Oracle® COMMUNICATIONS

Installation Instructions

Policy Management 12.3 Bare Metal Installation Guide

July 2017

E85333-01

MOS (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 MOS 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 12.3 Bare Metal Installation Guide

TABLE OF CONTENTS

1. PREFACE

This guide provides instructions for installing Oracle Communications Policy Management (also referred to as Policy Management) software for Wireless and Fixed Broadband 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 http://docs.oracle.com/cd/E57832_01/index.htm

[1] E4917—HP Solutions Firmware Upgrade Pack, Software Centric Release Notes, Release 2.2.9 (see Note)
[2] E76846—HP Solutions Firmware Upgrade Pack, Software Centric Release Notes, Release 2.2.10 (see Note)
[3] E67765—Oracle Firmware Upgrade Pack, Release Notes, Release 3.1.5
[4] E70315—Oracle Firmware Upgrade Pack, Release Notes, Release 3.1.6
[5] E67825—Oracle Firmware Upgrade Pack, Upgrade Guide, Release 3.1.5
[6] E70316—Oracle Firmware Upgrade Pack, Upgrade Guide, Release 3.1.6
[7] E53017—TPD Initial Product Manufacture, Release 6.7.2+
[8] E53486—Tekelec Platform 7.0.x, Configuration Guide
[9] E53018—Tekelec Virtualization Operating Environment (TVOE) 3.0, Software Upgrade Procedure
[10] E54387—PM&C Incremental Upgrade, Release 5.7 and 6.0

NOTE: The HP Solutions Firmware Upgrade Pack (HP FUP) is provided for customers who bought their HP hardware 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 12.3. (http://docs.oracle.com/cd/E85327_01/index.htm)

[1] E85328-01—Release Notes
[2] E85340-01—Configuration Management Platform, Wireless User's Guide, Release
[3] E85329-01—Platform Configuration User's Guide, Release
[4] E85330-01—Network Impact Report
[5] E85341-01—Policy Front End Wireless User's Guide
[6] E85342-01—Mediation Server User's Guide
[7] E85345-01—Troubleshooting Reference
[8] E85346-01—SNMP User's Guide
[9] E85343-01—Analytics Data Stream Wireless Reference
[10] E85347-01—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.)
OCUDR	Oracle Communications User Database 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	Definition
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.
Data Source	Interface that provides data to components
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) Also known as Multi-Protocol Routing Agent (MRA)	Scales the Policy Managementinfrastructure by distributing the PCRF load across multiple Policy Server (MPE) devices
Mediation	Component that interfaces with SPR and Boss to process subscriber profile and service subscription data
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 still retaining dedicated resources. This means software solutions that include multiple applications and require several physical machines can be installed on very few (possibly one) TVOE Hosts.
PM&C	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 adds configuration information into the policy server through the platcfg utility that brings the network interface for the server online and enables management and configuration from the CMP.
platcfg	Platform configuration utility used in TPD to configure IP and host values for a server.
Primary Site (Site1)	A site where the MPE/MRA/Mediation primary cluster exists with co-located Active and Standby servers
Secondary Site (Site2)	A site where the MPE/MRA/Mediation secondary cluster exists with co-located Active and Standby servers for disaster recovery
HP c-Class	HP blade server system

2. INSTALLATION OVERVIEW

This document describes how to install the 12.3 Policy Management applications on supported hardware platforms.

At the completion of installation, assuming that networking has been correctly configured, you should be able to 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 no 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
- Mediation—A required element in a Wireless-c network that manages subscriber resources and data

2.2 Overview of the Installation Process

There are two starting points for installation:

1. Equipment ordered from, pre-configured from, and installed by Oracle

2. Equipment ordered and installed by you

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

In the second case, you should 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 required. 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 Oracle hardware, the Oracle Integrated Lights Out Management (ILOM) feature, an independent subsystem inside an Oracle server which is used for out-of-band remote access
- 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 that interact with Policy Management.
- Determine the names and addresses of external data sources used in your network that interact with the Policy Management software. For example, subscriber profile repositories, online 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 a Mediation server; SMS Notification Statistics; and SCTP counters.

Oracle recommends contacting Oracle Consulting regarding your plans.

3.2 About Test Systems and Production Systems

Some customers 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 can be used to test and verify use cases before implementing in a production environment, as well as test new configurations or features ahead of implementation.

A test system could focus on only one integration point at one time; for example, throughput or connectivity. In some cases, a test system could use a traffic simulator instead of 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 should 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 currently supported with an uplink capacity of 10 GB or higher.

3.3.2 Networking (RMS Hardware)

Oracle and Netra X5-2 RMS, as well as HP RMS, are each 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 (PM&C), 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 (some of which has 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-7.0.3.0.0_86.46.0-OracleLinux6.7-x86_64.iso
- TPD.install-7.0.3.0.0_86.46.0-OracleLinux6.7-x86_64.usb

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

- TVOE-3.0.3.0.0_86.46.0-x86_64.iso
- TVOE-3.0.3.0.0_86.46.0-x86_64.usb

NOTE: TVOE is used for the PM&C (Platform Management and Configuration) server.

4.1.2 Platform Management and Configuration (PM&C)

For HP c-Class hardware, the Platform Management and Configuration (PM&C) server is required. PM&C is an Oracle application that provides tools to manage multiple enclosures and server software, as well as networking equipment (enclosure switches). The Platform Management and Configuration (PM&C) server can also be used for RMS installations but is optional.

- PMAC-6.0.3.0.2_60.28.0-x86_64.iso

4.1.3 Policy Management Application

The Policy Management software consists of the following products:

- CMP: cmp-12.3.0.0.0_x.x.x-x86_64.iso
- MPE: mpe-12.3.0.0.0_ x.x.x-x86_64.iso
- MRA (PFE): mra-12.3.0.0.0_ x.x.x-x86_64.iso
- Mediation: mediation-12.3.0.0.0_ x.x.x-x86_64.iso

4.1.4 Acquiring Software

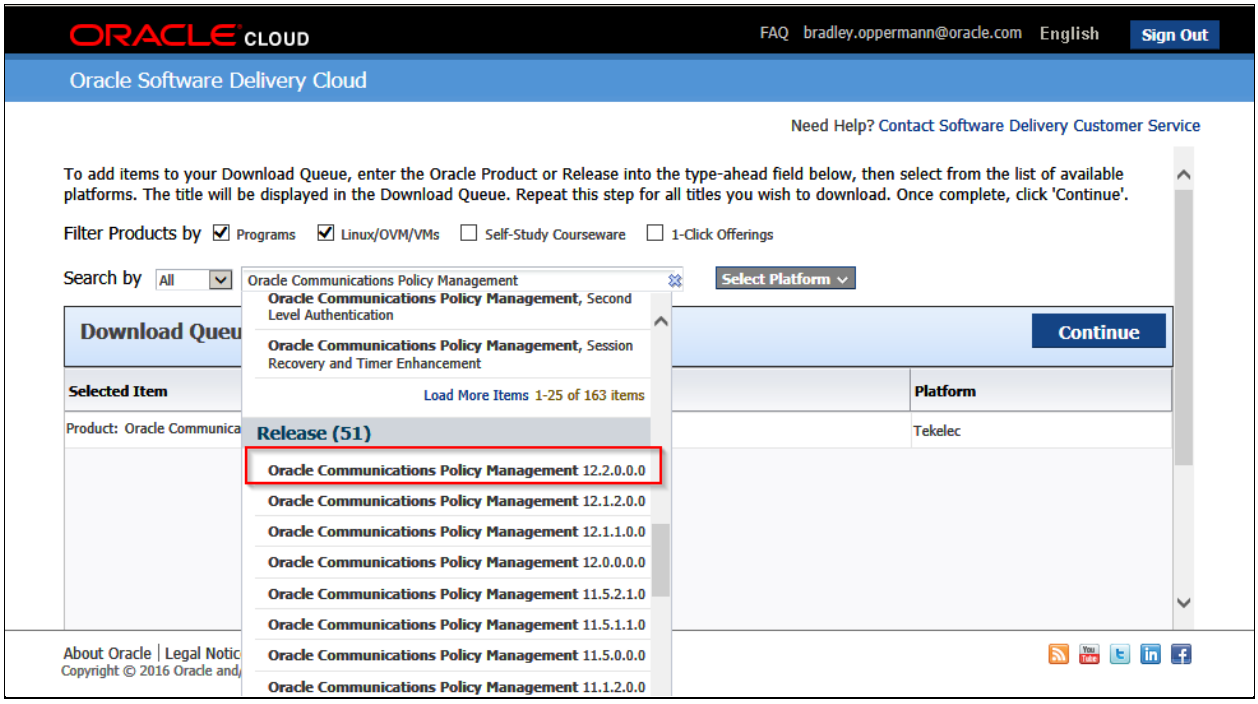
If you have a commercial license, you should download your software from the Oracle Software Delivery Cloud, which is specifically designed for customer fulfillment.

For patches, go to My Oracle Support.

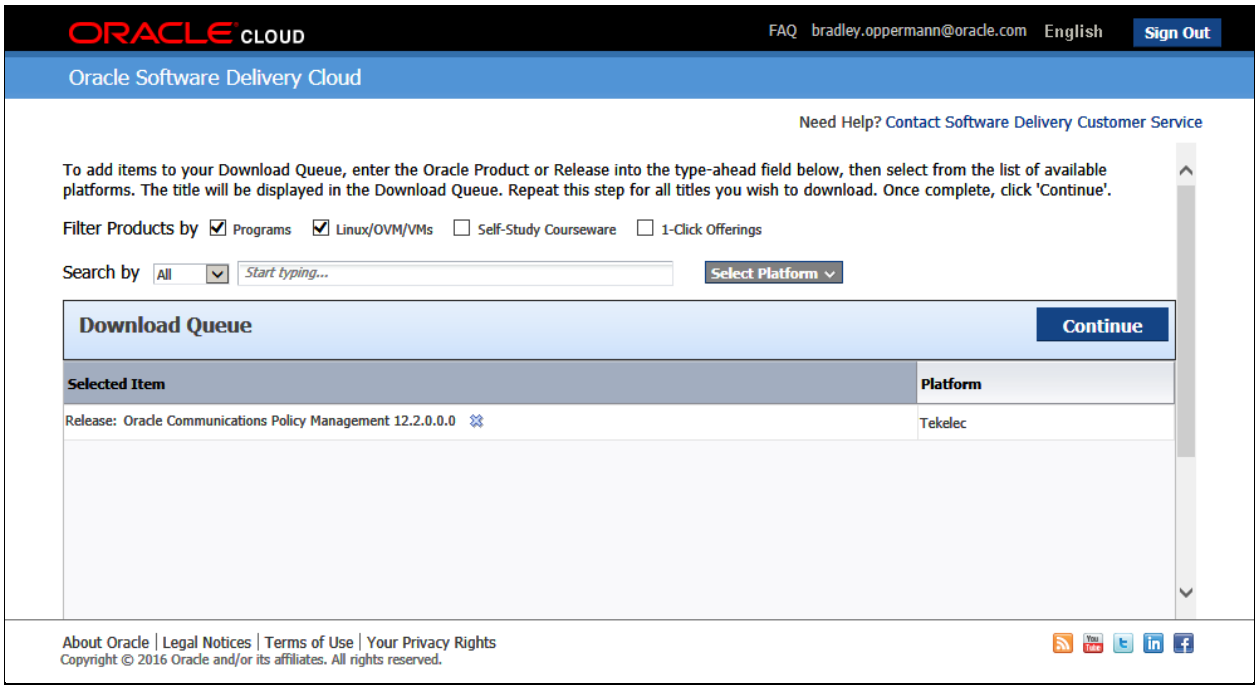
NOTE: The following is an example of downloading the Policy Management software.

5. Log into the Oracle Cloud.

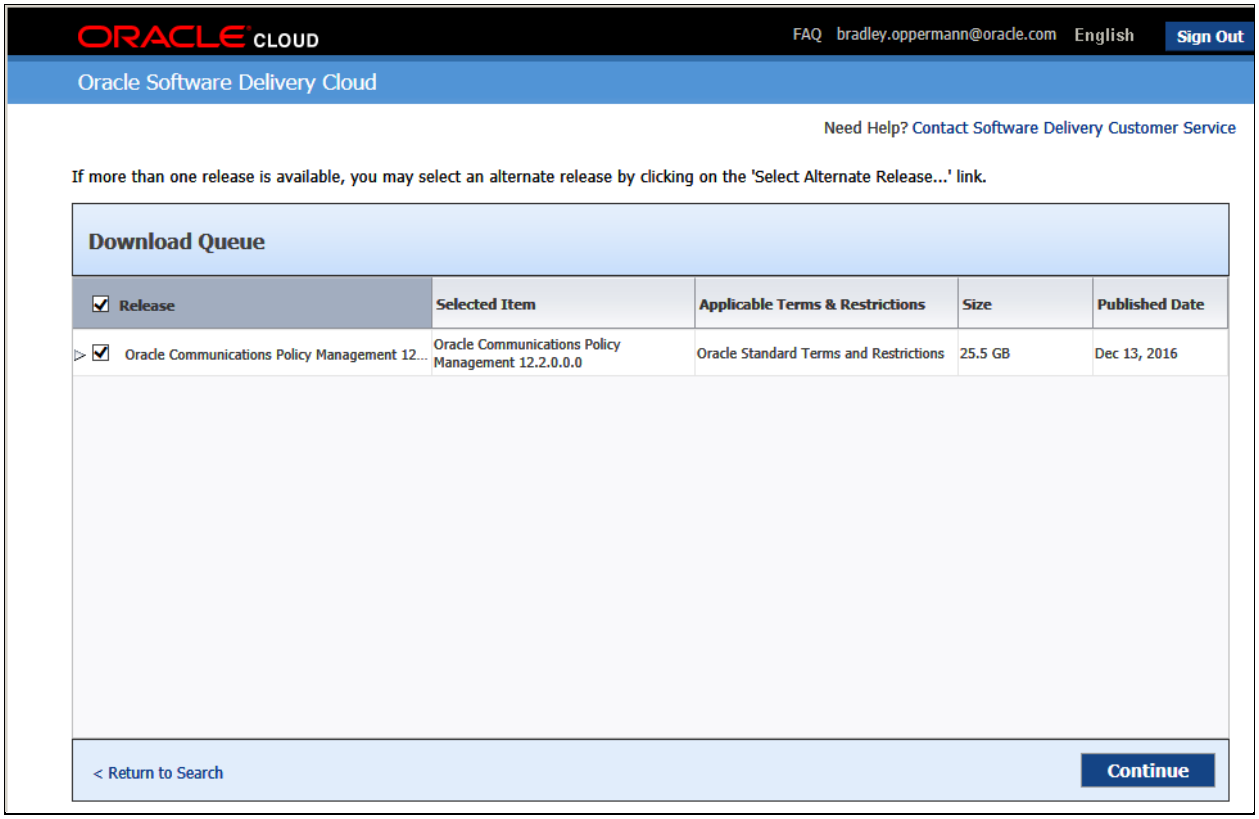
6. Select **Oracle Communications Policy Management 12.3.0.0.0**.



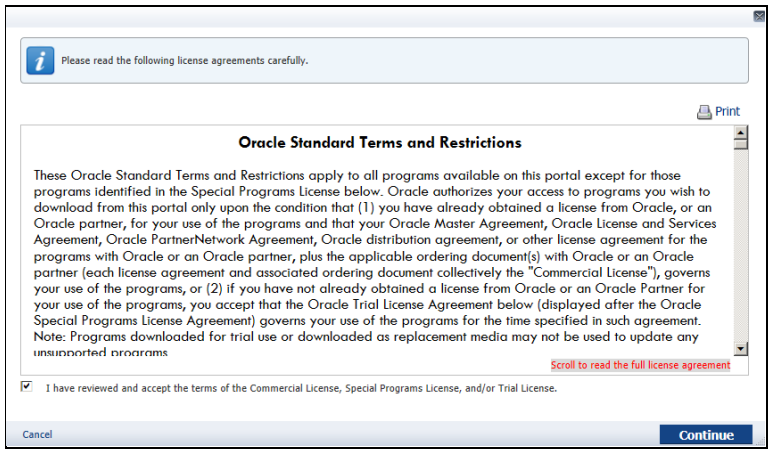
7. Click **Continue**.



Select **Oracle Communications Policy Management 12.3.0.0.0** checkbox and click **Continue**.



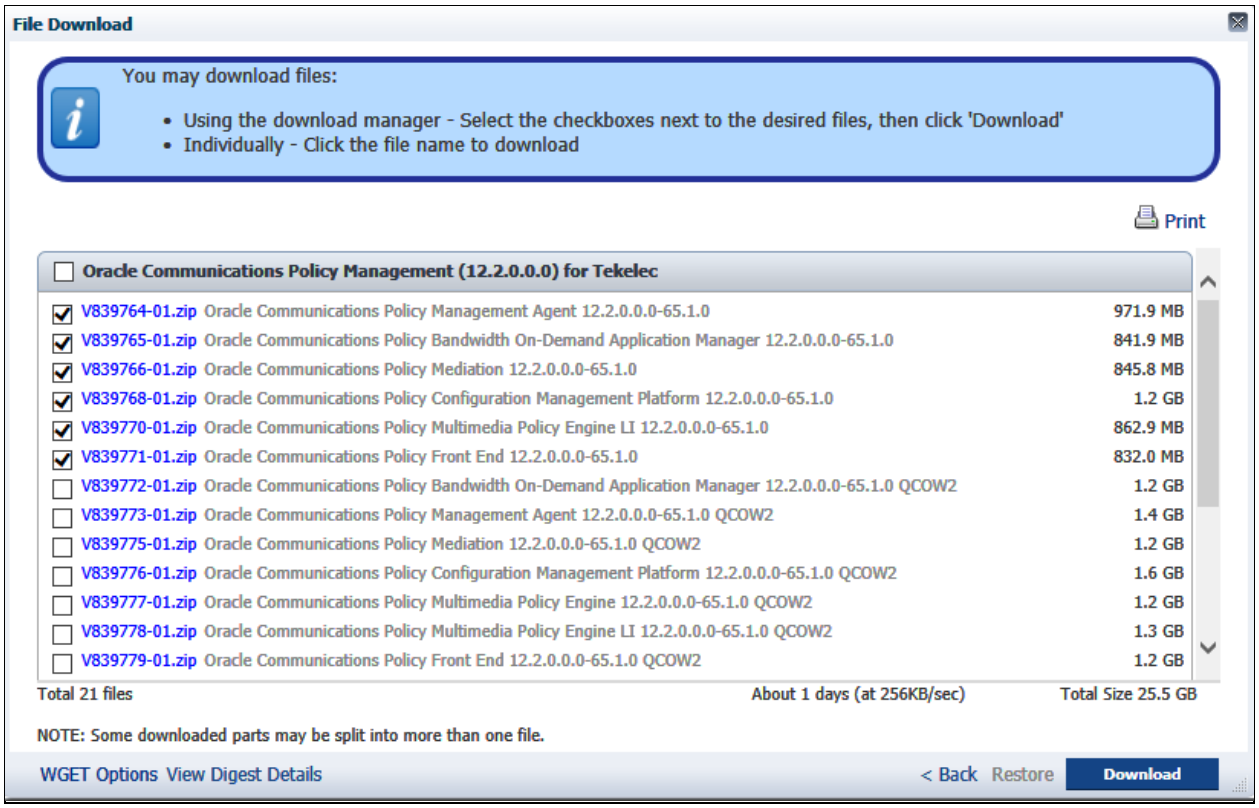
8. Confirm the License Agreement and click **Continue**.



9. Select the required software files.

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

10. Click **Download**.



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 PM&C netConfig tool uses network configuration files to configure enclosure and aggregation switches. The Policy Management ISO image files include switch configuration template files. You should edit these template files to make them specific for your installation and place them on the PM&C server after it is installed.

NOTE: These files change from release to release.

4.2 Hardware Requirements

The following servers are supported:

- Oracle X5-2 server (rack mount)
- Netra X5-2 server (rack mount)
- 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 PM&C 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 12.3 servers and devices may require firmware updates:

- Oracle X5-2 RMS server
- Netra X5-2 RMS Server
- 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 Oracle Hardware

If you have purchased Oracle X5-2 or Netra X5-2 servers directly from Oracle, see the discussion of Firmware Components in the Oracle Firmware Upgrade Pack, Release Notes, Release 3.1.5 or Oracle Firmware Upgrade Pack, Release Notes, Release 3.1.6 for information on how to acquire the firmware.

NOTE: You can obtain firmware upgrade media for the Oracle X5-2 RMS from the Oracle Help Center website. Specific downloading instructions are in the Oracle Firmware Upgrade Pack, Release Notes, Release 3.1.5 or Oracle Firmware Upgrade Pack, Release Notes, Release 3.1.6.

4.3.2 Acquiring Firmware for HP Hardware Purchased Through Oracle

The HP Solutions Firmware Upgrade Pack, Software Centric Release Notes, Release 2.2.9 and HP Solutions Firmware Upgrade Pack, Software Centric Release Notes, Release 2.2.10 are provided for customers who bought their HP hardware through Oracle. Each describes new functionalities, fixed bugs, known bugs, and any additional installation and configuration instructions required, relative to this release.

For Policy Management 12.3, the minimum supported firmware is 2.2.9. Contact My Oracle Support for assistance if needed.

Firmware is available as:

- ISO or USB image files of HP Smart Update Firmware:
  - FW2_SPP-2.2.8.0.0_10.43.0.iso
  - FW2_SPP-2.2.8.0.0_10.43.0.usb
- ISO image files of HP Misc Firmware ISO:
  - FW2_MISC-2.2.8.0.0_10.43.0.iso

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

4.3.3 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 2.2.9 or HP Solutions Firmware Upgrade Pack, Software Centric Release Notes, Release 2.2.10.

4.4 Information Requirements

You must determine and record the IP addresses that you are required to configure the equipment. You should also record switch ports, cable drops, and IP network address assignments 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 and Passwords

The standard configuration steps configures standard passwords for root, admusr, pmacadmin, HP OA, and some other accounts referenced in this procedure. These passwords are not included in this document. Contact My 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.

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 must first 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 Oracle X5-2 RMS Environment

The following procedures are specific to Oracle X5-2 and Netra X5-2 RMS servers.

5.1.1 ILOM Configuration Procedure

Oracle Integrated Lights Out Management (ILOM) is an independent subsystem inside an Oracle server which is used for out-of-band remote access. You must configure the ILOM subsystem.

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

5.1.2 Updating Oracle Server Firmware

Each server must have the correct release of firmware.

The procedure for updating Oracle server firmware is described in the Oracle Firmware Upgrade Pack, Upgrade Guide, Release 3.1.5 and Oracle Firmware Upgrade Pack, Upgrade Guide, Release 3.1.6.

5.1.3 ILOM Web GUI Settings

After you have performed the ILOM configuration procedure, ILOM is accessible through a web GUI interface. You should change the default password for the root account.

To complete this procedure, you must record the new password for the root account.

To change the password, while in the ILOM 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 Oracle and Netra X5-2 RMS Server

The procedures for BIOS configuration are located in section 7.3.3:BIOS Settings for Oracle Rack Mount 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 Oracle RMS server is ready to IPM.

5.1.5 IPM of an Oracle X5-2 RMS Server

Every Oracle X5-2 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

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

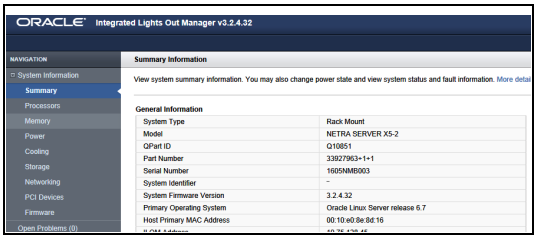
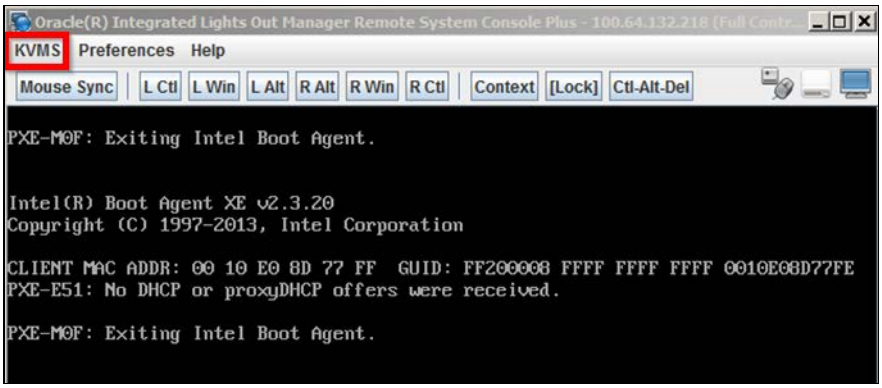
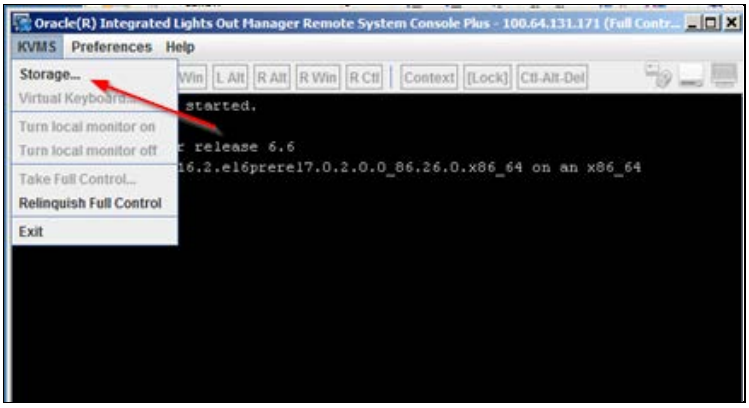
Required material

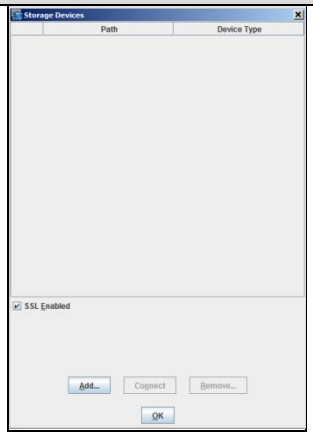
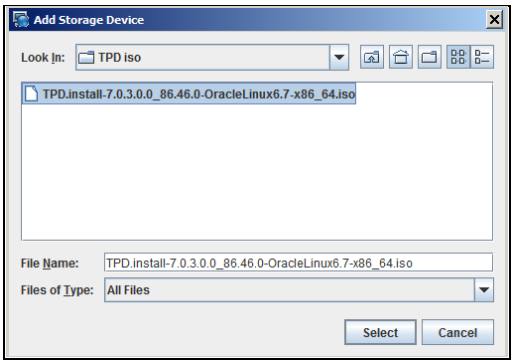
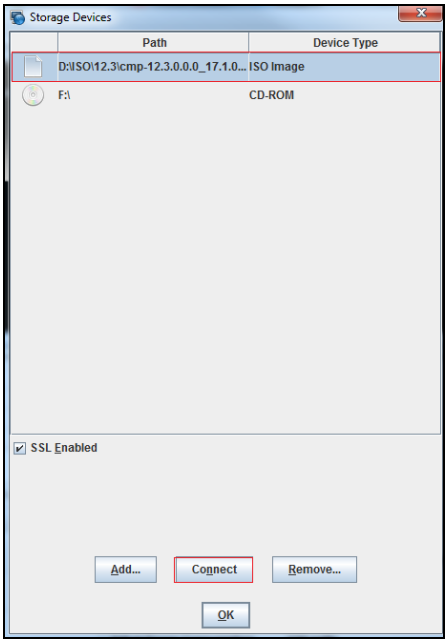
- TPD ISO image file for virtual mount accessible on laptop
- USB device prepared with bootable version of TPD image

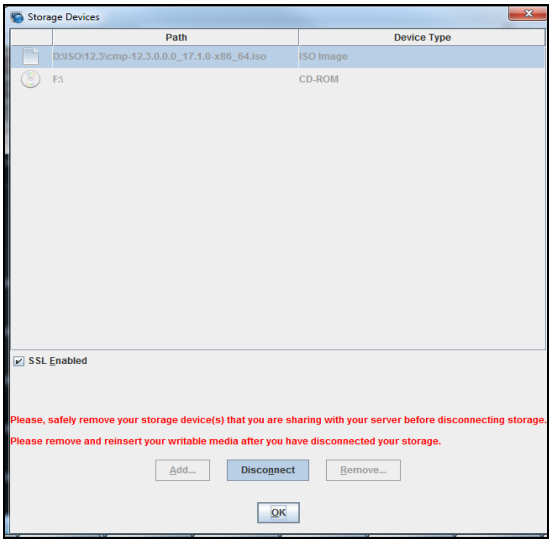
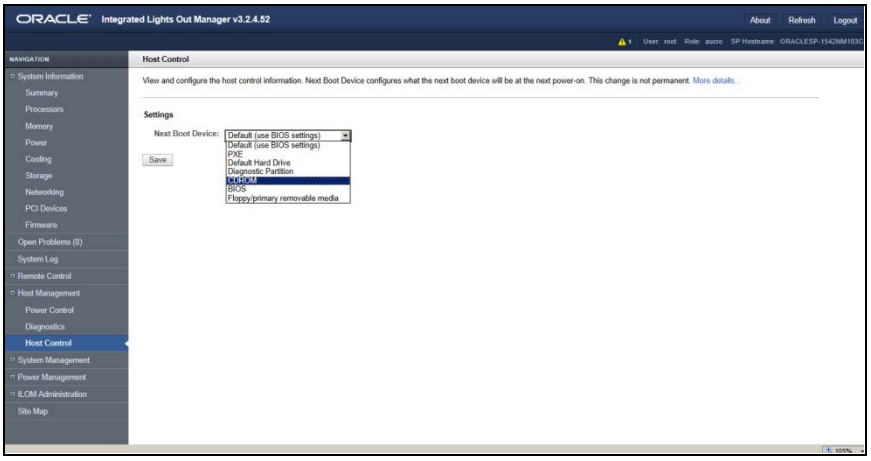
If this procedure fails, contact ORACLE TECHNICAL Services and ask for ASSISTANCE.

