter configuration of MPE	1. Nvaigate to **Policy Server→ Configuration→** <*MPE*>**→Policy Server** tab There are many configurations on Policy Server tab for an associated MPE. The most important configurations to define is Diameter Realm and identity to enable Diameter connections.

Step	Procedure	Details



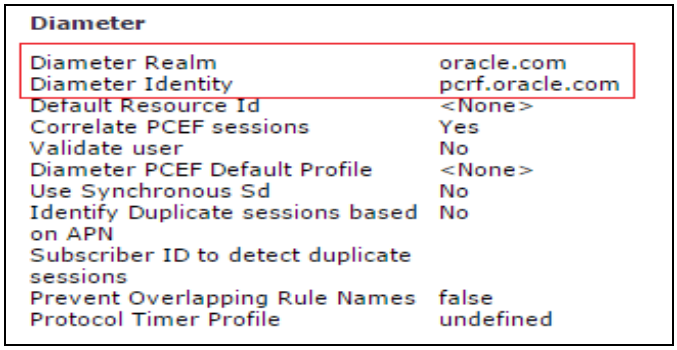
2. To define these Diameter parameters, click **Modify.**

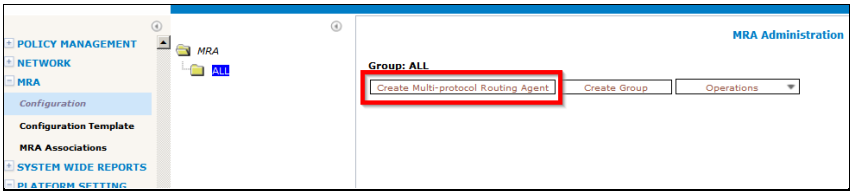
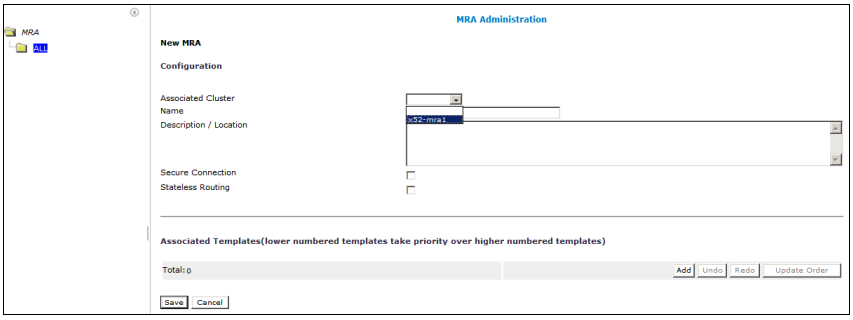
3. Enter the Diameter Realm and Identity for your network

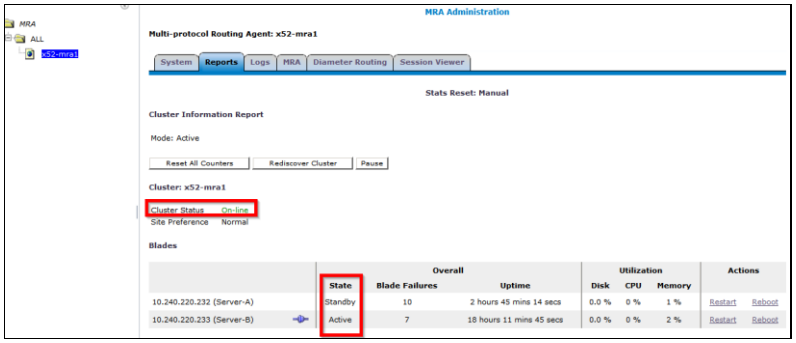
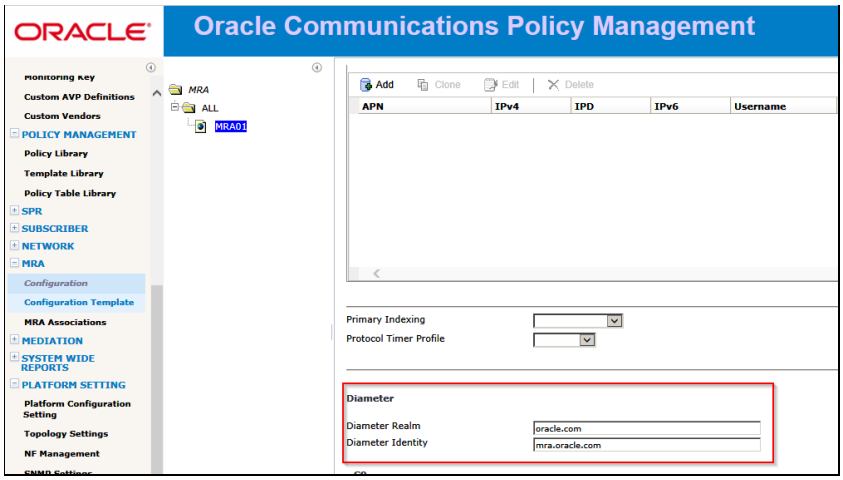
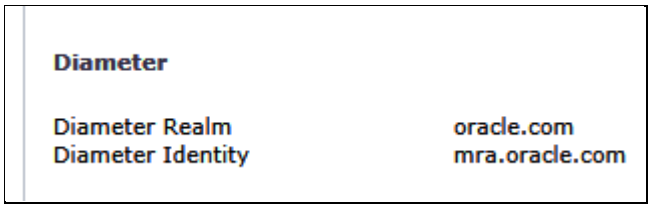
4. Click **Save**

Attribute	Description
Diameter Realm	The domain of responsibility (for example, `galactel.com`) for the MPE device.
Diameter Identity	The fully qualified domain name (FQDN) of the MPE device (for example, `mpe3.galactel.com`).

For example:



Step	Procedure	Details
4. ☐	Create MRA in CMP GUI	1. Navigate to **MRA →Configuration→ ALL**  2. Click **Create Multi-protocol Routing Agent** in the MRA Administration screen:  3. Enter information as appropriate for the MRA cluster: - **Associated Cluster** (required)—Select the MRA cluster from the list. - **Name** (required)—Enter a name for the MRA cluster. - **Description/Location** (optional)—Free-form text. Enter up to 250 characters. - **Secure Connection—**Select to enable a secure HTTP connection (HTTPS) instead of a normal connection (HTTP). The default is a non-secure (HTTP) connection. - **Stateless Routing—**Select to enable stateless routing. In stateless routing, the MRA cluster only routes traffic; it does not process traffic. The default is stateful routing. 4. Click **Save** and confirm that the configured MRA status is On-line.

Step	Procedure	Details
5. ☐	Check MRA cluster in Reports tab	1. Navigate to **MRA → Configuration → MRA → Reports** tab  2. Validate that MPE cluster status is On-line and that both active and standby servers display correctly.
6. ☐	Diameter configuration for MRA	1. Navigate to **MRA → Configuration → MRA → MRA** tab It is important to define Diameter Realm and identity to enable Diameter messaging to function:  **2.** To define these Diameter parameters, click **Modify** 3. Enter the Diameter Realm and Identity that your network uses. 4. Click **Save.** 
—End of Procedure—		

6.7.2 Configure MPE Pool on MRA (Policy Front End)

If MRAs (Policy Front End) are used in the Policy Management System, the MPEs for which the MRA acts as the Policy Front End, must be added to the MPE Pool on the MRA. If MPEs are not used in the Policy solution, skip this procedure.

This procedure adds the MPE clusters to the MPE Pool of the MRA (Policy Front End)

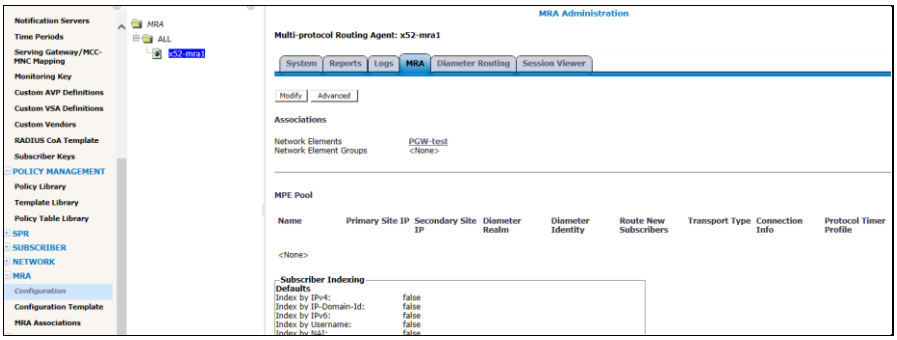
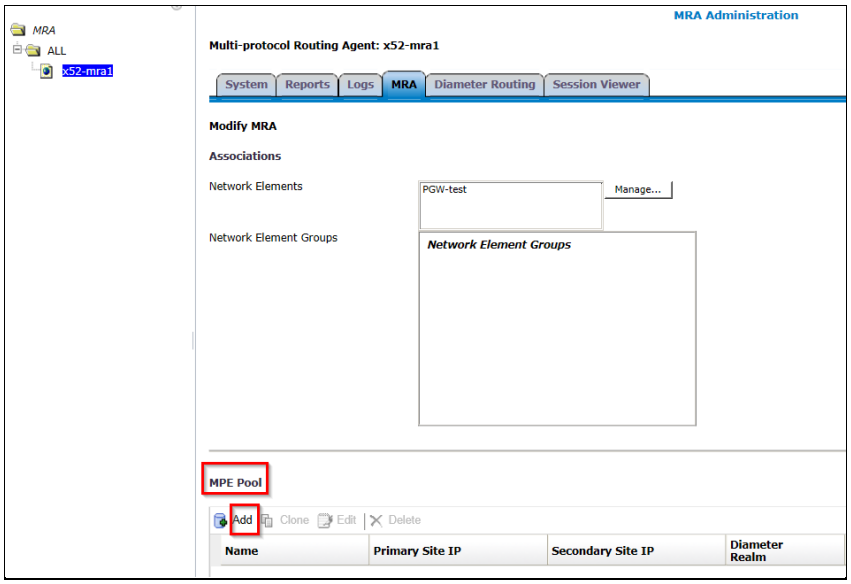
Prerequisite:

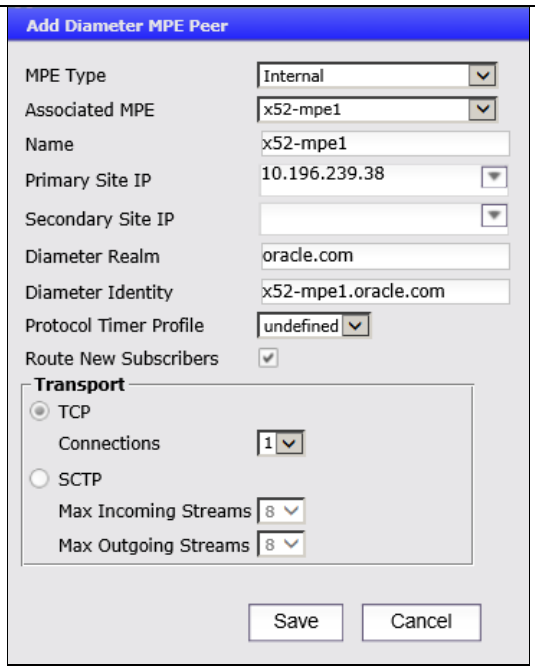
- Network access to the CMP OAM IP address, to open a web browser (HTTP)
- MRA and MPE clusters are added to the CMP Menu

Check off (√) each step as it is completed. Check boxes are provided next to each step number.

If this procedure fails, contact Oracle Technical Services and ask for assistance.

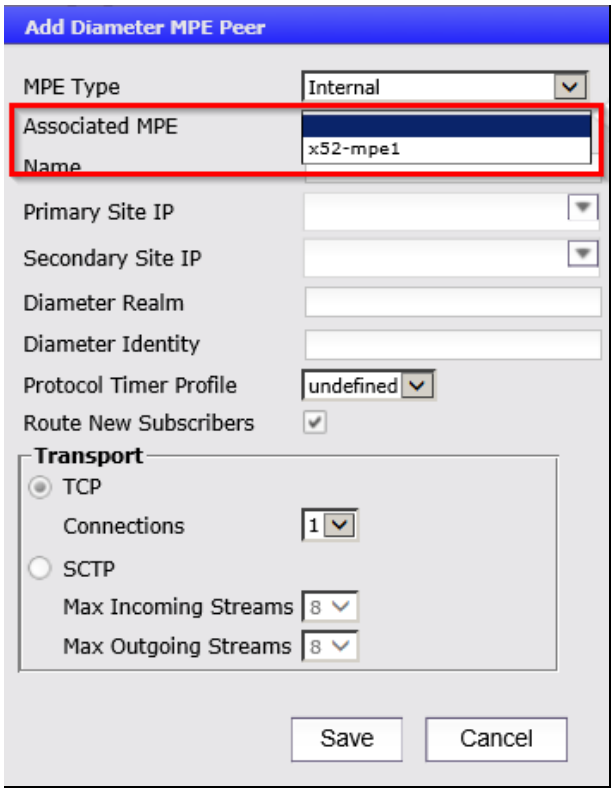
6.7.2: Configure MPE Pool on MRA (Policy Front End)

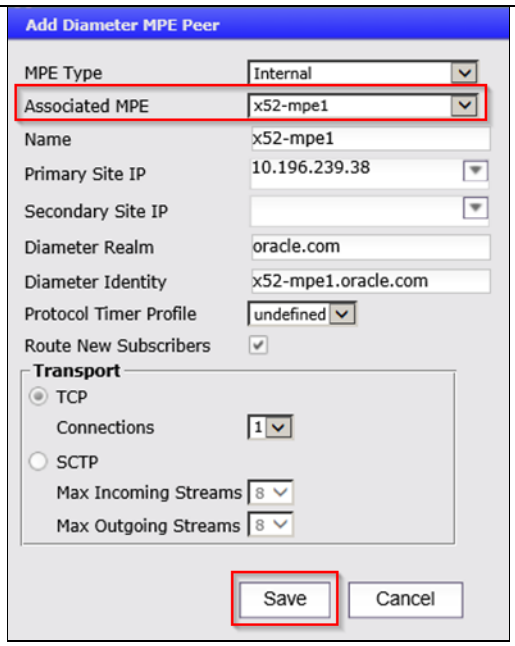
Step	Procedure	Details
1. ☐	Configure MPE Pool on MRA	1. Navigate to **MRA →Configuration→ <*MRA*>→MRA** tab  2. Click **Modify** in the MRA Administration screen: The MPE Pool configuration form opens.  3. Click **Add** under MPE Pool. The Add Diameter MPE Peer form opens.