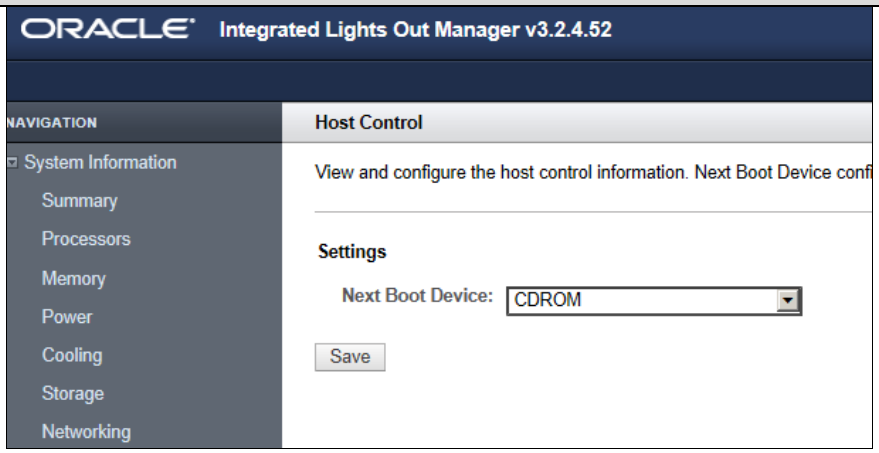
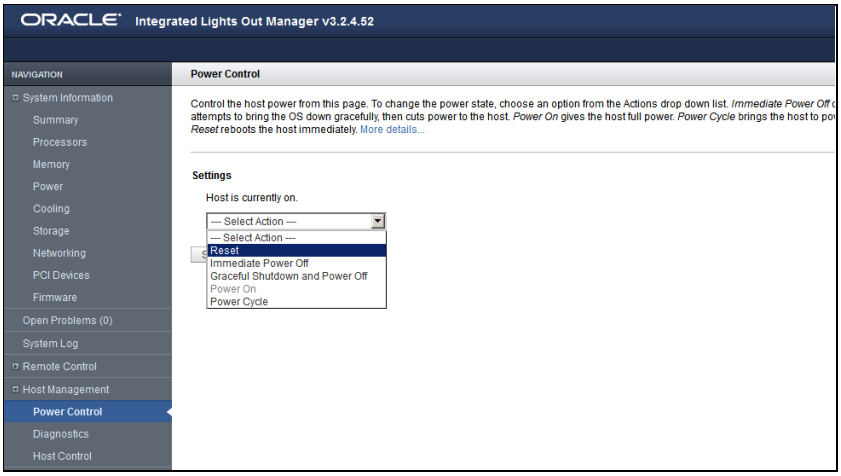
5.1.5: IPM of Oracle X5-2 RMS Server

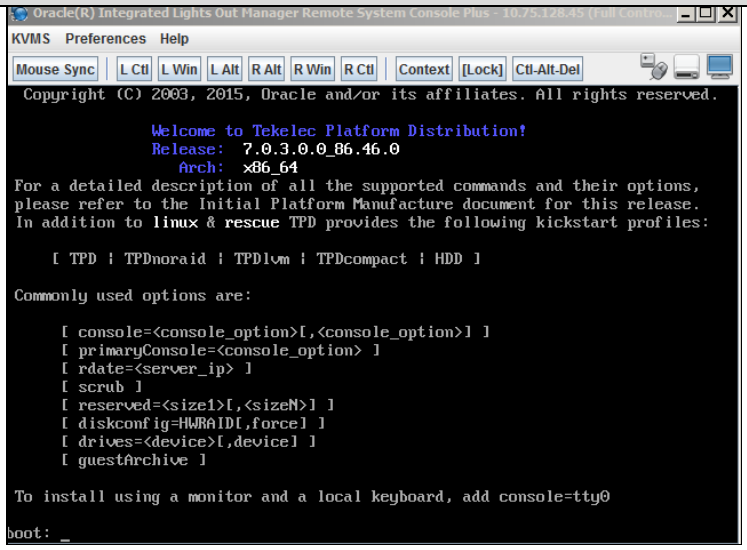
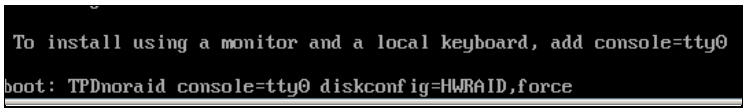
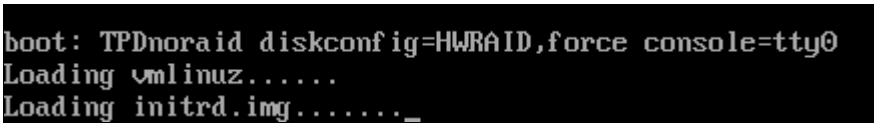
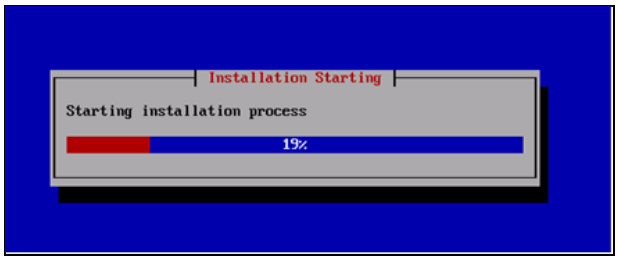
Step	Procedure	Details
1. ☐	Insert Bootable USB Media/mount TPD ISO	1. Create a bootable USB drive with the TPD ISO image file. Use the method provided in the README.txt file that is included with the downloaded Policy Software or other suitable method for creating a bootable USB device. There are several readily available utilities to achieve this. 2. 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 ILOM of the server has been enabled you can use the remote console capability of the X5-2 ILOM as per the following procedure See Section 7.1.2: Accessing the iLO VGA Redirection Window for Oracle RMS Servers. 3. Login to ILOM web interface and navigate to **System Information → Summary** then launch the remote console:

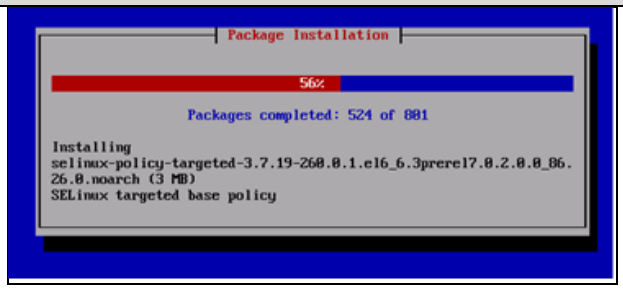
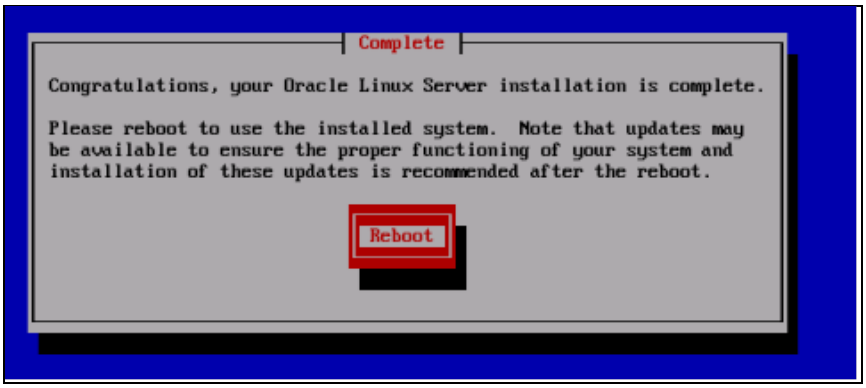
Step	Procedure	Details
		NOTE: This launches the video redirection console which is preferred to perform these procedures  The ILOM remote system console launches. If no OS has been previously installed something similar to the following screen opens:  4. From the KVMS menu, select **Storage**.  5. In the Storage devices window that opens up, click **Add**.

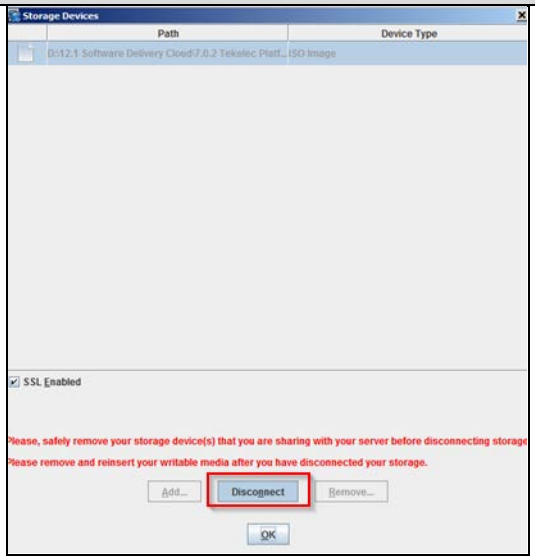
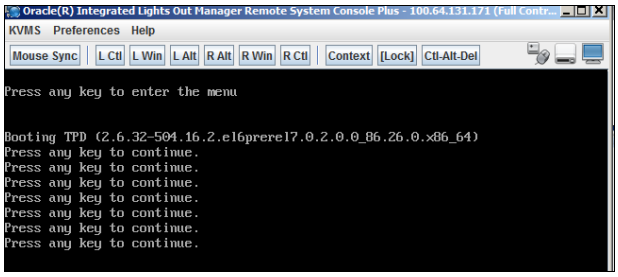
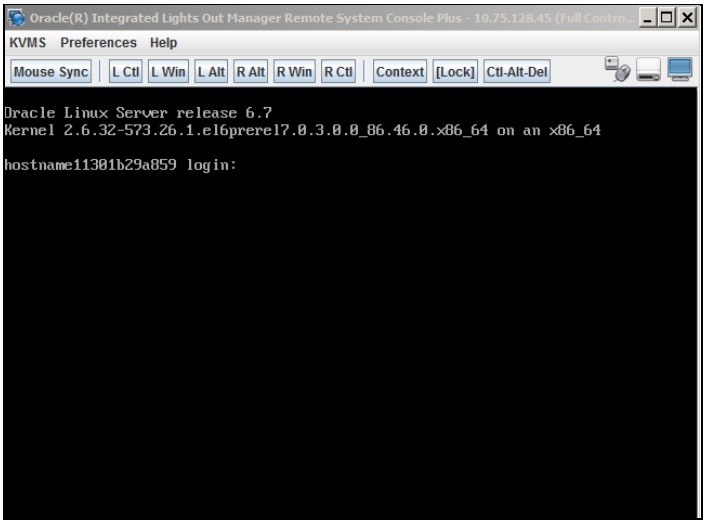
Step	Procedure	Details
		 6. Browse to ISO image file to mounted and click **Select**.  The Storage Devices form displays the selected ISO image file. 7. Highlight the file and the Connect option becomes available at the bottom of the form. Click **Connect**. And then confirm by clicking **OK**.  The Storage Devices indicate that the ISO image has successfully

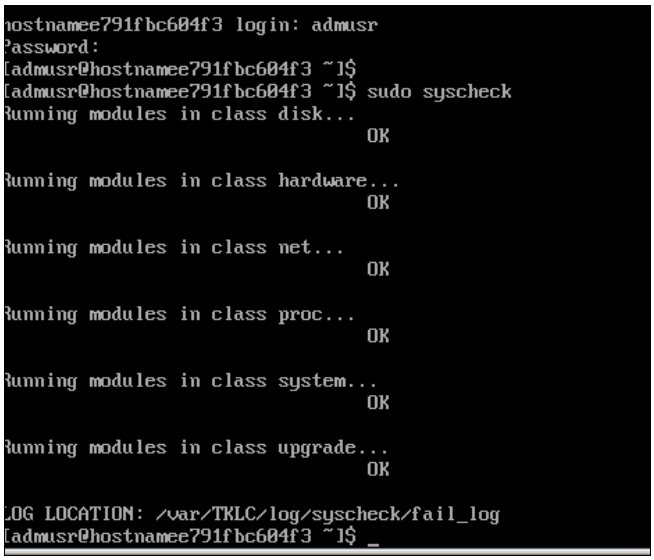
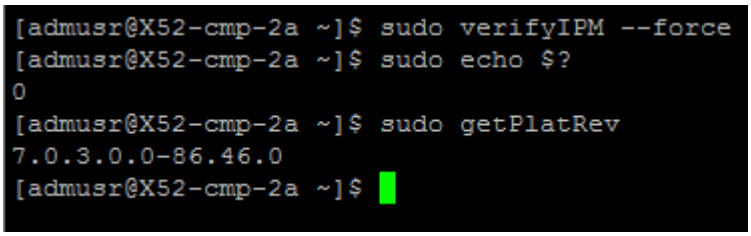
Step	Procedure	Details
		mounted/connected. Leave this window open. 
2. ☐	**Console:** Boot server, wait for TPD boot: form	1. Return to the iLO summary page and navigate to **Host Management → Host Control**.  2. Change to CDROM. 3. Click **Save**. This causes the server to boot to the virtually mounted ISO image.

Step	Procedure	Details
		 4. In the iLO, navigate to **Host Management → Power Control**. 5. Select **Reset** from the list to reboot the server. 6. Click **Save** and the server reboots to the mounted ISO image. 
3. ☐	**Console:** Enter TPD boot: command with correct options. TPD install takes approximately 20 to 40 minutes to complete.	The server boots to the virtually mounted TPD ISO image and the following screen opens:

Step	Procedure	Details
		 IPM the server using the following command at the boot prompt: `boot: TPDnoraid diskconfig=HWRAID,force console=tty0`  **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`. After the command has been entered, press **Enter** and you see something like the following screen indicating that the OS is installing  **NOTE:** If a non-Policy Management application was previously 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. See the TPD Initial Product Manufacture, Software Installation Procedure. The TPD installation takes approximately 20 to 40 minutes to complete, starting with some checks then installation starts:  Then you are able to monitor the packages installation progress:

Step	Procedure	Details
		 Then post installation scripts kick off:  After IPM the process is completed, you are prompted to press **Enter** to reboot the server.  At this time the media can be disconnected. Using the remote console for the ILOM, got to the Storage Devices form and unmount the image from the ILOM remote console. Then highlighting the remote console window, press **Enter** to reboot the server as per the following steps. . If a bootable USB device was used, remove the USB device To unmount the ISO image file, select the file and click **Disconnect** if the file was previously connected

Step	Procedure	Details
		 Press **Enter** to boot the server from TPD and complete the installation. The installed OS can be seen booting up 
4. ☐	**Console:** Login prompt	After the server reboots, the login prompt is displayed. Login into the server with admusr. **NOTE:** The server reboots more than once during the TPD installation process.  If a login prompt is not displayed after 15 minutes, contact My Oracle Support for assistance.

Step	Procedure	Details
5. ☐	**Console:** Run syscheck	From the CLI prompt, run the **`sudo syscheck`** command. This checks the health of each of the major subcomponents of the system, and displays OK if all passed, or a descriptive error of the problem if anything failed. The following shows a successful run of syscheck, where all subsystems pass, indicating the post-install process is complete.  hostnamee791fbc604f3 login: admusr Password: [admusr@hostnamee791fbc604f3 ~]$ [admusr@hostnamee791fbc604f3 ~]$ sudo 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 [admusr@hostnamee791fbc604f3 ~]$ _ If any of the modules return an error, do not continue; contact My Oracle Support and report the error condition.
6. ☐	**Console:** Verify Install success	Verify that IPM completed successfully by checking the install logs for errors and displaying the install TPD platform version.To do this, log in as admusr and then run the following commands: `$ sudo verifyIPM` (--force if needed) `$ sudo echo $?` (should return 0 errors) `$ sudo getPlatRev` (should return the current TPD version installed)  [admusr@X52-cmp-2a ~]$ sudo verifyIPM --force [admusr@X52-cmp-2a ~]$ sudo echo $? 0 [admusr@X52-cmp-2a ~]$ sudo getPlatRev 7.0.3.0.0-86.46.0 [admusr@X52-cmp-2a ~]$ Previous screen shows no errors returned which indicates the TPD installation process is completed. If errors are found, contact My Oracle Support.
---END OF PROCEDURE---		

5.1.6 Installing Policy Management Software

Use this procedure to install the Policy Management software on an Oracle rack mount server (RMS).

Prerequisites

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

- The appropriate release and application package(s) 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 ILOM remote console.
- If you are using the ILOM remote console, you need the IP address of the ILOM system and the login information.

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

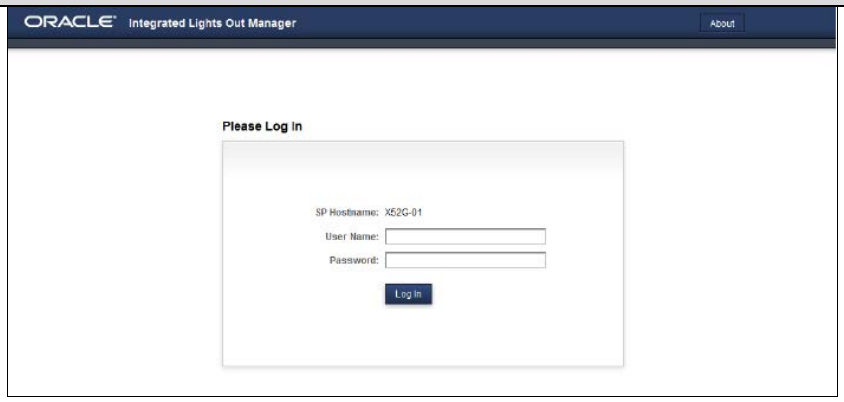
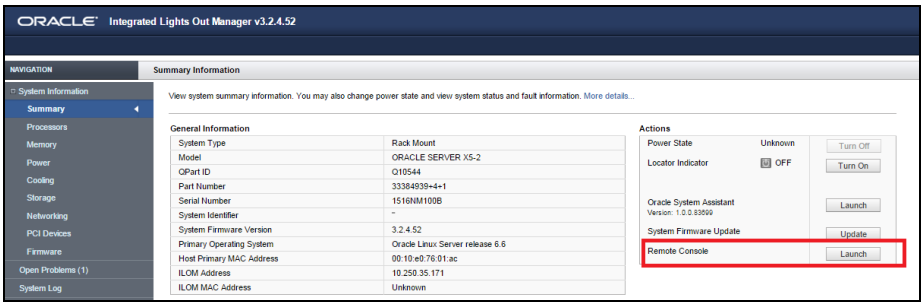
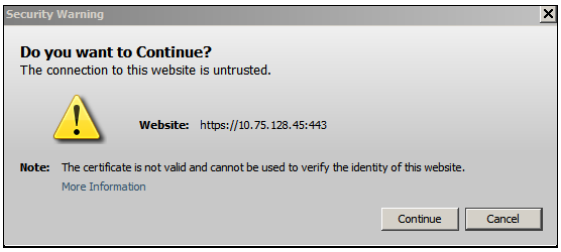
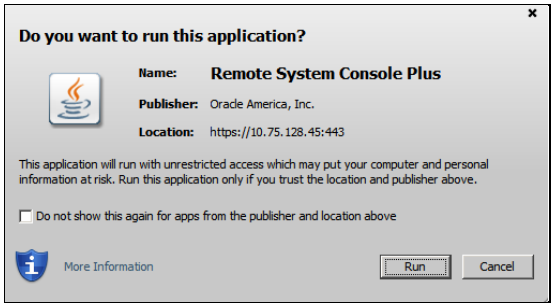
NOTE: There are two methods for installing the Policy Management application:

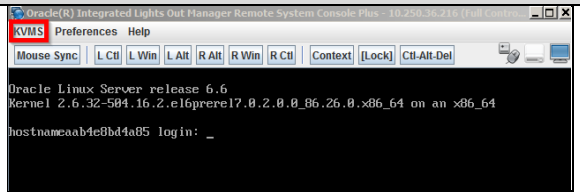
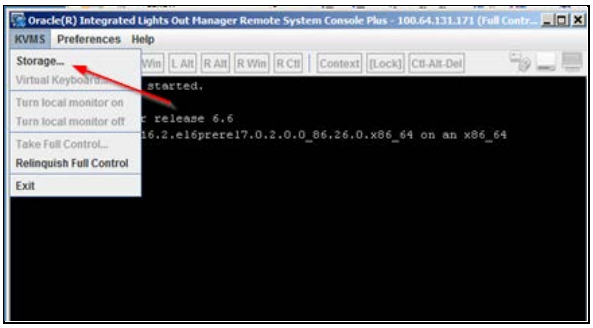
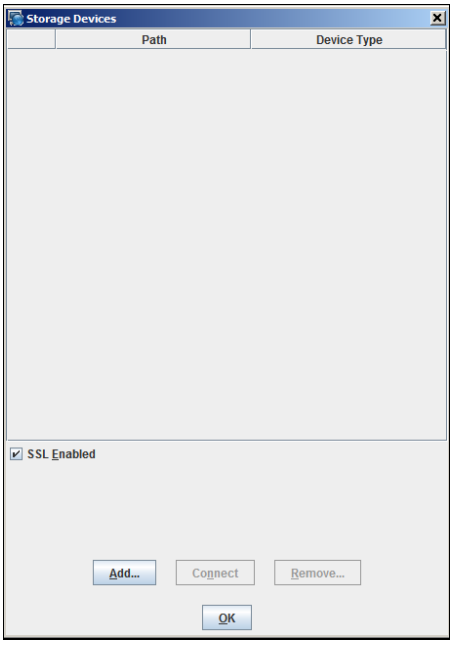
1. Use a USB drive inserted locally into the server. This is the preferred method.
2. Use the virtual mount capability of the iLO remote console over a network. This method is dependent on having a good network connection from the workstation where the ISO is located to the target server iLO. The browser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

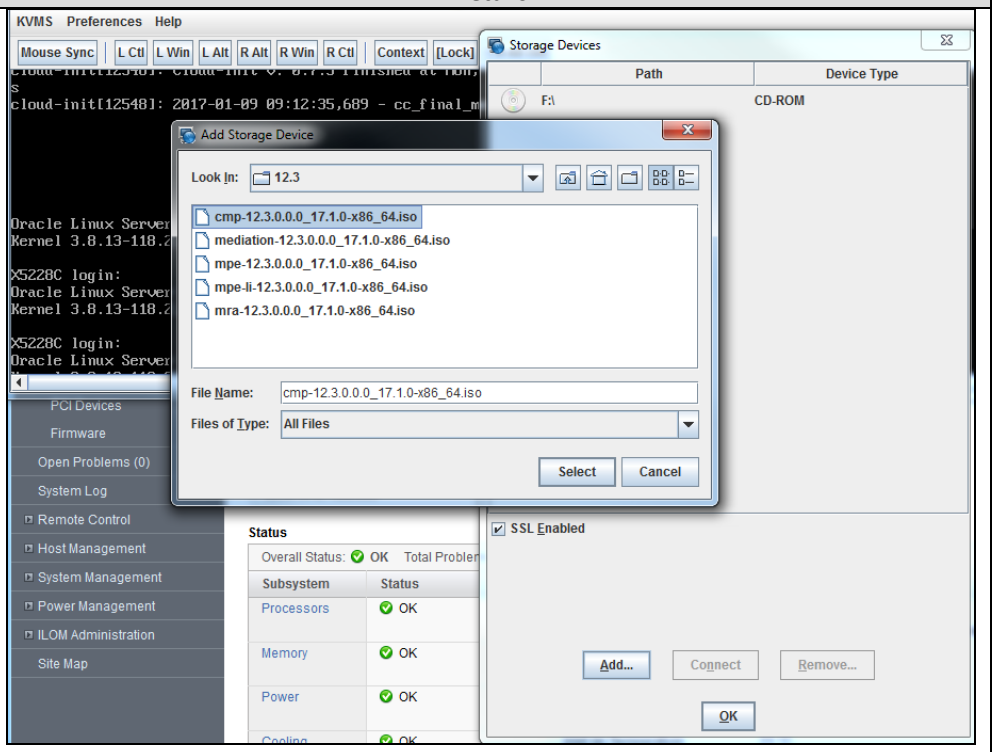
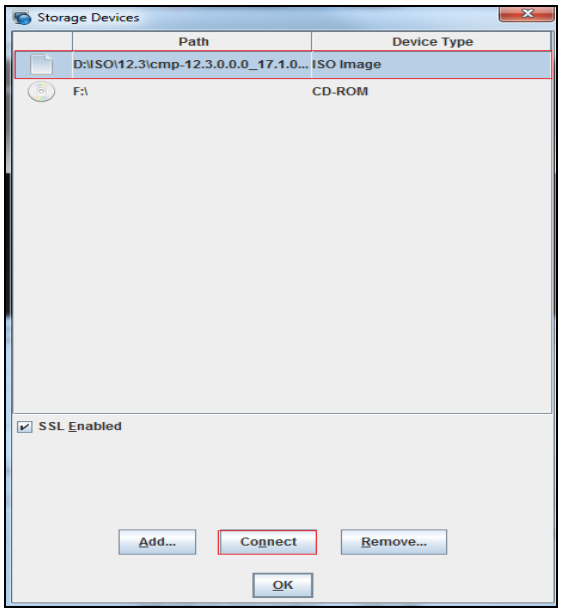
If this procedure fails, contact ORACLE TECHNICAL Services and ask for ASSISTANCE.

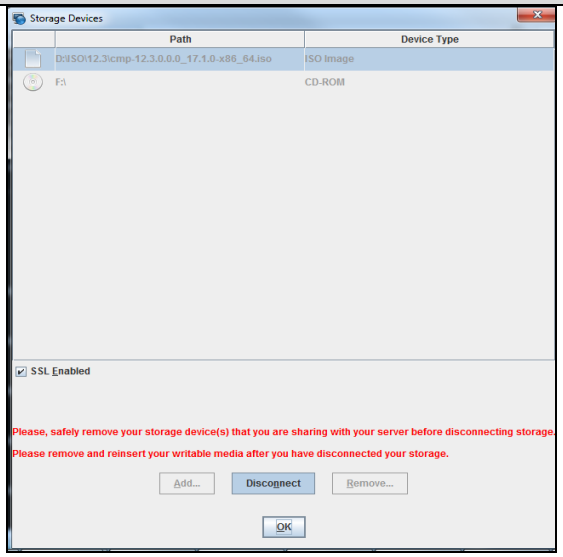
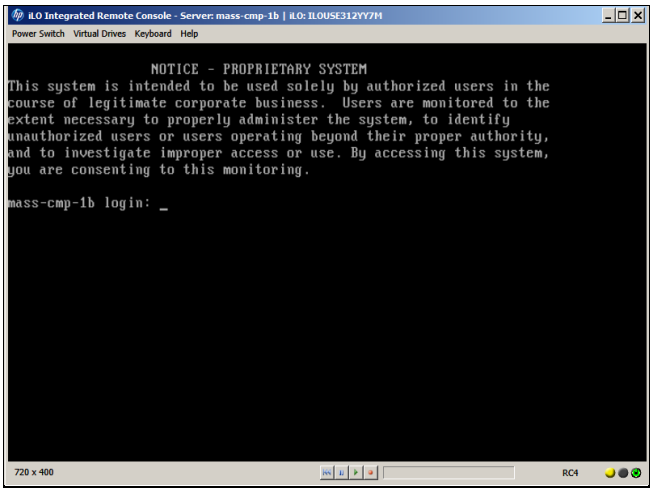
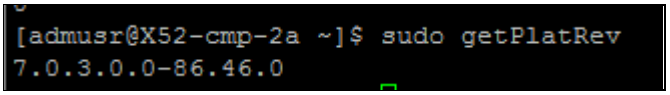
5.1.6: Installing Policy Management Software

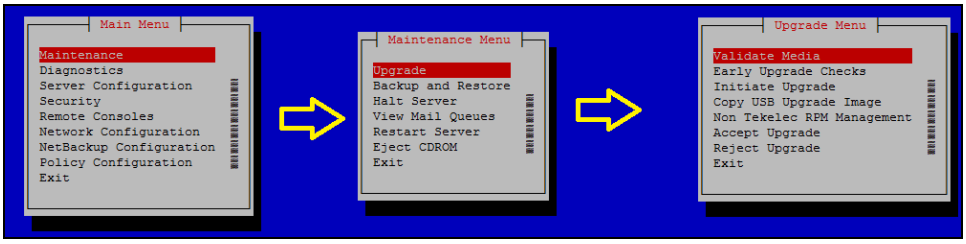
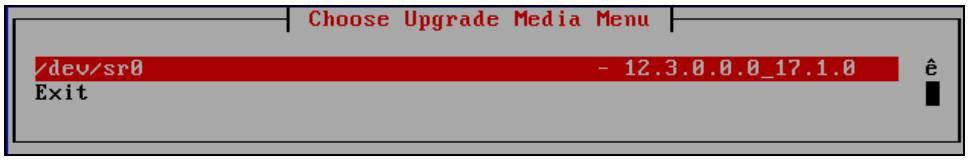
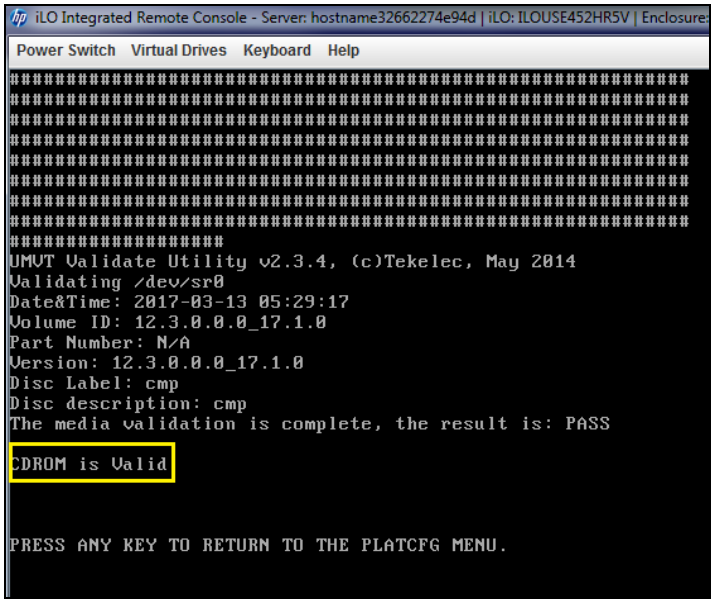
Step	Procedure	Details
1. ☐	Make the Policy Management application ISO images available for installation	Copy the Policy Management application ISO image file (CMP/MPE/MRA/Mediation) onto a USB drive and insert the USB drive locally into the server. Connect to the server Console or Remote Console: • Using a VGA Display and USB Keyboard • Using the Server iLO port and iLO Web Interface (to access Remote Console) Proceed to step 2 of this procedure. If you are using the ILOM remote console and have the Policy Management software as an ISO image file, do the following: 1. Open a browser, enter the URL of the ILOM system, and log in. For example:

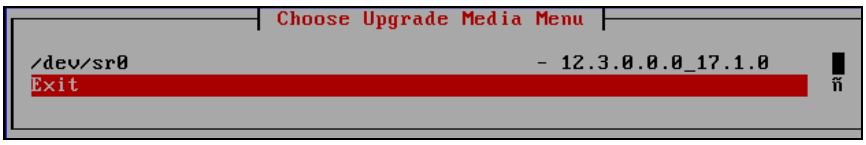
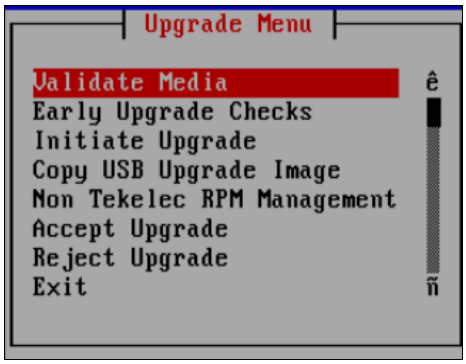
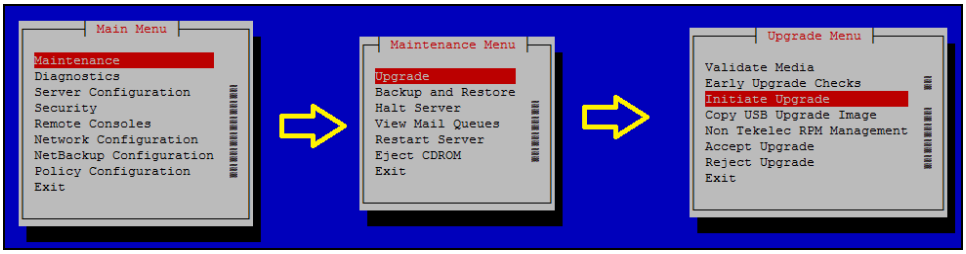
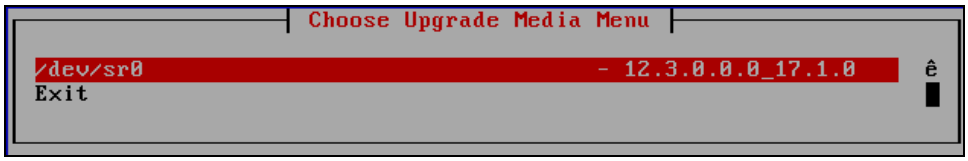
Step	Procedure	Details
		 2. Navigate to **System Information → Summary**. The *Summary Information* page opens. 3. Under *Actions*, locate Remote Console and click **Launch**. For example:  4. The ILOM remote system console starts. Click **Continue.**  5. Click **Run** if needed.  6. Select **KVMS → Storage**. The Storage Devices window opens.

Step	Procedure	Details
		 7. From **KVMS**, click **Storage**:  8. In the Storage Devices window, click **Add.** The Add Storage Device window opens.  9. Browse to the ISO image file to mount and click **Select**. **NOTE:** Make certain that the ISO image file selected (CMP/MPE/MRA/MEDIATION) is the correct one for the target server according to the Policy Solution Design!

Step	Procedure	Details
		 The Add Storage Device window closes, and the Storage Devices window displays the selected ISO image file. 10. Select the ISO image file. The Connect button, at the bottom of the form, becomes enabled. For example:  Click **Connect** and then **OK**. The Storage Devices window indicates that the ISO image file is successfully connected. For example:

Step	Procedure	Details
		 Leave this window open.
2. ☐	**Console:** Login as admusr	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 Login as admusr. 
3. ☐	**Console:** verify platform revision	You can verify the platform revision by logging in as the user admusr 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.

Step	Procedure	Details
		2. From the Main menu, navigate to **Maintenance → Upgrade → Validate Media.** 3. Select the ISO image file, and press **Enter**.  **NOTE:** Depending on the method used the platcfg utility searches for any mounted ISO files and, if successful, displays the Policy Management application ISO image file to install For example:  4. Select the ISO image. The utility displays **`Validating media or cdrom`** and a series of hash marks (#) signs. When it completes ,it displays information about the ISO image file and the message that the CDROM or media is valid. The following example shows a successful validation: 

Step	Procedure	Details
5. ☐	**Console:** verify platform revision	1. Press Enter to return to the menu. 2. Scroll to exit and press enter again.  The Main menu opens. 
6. ☐	**Console:** Select ISO to install, and confirm Application installation takea 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.  **NOTE:** The server reboots twice during the installation process. Do not remove the media at this time.

Step	Procedure	Details

7. ☐	**Console:** Verify Policy install version	After the application has completed the installation log and returned you back to the command line as admusr and confirms the installed TPD platform version and Policy Management application version.
		`$appRev`
		`[admusr@hostname32662274e94d ~]$ appRev`
		`Install Time: Mon Mar 13 06:43:14 2017`
		`Product Name: cmp`
		`Product Release: 12.3.0.0.0_17.1.0`
		`Base Distro Product: TPD`
		`Base Distro Release: 7.0.3.0.0_86.46.0`
		`Base Distro ISO: TPD.install-7.0.3.0.0_86.46.0-OracleLinux6.7-x86_64.iso`
		`ISO name: cmp-12.3.0.0.0_17.1.0-x86_64.iso`
		`OS: OracleLinux 6.7`
		Verify:
		• TPD revision installed
		• Policy Management application installed and its revision

8. ☐	**Console:** Verify Install success	Inspect the file `/var/TKLC/log/upgrade/upgrade.log` 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:
		`1467617932::This is an install`
		`1467617932::Running postUpgradeBoot() for Upgrade::Policy::QPLVMBasedBackout upgrade policy...`
		`1467617932::Running postUpgradeBoot() for Upgrade::Policy::QPMySQLPolicy upgrade policy...`
		`1467617932::Running postUpgradeBoot() for Upgrade::Policy::QPNTPFixes upgrade policy...`
		`1467617932::Running postUpgradeBoot() for Upgrade::Policy::QPRunPostRPMActionsPolicy upgrade policy...`
		`1467617932::Running postUpgradeBoot() for Upgrade::Policy::QPUpgradeCommon upgrade policy...`
		`1467617932::Running postUpgradeBoot() for Upgrade::Policy::QPUpgradeProgress upgrade policy...`
		`1467617932::Running postUpgradeBoot() for Upgrade::Policy::PlatformLast upgrade policy...`
		`1467617932::Updating platform revision file...`
		`1467617932::RCS_VERSION=1.1`
		`1467617932::Marking task 1467617076.0 as Success`
		`1467617932::Upgrade returned success!`
		`1467617933::Creating RC script to set alarm on next boot`
		`1467617933::`/mnt/upgrade/upgrade/upgradeStatus' -> `/sysimage/etc/rc.d/rc4.d/S99TKLCupgradeStatus'`
		`1467617933::Cleaning up chroot environment...`
		`1467617933::`
		`1467618026:: /etc/rc4.d/S99TKLCupgradeStatus - AlarmMgr daemon is not running, delaying by 1 minute`
		`1467618060:: /etc/rc4.d/S99TKLCupgradeStatus - Not setting 'Upgrade Accept/Reject' alarm`
		`1467618060:: /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, MEDIATION) on each server. Proceed to Section 6: Configure Policy Application Servers in Wireless Mode.
---END OF PROCEDURE---		

5.2 Preparing an HP RMS Environment

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

5.2.1 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)

5.2.2 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 2.2.9 and HP Solutions Firmware Upgrade Pack, Software Centric Release Notes, Release 2.2.10.

5.2.3 ILO Web GUI Settings

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

To complete this procedure, you must record the new password for the root account To change the password:

1. While in the ILO web interface, 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)

5.2.4 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.

5.2.5 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 the system OS (IPM) of the server.

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

Required material

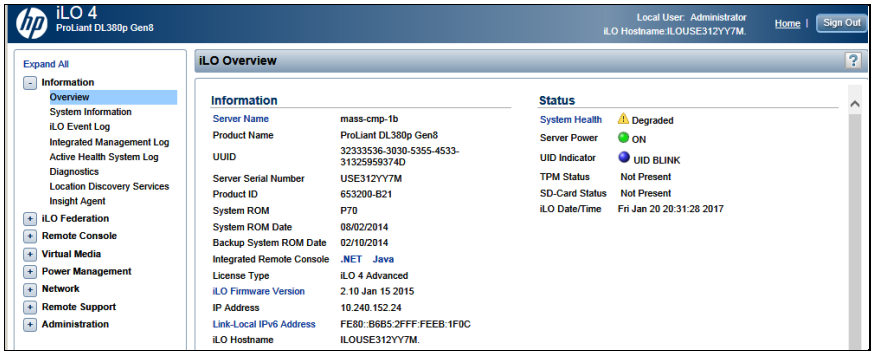
- TPD ISO image file for virtual mount accessible on laptop
- USB device prepared with bootable version of TPD image

If this procedure fails, contact ORACLE TECHNICAL Services and ask for ASSISTANCE.

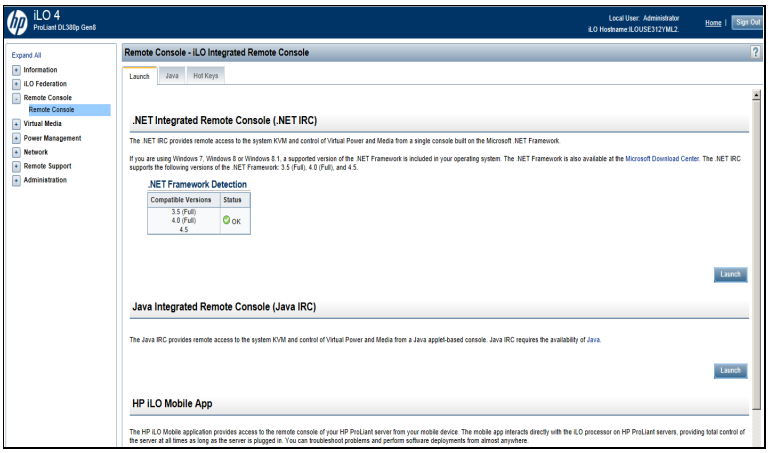
5.2.5: IPM of a HP DL380 RMS Server

Step	Procedure	Details
1. ☐	Insert bootable USB media/mount TPD ISO	1. 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. 2. 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 3. If local access to the server is not available and network access to the iLO of the server has been enabled you can use the remote console capability of the HP iLO as per the following procedure See Section 7.1.2: Accessing the iLO VGA Redirection Window for HP Servers. 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: 4. Open a browser, enter the URL of the iLO system (management_server_iLO_ip), and log in. For example:

Step	Procedure	Details

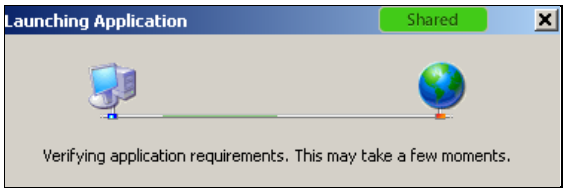


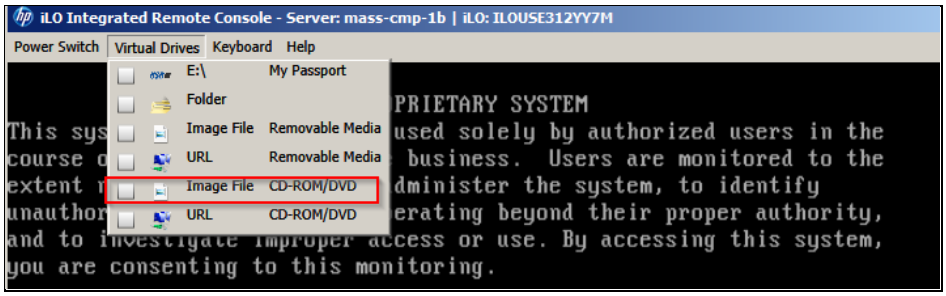
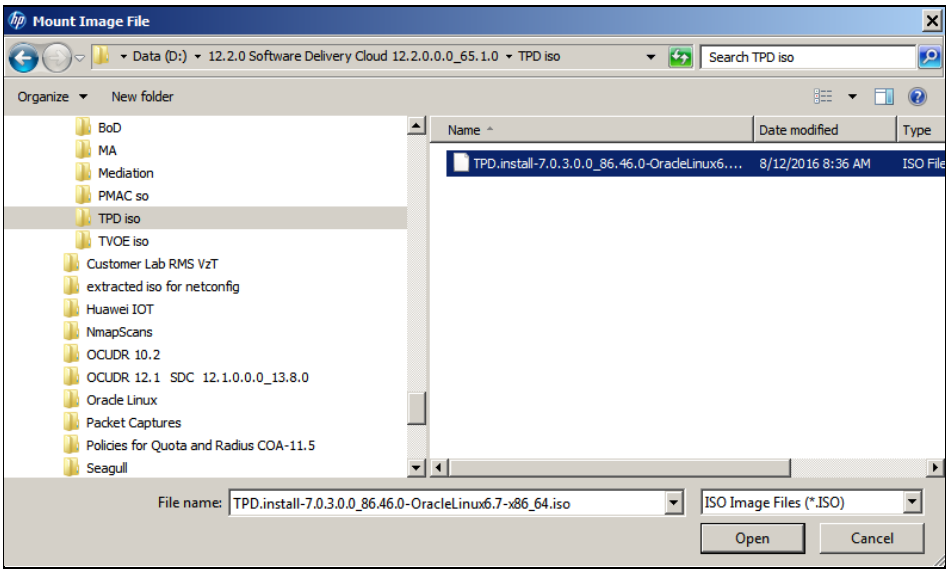
5. On the home page, select **Remote Console → Remote Console**. The Remote Console page opens. For example:

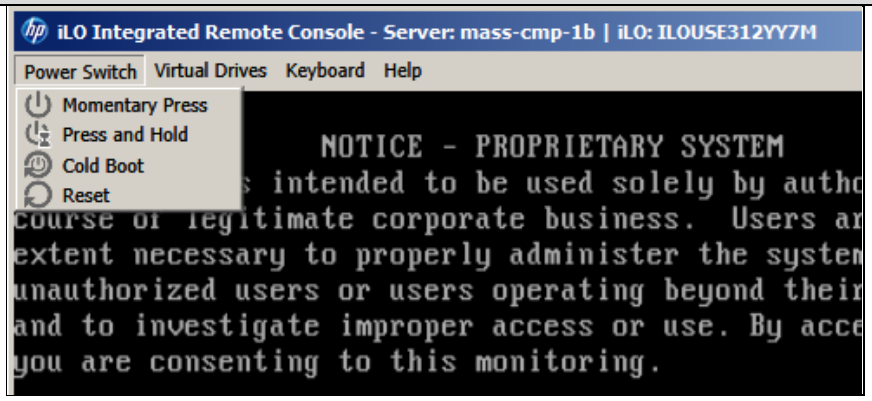
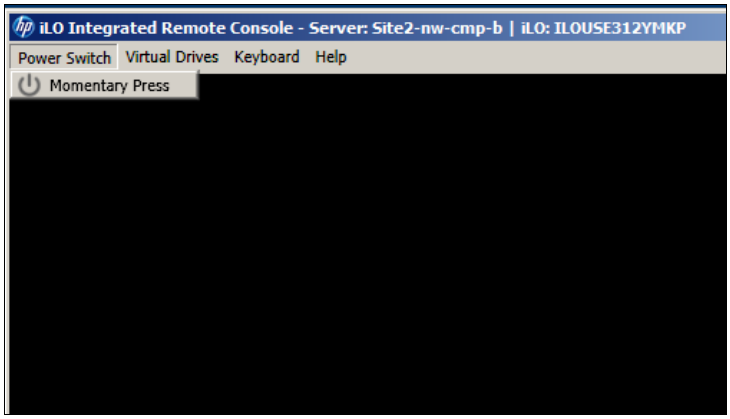
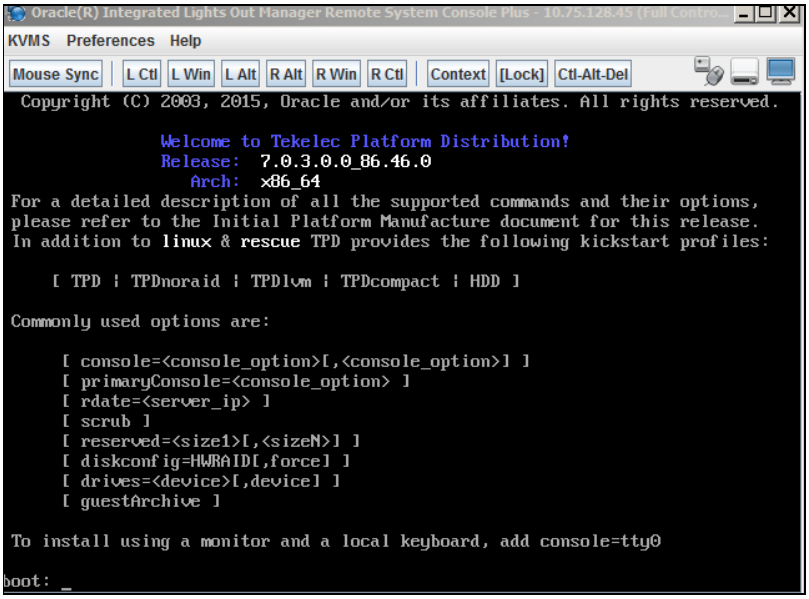


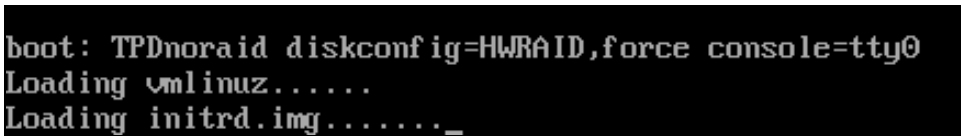
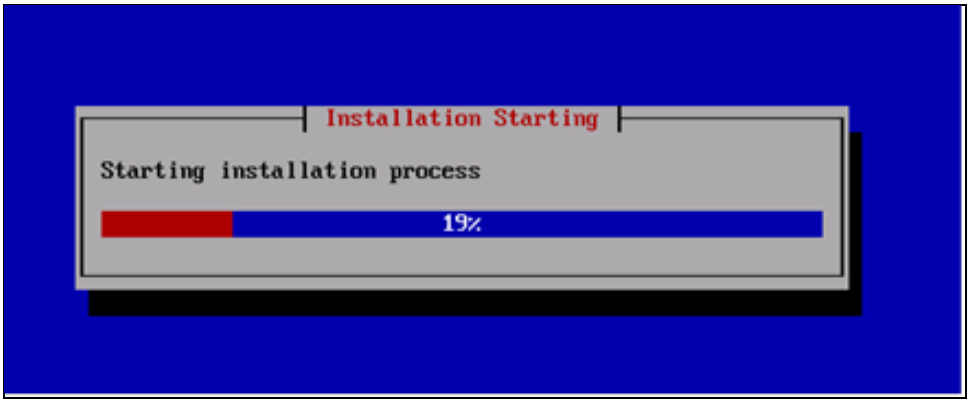
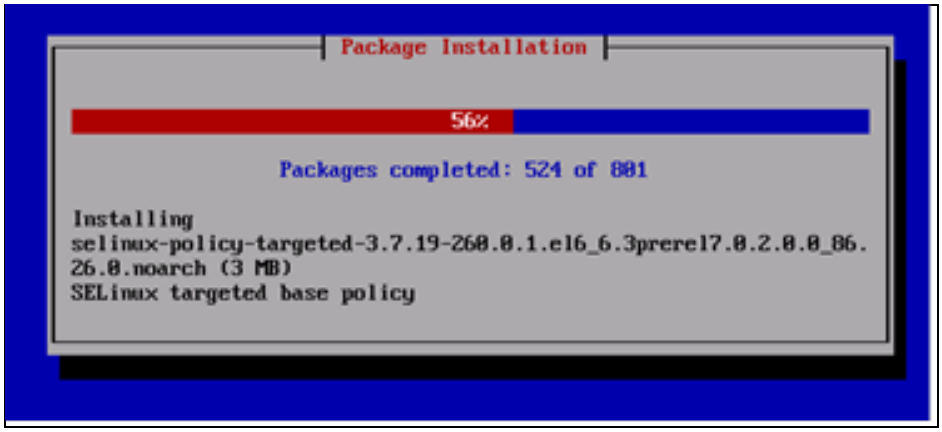
NOTE: When launching a remote console, the .NET application is compatible with a Windows browser; Java is compatible with both Windows and Firefox browsers.