4. On the Add Diameter MPE Peer form, select an MPE cluster in the Associated MPE list.

   The Associated MPE list, shows the MPE clusters configured in the CMP topology.



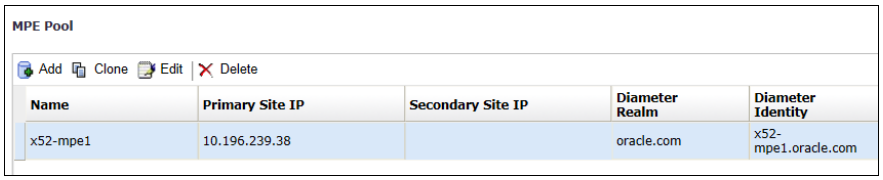


The required fields auto-populate.

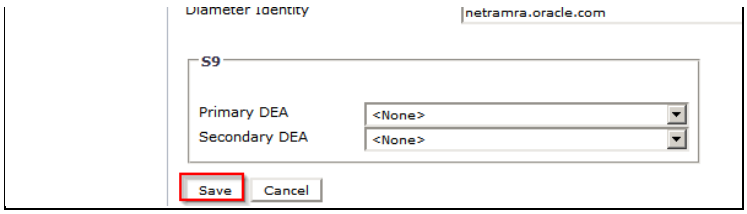
5. Click **Save**

   NOTE: The Diameter Realm and Diameter Identity must be configured on the MPE.

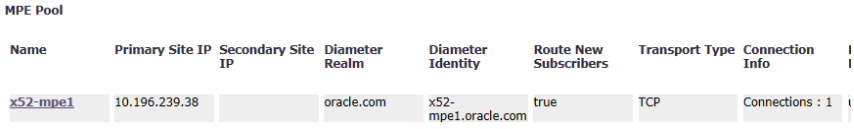
   The MPE cluster is listed in the MPE Pool.



6. Navigate to the bottom of the form and click **Save** again.

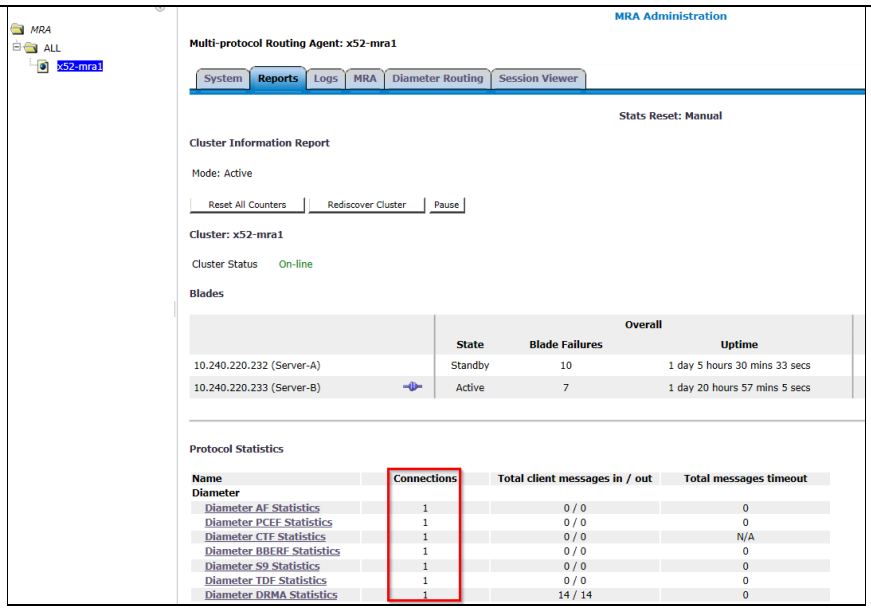


   The MPE cluster is listed in the MPE Pool.



7. Confirm the Diameter connection to the MPE from the MRA on the MRA Reports tab

   Navigate to **MRA → Configuration →** <*MRA*> **→ Reports** tab



A 1401 Log is noted in the MPE Trace Log that the Diameter connection between the MRA and the MPE is established.

1401	Warning	Diameter:Transport connection opened with peer 10.196.68.10:34824

—End of Procedure—

6.7.3 Define and Add Network Elements

Network elements are configured in the CMP to define the external systems that the Policy Server communicates.

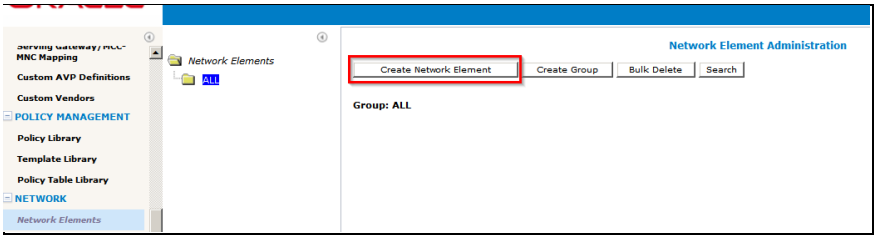
Prerequisite:

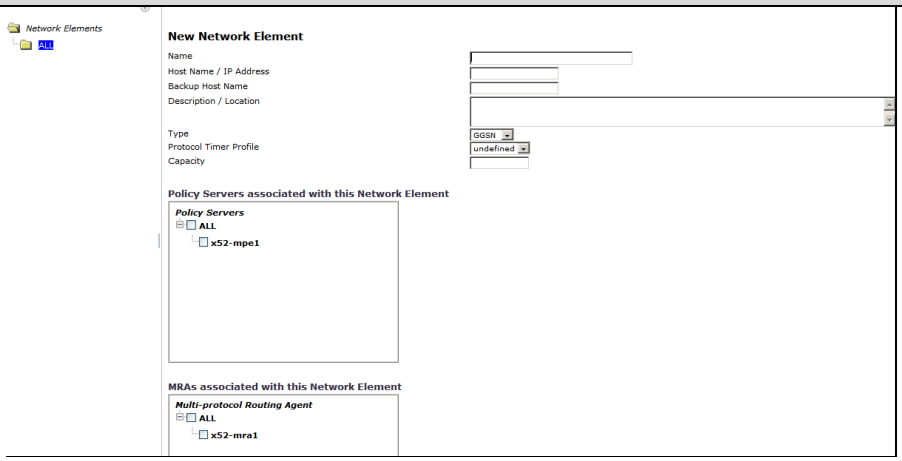
- Network access to the CMP OAM IP address, to open a web browser (HTTP)
- MRA and MPE clusters are added to the CMP Menu

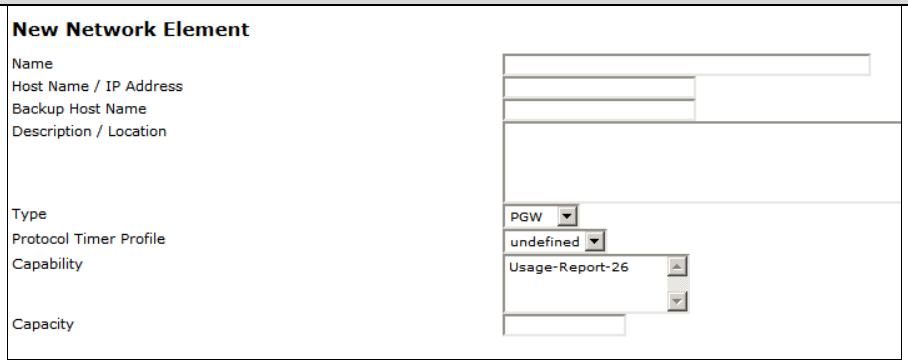
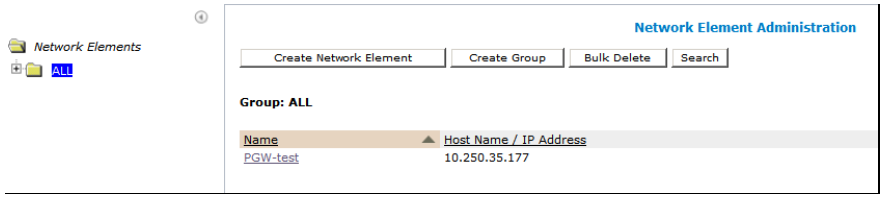
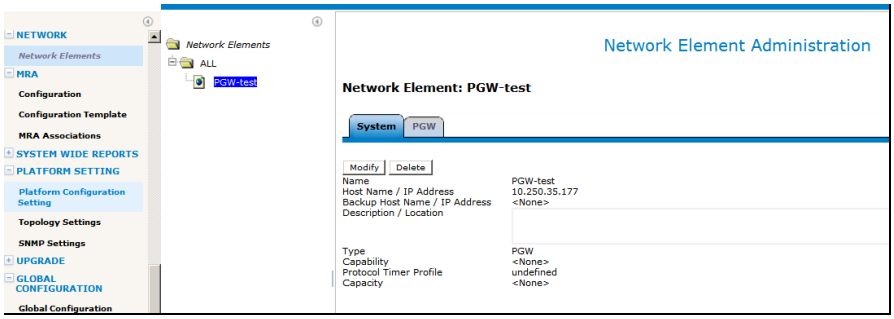
Check off (√) each step as it is completed. Check boxes are provided next to each step number.

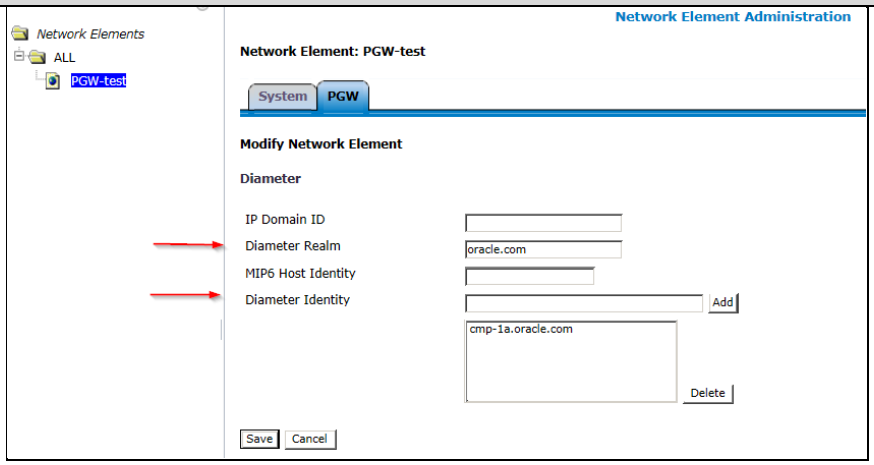
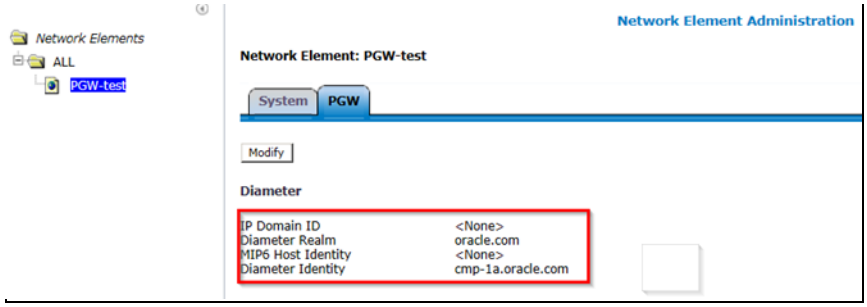
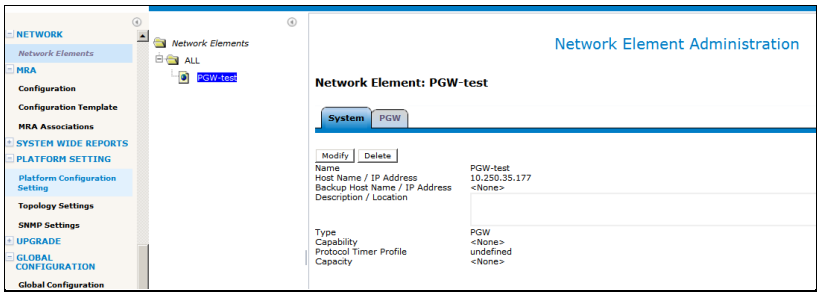
If this procedure fails, contact Oracle Technical Services and ask for assistance.

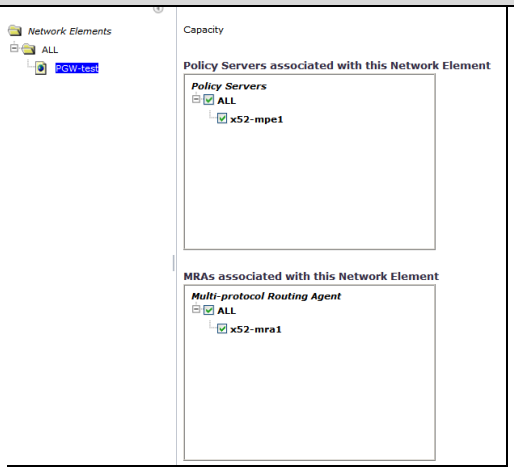
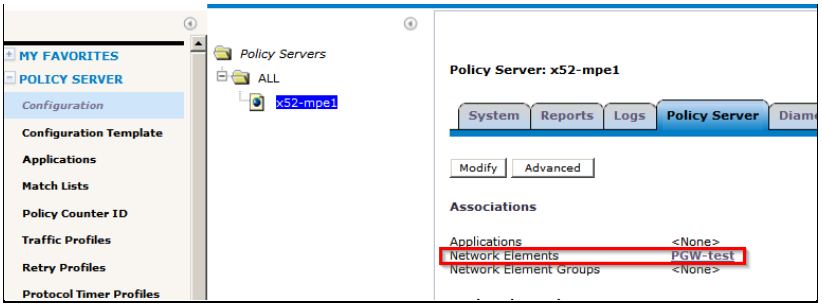
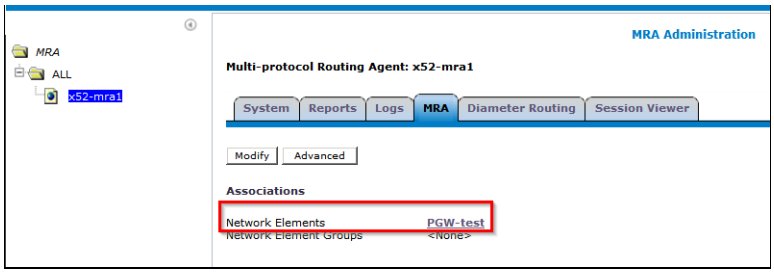
6.7.3: Define and Add Network Elements

Step	Procedure	Details
1. ☐	Create Network Element in CMP GUI	1. Navigate to **Network→Network Elements→All**  2. Click **Create Network Element** on the Network Element Administration screen:

Step	Procedure	Details
		 3. Enter information for the network element: a. **Name** (required)—The name of the network element. b. **Host Name/IP Address** (required)—Registered domain name, or IP address in IPv4 or IPv6 format, of the network element. c. **Backup Host Name** (optional)—Alternate address that is used if communication between the MPE device and the primary address for the network element fails. d. **Description/Location** (optional)—Free-form text. Enter up to 250 characters. e. **Type** (required)—Select the type of network element. The supported types are: **NOTE:** This list varies depending on the configuration of the CMP system. ▫ **PDSN—**Packet Data Serving Node (with the sub-types Generic PDSN or Starent) ▫ **HomeAgent—**Customer equipment Home Agent ▫ **GGSN** (default)—Gateway GPRS Support Node ▫ **HSGW—**HRPD Serving Gateway ▫ **PGW—**Packet Data Network Gateway ▫ **SGW—**Serving Gateway ▫ **DPI—**Deep Packet Inspection device ▫ **DSR—**Diameter Signaling Router device ▫ **NAS—**Network Access Server device f. **Protocol Timer Profile**—select a protocol timer profile. For information on creating protocol timers, see Managing Protocol Timer Profiles in the Configuration Management Platform Wireless User's Guide g. **Capacity**—Not applicable. h. When you finish, click **Save**. i. For this example a PGW Network Element is defined.