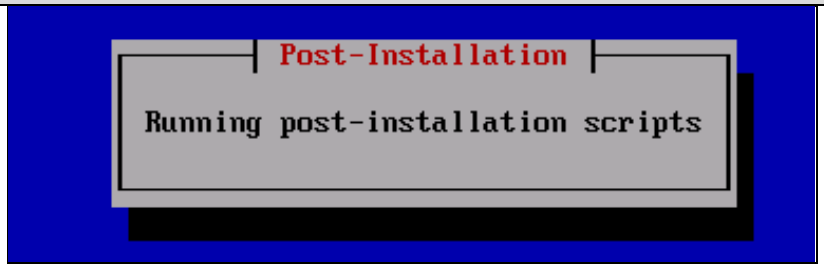
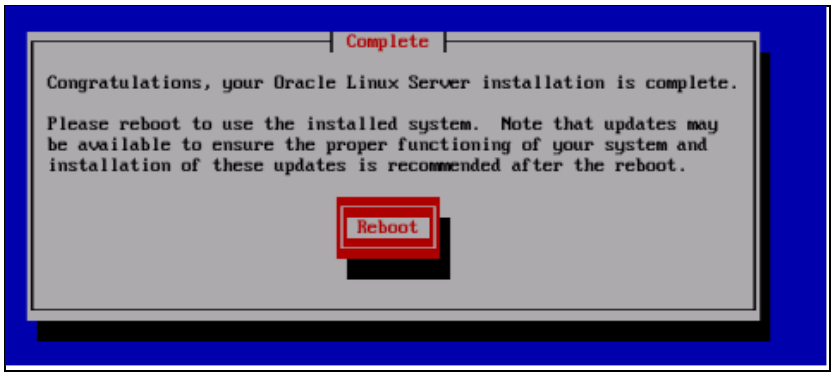
6. In the *Java Integrated Remote Console* section, click **Launch**. A security warning window opens, prompting for confirmation that you want to run the application. For example:

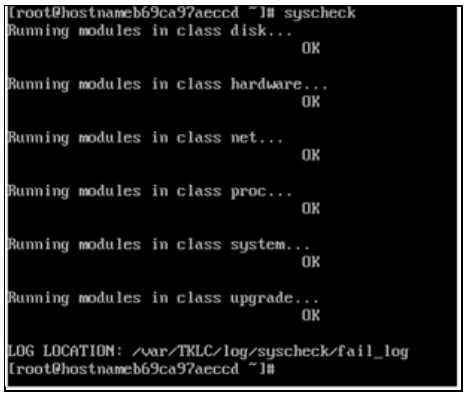


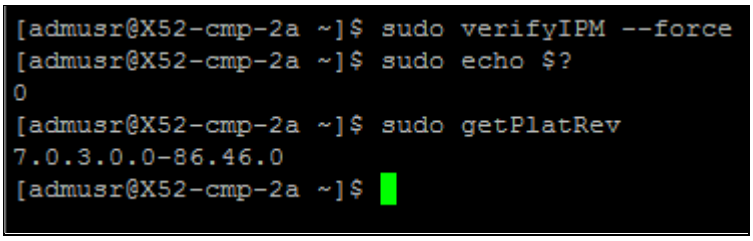
Step	Procedure	Details
		7. Click Run. The Remote Console window opens.  8. Select **Virtual Drives → Image File CD-ROM/DVD.** 9. Browse to the ISO image file location, and click **Open**. The ISO image file is mounted.  10. Select the image file CD-ROM/DVD and browse to the TPD ISO location then click open:  11. Select **Power Switch → Momentary Press**. The server powers down.

Step	Procedure	Details
		 12. When the Power Switch options display the Momentary Press option, click **Momentary Press** again.  13. The server starts, and after completion of the boot process, displays a screen similar to the following: 
2. ☐	**Console:** Enter TPD boot:	Enter the following command at the boot prompt to initiate the initial product manufacture (IPM) process.

Step	Procedure	Details
	command with correct options TPD install takes approximately 20 to 40 minutes to complete	`boot: 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 previously 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. See TPD Initial Product Manufacture, Software Installation Procedure (Section 3.4) TPD installation takes 20–40 minutes. During this process you see in-progress windows similar to the following   Then you are able to monitor the installation progress of the package:  Then post installation scripts kick off:

Step	Procedure	Details
		 After IPM process is completed, 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.  When you see the Complete window, the IPM process is complete.
3. ☐	Remove or unmount the installation media.	If installation is done remotely using the remote console for the iLO, unmount the image from the virtual drives menu of the console (uncheck the image file option) then press **Enter** to reboot the server. If a bootable USB device was used, remove the USB device If you reboot the server without removing the installation media, the server boots to the bootable media. If this happens, wait until you see the Complete window, remove the bootable image, and restart again.
4. ☐	**Console:** Press Enter to reboot	Make sure 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 does not display after waiting 15 minutes, contact My Oracle Support for assistance.

Step	Procedure	Details
6. ☐	**Console:** Run syscheck	Log in as the user root 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@hostnameb69ca97aeccd ~]# 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@hostnameb69ca97aeccd ~]# 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 via the following commands:
		`$ sudo verifyIPM (--force if needed)`
		`$ sudo echo $? (should return 0 errors)`
		`$ sudo getPlatRev (should return the current TPD version installed)`
		The following example shows a successful installation:
		 
		[admusr@X52-cmp-2a ~]$ sudo verifyIPM --force
		[admusr@X52-cmp-2a ~]$ sudo echo $?
		0
		[admusr@X52-cmp-2a ~]$ sudo getPlatRev
		7.0.3.0.0-86.46.0
		[admusr@X52-cmp-2a ~]$
		NOTE: If you see any errors, contact My Oracle Support.
		Repeat this procedure for every server.

---END OF PROCEDURE---		

5.2.6 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 package(s) 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.

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

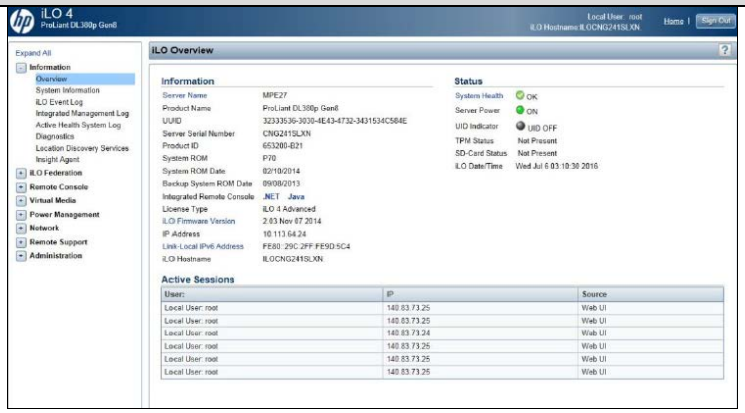
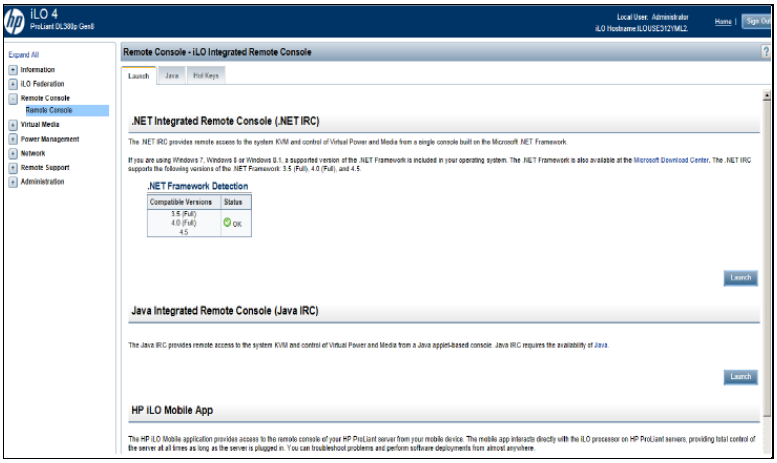
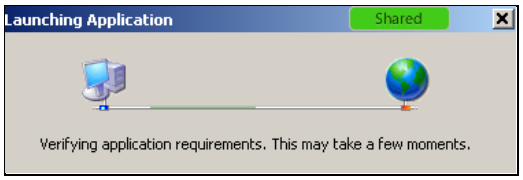
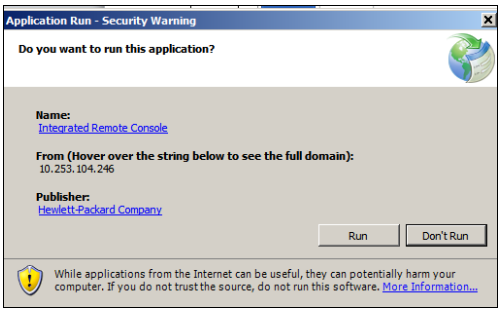
NOTE: There are two methods for installing the Policy Management application:

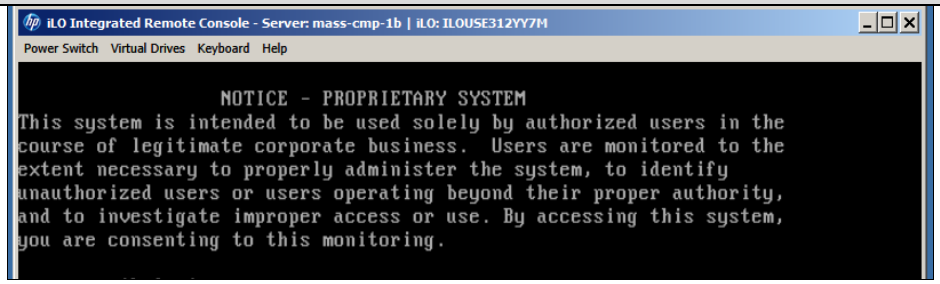
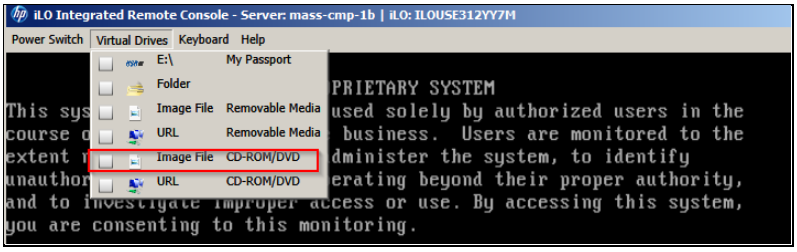
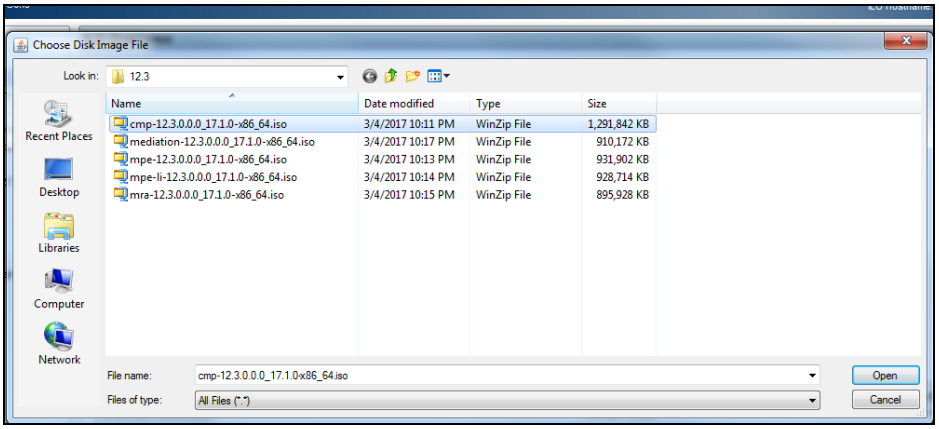
- Use a USB drive inserted locally into the server. This is the preferred method.
- Use the virtual mount capability of the iLO remote console over a network. This method is dependent on having a good network connection from the workstation where the ISO is located to the target server iLO. The browser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

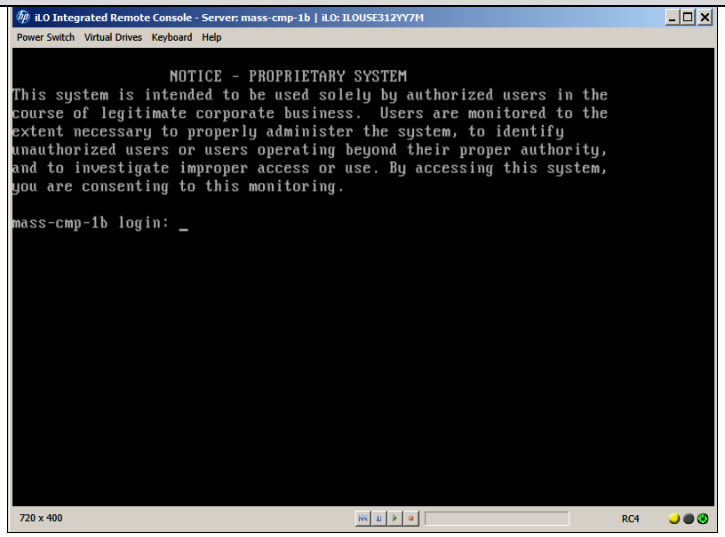
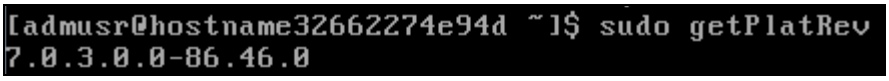
If this procedure fails, contact ORACLE TECHNICAL Services and ask for ASSISTANCE.

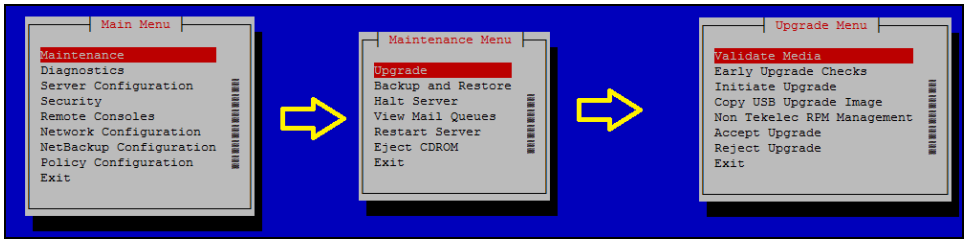
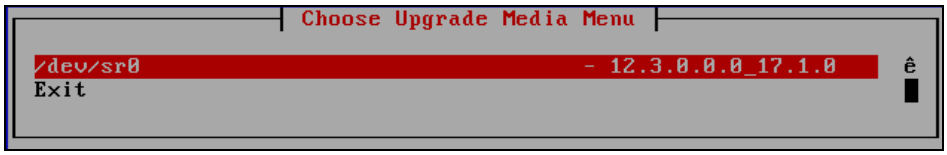
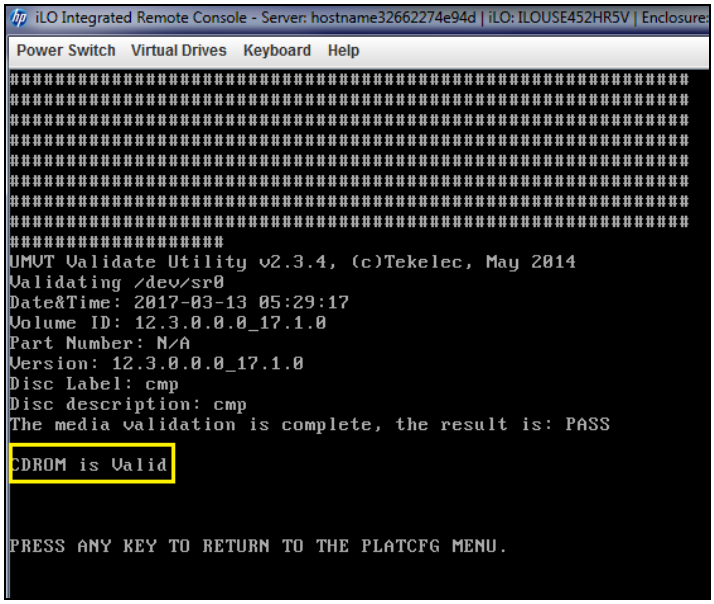
5.2.6: Installing Policy Management Software

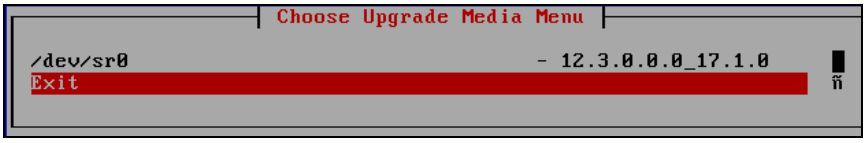
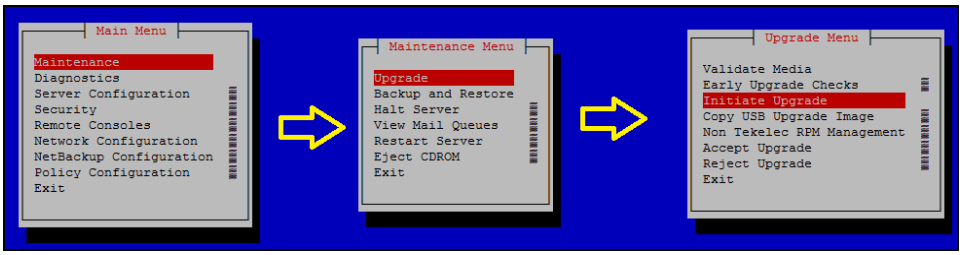
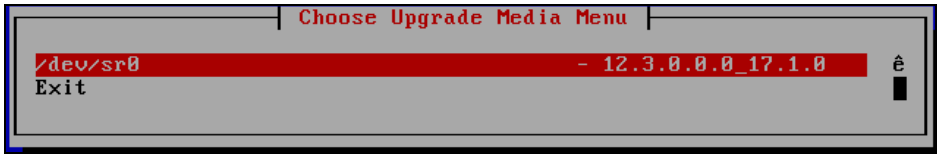
Step	Procedure	Details
1. ☐	Make the Policy Management application ISO images available for installation	Copy the Policy Management application ISO image file (CMP/MPE/MRA/Mediation) onto a USB drive and insert the USB drive locally into the server. Connect to the server Console or Remote Console: • Using a VGA Display and USB Keyboard • Using the Server iLO port and iLO Web Interface (to access Remote Console) Proceed to step #2 of this procedure 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 should be co-located with the ISO file repository. 1. Open a browser, enter the URL of the iLO system (management_server_iLO_ip), and log in. For example:  After login, the iLO home page displays.

Step	Procedure	Details
		 2. On the home page, select **Remote Console**. The *Remote Console* page opens.  **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:   4. Click Run. The Remote Console window opens.

Step	Procedure	Details
		 5. 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:** Make certain that the ISO image file selected (CMP/MPE/MRA/MEDIATION) is the correct one for the target server according to the Policy Solution Design!  In this example, the CMP ISO image has been selected. Click **Open** to mount the required ISO image file, the dialog 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.

Step	Procedure	Details
		
3. ☐	**Console:** verify platform revision	You can verify the platform revision by logging in as the user admusr and entering the following command: $ sudo getPlatRev For example: `#sudo getPlatRev` 

Step	Procedure	Details
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.** 3. Select the ISO image file, and press **Enter**.  **NOTE:** Depending on the method used the platcfg utility searches for any mounted ISO files and, if successful, displays the Policy Management application ISO image file to install For example:  4. Select the ISO image and press **Enter**. The utility displays the valid media or CDROM message and a series of hash marks (#) signs. When it finishes, it displays information about the ISO image file and the message that the CDROM or media is valid. The following example shows a successful validation: 

Step	Procedure	Details
5. ☐	**Console:** verify platform revision	1. Press Enter to return to the menu. 2. Scroll to exit and press enter again.  The Main menu opens.
6. ☐	**Console:** Select ISO to install, and confirm Application install takes approximately 20 minutes. If you are installing using 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 Management application version.
		`$appRev`
		`[admusr@hostname32662274e94d ~]$ appRev`
		`Install Time: Mon Mar 13 06:43:14 2017`
		`Product Name: cmp`
		`Product Release: 12.3.0.0.0_17.1.0`
		`Base Distro Product: TPD`
		`Base Distro Release: 7.0.3.0.0_86.46.0`
		`Base Distro ISO: TPD.install-7.0.3.0.0_86.46.0-OracleLinux6.7-x86_64.iso`
		`ISO name: cmp-12.3.0.0.0_17.1.0-x86_64.iso`
		`OS: OracleLinux 6.7`
		Verify:
		• TPD revision installed
		• Policy Management application installed and its revision

Step	Procedure	Details

8.	**Console:** Verify Install success	Inspect the file `/var/TKLC/log/upgrade/upgrade.log` 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:
		`1489401794::Running postUpgradeBoot() for Upgrade::Policy::QPNTPFixes upgrade policy...`
		`1489401794::Running postUpgradeBoot() for Upgrade::Policy::QPRunPostRPMActionsPolicy upgrade policy...`
		`1489401794::Running postUpgradeBoot() for Upgrade::Policy::QPUpgradeCommon upgrade policy...`
		`1489401794::Running postUpgradeBoot() for Upgrade::Policy::QPUpgradeProgress upgrade policy...`
		`1489401794::Running postUpgradeBoot() for Upgrade::Policy::PlatformLast upgrade policy...`
		`1489401794::Updating platform revision file...`
		`1489401794::RCS_VERSION=1.1`
		`1489401794::Upgrade returned success!`
		`1489401795::Creating RC script to set alarm on next boot`
		`1489401795::`/mnt/upgrade/upgrade/upgradeStatus' -> `/sysimage/etc/rc.d/rc4.d/S99TKLCupgradeStatus'`
		`1489401795::Cleaning up chroot environment...`
		`1489401795::`
		`1489401884:: /etc/rc4.d/S99TKLCupgradeStatus - AlarmMgr daemon is not running, delaying by 1 minute`
		`1489401900:: /etc/rc4.d/S99TKLCupgradeStatus - Not setting 'Upgrade Accept/Reject' alarm`
		`1489401900:: /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, MEDIATION) on each server. For Wireless mode, proceed to Section 6: Configure Policy Application Servers in Wireless Mode
---END OF PROCEDURE---		

5.3 Preparing a c-Class Environment

5.3.1 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 Tekelec Platform 7.0.x, Configuration Guide.

It is necessary to IPM the Management Serrver and udate the Firmware according to the type of Hardware that is used for the Management Server.

See Section 3.6 Management Server Procedures

- 3.6.1 IPM Management Server
- 3.6.2 Upgrade Management Server Firmware

To install the Platform Management and Configuration (PM&C) application on the Management Server, see Section 3.7 PM&C Procedures.

- 3.7.1 Deploying Virtualized PM&C Overview
- 3.7.2 Installing TVOE on the Management Server
- 3.7.3 TVOE Network Configuration
- 3.7.4 Deploy PM&C Guest

The procedures referenced in this section deploy PM&C on the management server. In Policy Management 12.3, the management server is used for installation, adding new 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.

5.3.2 HP C-7000 Enclosure Configuration

Procedures for Installing and configuring a HP C-7000 enclosures can be found in Tekelec Platform 7.0.x, Configuration Guide.

See Section 3.5 C7000 Enclosure Procedures

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

- Section 3.5.1 Configure Initial OA IP

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

- Section 3.5.2 Configure Initial OA Settings Using the Configuration Wizard

This procedure configures the initial OA settings using a configuration wizard. This procedure should be used for initial configuration only and should be 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 the Cisco 4948/4948E switches must be configured.

- Section 3.5 C7000 Enclosure Procedures
  - Section 3.5.3 Configure OA Security
- This procedure disables telnet access to OA.
  - Section 3.5.4 Upgrade or Downgrade OA Firmware

This procedure updates the OA firmware.

- Section 3.5.5 Store OA Configuration on Management Server

This procedure backs up OA settings on the management server.

- Section 3.5.9 Updating IPv4 Addressing

This procedure updates the IP addressing for a C7000 enclosure.

- Section 3.5.10 Updating IPv6 Addressing

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

- Section 3.5.11 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.

5.3.3 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:

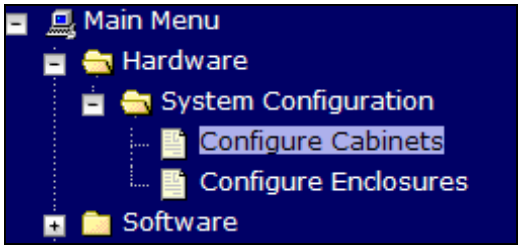
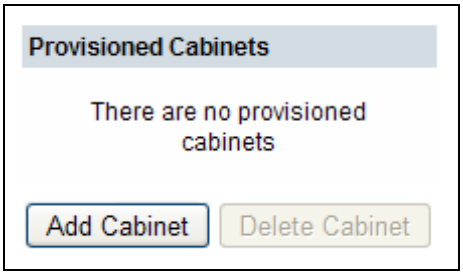
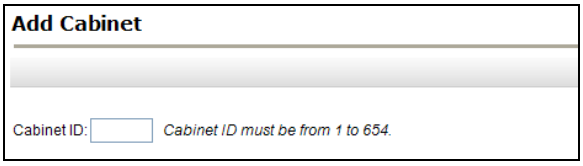
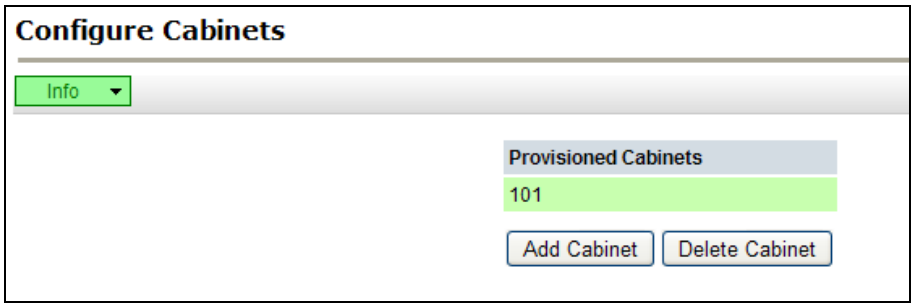
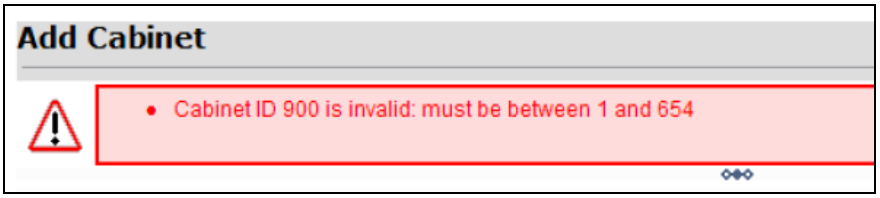
- The cabinet ID (cabinet_id), a number from 1 to 654.
- The Location ID (location_id), a number from 1 to 4, used to uniquely identify the enclosure within the cabinet. The cabinet ID and location ID are combined to create a globally unique ID for the enclosure (for example, an enclosure in cabinet 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.