Step	Procedure	Details
		 4. After completing the form, click **Save**.  The Network Element is created.
2. ☐	Configure Network Element in CMP GUI	1. Navigate to **Network→Network Elements→Network Element** entity  The created Network Element displays on the System tab, showing the configuration from the previous step. For an initial call to the Policy Management System, the Network Element needs connectivity to the Policy Management System. In addition the Network Element needs a Diameter Identity used to authenticate the Diameter connection from the Network Element. 2. Navigate to the **Network Element → PGW** tab of the to configure the Diameter Identity that is used to authenticate the Policy Management System. 3. Click **Modify**.

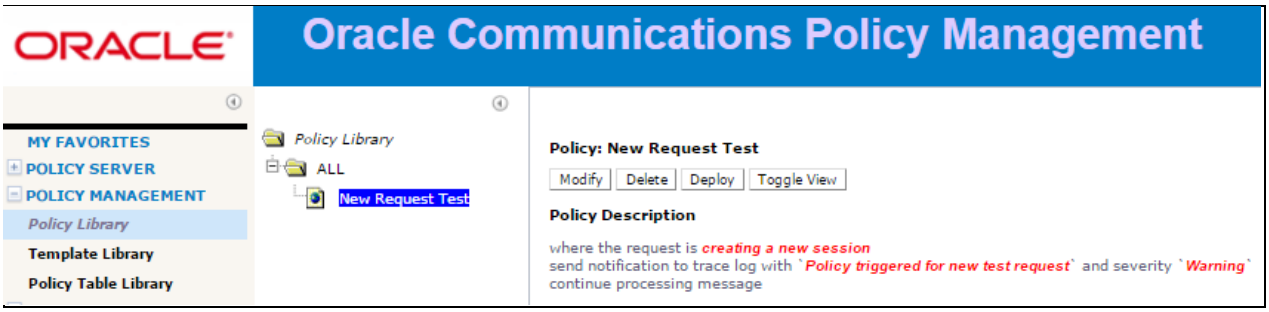
Step	Procedure	Details
		 **NOTE:** This tab is dependent on the Network Element type that was configured during the previous step. In this example the Network Element type used is a PGW (Packet Gateway) which is used to establish a Diameter connection to the Policy Management System. 4. When you finish, click **Save**. 
3. ☐	Deploy Network Element in CMP GUI	1. Navigate to **Network→Network Elements →<*Network Element entity*>**  2. Click **Modify** in the Network Element Administration screen and select the options to deploy the network element to the MPE and MRA (if present).

Step	Procedure	Details
		 3. Click **Save**. 4. Navigate to **Policy Server →Configuration→** <*MPE*> **→Policy Server** tab  5. Confirm the deployed Network Element is associated with the MPE. 6. Navigate to **MRA →Configuration→**<*MRA*> **→MRA** tab  7. Confirm the deployed Network Element is associated with the MRA.
—End of Procedure—		

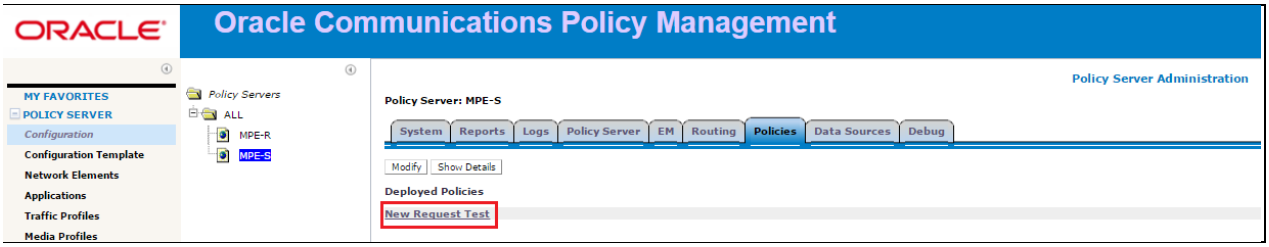
6.8 Load Policies and Related Policy Data

This step is optional. Policies are not required to process a test call but for the purpose of verification, a basic policy is installed manually, or using an import action and an xml file. The policy must be deployed to the MPE which processes the test call.

Here is an example of a very simple policy that is used to confirm session creation for a test call by viewing the trace logs on the MPE that processes the test call.

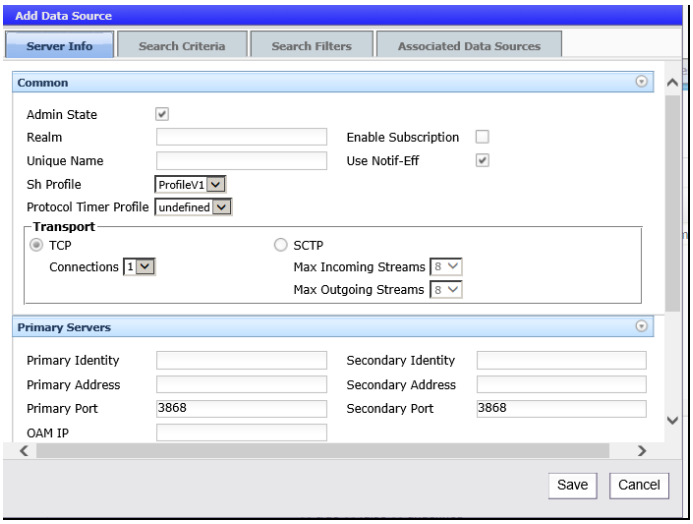


NOTE: This policy must be deployed to the MPE that processes Diameter session requests. Deployed policies are verified using the Policies tab for the MPE that processes the test request:

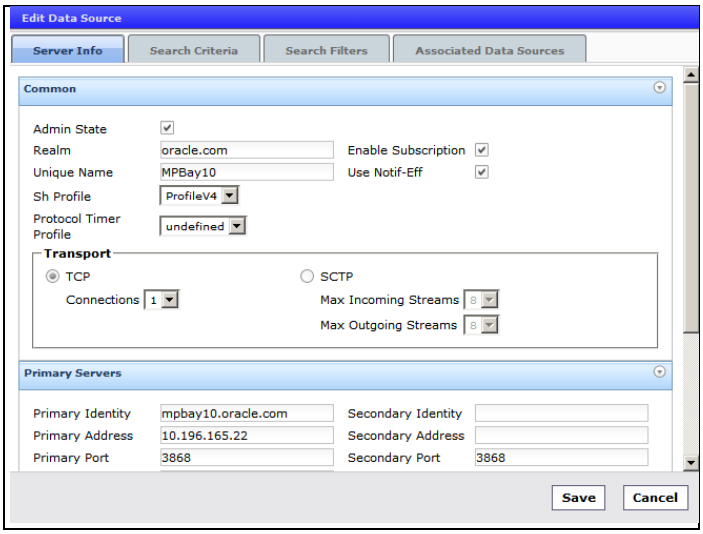


6.9 Add a Data Source

This step is optional. When the test call is received by the MPE, the MPE is configured to perform a Subscriber lookup to an appropriately configured Subscriber Database. Refer to [Configuration Management Platform Wireless User's Guide] for more information.



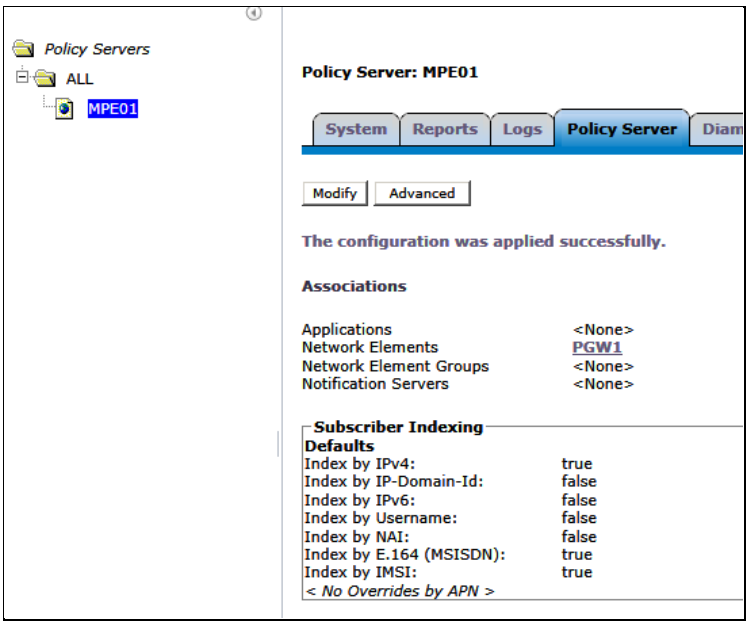
Here is a sample configuration. This form is specific to the site.



6.10 Perform Test Call

A basic test call confirms that the system is ready for testing of call scenarios defined by the customer. The test call is initiated from the network element that was created. For example, a PGW (Packet Gateway) first establishes a Diameter connection with the PCRF and then initiate the test call by sending an Initial Diameter CCR-I message.

NOTE: Customer specific information such as Indexing and Diameter Realm and Diameter Identity may be required on the **MPE →Policy Server** tab for the test call. The following is a sample for reference only.



6.11 Pre-Production Configurations

There are other steps required to verify the Operations configuration of the system. For example, to verify that the SNMP traps (Aarms) are being delivered to the Network Management centers. These are outside the scope of this document, but also need to be planned and performed.

Reference the following document for information on configuring SNMP:

SNMP User's Guide 12.6

Additional procedures are referenced from the following documents:

- Platform Configuration User's Guide
- Configuration Management Platform, Wireless User's Guide

Changes in the behavior of Release 12.6 are documented in the Oracle® Communications Policy Management Release Notes Release 12.6

Behavior Modifications

Firewall Enabled by Default—ER 22536198

Firewall functionality is enabled by default. The server firewall protects Policy Management against DDoS, flooding attacks, and unwanted connections. The settings are not altered during the upgrade.

7. SUPPORTING PROCEDURES

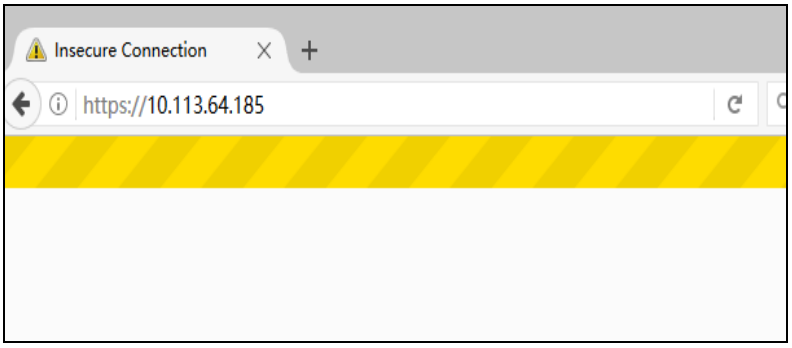
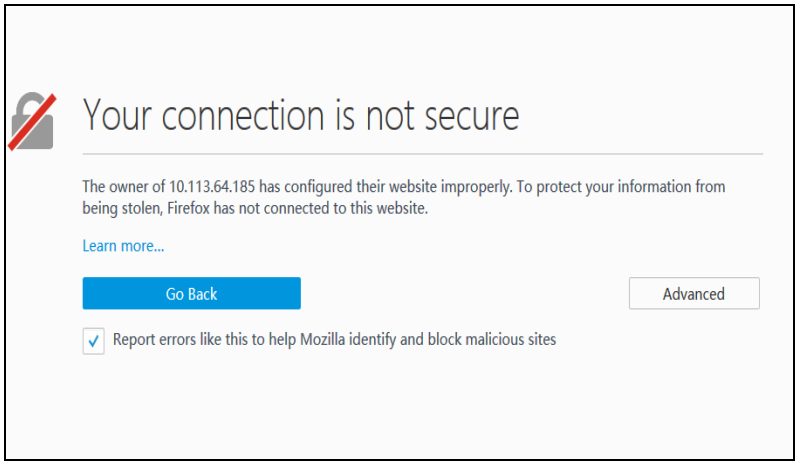
The following procedures may be referenced during installation.