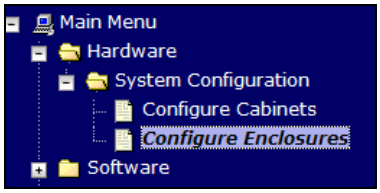
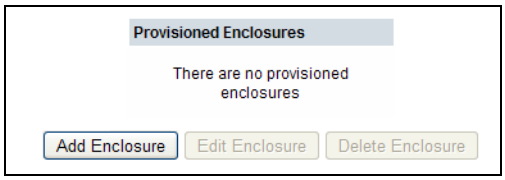
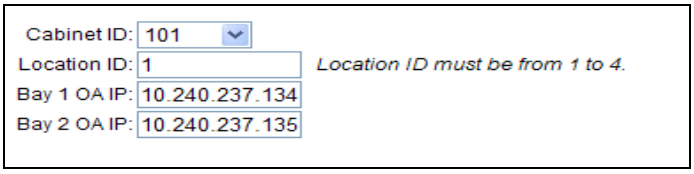
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

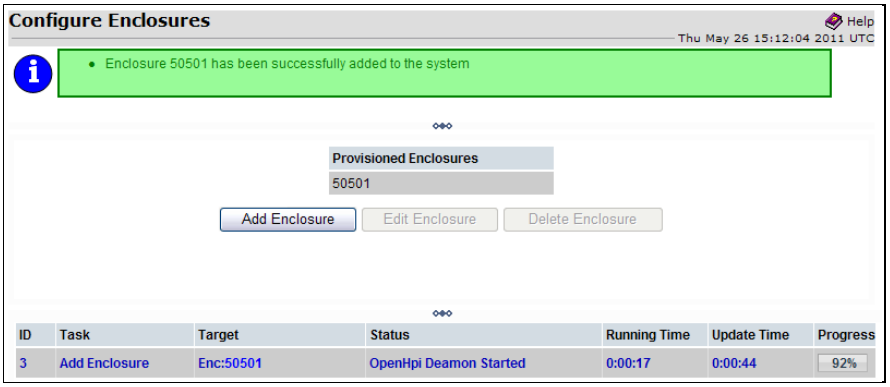
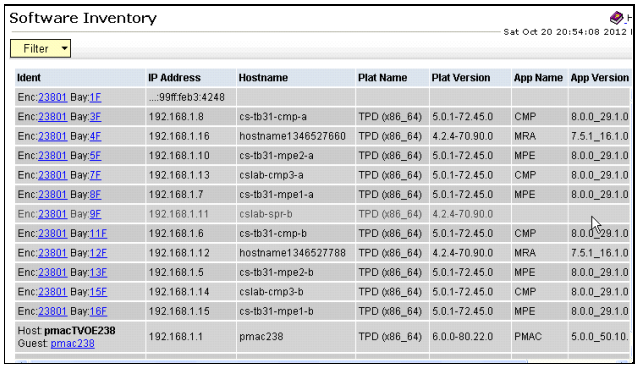
If this procedure fails, contact ORACLE TECHNICAL Services and ask for ASSISTANCE.

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 no error is reported, you see the following:  Or you see an 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 Provisioned Enclosures dialog, click **Add Enclosure**. 
8. ☐	**PM&C GUI:** Add Enclosure	1. On the Add Enclosure dialog, enter: - Cabinet ID - Location ID - Two OA IP addresses (the s active and standby OA for the enclosure).  2. Click **Add Enclosure**.  **NOTES:** • Location ID is used to uniquely identify the enclosure within 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 in location number 1.

Step	Procedure	Details
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%. 
10. ☐	**PM&C GUI:** Background Task monitoring	This page enables you to monitor status updates:  **NOTE:** DO NOT click the ⊠ (delete icon), this deletes the selected task from the *Background Task Monitoring* status.
11. ☐	**PM&C GUI:** Wait until the Add Enclosure task finishes	The color of the progress bar changes to green when complete:  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 properly configured, the blades have TPD installed (at minimum), and the enclosure switches have a control network configured. The Software Inventory form displays the blade server information. Example below:  **NOTE:** The procedure to configure the Enclosure switches, if they have not been previously configured, is yet to be performed.
---END OF PROCEDURE---		

5.3.4 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:

5. On the PM&C server, in the `/usr/TKLC/smac/html` directory, create the following subdirectory: `/ilo_passwd`.
6. Set the directory permissions to an appropriate level. For example:

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

7. 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
```

8. Copy the file to the following directory:

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

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

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

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

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

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

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

After the command finishes, verify that no errors 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
```

5.3.5 Configuring c-Class Aggregation and Enclosure Switches Using netConfig

The c-Class environment includes paired aggregation switches and enclosure switches. You should prepare and verify network configuration files (used to configure the switches) in advance.

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 Gbps copper uplink)
  - 6120XG_LAG_Uplink_configure.xml (for connections using a bundle of four 1 Gbps 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 Gbps copper uplink)
  - 6125XLG_LAG_Uplink_configure.xml (for connections using a bundle of four 1 Gbps 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 Tekelec Platform 7.0.x, Configuration Guide.

Tips: 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.

5.3.6 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.

5.3.7 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 2.2.9 and HP Solutions Firmware Upgrade Pack, Software Centric Release Notes, Release 2.2.10.

5.3.8 Confirming and Updating Application Blade BIOS Settings

You must 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 (use the root account instead of the administrator account)
- You are not required to reset the date and time

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).

5.3.9 Loading Policy Management Software Images onto the PM&C

Prerequistes:

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

See Section 4.1:Software Requirements.

The procedure for loading software images onto the PM&C server is described in the Tekelec Platform 7.0.x, Configuration Guide Section 3.7.9, IPM Enclosure Blades Using the PM&C Application.

5.3.10 IPM Enclosure Blades Using the PM&C

This procedure provides the steps to install TPD on Blade servers from PM&C.

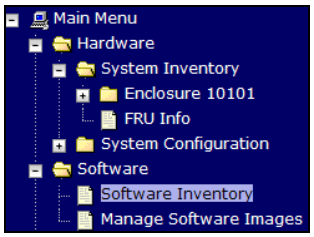
Prerequisites

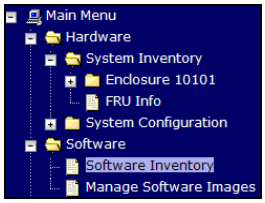
- Enclosures containing the blade servers targeted for IPM that have been configured.
- Appropriate version of TPD is previously added to the PM&C Software Image management.

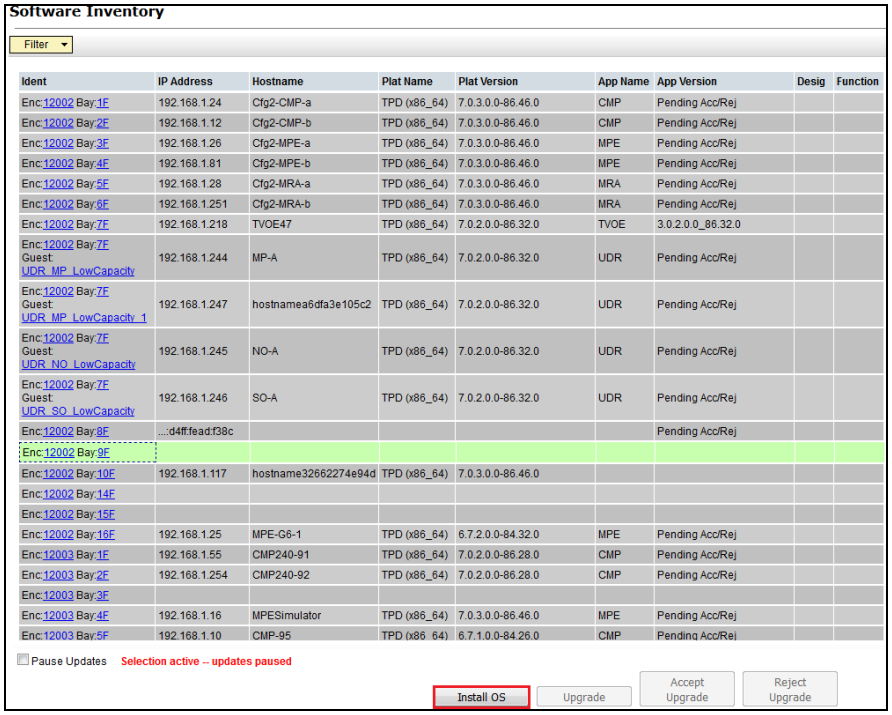
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, contact ORACLE TECHNICAL Services and ask for ASSISTANCE.

5.3.10: IPM Enclosure Blades Using the PM&C

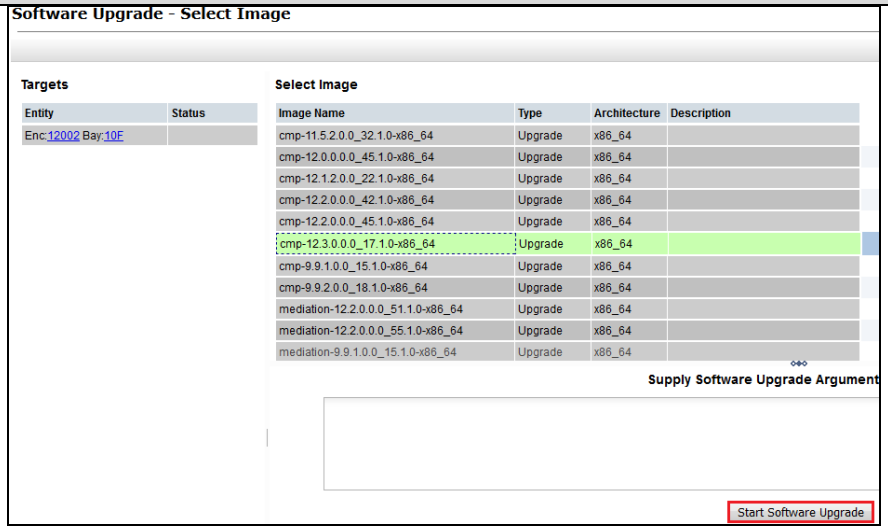
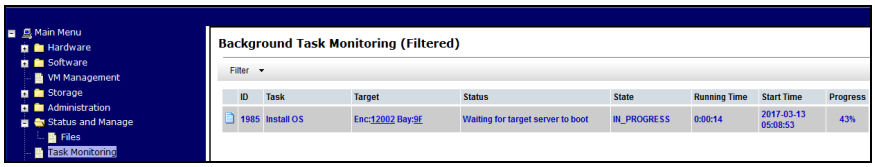
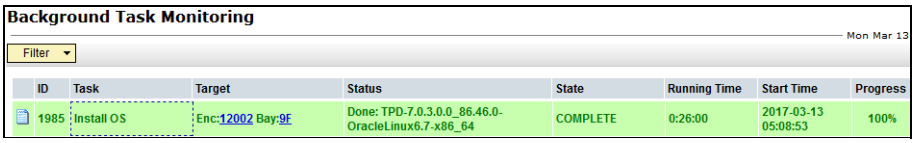
Step	Procedure	Details
1. ☐	**PM&C GUI:** Verify if PM&C Contol Network is established to the blades.	Navigate to **Software → Software Inventory**.  Ident / IP Address Enc:50301 Bay:1F — 192.168.1.6 Enc:50301 Bay:2F — 192.168.1.12 Enc:50301 Bay:3F — 192.168.1.8 Enc:50301 Bay:8F — 192.168.1.5 Enc:50301 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 and enclosures. PM&C always takes the address of 192.168.1.1. If the server has requested an IP address from PM&C, the IP address displays in the IP Address column. TPD always does this when a server blade is booted, and also periodically after this point. If there are no 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 has been previously installed.

<table>
<tr><th>Step</th><th>Procedure</th><th>Details</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>Enc:801 Bay:6F</td><td>192.168.1.21</td><td>hostnameb9d92a84cefe</td><td>TPD (x86_64)</td><td>7.0.2.0.0-86.28.0</td></tr>
<tr><td>Enc:801 Bay:8F</td><td>192.168.1.16</td><td>hostname6de5d09f047e</td><td>TPD (x86_64)</td><td>7.0.2.0.0-86.28.0</td></tr>
</table>
Preceed to the next step to IPM (install the OS) on the selected blade.
</td></tr>
<tr><td>2. ☐</td><td>PM&C GUI:
Initiate OS Install</td><td>
1. Navigate to Software → Software Inventory.


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 can select multiple servers by clicking multiple rows individually. Selected rows are highlighted in green.


NOTE: IPM is a useful recovery procedure for a server is in a bad or unknown condition, or was configured with a different application because the IPM removes all the existing software and disk configurations from the server, and brings the server to a clean state.

After selecting Install OS the Software Install –Select Image page displays:
</td></tr>
</table>

Step	Procedure	Details
		 Any bootable images in the PM&C repository are present. Select the correct bootable image to proceed with the OS installation of the selected blade and click **Software Start Install**.
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 is listed for each blade affected.  When the installation is complete, the task changes to green and the Progress bar indicates 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---		

5.3.11 Install Policy Management Software on Blades using PM&C

Use this procedure to install 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. This can be a source of confusion.

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:

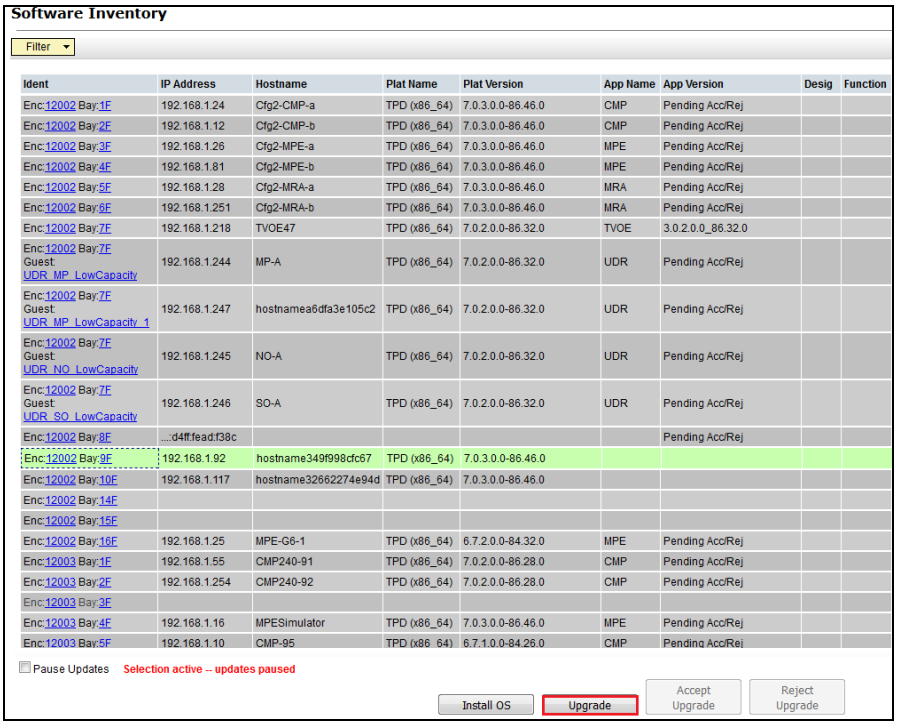
- The appropriate release and Policy Management Application iso image(s) of the Policy Management software stored on the PM&C server.
- Layout diagram for c-Class enclosure(s), identifying which bays run which Policy Management application.

Check off (√) each step as it is completed. Boxes have been provided for this purpose under 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. 

Step	Procedure	Details
2. ☐	**PM&C GUI:** Select Servers for Application install	1. Navigate to **Software → Software Inventory**.  2. Select the servers to install the application. If you want to install the same application image to more than one server, you can select multiple servers. Selected rows are highlighted in green. **NOTE:** After the TPD OS has been installed, the system assigns a given hostname. **NOTE:** 8 is the maximum number that can be selected at one time. 3. Click **Upgrade.**

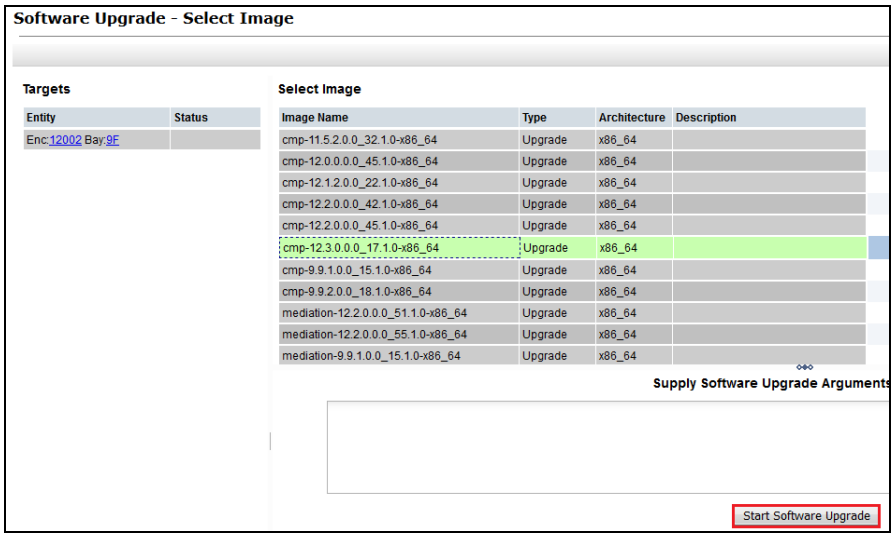
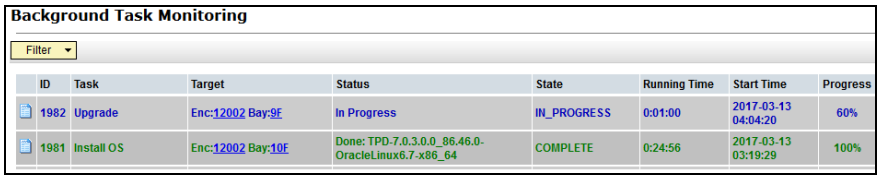
Software Inventory

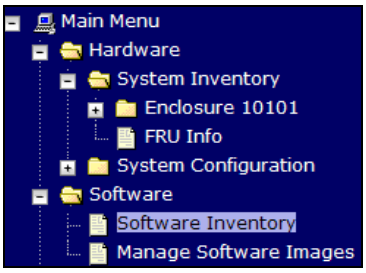
Filter

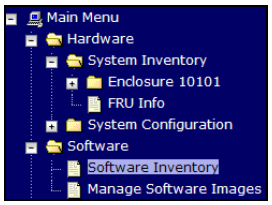
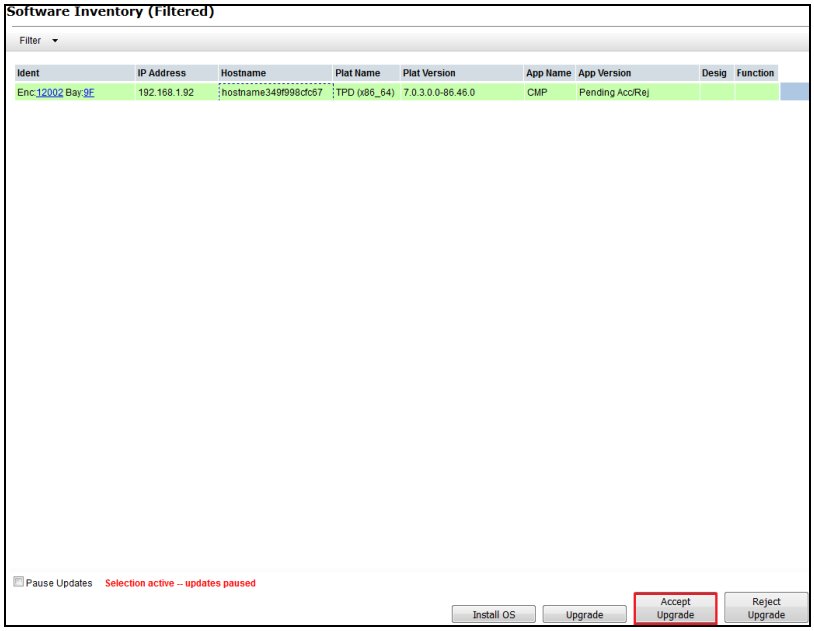
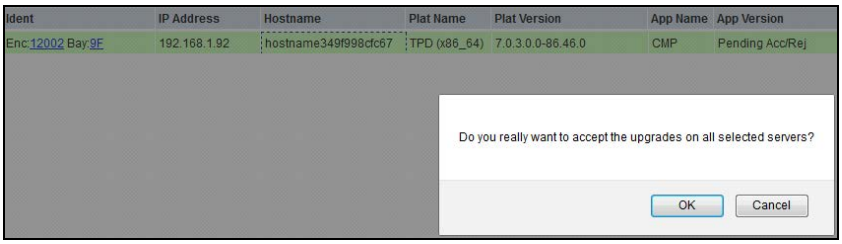
Ident	IP Address	Hostname	Plat Name	Plat Version	App Name	App Version	Desig	Function
Enc:12002 Bay:1F	192.168.1.24	Cfg2-CMP-a	TPD (x86_64)	7.0.3.0.0-86.46.0	CMP	Pending Acc/Rej		
Enc:12002 Bay:2F	192.168.1.12	Cfg2-CMP-b	TPD (x86_64)	7.0.3.0.0-86.46.0	CMP	Pending Acc/Rej		
Enc:12002 Bay:3F	192.168.1.26	Cfg2-MPE-a	TPD (x86_64)	7.0.3.0.0-86.46.0	MPE	Pending Acc/Rej		
Enc:12002 Bay:4F	192.168.1.81	Cfg2-MPE-b	TPD (x86_64)	7.0.3.0.0-86.46.0	MPE	Pending Acc/Rej		
Enc:12002 Bay:5F	192.168.1.28	Cfg2-MRA-a	TPD (x86_64)	7.0.3.0.0-86.46.0	MRA	Pending Acc/Rej		
Enc:12002 Bay:6F	192.168.1.251	Cfg2-MRA-b	TPD (x86_64)	7.0.3.0.0-86.46.0	MRA	Pending Acc/Rej		
Enc:12002 Bay:7F	192.168.1.218	TVOE47	TPD (x86_64)	7.0.2.0.0-86.32.0	TVOE	3.0.2.0.0_86.32.0		
Enc:12002 Bay:7F Guest: UDR_MP_LowCapacity	192.168.1.244	MP-A	TPD (x86_64)	7.0.2.0.0-86.32.0	UDR	Pending Acc/Rej		
Enc:12002 Bay:7F Guest: UDR_MP_LowCapacity_1	192.168.1.247	hostnamea6dfa3e105c2	TPD (x86_64)	7.0.2.0.0-86.32.0	UDR	Pending Acc/Rej		
Enc:12002 Bay:7F Guest: UDR_NO_LowCapacity	192.168.1.245	NO-A	TPD (x86_64)	7.0.2.0.0-86.32.0	UDR	Pending Acc/Rej		
Enc:12002 Bay:7F Guest: UDR_SO_LowCapacity	192.168.1.246	SO-A	TPD (x86_64)	7.0.2.0.0-86.32.0	UDR	Pending Acc/Rej		
Enc:12002 Bay:8F	...:d4ff:fead:f38c					Pending Acc/Rej		
Enc:12002 Bay:9F	192.168.1.92	hostname349f998cfc67	TPD (x86_64)	7.0.3.0.0-86.46.0				
Enc:12002 Bay:10F	192.168.1.117	hostname32662274e94d	TPD (x86_64)	7.0.3.0.0-86.46.0				
Enc:12002 Bay:14F								
Enc:12002 Bay:15F								
Enc:12002 Bay:16F	192.168.1.25	MPE-G6-1	TPD (x86_64)	6.7.2.0.0-84.32.0	MPE	Pending Acc/Rej		
Enc:12003 Bay:1F	192.168.1.55	CMP240-91	TPD (x86_64)	7.0.2.0.0-86.28.0	CMP	Pending Acc/Rej		
Enc:12003 Bay:2F	192.168.1.254	CMP240-92	TPD (x86_64)	7.0.2.0.0-86.28.0	CMP	Pending Acc/Rej		
Enc:12003 Bay:3F								
Enc:12003 Bay:4F	192.168.1.16	MPESimulator	TPD (x86_64)	7.0.3.0.0-86.46.0	MPE	Pending Acc/Rej		
Enc:12003 Bay:5F	192.168.1.10	CMP-95	TPD (x86_64)	6.7.1.0.0-84.26.0	CMP	Pending Acc/Rej		

Pause Updates Selection active -- updates paused

Install OS Upgrade Accept Upgrade Reject Upgrade

Step	Procedure	Details
3. ☐	**PM&C GUI:** Initiate Application Install	The Software—Upgrade Page opens. The left side of this page lists the servers where the Application Software is applied. 1. From the list of available images, select the correct version and application software package (CMP/MRA/MPE/Mediation) 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 is listed for each blade affected.  When the installation is complete, the task changes to green and the Progress bar indicates 100%. 
5. ☐	REPEAT for each Application	Repeat steps 3 and 4 for each application being installed at the site.

Step	Procedure	Details
6. ☐	Verify Application installations- Accept Upgrade	1. Navigate to **Software → Software Inventory**.  At this point, all the target servers have had their correct applications newly installed and the AppVersion appears as Pending Acc/Rej. **Software Inventory (Filtered)** Filter Ident: Enc:12002 Bay:9F IP Address: 192.168.1.92 Hostname: hostname349f998cfc67 Plat Name: TPD (x86_64) Plat Version: 7.0.3.0.0-86.46.0 App Name: CMP App Version: Pending Acc/Rej - Verify the App Name shows the correct name (CMP/MPE/MRA/Mediation) for each server where the Applications are installed. - Confirm the correct Enclosure and Bay position. - Confirm all assignments are per the design. 2. Select the servers to Accept Upgrade. The **Accept Upgrade** is available to click. Confirm the Upgrade.

Step	Procedure	Details
7. ☐	Verify Application installations- Accept Upgrade	1. Navigate to **Software → Software Inventory**.  At this point, all the target servers have had their correct applications installed and the AppVersion shows as Pending Acc/Rej. **Software Inventory (Filtered)** Filter Ident: Enc:12002 Bay:9F; IP Address: 192.168.1.92; Hostname: hostname349f998cfc67; Plat Name: TPD (x86_64); Plat Version: 7.0.3.0.0-86.46.0; App Name: CMP; App Version: Pending Acc/Rej - Verify the App Name shows the correct name (CMP/MPE/MRA) for each server where the Applications are installed. - Confirm the correct Enclosure and Bay position. - Confirm all assignments are per the design. 2. Select the servers to upgrade. 3. Click **Accept Upgrade**. Confirm the upgrade.  4. Click **OK** to confirm the upgrade. 

Step	Procedure	Details
8. ☐	Verify Application Installations	Navigate to **Software → Software Inventory**. **Software Inventory (Filtered)** Filter Ident: Enc:12002 Bay:9F; IP Address: 192.168.1.92; Hostname: hostname349f998cfc67; Plat Name: TPD (x86_64); Plat Version: 7.0.3.0.0-86.46.0; App Name: CMP; App Version: 12.3.0.0.0_17.1.0 You can confirm that the App Version column no longer displays the Pending Acc/Rej status but rather shows the correct Application Version.
---END OF PROCEDURE---		

6. CONFIGURE POLICY MANAGEMENT APPLICATION SERVERS IN WIRELESS MODE

The following procedures configure the Policy Management Application and establish the network relationships, to a level that would allow 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 have been completed prior to 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

See the 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 procedure on every server in the Policy Management network.