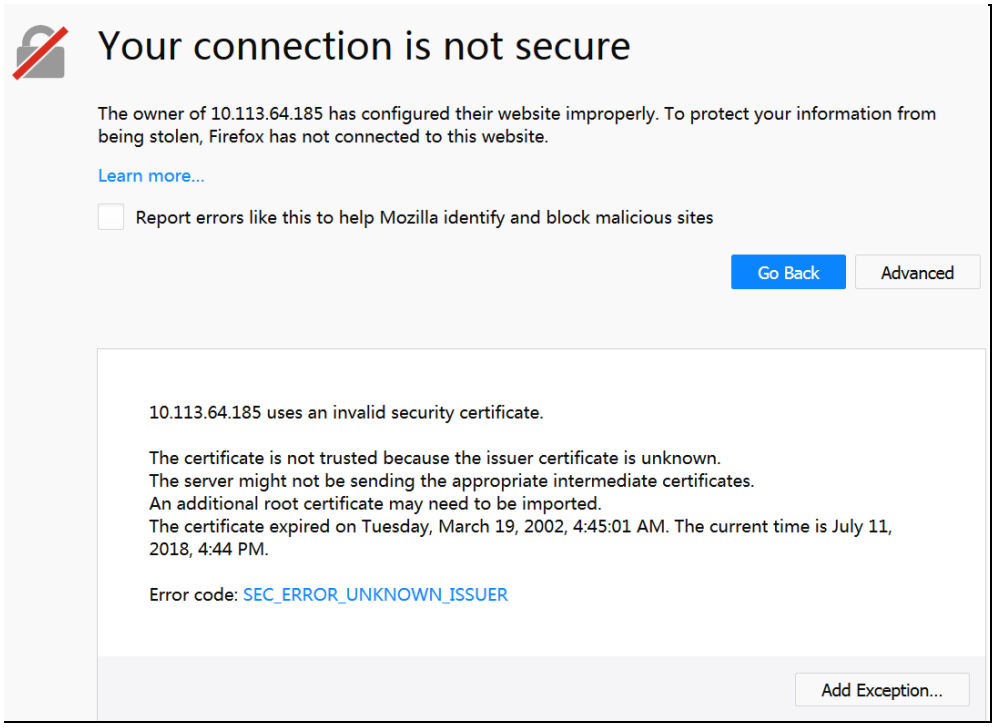
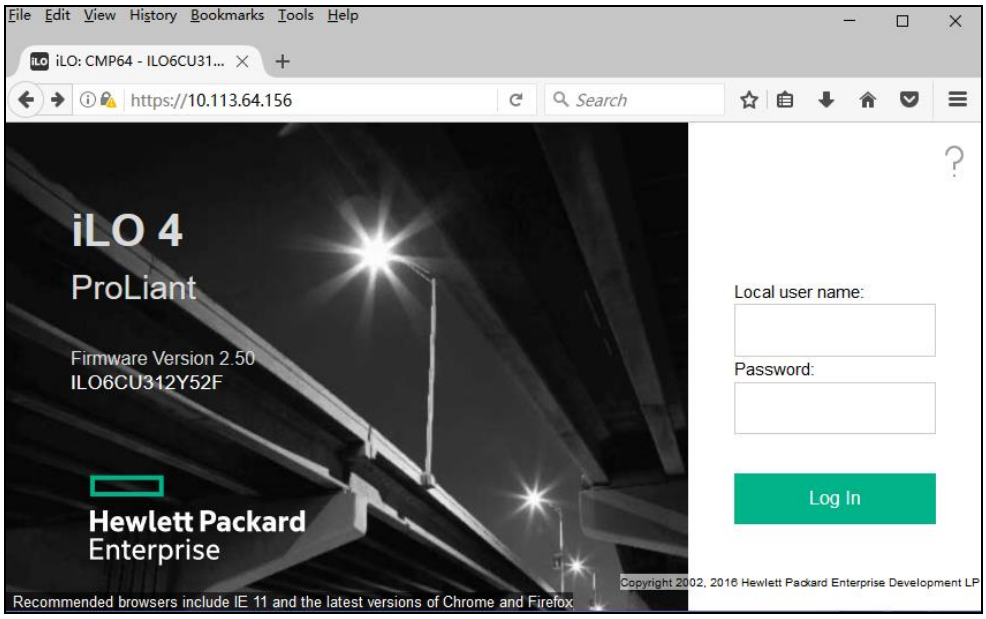
7.1 Accessing the iLO VGA Redirection Window

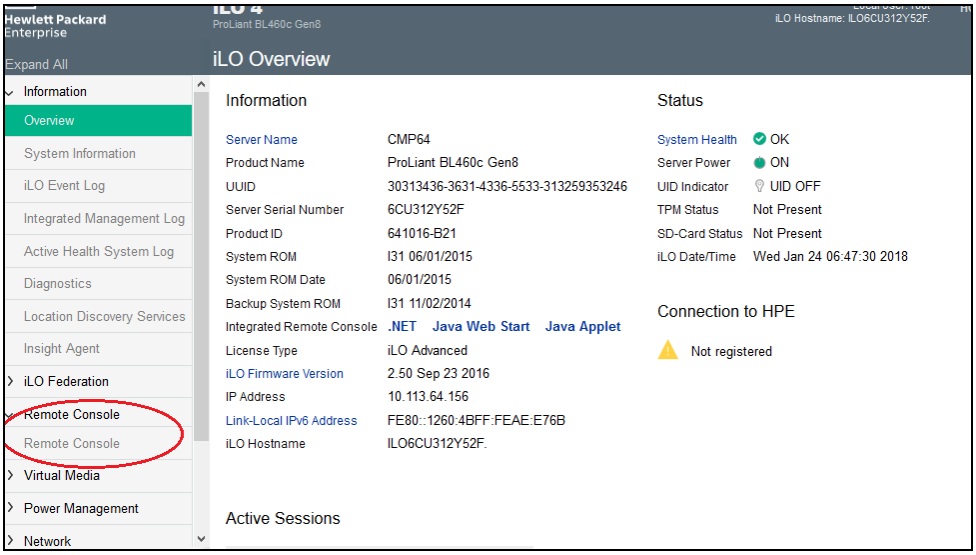
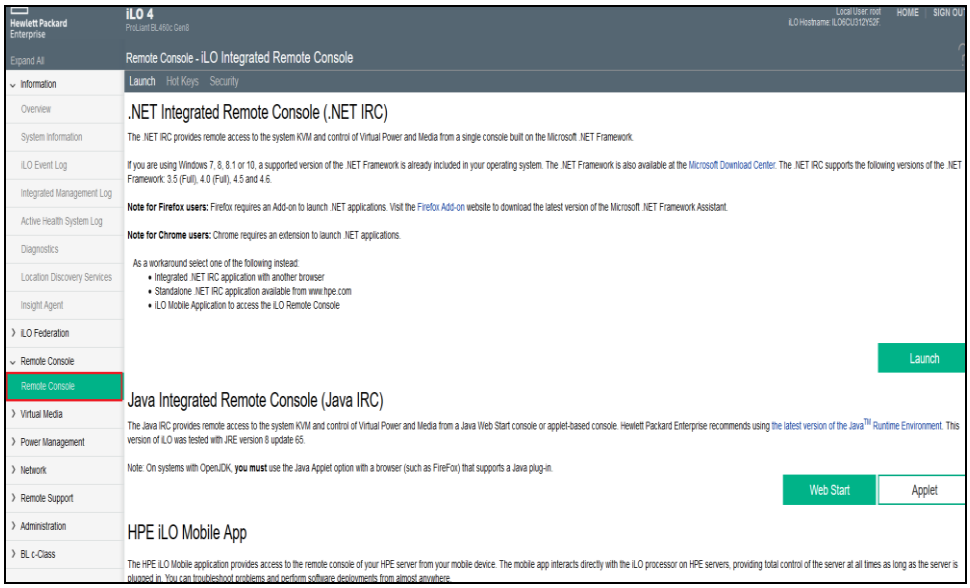
7.1.1 Accessing the iLO VGA Redirection Window for HP Servers

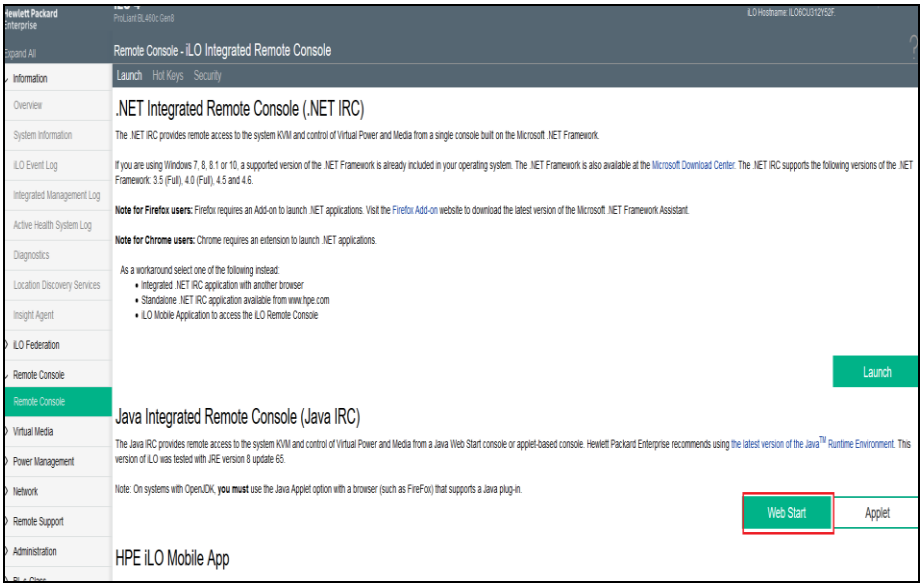
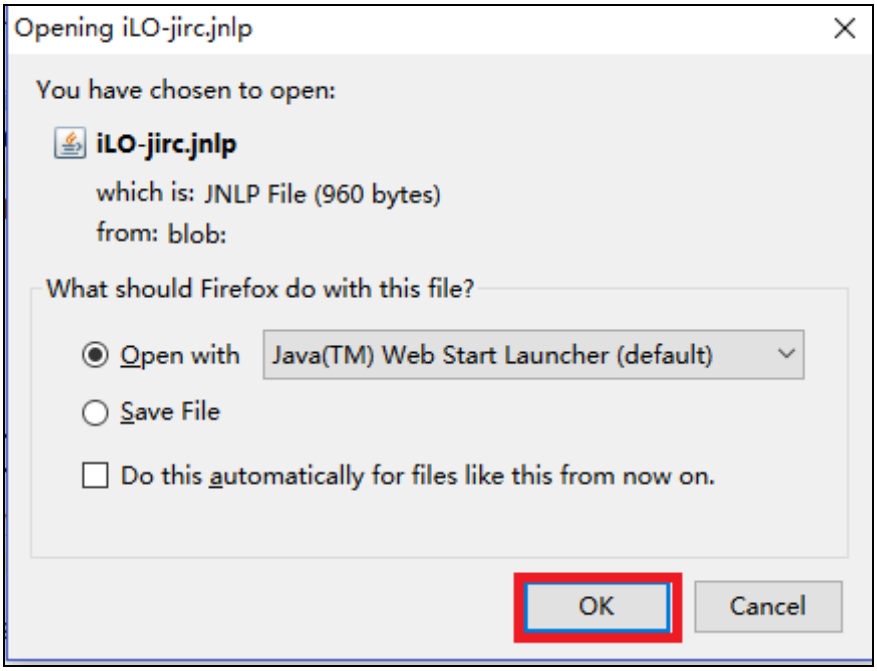
This procedure may very slightly depending the browser is used. If security certificates are installed on the client browser the security exceptions are not encountered.

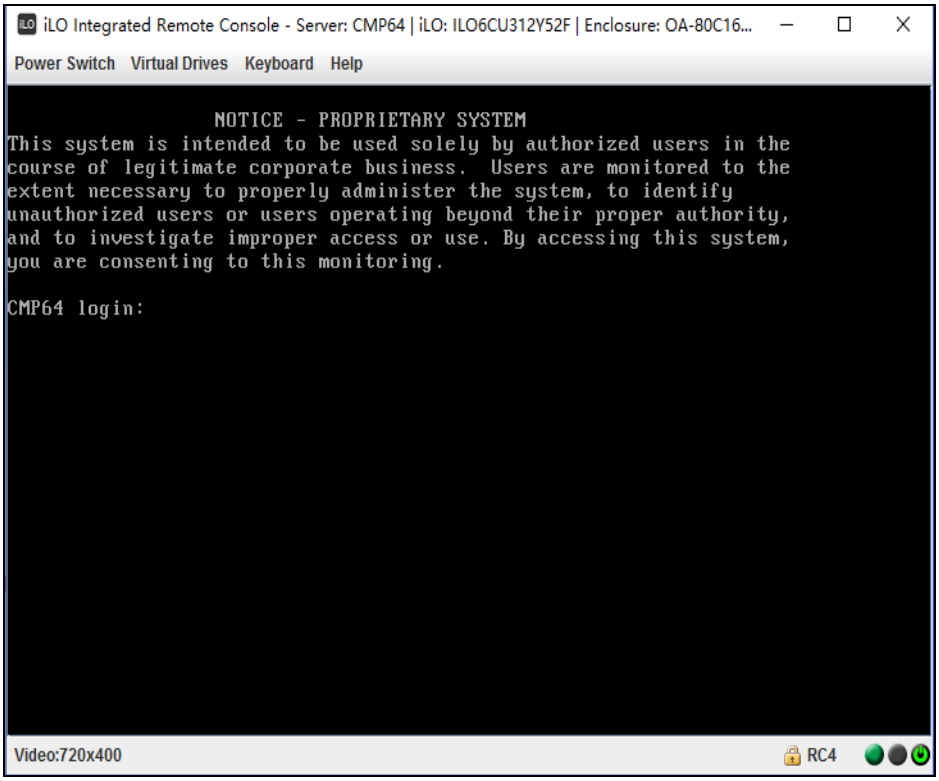
Accessing the iLO VGA Redirection Window for HP

Step	Procedure	Result
1. ☐	Launch an approved web browser and connect to the iLO interface **NOTE:** Always use `https://` for iLO GUI access.	
2. ☐	The first time the web browser connects to the iLO a Security Certificate warning message displays.	

3. ☐	Configure security exception	**1.** Click **Advanced.** 2. Click **Add Exception.** 3. Click **Confirm Security Exception** in the resulting window. 
4. ☐	Login to the iLO console as administrator	

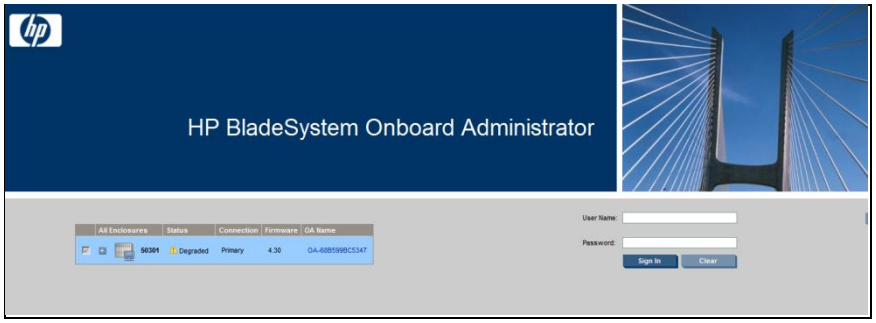
5. ☐	The administration GUI is displayed. Expand the Remote Console section in the left pane of the GUI.	
6. ☐	The Remote Console tab is expanded Select the **Remote Console** option	

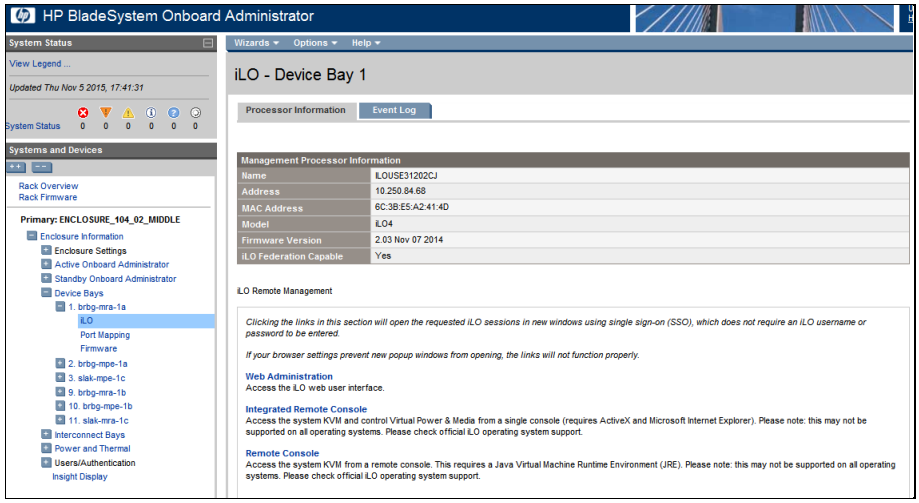
7. ☐	The Remote Console GUI is displayed Click **Web Start** in the Java Integrated Remote Console section	
8. ☐	The Opening iLo-jirc.jnlp window opens. Click **OK** to Open with Java(TM) Web Start Launcher	

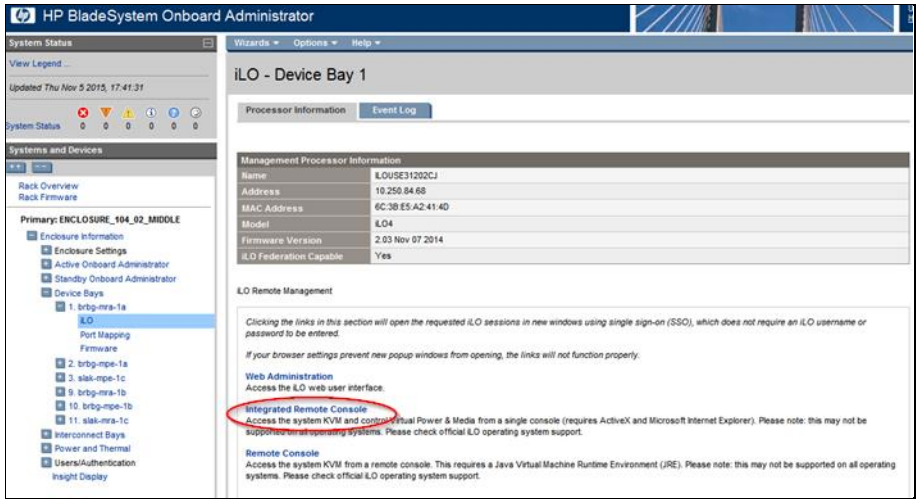
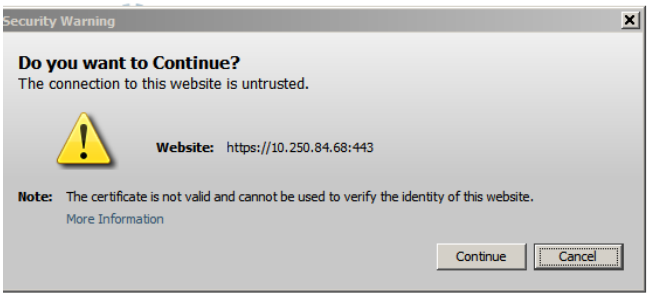
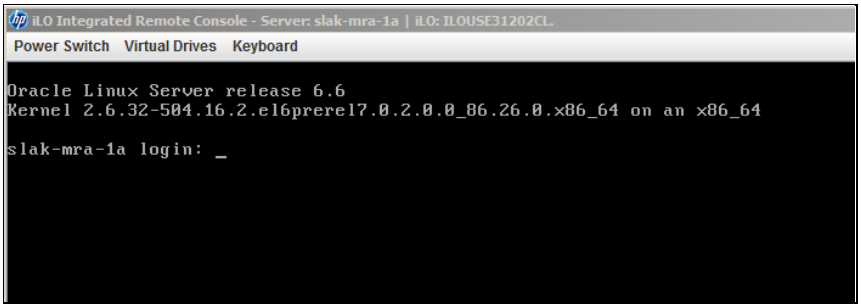
9. ☐	The iLO Console window is displayed.	
—End of Procedure—		

7.1.2 Accessing the Remote Console using the OA (c-Class)

7.1.4: Accessing the Remote Console using the OA (c-Class)

Step	Procedure	Result
1. ☐	**Web Browser:** Access Onboard Administrator Login (must be active OA)	Open a web browser and navigate to the OA IP address. Note that you be prompted with a warning for security certificates, because the certificate is self-signed. You must select Continue to access this page. 
2. ☐	**Web Browser:** Login as Administrator, and view available server blades	Log in to HP OA as a user with administrative privilege.

Step	Procedure	Result
3.	**Web Browser:** Open the iLO form for the server blade you wish to connect to	From the navigation pane, select **Device Bays**, select the expand icon for the device, and click **iLO**. 

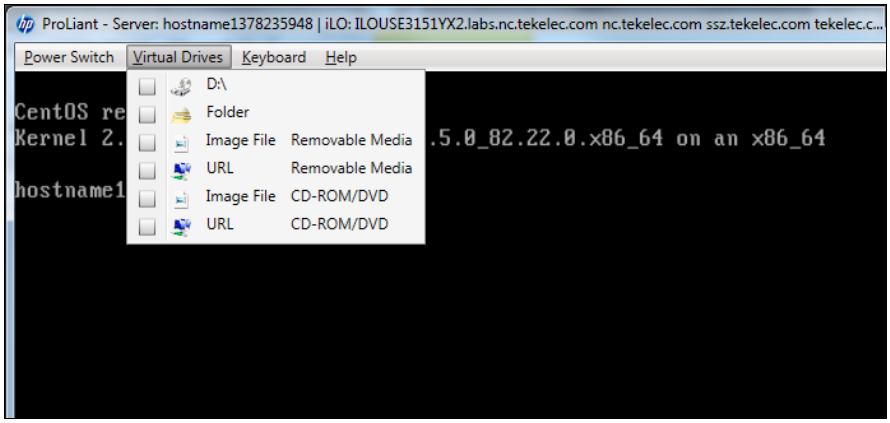
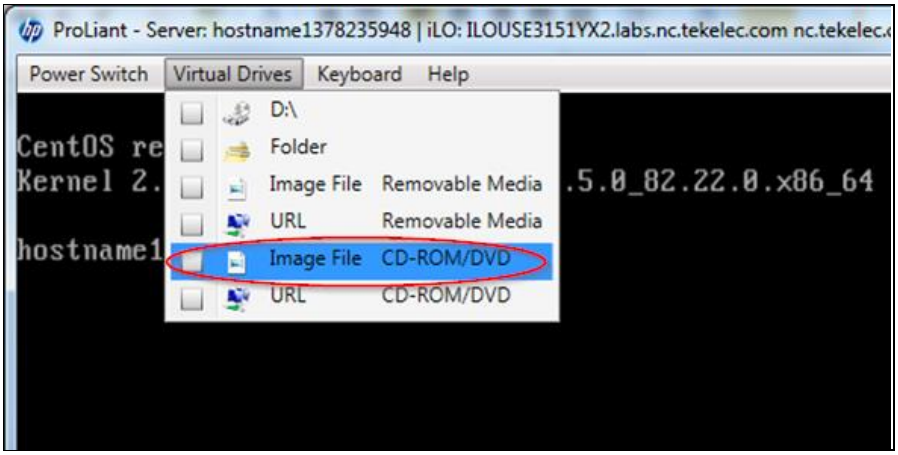
Step	Procedure	Result
4. ☐	**Web Browser:** Click the remote Console link	1. Click **Integrated Remote Console**, and a browser window opens.  2. You may be prompted with a security certificate warning, as well as a warning about running content from an untrusted site. Click though the prompts. **Java Integrated Remote Console** Access the system KVM and control Virtual Power & Media from an applet-based console requiring the availability of Java.  **3.** You must click **Continue** or **Yes** to proceed.
5. ☐	**Web Browser**	After a few moments, the Console window opens. 
—End of Procedure—		

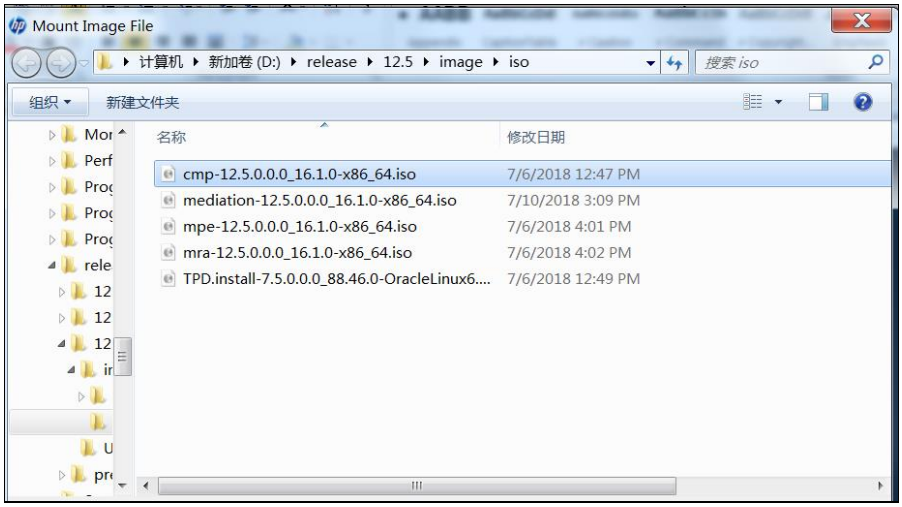
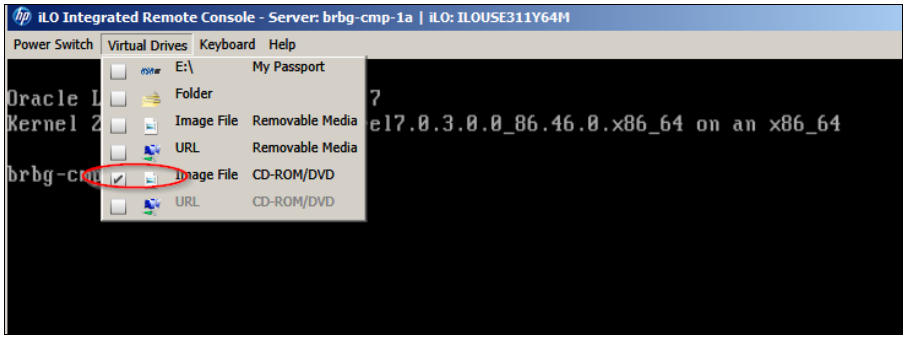
7.2 Mounting Media (Image Files)

7.2.1 Mounting Virtual Media on HP Servers

This procedure contains steps to mount media on HP rack mount servers using ILO for ISO access or other file transfer.

7.2.2: Mounting Virtual Media on HP Rack Mount Servers

Step	Procedure	Details
1. ☐	Access the ILO VGA for the servers.	Connect to the ILO VGA for the server using the access method described Section Error! Reference source not found.
2. ☐	**ILO Remote Console:** Select **Virtual Drives** from the menu bar.	
3. ☐	**HP Server:** To access a bootable ISO image file on your client laptop, select **Image File CD-ROM/DVD** from the Virtual Drives menu. To access a bootable ISO image file on the network, select **URL CD-ROM/DVD** from the Virtual Drives menu.	From the Virtual Drives menu, select **Image File CD-ROM/DVD** 

Step	Procedure	Details
4. ☐	**HP Server:** Select an image file to mount	A window opens for you to browse the client browser workstation or laptop.  Select the image file.
5. ☐	**HP Server:** Confirm that the target image file is mounted	Return to the Virtual Drives menu and the **Image File CD-ROM/DVD** is checked indicating that the image file is mounted. 
—End of Procedure—		

7.3 Hardware Setup (Bios Configuration)

Reference material:

- TPD Initial Product Manufacture, Release 7.6
- PMAC 6.6 Configuration Reference Guide

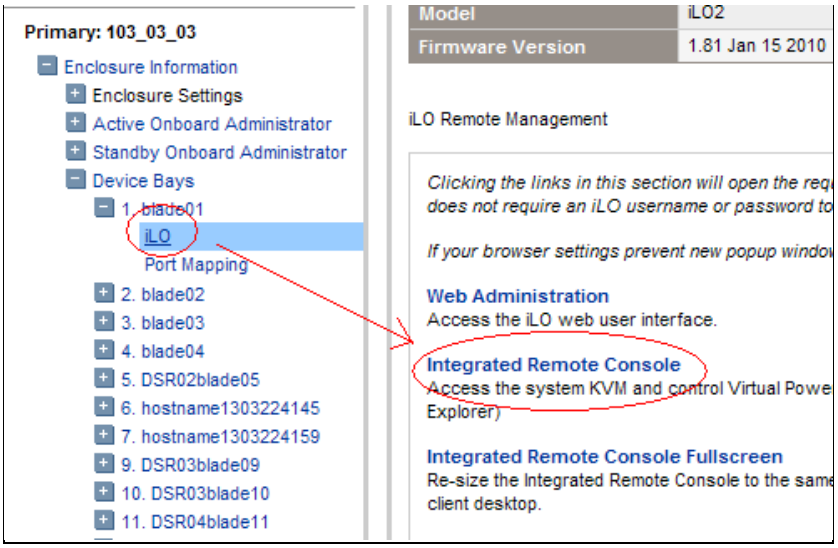
7.3.1 BIOS Settings for HP Gen 8 Blade

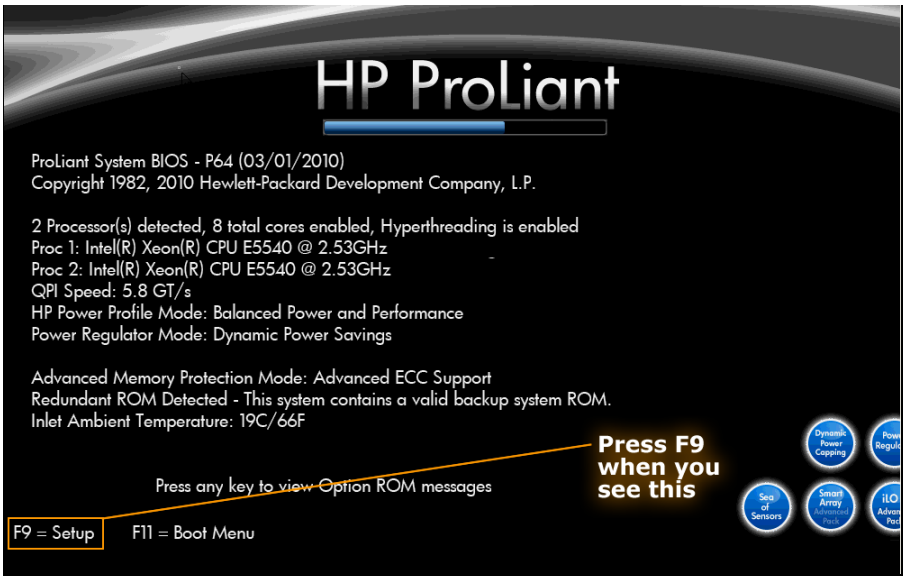
This procedure configures HP BIOS settings for Gen 8 Blade.