Prerequisites

To complete this procedure, you need the following information:

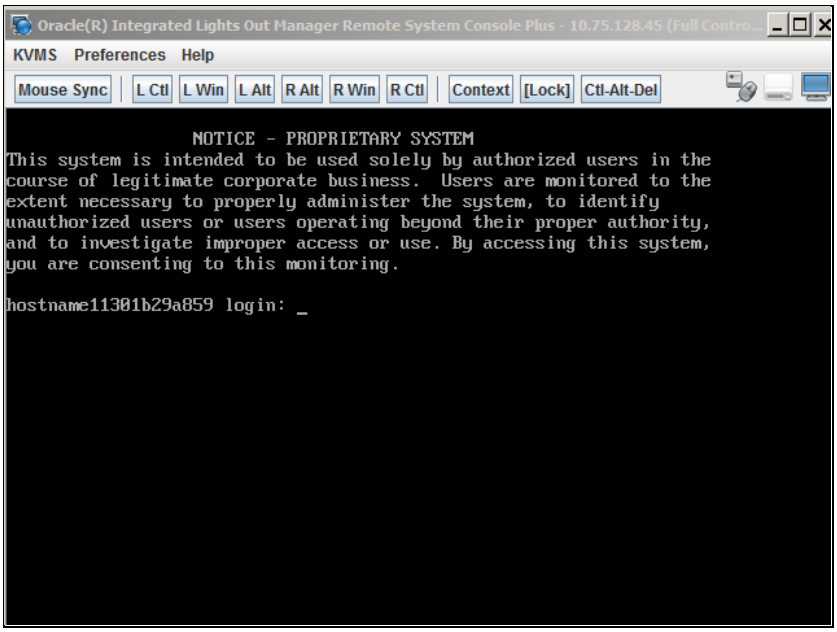
- This procedure assumes that you are using Policy Management in a Wireless or Wireless-C (Wireless with Mediation).
- Know whether or not the server has an optional Ethernet Mezzanine card installed.
- Hostname—The unique hostname for the device being configured.
- OAM Real IP IPv4 Address—The IP address that is permanently assigned to this device.
- OAM Default IPv4 Route—The default route of the OAM network. The MPE and MRA system can 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 Server(s)—A reachable NTP server(s) (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.

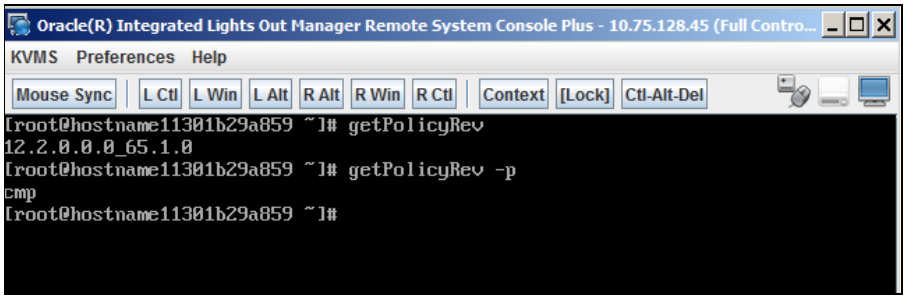
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

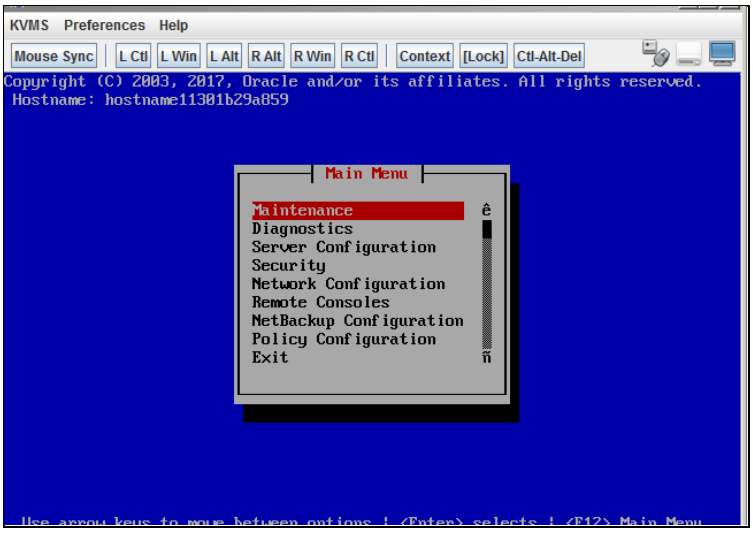
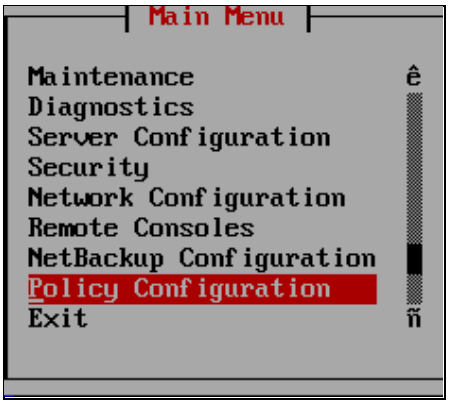
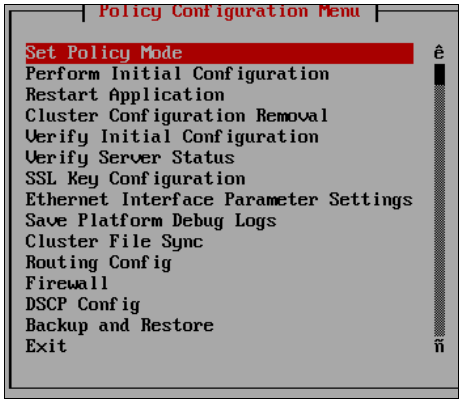
If this procedure fails, contact ORACLE TECHNICAL Services and ask for ASSISTANCE.

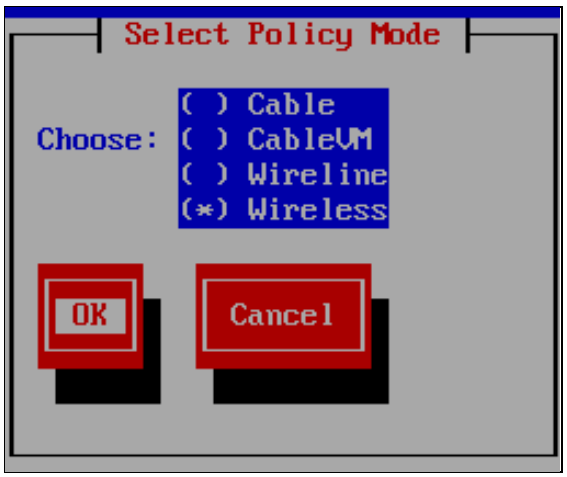
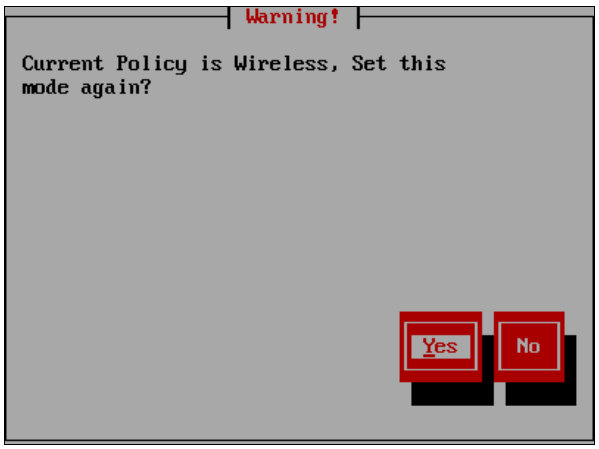
6.1: Perform Initial Server Configuration of Policy Servers—platcfg

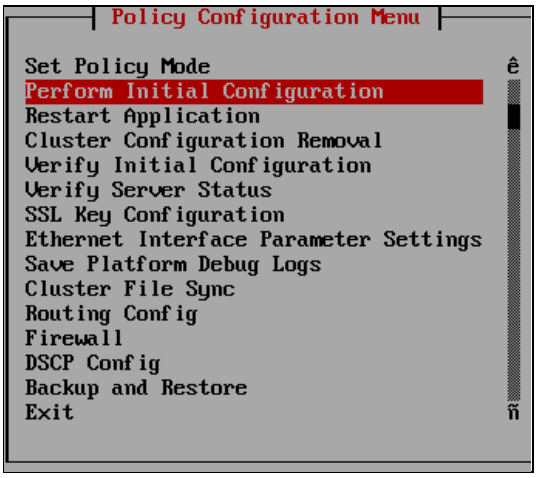
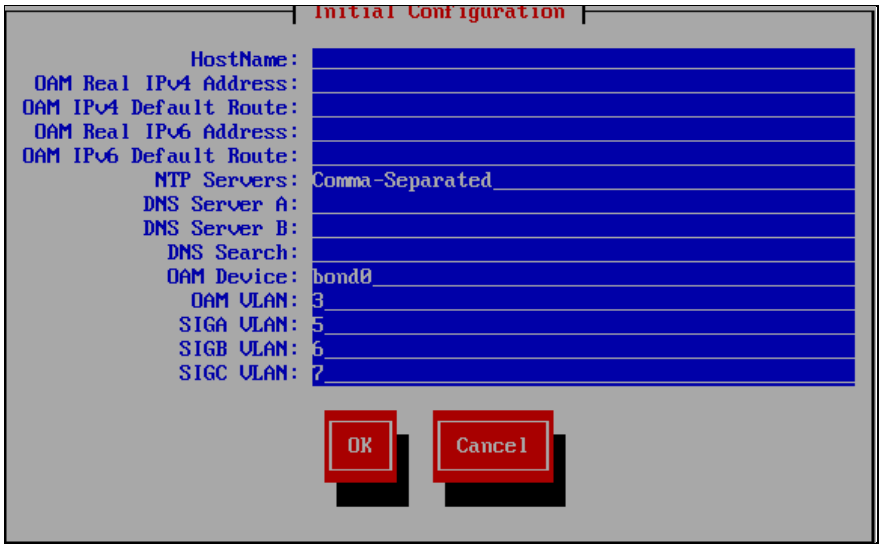
Step	Procedure	Details
1. ☐	Login to server as root via Console	Access the iLO GUI, and open a Remote Console session then login as root **NOTE:** iLO procedures can be found in section 7:Accessing the iLO VGA Redirection Window 

Step	Procedure	Details

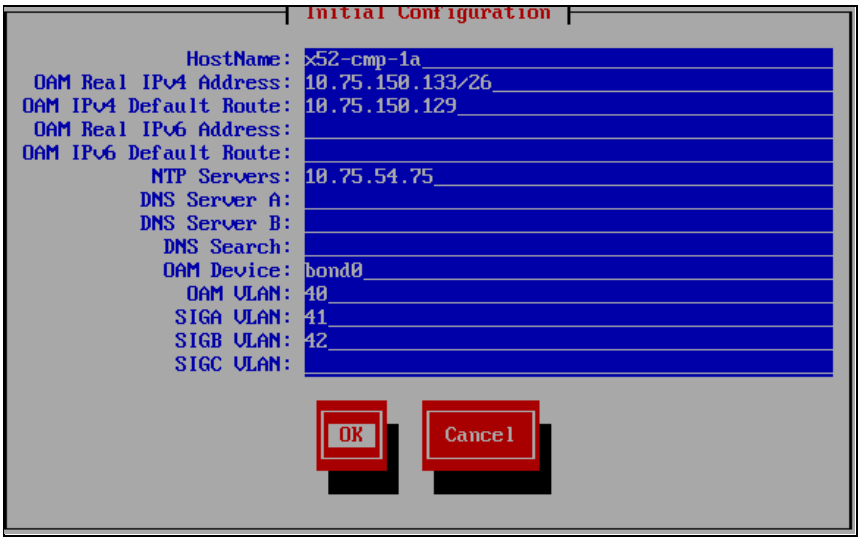
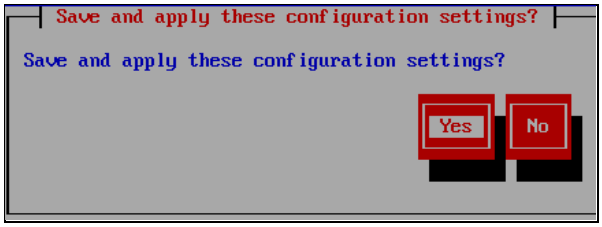
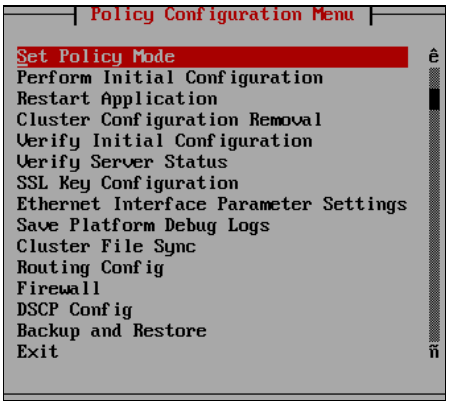
2. ☐	**Remote Console:** Verify the type of server	Login as root, via the Remote Console, and confirm the installed Policy Management software version and server profile
		`# getPolicyRev`
		`# getPolicyRev -p`
		 
		
		The Server Profile is cmp, mpe, mra, or mediation.

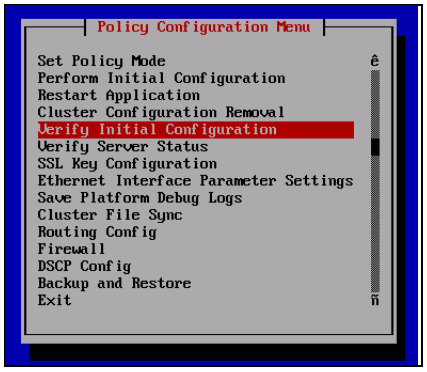
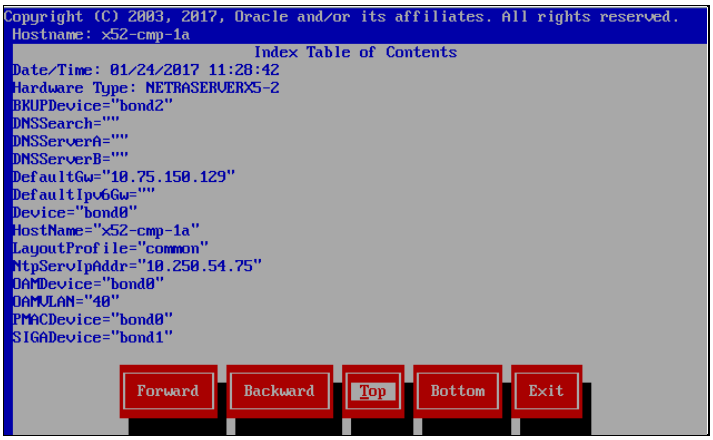
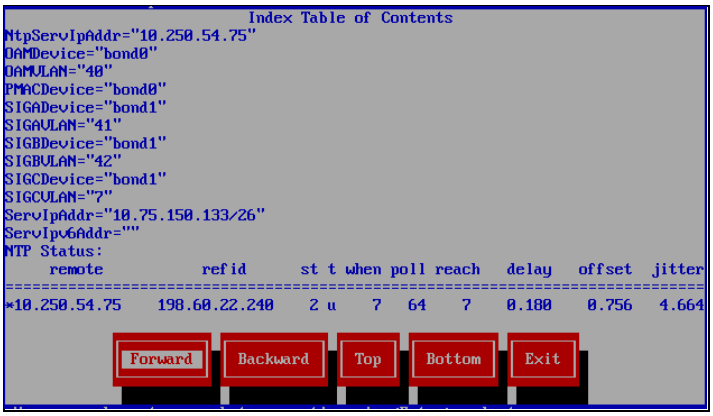
Step	Procedure	Details
3. ☐	**Remote Console:** Login to platcfg	1. Open the platcfg tool by running the following command: `# su - platcfg`  The platcfg tool opens 2. Select **Policy Configuration**.  The *Policy Configuration Menu* opens 

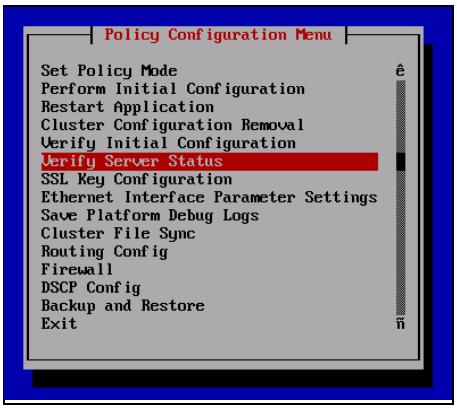
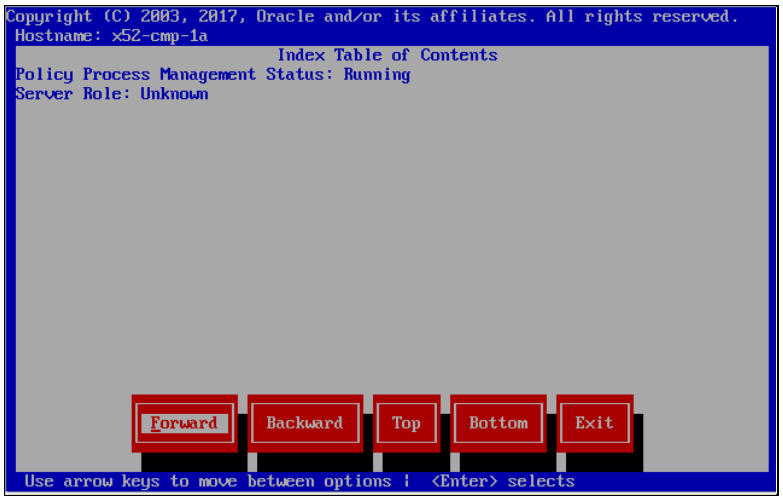
Step	Procedure	Details
4. ☐	**Remote Console**: Set Policy Mode	Set Policy Mode from the Select Policy Mode menu. 1. Select **Wireless Policy** from the options available.  2. Click **OK.** Wireless is the default configuration, if the current Policy Mode is Wireless the warning is not displayed and the Wireless Mode is set. Skip step 3. 3. Click **Yes**.  Depending on the hardware configuration, you may see a Select Network Layout window. See Configuration Management Platform Wireless User's Guide Release 12. (Setting Policy Management Mode) for further detail. If the Select Network Layout window does not open, 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 IP Address**—The IP address that is permanently assigned to this device. • **OAM Real IPv4 Address**—The IPv4 address that is permanently assigned to this device. • **OAM Default Route**—The default route of the OAM network. • **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 should be used, as changing this value is not supported. • •**OAM VLAN**—The OAM network VLAN ID (only applies to c-Class servers or Oracle X5-2 RMS; field does not display otherwise). • **SIG A VLAN** —The Signaling-A network VLAN ID (only applies to c-Class servers or Oracle X5-2 RMS; field does not display otherwise). • **SIG B VLAN** (optional)—The Signaling-B network VLAN ID (only applies to c-Class servers or Oracle X5-2 RMS; field does not display otherwise). • **SIG C VLAN** (optional)—The Signaling-B network VLAN ID (only applies to c-Class servers or Oracle X5-2 RMS; field does not display otherwise). **NOTES:** • All of the fields listed above are required, except for fields DNS Server and DNS Search, which are optional but recommended. • Every network service and IP flow that is supported by IPv4 is supported by IPv6. • Either interface or a combination of the two can be configured.

Step	Procedure	Details
7. ☐	**Remote Console:** Perform Initial Configuration	**For example:**  Click **OK** to save and apply the configuration. At this point the screen pauses for approximately a minute. This is normal behavior. 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 within the platcfg utility.  A display similar to the following is shown.  **NOTE:** The NTP status may not have updated. This is normal behavior. You might have to click **Forward** to view the NTP status. 

Step	Procedure	Details
9. ☐	**Remote Console:** Verify Server Status	1. Exit from this page and select **Verify Server Status**.  The server should be in a running state. For example:  **NOTE:** At this point in the installation the Server Role is `Unknown`. Unknown is a valid state during initial configuration because the cluster has not yet been formed. 2. Click Exit until completely 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 make sure the gateway is reachable. Ping the OAM gateway to make sure it is reachable: `Using username "admusr".` `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.`  `Last login: Thu Jan 19 16:49:33 2017` `[admusr@x52-cmp-1a ~]$ ping 10.75.150.129` `PING 10.75.150.129 (10.75.150.129) 56(84) bytes of data.` `64 bytes from 10.75.150.129: icmp_seq=1 ttl=255 time=0.441 ms` `64 bytes from 10.75.150.129: icmp_seq=2 ttl=255 time=0.486 ms` `^C` `--- 10.75.150.129 ping statistics ---` `2 packets transmitted, 2 received, 0% packet loss, time 1459ms` `rtt min/avg/max/mdev = 0.441/0.463/0.486/0.031 ms` `[admusr@x52-cmp-1a ~]$`  If the gateway is reachable it should be 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 no 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.
		
		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`
		`==========`
		`*10.250.54.75  198.60.22.240  2 u  45  64  377  0.173  70.008  17.056`
		`[admusr@x52-cmp-1a ~]$`
		
		The * (asterisk) beside the NTP server IP indicates the NTP server is in sync.
		
		If the sign is not there, you can try to manually sync with the NTP server using the following commands:
		
		`# service ntpd stop`
		`# ntpdate <ntpserver address>`
		
		Bad response:
		
		26 Jun 16:47:25 ntpdate[16364]: no server suitable for synchronization found
		
		Good response:
		
		`[root@Site1-CMP-A ~]#`
		`[root@Site1-CMP-A ~]# service ntpd stop`
		`Shutting down ntpd:  [ OK ]`
		`[root@Site1-CMP-A ~]# ntpdate 10.250.32.10`
		`1 Oct 10:03:11 ntpdate[32563]: 10.250.32.10 rate limit response from server.`
		`1 Oct 10:03:11 ntpdate[32563]: adjust time server 10.250.32.10 offset 0.001129 sec`
		`[root@Site1-CMP-A ~]#`
		`[root@Site1-CMP-A ~]#`
		`[root@Site1-CMP-A ~]#`
		
		`# service ntpd start`
		
		If the **`ntpdate`** utility 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 Management component servers that are planned for service. If the solution is georedundant, this procedure must be performed on site1 and site2 Policy servers.
---END OF PROCEDURE---		

6.2 Perform Initial Configuration of the Policy Servers—CMP GUI

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

NOTE: In a deployment that has Georedundant 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 (Georedundant) 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 bring up a web browser GUI (http)

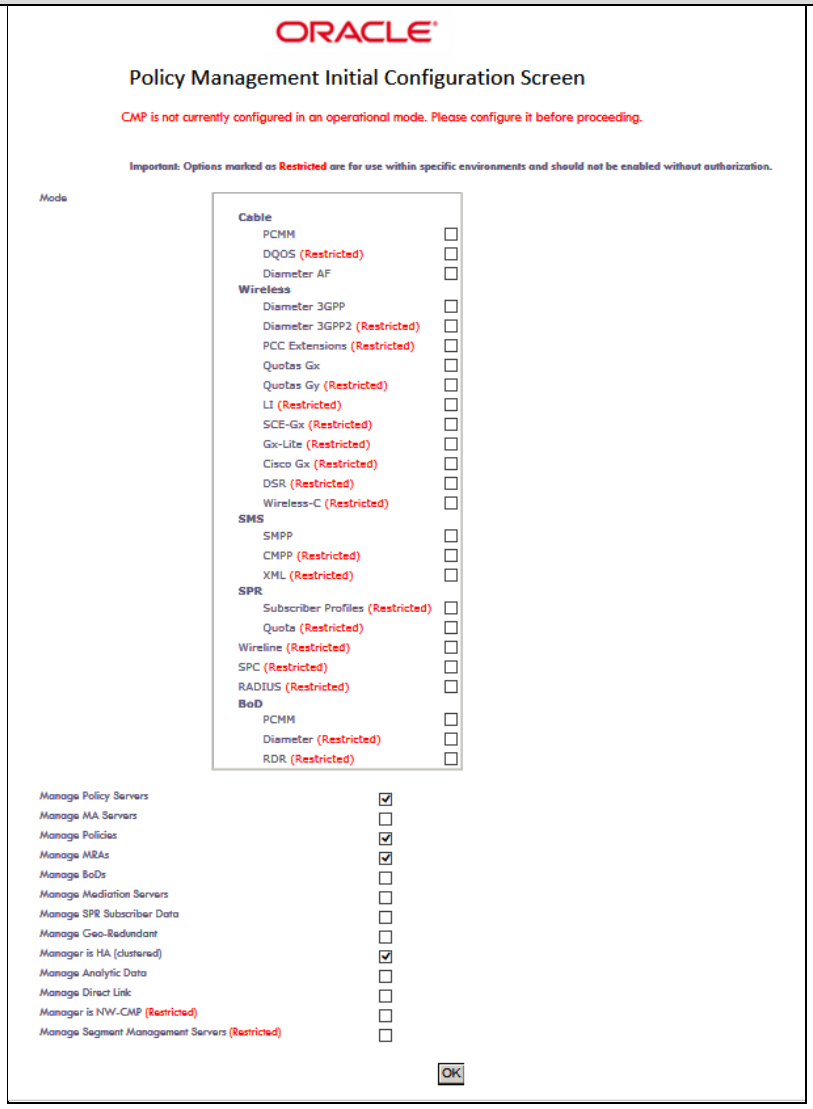
If network access to the CMP is not available and the installation has an Aggregation switch, then a laptop can be configured to use a port on the Aggregation switch to access the CMP GUI. If an Aggregation switch is not available, a temporary switch may be used to provide network access to the CMP GUI.

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, contact ORACLE TECHNICAL Services and ask for ASSISTANCE.

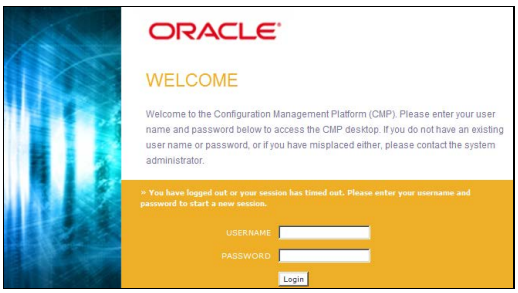
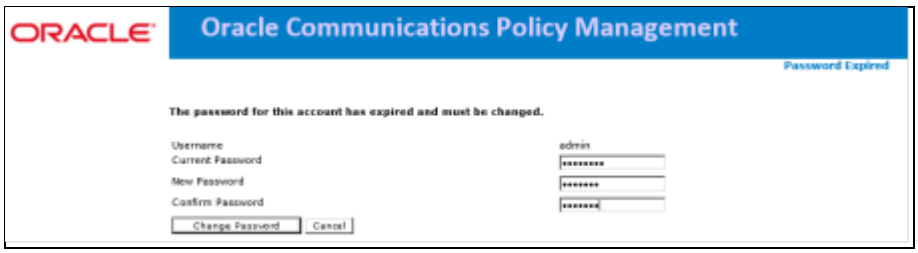
6.2: Perform Initial Configuration of the Policy Servers —CMP GUI

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 can be performed on either CMP that is located at Site1. If this is not a georedundant solution there is not a Site 2 location. If Network access has not been been enabled and the Installation has an Aggregation switch, then a laptop can be 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.
2. ☐	**CMP GUI**: Set CMP Mode in first selected CMP	When you are connect to the CMP GUI for the first time, you are prompted to configure the operation mode settings for the system. The mode defines what functionality is configurable from the CMP GUI. The selection depends on the customer deployment. The *Policy Management Initial Configuration* page opens:

Step	Procedure	Details
		 **NOTE:** Modes can be changed at a later time if needed, but the method to access to this mode selection is not documented. Contact My Oracle Support if the mode must be changed after the initial configuration.
3. ☐	**CMP GUI:** Set CMP Mode in 1st selected CMP	Below is an example of a configuration that provides basic functionality for a Policy 12.3.x Wireless solution. The wireless mode of operation has been confirmed in earlier procedures. (Checkboxes are for example only). For greater detail see the CMP Modes section in the the Configuration Management Platform Wireless User's Guide.