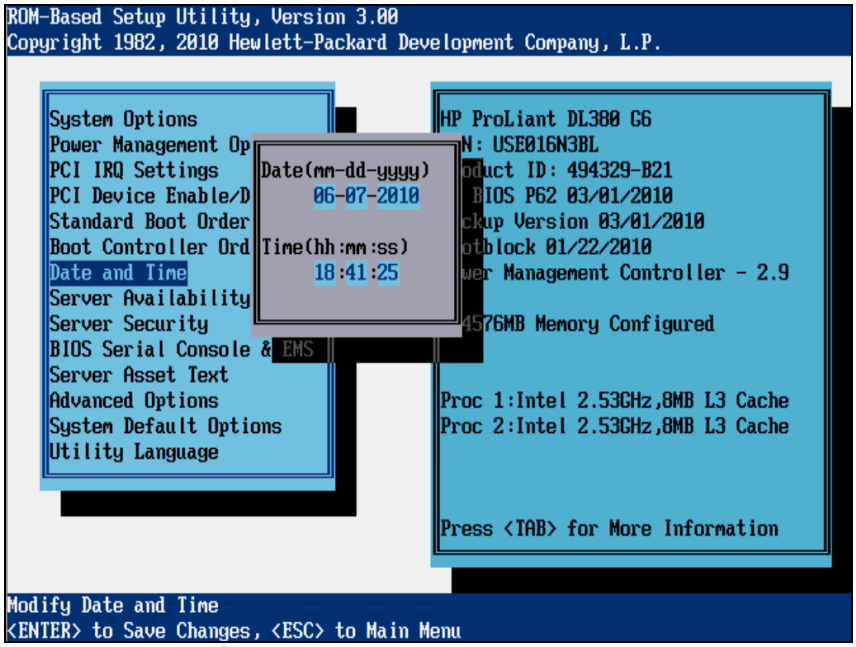
Check off (√) each step as it is completed. Check boxes are provided next to each step number.

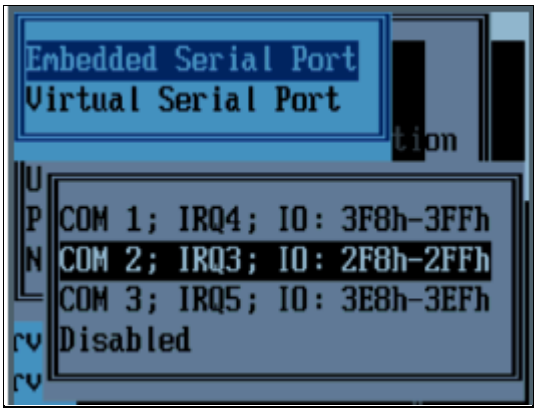
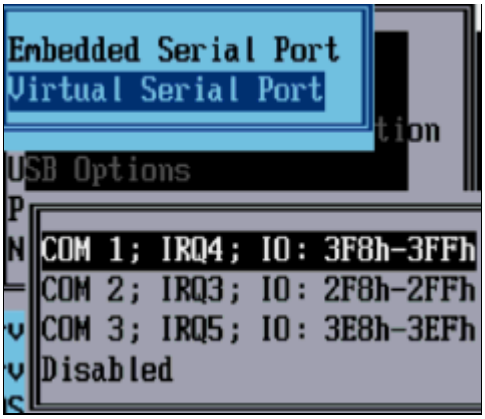
If this procedure fails, contact Oracle Technical Services and ask for assistance.

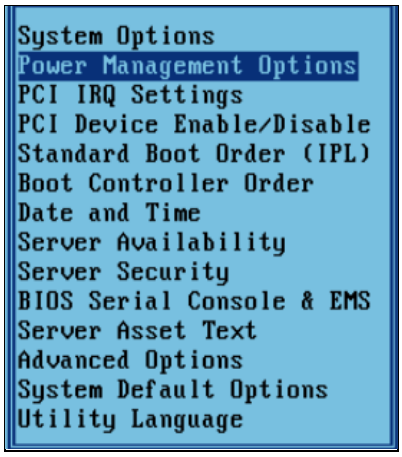
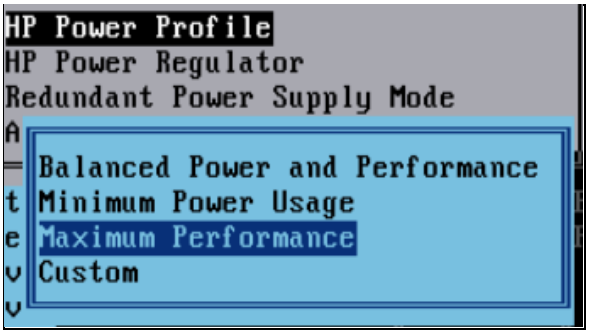
7.3.1:BIOS Settings for HP Gen 8 Blade

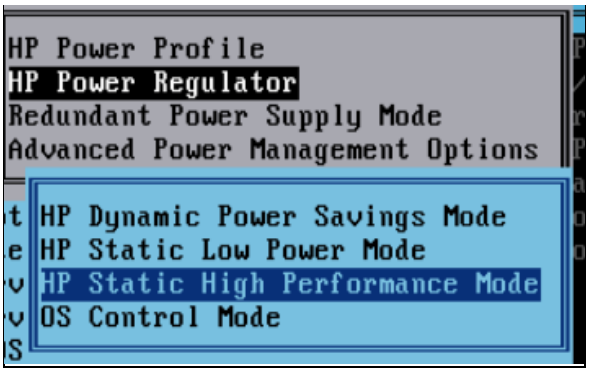
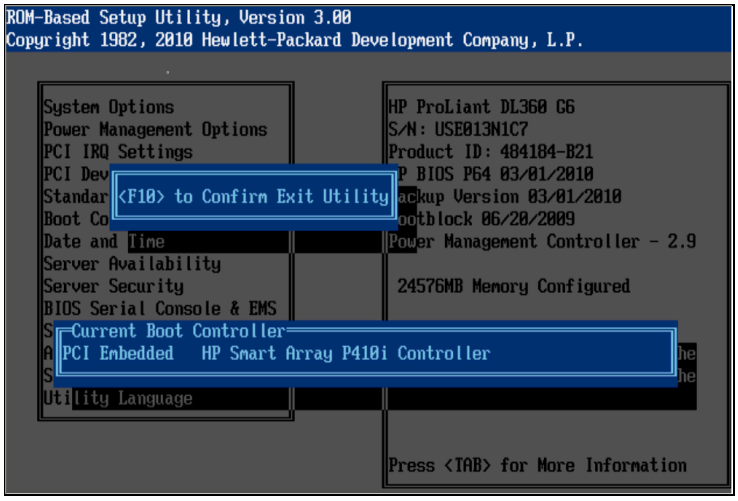
Step	Procedure	Details
1. ☐	Access the console for the HP server.	Connect to the console for the server using one of the access methods described in Section 7.1.1
2. ☐	Access the console for the HP server according to its hardware type	For Blade servers: 1. Navigate to the IP address of the active OA. 2. Login as an administrative user. 3. Navigate to **Enclosure Information → Device Bays →** *<Blade 1>* **→ iLO** 4. Click **Integrated Remote Console**  **NOTE:** This launches the iLO interface for the blade. If this is the first time the iLO is being accessed, you are prompted to install an add-on to your web browser, follow the on screen instructions.

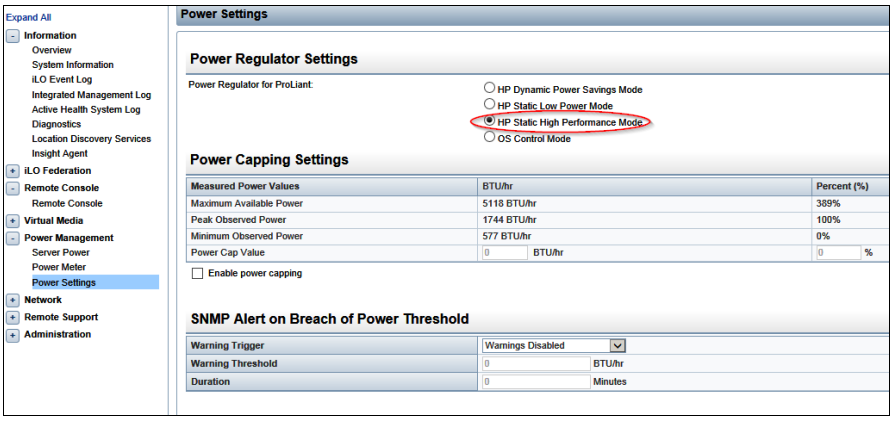
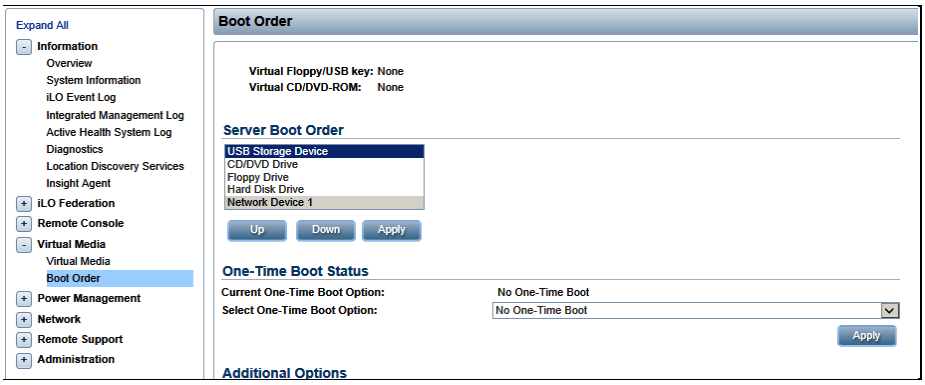
Step	Procedure	Details
3. ☐	Access the Server BIOS	Reboot the server. • For Blade, navigate to **Power Management→Server Power** and select **Cold Boot** under the Integrated Console menu. As soon as you see `F9=Setup` in the lower left corner of the screen, press **F9** to open the BIOS setup screen. You may be required to press **F9** two or three times. The `F9=Setup` changes to `F9 Pressed` after it is accepted. See example below.  **Expected Result:** ROM-Based Setup Utility opens and the ROM-Based Setup Utility menu displays.

Step	Procedure	Details
4. ☐	Set Server CMOS Clock	1. Select **Date and Time** and press **Enter** 2. Set the date and time and press **Enter**.  Time and Date is set.

Step	Procedure	Details
5. ☐	Configure iLO serial port settings **(RMS Only)**	For RMS only, the serial ports on HP DL360 G8 rack mount servers need to be configured so the serial port used by the BIOS and TPD are connected to the VSP on the iLO. This allows the remote administration of the servers without the need for external terminal servers. If this configuration is not completed and the server rebooted, the syscheck `syscheck -v hardware serial` test fails. 1. Select **System Options** option and press **Enter**. 2. Select Serial Port Options option and press **Enter**. 3. Change Embedded Serial Port to COM2 and press **Enter**.  Change **Virtual Serial Port** to **COM1** and press **Enter**.  Press **ESC** twice

Step	Procedure	Details
6. ☐	Configure power profile settings	The power profile on HP servers must be configured for optimum software performance on both RMS and blade hardware. 1. Select **Power Management Options** option and press **Enter**.  2. Select **HP Power Profile** option and press **Enter**. 3. Select **Maximum Performance** and press **Enter**. 

Step	Procedure	Details
7. ☐	Configure Power Regulator settings	The Power Regulator on HP servers must be configured for optimum performance on both RMS and blade hardware. 1. In the Power Management Options menu, select **HP Power Regulator** and press **Enter**. **NOTE:** A message may display to indicating that certain processors support only one power state. If this message displays, press **ESC**. 2. Select **HP Static High Performance Mode** and press **Enter**. 
8. ☐	Save configuration and Exit	1. Press **ESC** two times 2. Press **F10** to save the configuration and exit. The server reboots.  **Expected Result:** Settings are saved and server reboots.

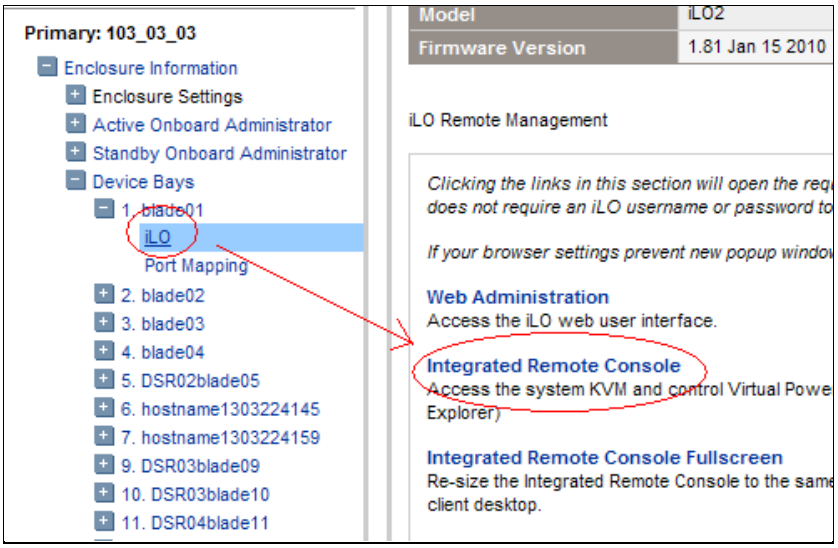
Step	Procedure	Details
9. ☐	Confirm the Power Regulator setting for the HP server.	If not connected to the iLO for the server, connect using 7.1.1 Accessing the iLO VGA Redirection Window for HP. On the iLO for the HP Server: 1. Navigate to **Power Management→Power Settings** 2. Confirm Power Regulator for ProLiant is set to:**HP Static High Performance Mode** 
10. ☐	**Server ILO:** Verify the Boot Order	From left tree menu, select **Virtual Media → Boot Order**.  **NOTE:** The boot order looks like the above image unless the you have specified otherwise.
—End of Procedure—		

7.3.2 BIOS Settings for HP Gen 9 Blade and Rack Mount Servers

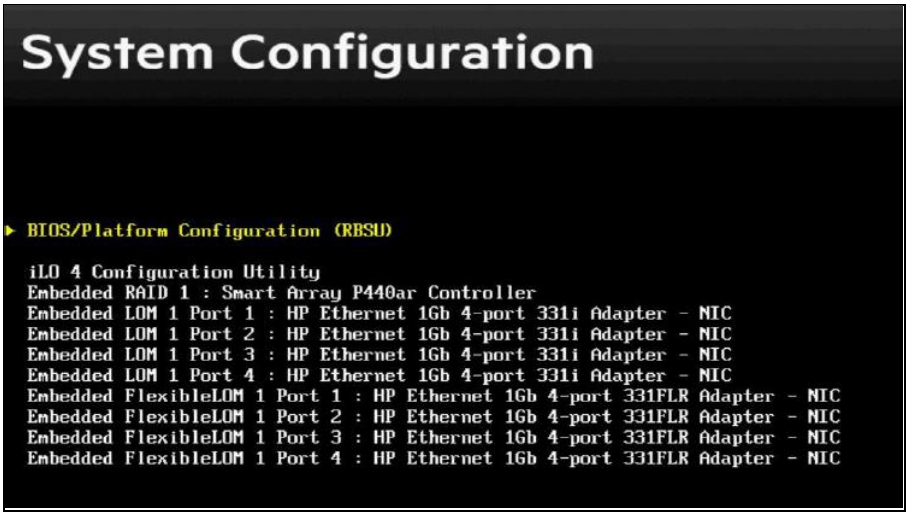
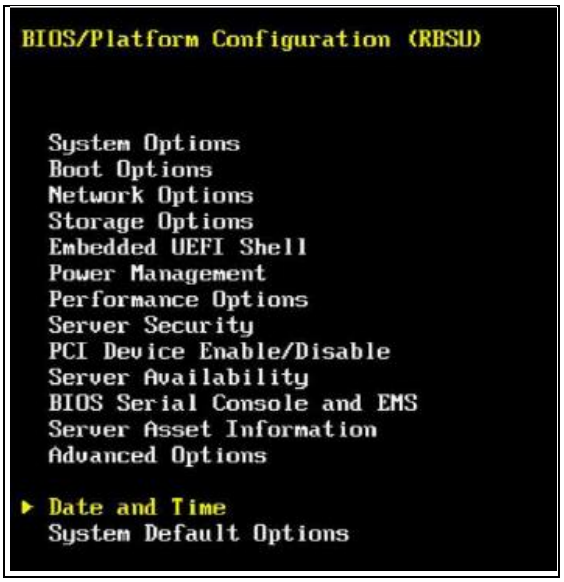
In this procedure you configure BIOS settings for HP hardware.

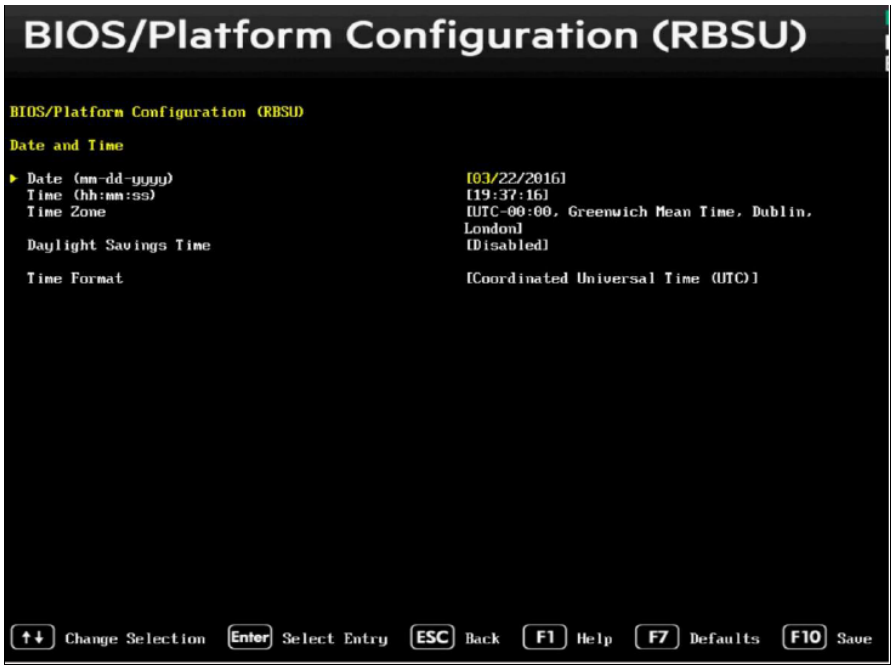
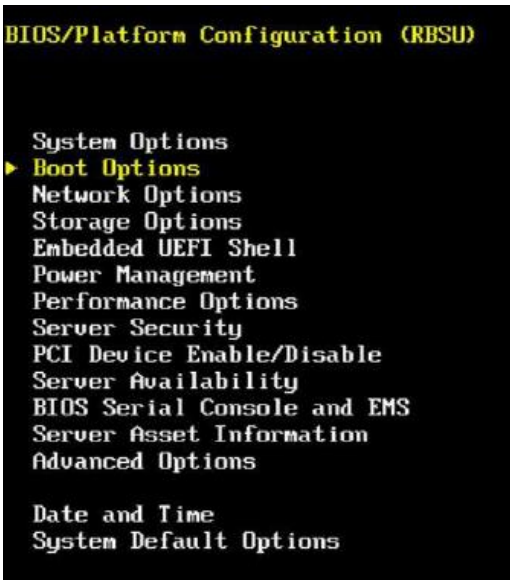
7.3.2:BIOS Settings for HP Gen 9 Blade and Rack Mount Servers

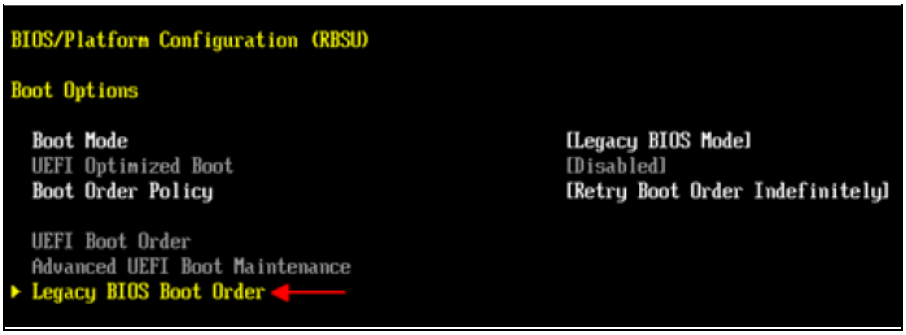
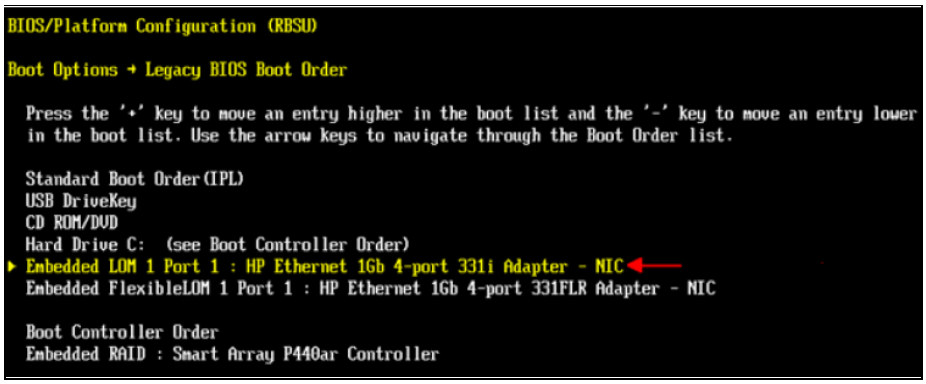
Step	Procedure	Details
1. ☐	Access the console for the HP server.	Connect to the console for the server using one of the access methods described in *Section 7.1.1*

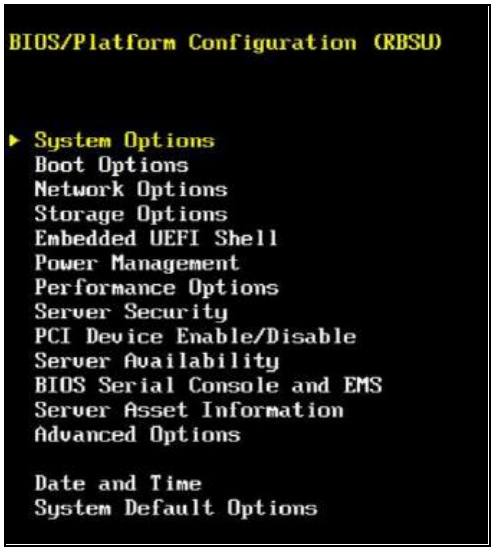
Step	Procedure	Details
2. ☐	Access the console for the HP server according to its hardware type.	For Rack Mount Servers (RMS), connect to the console for the server using one of the access methods described in *Section 7.1.1* For Blade servers: 1. Navigate to the IP address of the active OA. Login as an administrative user. 2. Navigate to **Enclosure Information → Device Bays →** <*Blade 1*> **→ iLO** 3. Click **Integrated Remote Console**  **NOTE:** This launches the iLO interface for that blade. If this is the first time the iLO is being accessed, you are prompted to install an add-on to your web browser, follow the on screen instructions.

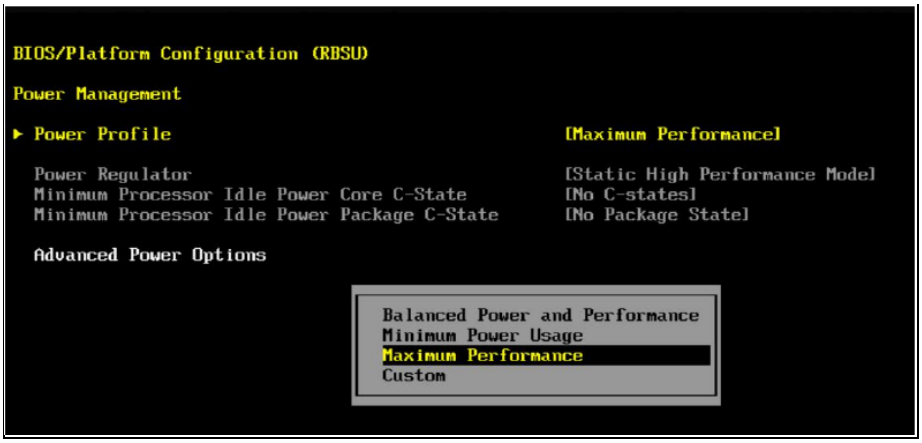
Step	Procedure	Details
3. ☐	Access the Server BIOS	Reboot the server. • For Blade and RMS, this is achieved by selecting **Cold Boot** from the **Power Management→Server Power** menu of the Integrated Console. • For RMS, this can also be achieved by pressing and holding the power button until the server turns off, then after approximately 5 to 10 seconds press the power button to enable power. As soon as you see `F9=Setup` in the lower left corner of the screen, press **F9** to access the BIOS setup screen. You may be required to press **F9** two to three times. The `F9=Setup` changes to `F9 Pressed` after it is accepted. See example below. **Expected Result:** System Utilities screen displays
4. ☐	System Utilities Configuration	From the System Utilities screen, select System Configuration, then select **Enter**

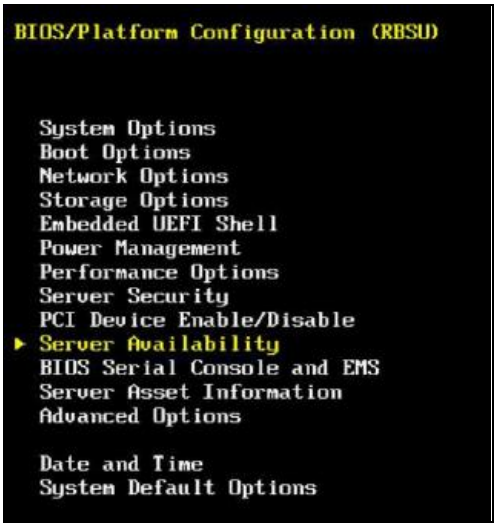
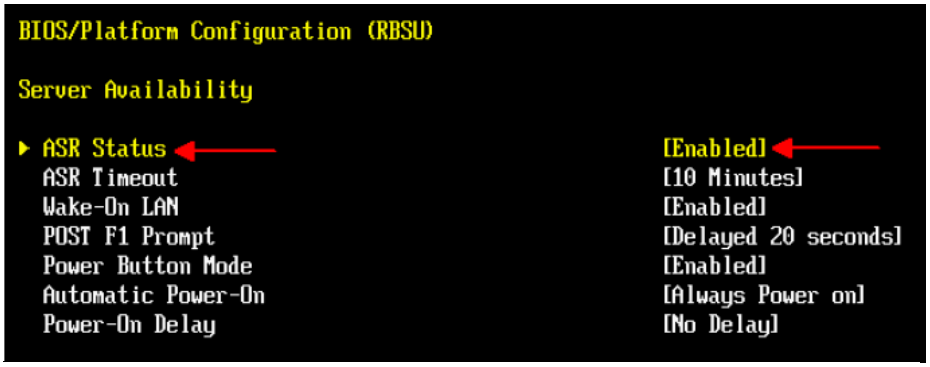
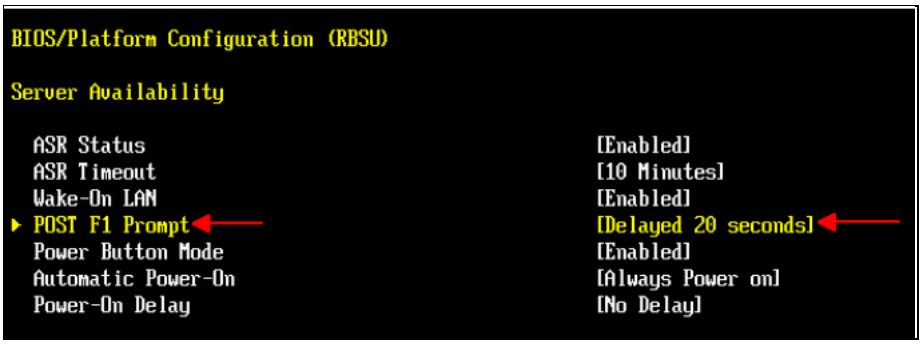
Step	Procedure	Details
5. ☐	System Utilities Configuration	From the System Configuration screen, select **BIOS/Platform Configuration (RBSU)**, then press **Enter**. 
6. ☐	System Utilities Configuration	From the Bios/Platform Configuration screen, select **Date and Time**, then press **Enter**. 