Step	Procedure	Details
		ORACLE Policy Management Initial Configuration Screen CMP is not currently configured in an operational mode. Please configure it before proceeding. Important: Options marked as Restricted are for use within specific environments and should not be enabled without authorization. Mode Cable PCMM ☐ DQOS (Restricted) ☐ Diameter AF ☐ Wireless Diameter 3GPP ☑ Diameter 3GPP2 (Restricted) ☐ PCC Extensions (Restricted) ☐ Quotas Gx ☑ Quotas Gy (Restricted) ☐ LI (Restricted) ☐ SCE-Gx (Restricted) ☐ Gx-Lite (Restricted) ☐ Cisco Gx (Restricted) ☐ DSR (Restricted) ☐ Wireless-C (Restricted) ☐ SMS SMPP ☑ CMPP (Restricted) ☐ XML (Restricted) ☐ SPR Subscriber Profiles (Restricted) ☐ Quota (Restricted) ☐ Wireline (Restricted) ☐ SPC (Restricted) ☐ RADIUS (Restricted) ☐ BoD PCMM ☐ Diameter (Restricted) ☐ RDR (Restricted) ☐ Manage Policy Servers ☑ Manage MA Servers ☐ Manage Policies ☑ Manage MRAs ☑ Manage BoDs ☐ Manage Mediation Servers ☐ Manage SPR Subscriber Data ☐ Manage Geo-Redundant ☐ Manager is HA (clustered) ☑ Manage Analytic Data ☐ Manage Direct Link ☐ Manager is NW-CMP (Restricted) ☐ Manage Segment Management Servers (Restricted) ☐ **NOTE:** Restricted mode options should only be selected with the advice of an Oracle support representative. The following examples are for reference only. The particular requirements for any given customer configuration may be specific that customer. **For a Wireless network:** • Wireless: Diameter 3GPP • Quotas Gx • Manage Policy Servers • Manage Policies • Manage MRAs • Manage Georedundant • Manager is HA (clustered)

Step	Procedure	Details
		For a Wireless-C network: • Wireless: Diameter 3GPP, Quotas Gx, DSR, Wireless-C; SMS: CMPP • Manage Policy Servers • Manage Policies • Manage MRAs • Manage Mediation Servers • Manage SPR Subscriber Data • Manager is HA (clustered) **About using Wireless-C Mode:** Wireless-C: Supports a wireless system supporting a Mediation server; SMS Notification Statistics; and SCTP counters To support a Mediation server, the Policy Management system must be configured for Wireless-C mode and have Manage Mediation Servers enabled. The Mediation server provides the interface between a Subscriber Profile Repository (SPR) server and a business and operation support system (BOSS) client to manage subscriber data. The Mediation server uses SOAP messaging over HTTP or HTTPS protocol to process subscriber profile and service subscription data. **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 performs LI (Lawful Intercept) functions. To use this option the LI version of the MPE ISO image must have been installed on the MPEs in the Policy Management Solution. Contact My 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 and is typically used in customer deployments. **Manager is NW CMP** and **Manager is S-CMP** are specific to a Tiered CMP System deployment. See the 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 customer deployment and should conform with the engineering team responsible for the planned Policy Management Solution deployment.

Step	Procedure	Details
4. ☐	**CMP GUI:** Login to CMP GUI	After configuring the policy mode selection, click **OK.** The login dialog displays. 
5. ☐	**CMP GUI:** Set admin password	1. Login is admin using the password policies. System prompts you to change the admin password.  2. 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 georedundant 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 (georedundant) CMP servers later.

Prerequisites

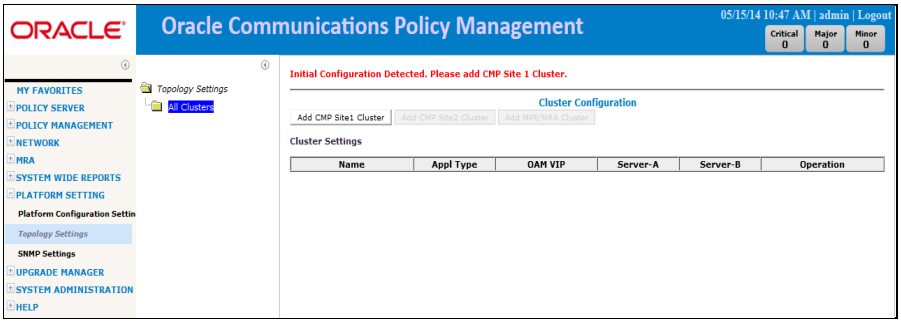
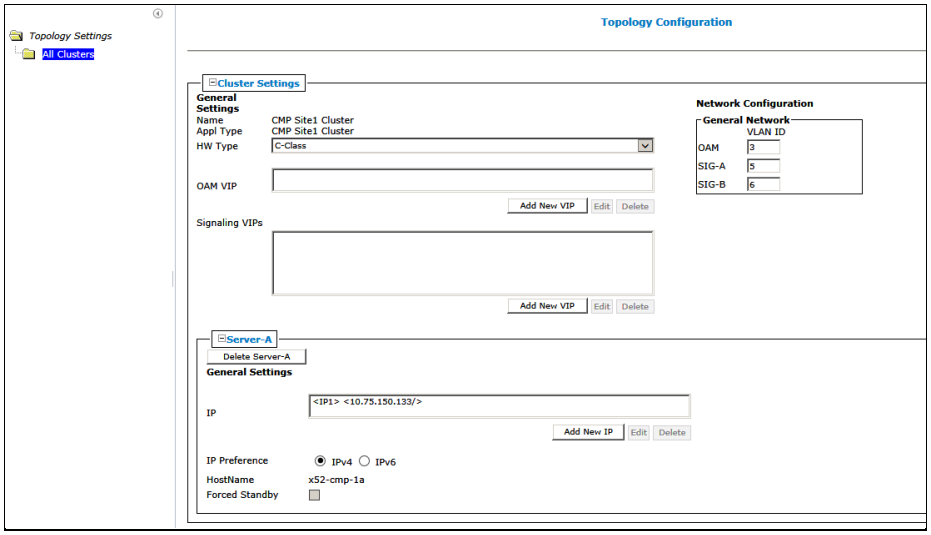
To complete this procedure, you need the following information:

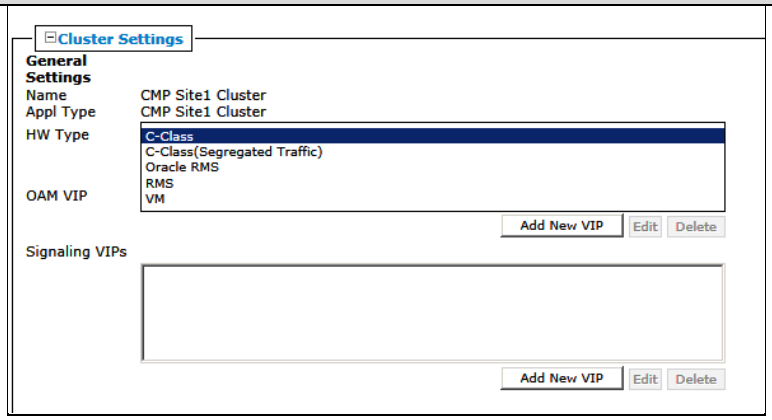
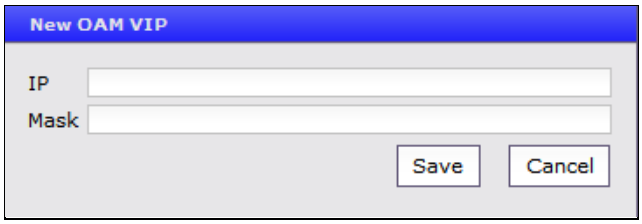
- OAM VIP—IP address and netmask for the cluster VIP address on the OAM network.
- Hostname—The names you choose for each server in the cluster.
- Signaling VIPs (optional)—Up to four IPv4 or IPv6 addresses and netmasks of the signaling VIP addresses. For each, select None, SIG-A, SIG-B, or SIG-C to 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 previously 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 Netra hardware, VLANs are required. For RMS hardware, VLANs are not 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 previously defined.
- Network access to the CMP OAM IP address, to bring up a web browser GUI (http)

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

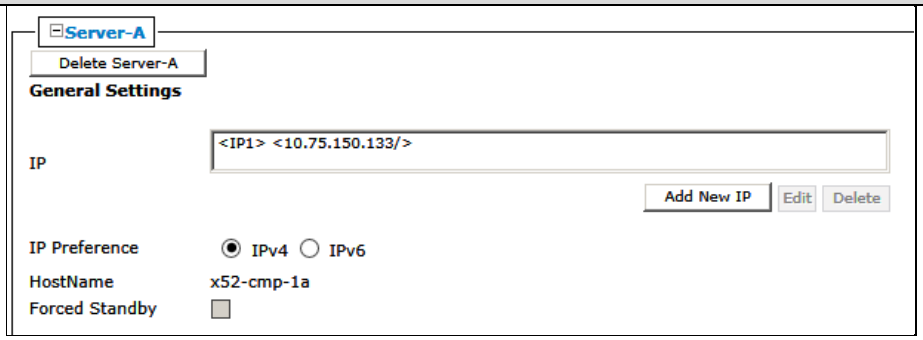
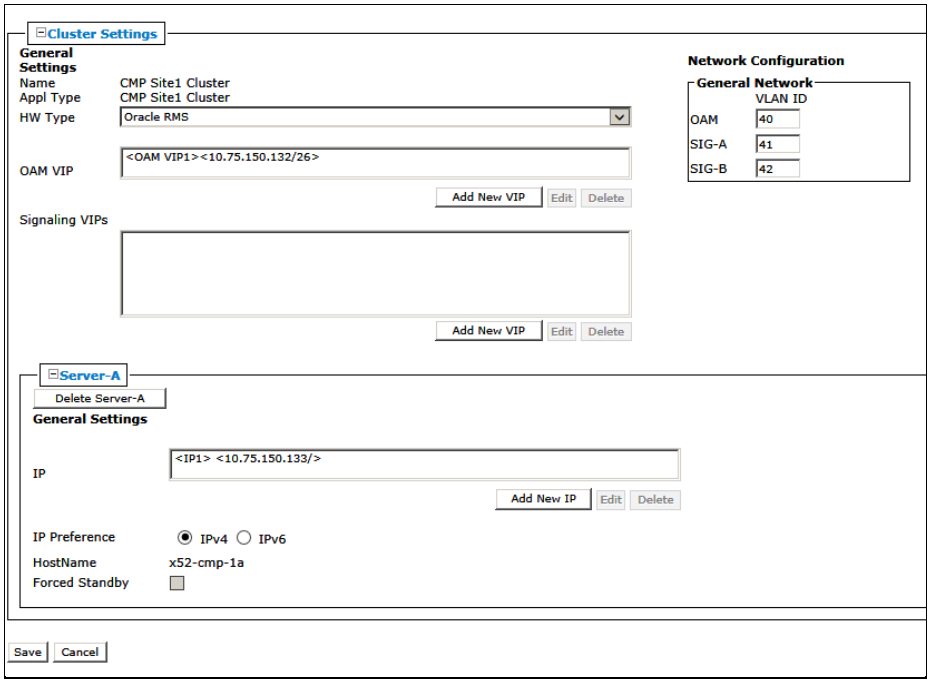
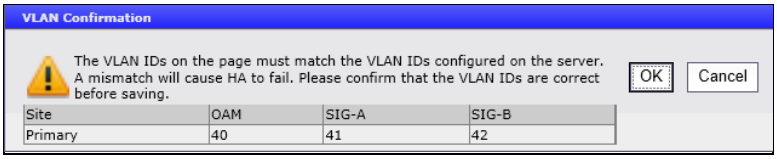
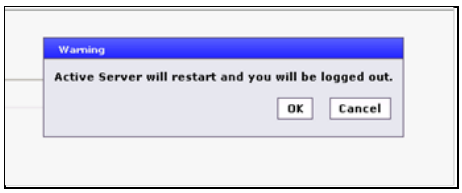
If this procedure fails, contact ORACLE TECHNICAL Services and ask for ASSISTANCE.

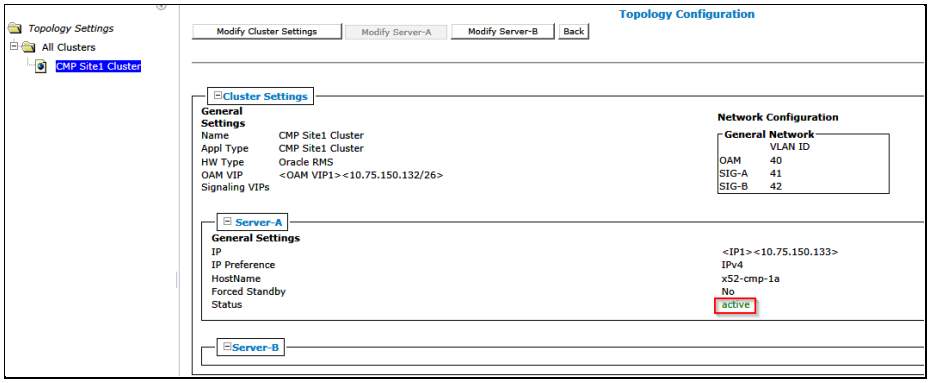
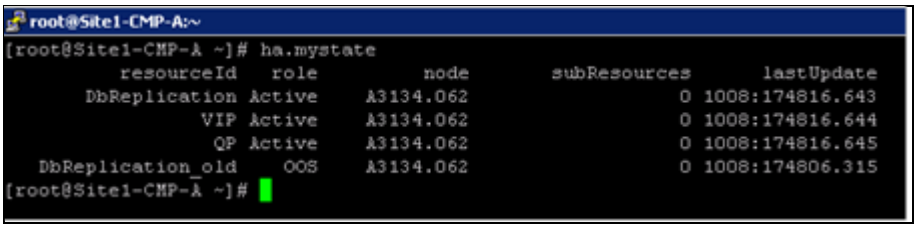
6.3: CMP Site1 Cluster Topology Configuration

Step	Procedure	Details
1. ☐	**CMP GUI**: View Topology Settings	**NOTE:** Only the following web browsers are supported in OCPM 12.3 • Mozilla Firefox® release 31.0 or later • Google Chrome version 40.0 or later Navigate to **Platform Settings → Topology Settings → All Clusters**. The initial form opens, and displays a message that the initial configuration detected and CMP Site 1 cluster should be added. 
2. ☐	**CMP GUI:** Add CMP Site 1 Cluster—Server A	1. Click **Add CMP Site 1 Cluster**. The Topology Configuration form displays.  In this form, the CMP cluster can be given a name, and certain characteristics of the cluster are defined. This form defines the 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.

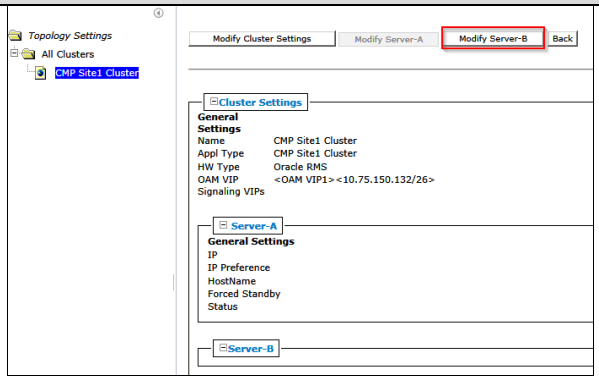
Step	Procedure	Details
		 Available options are: - C-Class (default)—HP Enterprise ProLiant BL460 Gen8 or Gen9 server - C-Class (Segregated Traffic) (a configuration where Signaling and other networks are separated onto physically separate equipment)—HP Enterprise ProLiant BL460 Gen8 or Gen9 server - Oracle RMS (rack-mounted servers using tagged VLANs) - RMS (for a rack-mounted server not using VLANs) - VM (virtual machine) 3. If you selected C-Class, C-Class (Segregated Traffic), or Oracle RMS, enter the General Network—VLAN IDs. 4. Enter the OAM, SIG-A, and (optionally) SIG-B virtual LAN (VLAN) IDs. VLAN IDs are in the range 1–4095. The default values are: - OAM—3 - SIG-A—5 - SIG-B—6 5. Click **Add New VIP**. The New OAM VIP dialog box appears: 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

Step	Procedure	Details
		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 Host Name of Server-A are the IP address and Host Name used during the Initial Configuration of the server from section 6.1, Perform Initial Server Configuration of Policy Servers—platcfg. They 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 have been defined. The CMP loads the hostname from the IP reachable server. This confirms network connectivity and minimizes the possibility of incorrectly defining the Host Name. 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 dialog box 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 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. 10. Enter the HostName of the server. This must exactly match the host name provisioned for this server (the output of the Linux command `uname -n`). **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 indicates 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:**

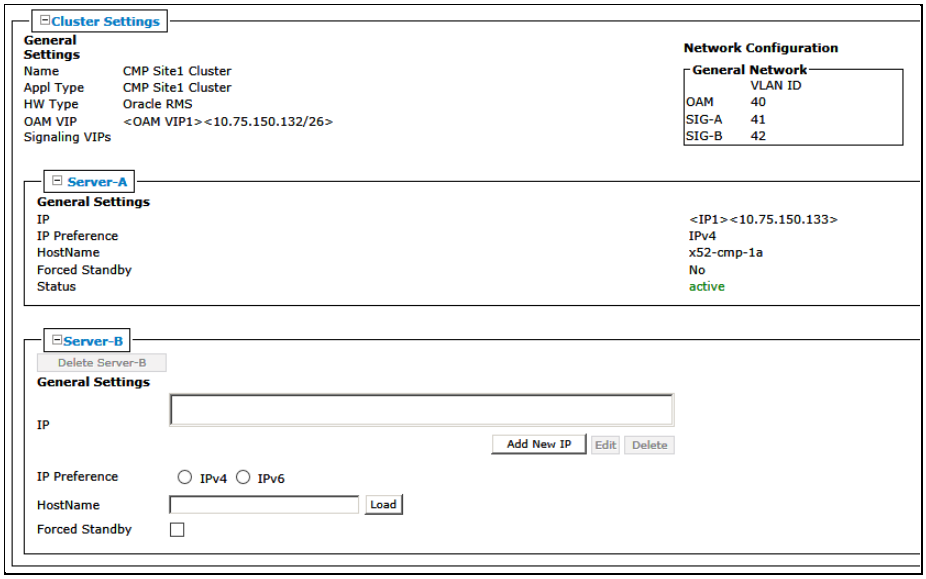
Step	Procedure	Details
		 Topology Configuration of the HW Type Oracle RMS example:  Click **Save** and then click **OK**. If the configuration contains VLAN IDs you will be prompted to confirm the VLAN IDs.  Then the following confirmation prompt appears. Click **OK**.  At this point you are logged out of CMP GUI.

Step	Procedure	Details
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 Active.
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 as shown below. `# ha.mystate`  **NOTE:** DbReplication_old with role OOS is not an indication of a problem and can be ignored. To verify that the Topology Configuration was done correctly, you can login to the CMP server with its real IP address.
5. ☐	**CMP GUI:** Modify CMP Site 1 Cluster—Add Server B	**Modify CMP Site 1 Cluster—Add Server B** 1. Navigate to **Platform Settings → Topology Settings**. 2. Click **View** for CMP Site 1 Cluster. 3. Click **Modify Server B**.

Step	Procedure	Details



The Topology Configuration for Server-B opens.



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 dialog box opens.

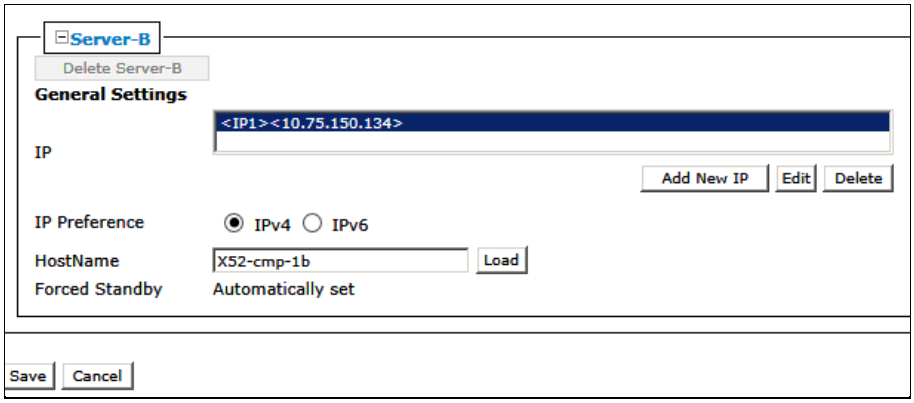
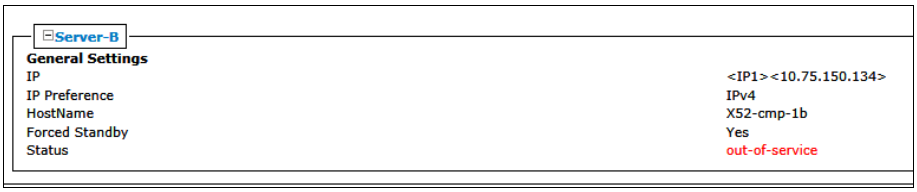
5. Enter the IP address in either IPv4 or IPv6 format.

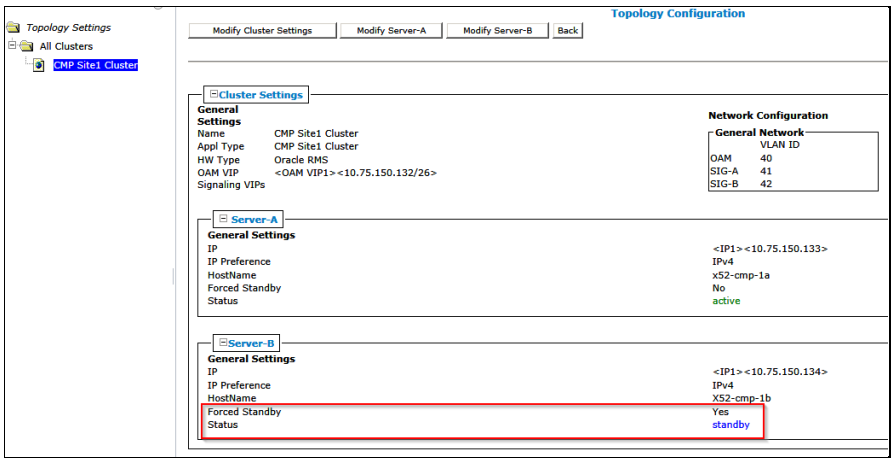
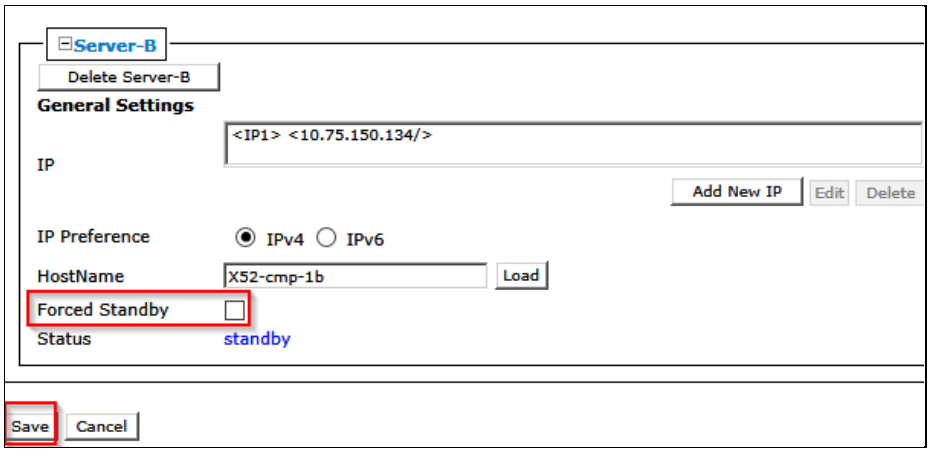
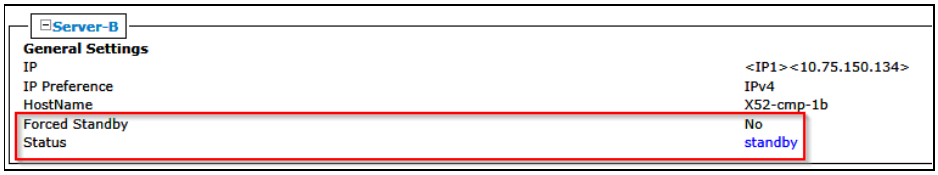
   - This is the IP address of the server. For an IPv4 address, enter it in the standard IP dot-format.
   - For an IPv6 address, enter it in the standard 8-part colon-separated hexadecimal string format.

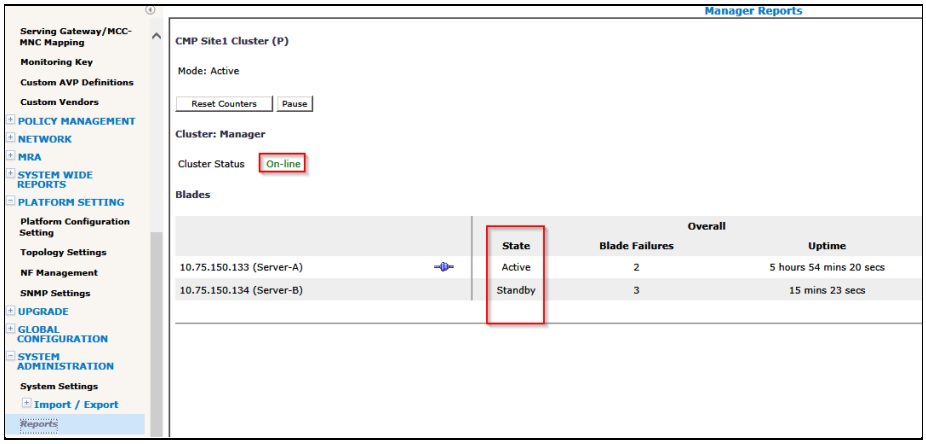
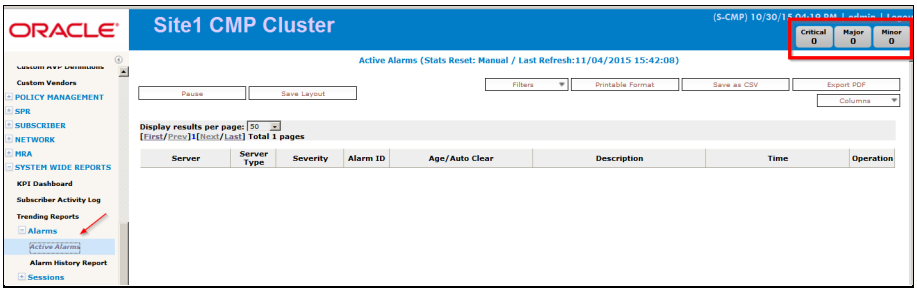
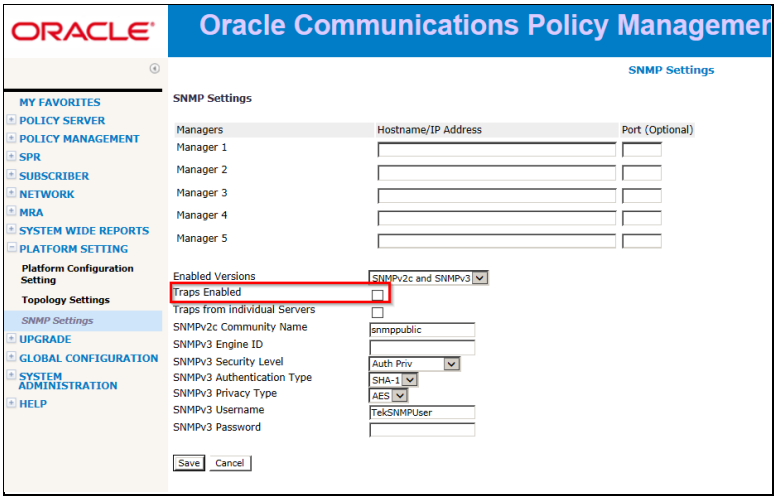
6. Select the IP Preference: IPv4 or IPV6.