Step	Procedure	Details
7. ☐	System Utilities Configuration	From the Date and Time list, set Date and Time to the UTC (Greenwich Mean Time), the Time Zone to UTC, and the Time Format to Coordinated Universal Time (UTC), then select F10 to save your changes. After saving, select ESC to return to the Bios/Platform Configuration screen. 
8. ☐	System Utilities Configuration	From the Bios/Platform Configuration screen, select Boot Options and press Enter. 

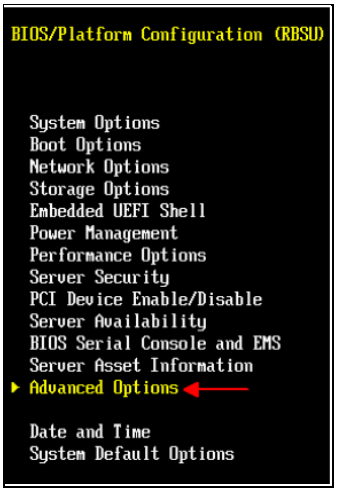
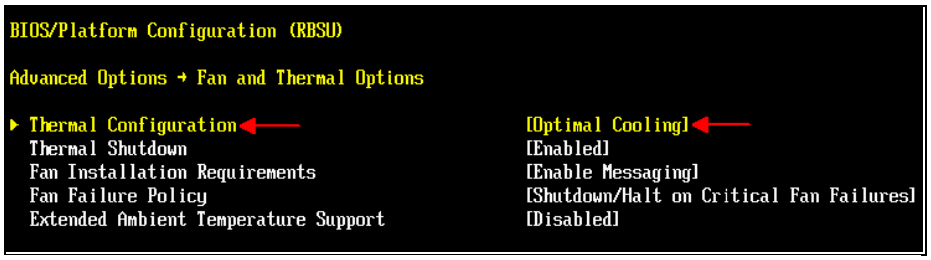
Step	Procedure	Details
9. ☐	System Utilities Configuration	1. From the Boot Options list, set: a. Boot Mode to **Legacy BIOS Mode** b. UEFI Optimized Boot to **Disabled** c. Boot Order Policy to **Retry Boot Order Indefinitely** 2. Press **F10** to save your changes. 3. Select the **Legacy BIOS Boot Order Option** 4. Press **Enter** 
10. ☐	System Utilities Configuration	From the Legacy BIOS Boot Order Option screen, ensure that: • USB DriveKey • CD ROM/DVD • Hard Dive C • Embedded LOM 1 Port 1 • Embedded FlexibleLOM 1 Port 1 are listed in this order under Standard Boot Order (IPL); if not, change their order and select **F10** to save your changes. Press **ESC** to return to the Boot Options screen. 

Step	Procedure	Details
11. ☐	System Utilities Configuration	Press **ESC** again to return to the Bios/Platform Configuration screen, then select System Options and press Enter. 
12. ☐	System Utilities Configuration	From the System Options list, select Serial Port Options and press **Enter**.
13. ☐	System Utilities Configuration	1. From the Serial Port Options list, set Embedded Serial Port to COM2 and set Virtual Serial Port to COM1. 2. Press **F10** to save your changes. 3. Press **ESC** twice to return to the Bios/Platform Configuration screen.

Step	Procedure	Details
14. ☐	System Utilities Configuration	From the Bios/Platform Configuration screen, select **Power Management Option** and press **Enter**.
15. ☐	System Utilities Configuration	1. From the Power Management screen, set the power profile to **Maximum Performance**. 2. Press **F10** to save your changes. 3. Press **ESC** to return to the Bios/Platform Configuration screen. 

Step	Procedure	Details
16. ☐	System Utilities Configuration	From the Bios/Platform Configuration screen, select **Server Availability Option** and press **Enter**. 
17. ☐	System Utilities Configuration	From the Server Availability screen, set ASR Status to Enabled. 
18. ☐	System Utilities Configuration	Set POST F1 Prompt to **Delayed 20** seconds. 

Step	Procedure	Details
19. ☐	System Utilities Configuration	Set Power-On Delay to **No Delay**.
20. ☐	System Utilities Configuration	1. Set Automatic Power-On to **Restore Last Power State**. 2. Press **F10** to save your changes. 3. Press **ESC** to return to the Bios/Platform Configuration screen.

Step	Procedure	Details
21. ☐	System Utilities Configuration	From the Bios/Platform Configuration screen, select Advanced Options and press Enter. 
22. ☐	System Utilities Configuration	1. Set Thermal Configuration to Optimal Cooling. 2. Press **F10** to save your changes. 3. Press **ESC** to return to the Bios/Platform Configuration screen.  4. Press **ESC** to return to the System Utilities screen.
—End of Procedure—		

7.3.3 Using c-Class Enclosure OA to Update the BIOS Settings for the Application Blade

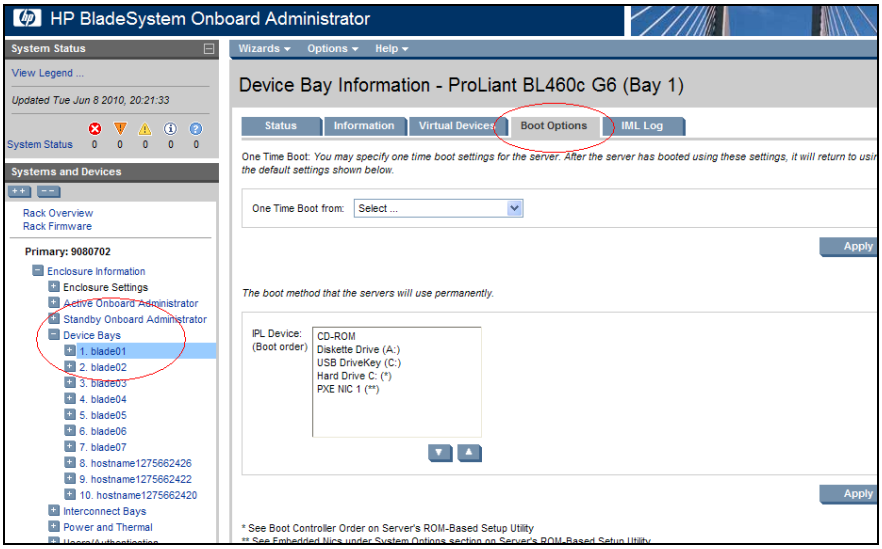
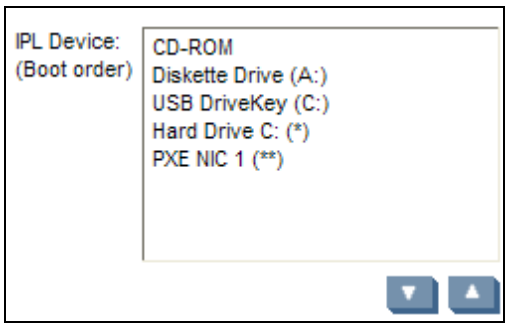
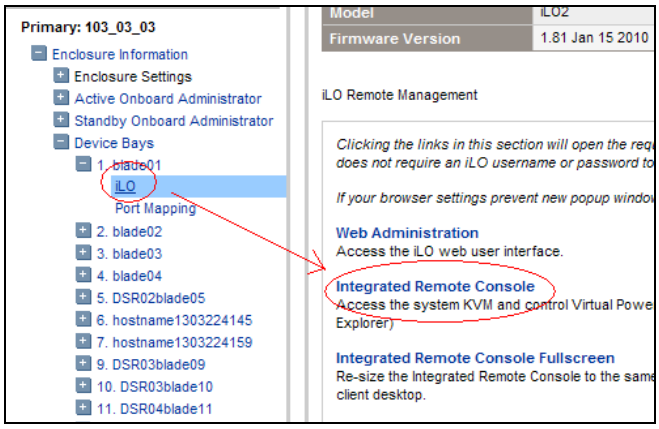
This procedure provides the steps to confirm and update the BIOS configuration on Blade servers using the C-Class enclosure OA.

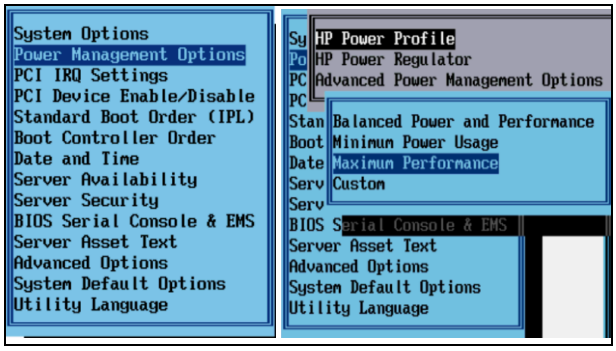
Check off (√) each step as it is completed. Check boxes are provided next to each step number.

If this procedure fails, contact Oracle Technical Services and ask for assistance.

7.3.5: Using c-Class Enclosure OA to Update BIOS Settings for the Application Blade

Step	Procedure	Details
1. ☐	**OA GUI:** Login	1. Open your web browser and navigate to the OA IP address 2. Login to HP OA as Administrator. Original password is on paper card attached to each OA.

Step	Procedure	Details
2. ☐	**OA:** Navigate to device Bay Settings	1. Navigate to **Enclosure Information → Device Bays →** <*Blade 1*> 2. Click **Boot Options** tab. 
3. ☐	**OA:** Verify/update Boot device Order	Verify that the Boot order is as follows. If it is not, use the up and down arrows to adjust the order to match the picture below, then click **Apply**. 
4. ☐	**OA:** Access the Blade iLO	1. Navigate to **Enclosure Information → Device Bays →** <*Blade 1*> **→ iLO** 2. Click **Integrated Remote Console**  This launches the iLO interface for that blade. If this is the first time the iLO is being accessed, you may be prompted to install an add-on to your web browser, follow the on screen instructions to do so.

Step	Procedure	Details
5. ☐	**OA:** restart the blade and access the bios	You might be prompted with a certificate security warning, just press continue. After a prompt is displayed, login onto the blade using the root username. After logged in, Reboot the server (using the reboot command). After the server is powered on and is booting , press **F9** to access the BIOS setup screen (as soon as you see `<F9=Setup>` in the lower left corner of the screen).
6. ☐	**OA:** Update bios settings	1. Scroll down to **Power Management Options** and press **Enter** 2. Select **HP Power Profile** and press **Enter** 3. Scroll down to **Maximum Performance** and press **Enter**  4. Press **Esc** twice to exit the BIOS setup screen. 5. Press **F10** to confirm Exiting the utility. The blade reboots.
7. ☐	**OA:** Repeat for the remaining blades	Repeat Steps 2 through 6 for the remaining blades. When conmpeted, exit the OA GUI.
—End of Procedure—		

8. TROUBLESHOOTING THE INSTALLATION

This chapter describes how to troubleshoot the installation.

8.1 Common Problems and Their Solutions

The following sections describe and present solutions to common installation problems.

Problem

Verifying firmware levels

You are not sure if the hardware is at the required firmware level.

Solution

If the installation is HP c-Class then the OA (On-line Administrator) GUI has a summary of the firmware revisions of all the equipment in the c-Class enclosure. (It generally is not be possible to access this until installation of the enclosure is complete.)

In general, you can update firmware after installation, but you must complete these updates before the system goes into service.

Problem:

You want to configure Cisco or HP switches without using the PM&C netConfig tool

Configuring outside of the netConfig tool is not recommended.

Solution:

You can log in to the switches from PM&C and make configuration changes while troubleshooting: for example, to disable a port, turn on port mirroring, or add a route. However, the configurations that are generated from netConfig have many important settings to make the configuration work. Back up the final switch configuration to PM&C so that it is restored in a repair operation.

NOTE: The netConfig files are not used for restore operation because you made the configuration changes outside of this tool.

Problem:

You need the netConfig template files

Solution:

The latest releases of the netConfig template files are included in the Policy Management ISO image file. After the Policy Management software is installed on a server, you find the files in the `/usr/TKLC/plat/etc/netconfig/` directory.

Several templates are provided, depending on the networking choices at your site. You must choose the templates.

Problem:

Networking issues: When you open the ports, there may be troubleshooting required of:

1. Cabling
2. Policy Management server IP network configuration
3. Your IP network configuration

Solution

This may be easier to resolve if you can trace cables and plug a laptop into a switch to run port mirroring. If PM&C iLO connectivity is in place, issues can also be resolved remotely.

Problem

If you were on R12.3.1 CMP with netbackup client R7.1 installed, then upgrade the CMP to R12.5 and install R7.7 netbackup client, the installation fails.

Solution

Perform the following steps:

1. Force standby the CMP server to install or upgrade netbackup client:
   `Vim /etc/fstab` to make the **/tmp** mount options back to defaults
   Find the below line:
   `/dev/mapper/vgroot-plat_tmp /tmp  ext4  noexec,nosuid,nodev  1 2`

   update to:
   `/dev/mapper/vgroot-plat_tmp /tmp  ext4 defaults  1 2`
2. Reboot the server for re-mount the **/tmp** with defaults.
3. Perform the netbackup client following installation steps. The netbackup client must be installed successfully on the CMP server.
4. Back the **/etc/fstab** for **/tmp** to the original value.
5. Reboot the server.
6. The netbackup server could retrieve the backup content from the CMP server.

8.2 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 (CAS) can assist you with My Oracle Support registration.

Call the CAS 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 sequence on the Support telephone menu:

1. 1. Select **2** for New Service Request
2. 2. Select **3** for Hardware, Networking and Solaris Operating System Support
3. 3. Select one of the following options:
   a. a. For Technical issues such as creating a Service Request (SR), select **1**
   b. b. For Non-technical issues such as registration or assistance with My Oracle Support, Select **2**

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.