   The server 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.

Step	Procedure	Details
		7. Enter the HostName of the server. This must exactly match the host name provisioned for this server (the output of the Linux command **`uname -n`**). **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 indicates 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** then **OK** to confirm the restart.  The server status is out-of-service for a few minutes and that is expected until the cluster forms.  **NOTE:** Wait for any alarms, such as the following, to clear. This takes about 5 minutes 31282 — The HA manager (cmha) is impaired by a s/w fault

Step	Procedure	Details
6. ☐	**CMP GUI:** Verify Server B is added	1. Refresh the CMP GUI. 2. Navigate to **Topology → CMP Site 1 Cluster**.  3. Verify status is: - Forced Standby is yes (automatically set upon entering CMP Server-B information) - Status is standby (after refreshing the page)
7. ☐	**CMP GUI:** Remove Force Standby on Server B	1. Click **Modify Server-B** and clear **Force Standby**. 2. Click **Save** and **OK** for the confirmation message.  3. Verify status becomes: - Forced Standby is no - Status is Standby 

Step	Procedure	Details
8. ☐	**CMP GUI:** Verify CMP cluster	1. Navigate to **SYSTEM ADMINISTRATION → Reports**. 2. Verify both CMP servers are present , with one Activ and the other in Standby status and 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 no active alarms on CMP(s). 
10. ☐	**CMP GUI:** Add SNMP Servers	1. Navigate to **PLATFORM SETTING → SNMP Settings**. 2. Configure the SNMP destination, version, and community string. 3. Click **Save**.  **NOTE:** De-select the checkbox for Traps Enabled until ready to go live.

Step	Procedure	Details
---END OF PROCEDURE---		

6.4 Configuring Additional Clusters

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

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

NOTE: To establish full management relationships, certain IP network services must be 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 raised at the CMP system.

6.4.1 Adding a CMP Site2 Cluster for CMP Georedundancy

This procedure configures a Georedundant 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 for the georedundant CMP relationship to be established. Incorrectly configured firewalls in the network can cause issues. It is highly 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 will form the CMP Site2 Cluster and they must have been configured with network time protocol (NTP), IP routing, and OAM IP addresses. See Section 5:Preparing the System Environment in this document.

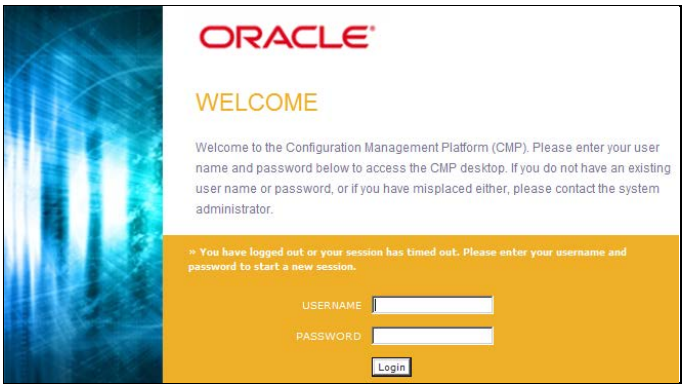
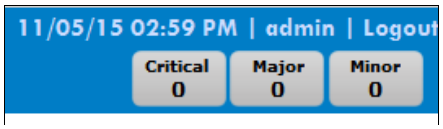
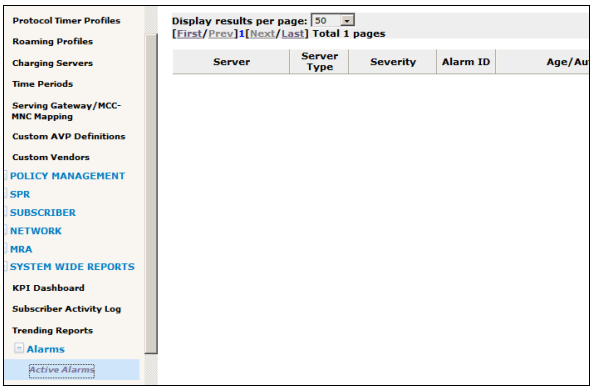
To complete this procedure, you need the following:

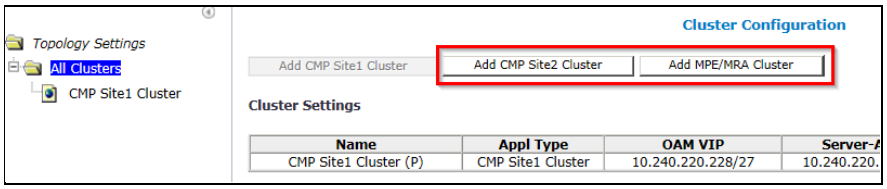
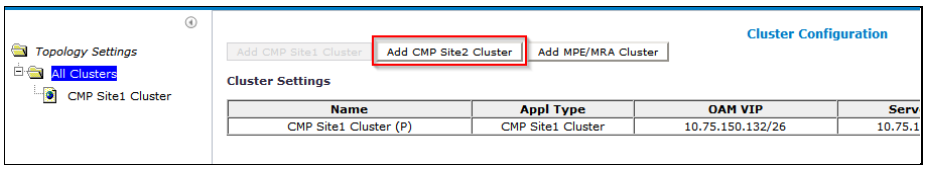
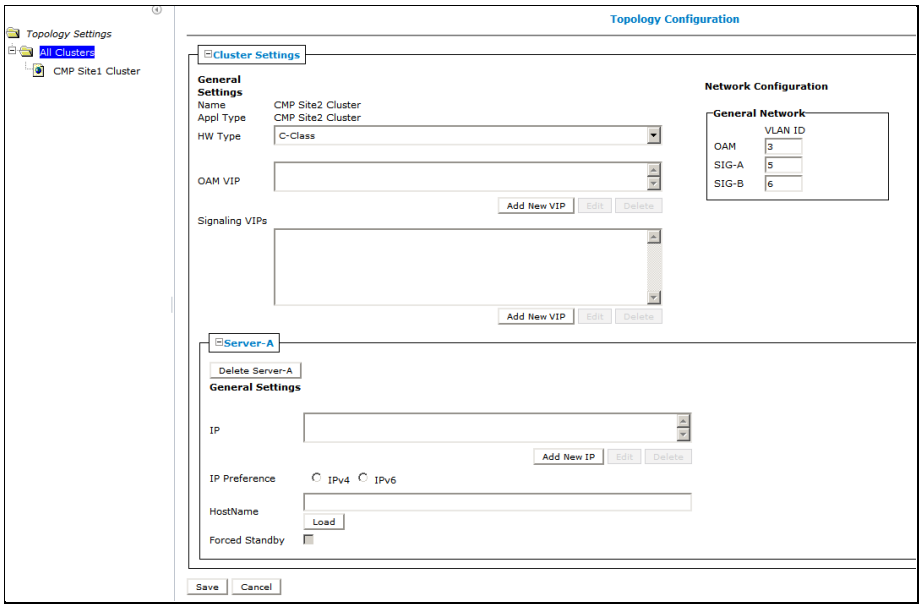
- HW Type—Determines whether VLANs are required. If you select c-Class, c-Class (segregated traffic), or Netra hardware, VLANs are required. For RMS hardware, VLANs are not required.
- OAM VIP—The IP address and netmask the CMP cluster uses to communicate with an MPE or MRA cluster.
- Network VLAN IDs (depends on HW Type)—The values designated during the Initial Configuration done with placfg.
- The information that you previously configured for the CMP Site 1 cluster

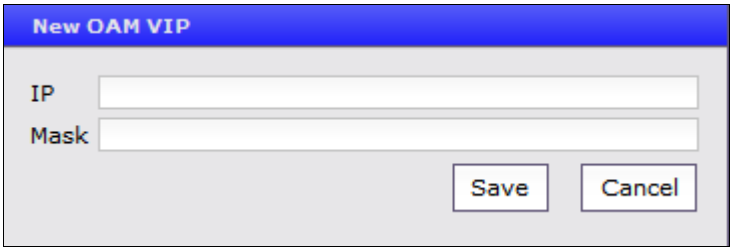
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

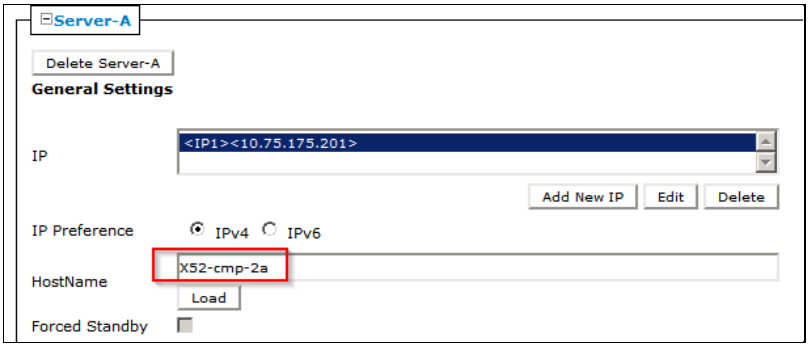
If this procedure fails, contact ORACLE TECHNICAL Services and ask for ASSISTANCE.

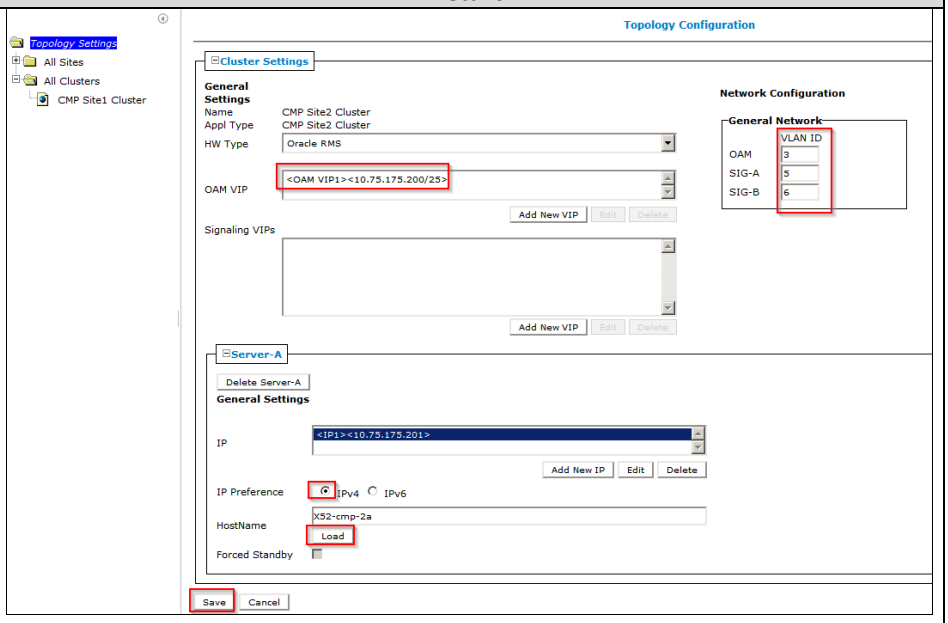
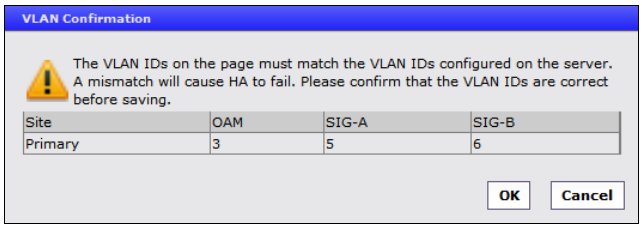
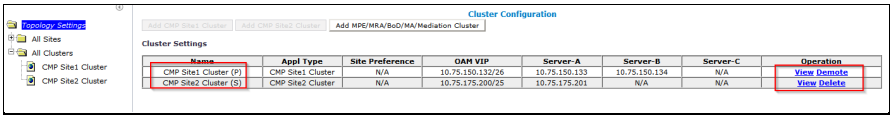
6.4.1: Adding a CMP Site2 Cluster for CMP Georedundancy

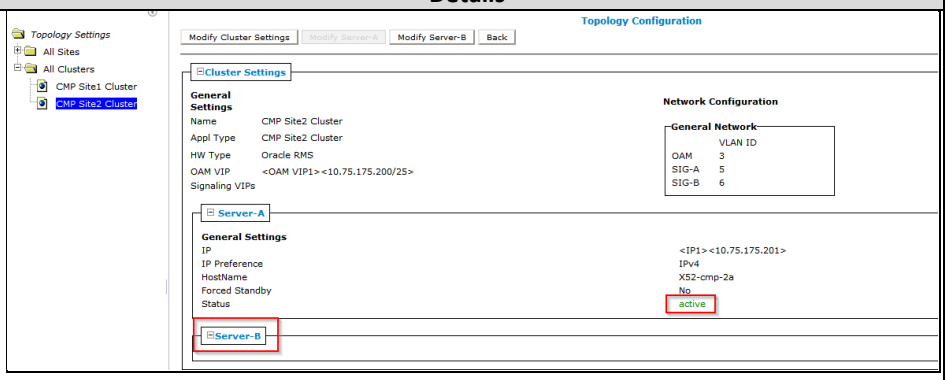
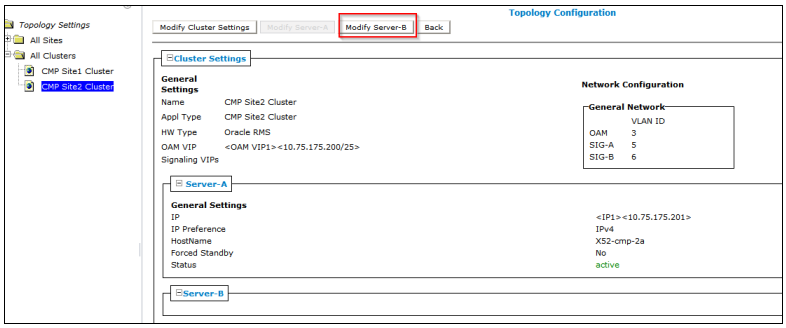
Step	Procedure	Details
1. ☐	**CMP GUI:** Login to CMP Server GUIs (using VIP)	1. From a browser, enter CMP Server VIP in Navigation string. **NOTE:** Only the following web browsers are supported in OCMP 12.3 - Mozilla Firefox® release 31.0 or later - Google Chrome version 40.0 or later  2. Login as admin (or a user with admin privileges).
2. ☐	**CMP GUI**: View Active Alarms	It is recommended to view the active alarms in the system before performing configuration work. Check alarm information and determine if any alarms present may affect configuration activies. • View alarms from CMP GUI upper right banner  • View alarms from **System Wide Reports → Active Alarms**.  ***IMPORTANT: In Policy 12.3.x, there is online help provided for alarm descriptions:*** • Go to **Alarms → Active** alarms, click the alarm ID to open the alarm description help page. • Go to **Help → Online Help**, and select **Troubleshooting Guide**. Search for the alarm ID.

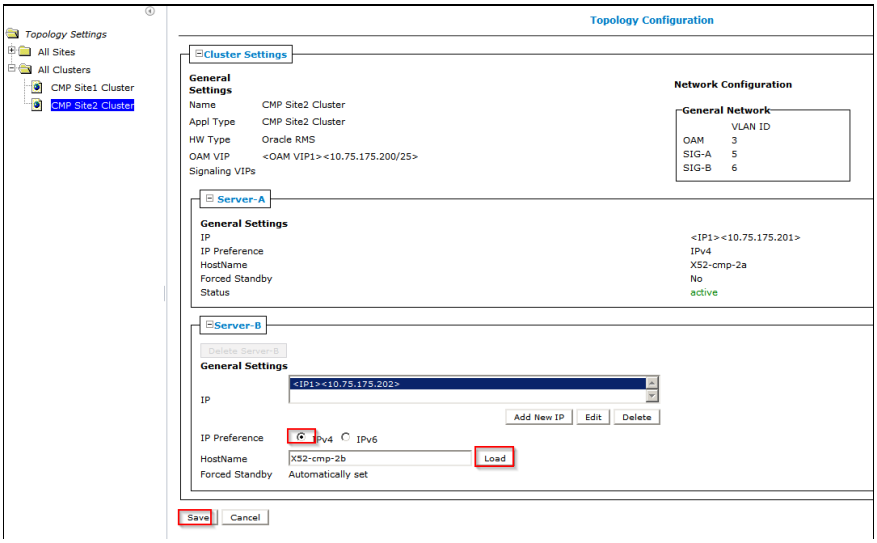
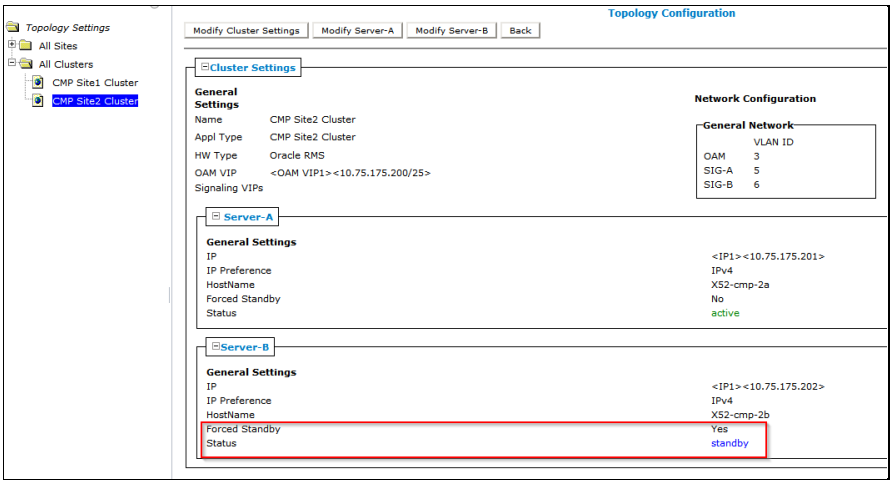
Step	Procedure	Details
3. ☐	**CMP:** View Topology Settings	Navigate to **PLATFORM SETTINGS → Topology Settings**.  The *Topology Settings* section contains the buttons for adding a CMP Site2 Cluster (used for CMP cluster georedundancy) and adding an (MPE/MRA) cluster. **NOTE:** Adding a CMP Site2 Cluster does not require the Manage Georedundant mode option. This option is for adding georedundant MPE/MRA/Mediation 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 page. 1. Navigate to **PLATFORM SETTINGS →Topology Settings**.  2. Click **Add CMP Site2 Cluster** and the Topology Configuration from opens.  **Complete the form according to the system design.** 3. Define the cluster settings. a. Select the HW Type from the list. Available options are: ▪ C-Class (default)—HP Enterprise ProLiant BL460 Gen8 or Gen9 server ▪ C-Class (Segregated Traffic) (a configuration where Signaling and other

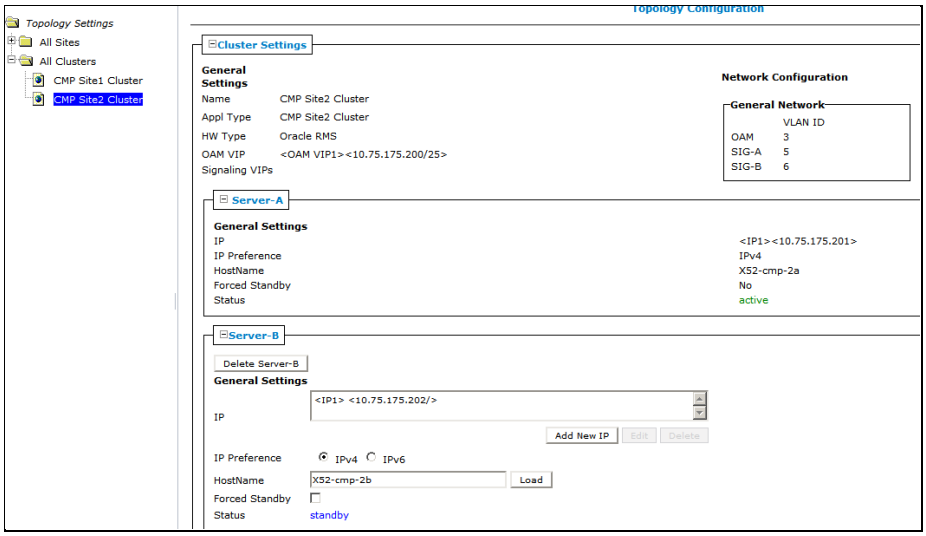
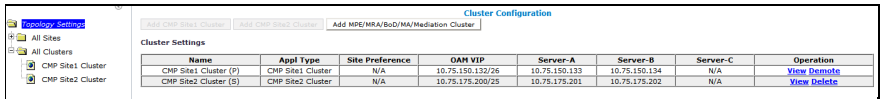
Step	Procedure	Details
		networks are separated onto physically separate equipment)—HP Enterprise ProLiant BL460 Gen8 or Gen9 server ▪ Oracle RMS (rack-mounted servers using tagged VLANs) ▪ RMS (for a rack-mounted server not using VLANs) ▪ VM (virtual machine) b. If you selected C-Class, C-Class (Segregated Traffic), or Oracle RMS, enter the General Network—VLAN IDs. c. Enter the OAM, SIG-A, and (optionally) SIG-B virtual LAN (VLAN) IDs. VLAN IDs are in the range 1–4095. The default values are: ▪ OAM—3 ▪ SIG-A—5 ▪ SIG-B—6 4. Click **Add New VIP**. The New OAM VIP dialog box appears: 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. 5. 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 Host Name of Server-A are the IP address and Host Name used during the Initial Configuration of the server from section 6.1, Perform Initial Server Configuration of Policy Servers—platcfg. They 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 have been defined. The CMP loads the hostname from the IP reachable server. This confirms network connectivity and minimizes the possibility of incorrectly defining the Host Name. To configure Server-A, in the Server-A section of the page: 6. (Required) Click **Add New IP** to enter the IP address.

Step	Procedure	Details
		The Add New IP dialog box 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 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. 9. Enter the HostName of the server. This must exactly match the host name provisioned for this server (the output of the Linux command **`uname -n`**). **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 indicates 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:** In this example, the HostName has been populated by clicking **Load**.  An example of the completed form for Oracle RMS HW Type.

Step	Procedure	Details
		 10. Click **Save** and confirm the VLAN IDs if needed  There is a transition period where alarms display that 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**.  **NOTE:** For further detail of how this relationship between the Primary Site1 CMP Cluster (P) and the Site2 CMP Cluster (S) see the [Configuration Management Platform Wireless User's Guide]. Confirm the Site2 CMP Cluster Server-A is active. Navigate to **PLATFORM SETTINGS →Topology Settings→CMP Site2 Cluster**.

Step	Procedure	Details
		 **NOTE:** Server-B is visible and available for the next step.
5. ☐	**CMP GUI:** Add Site 2 CMP Cluster	CMP-Site2 Cluster must add Server-B to complete the cluster configuration. 1. From the Topology Setting menu click **CMP Site2 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 dialog box 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. 5. 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. 6. Enter the HostName of the server. This must exactly match the host name provisioned for this server (the output of

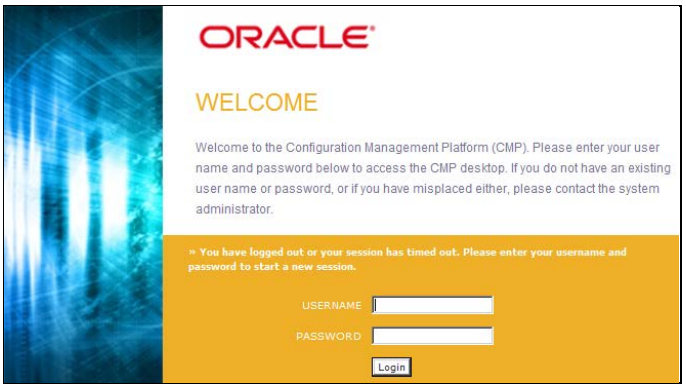
Step	Procedure	Details
		the Linux command **`uname -n`**). **NOTE:** If the server has a configured server IP, you can click **Load** to retrieve the remote server host name. If the retrieve fails, this indicates that the IP address configured is not accessible across the network. Alternately, you may 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 **For example:**  There is a transition period where alarms display that clear after a few minutes while the Site1 CMP Cluster configures the Georedundant CMP Site2 Server-B. Wait for all alarms to clear and then then confirm that Server B in the CMP Site2 Cluster is standby. **PLATFORM SETTINGS →Topology Settings→CMP Site2 Cluster**  **NOTE:** Forced Standby of Server-B status is Yes.

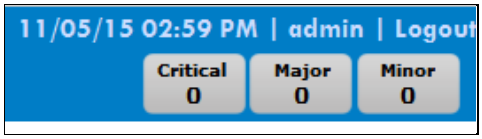
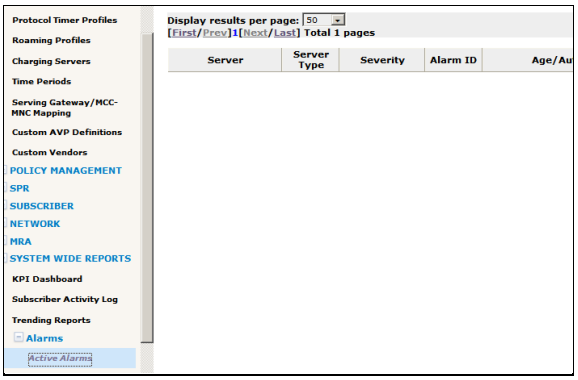
Step	Procedure	Details
6. ☐	**CMP GUI:** Clear Forced Standby—Server-B	1. From the *Topology Settings* menu select **CMP Site2 Cluster**. 2. Click **Modify Server-B**. 3. Remove the Forced Standby state of Server-B by unchecking the Forced Standby box. 4. Click **Save**.  The Georedundant Site2 cluster confugration has been completed. The CMP Site1 Cluster is marked with a (P) for primary and the CMP Site2 Cluster is marked with an (S) for secondary. Navigate to **PLATFORM SETTINGS →Topology Settings**. 
---END OF PROCEDURE---		

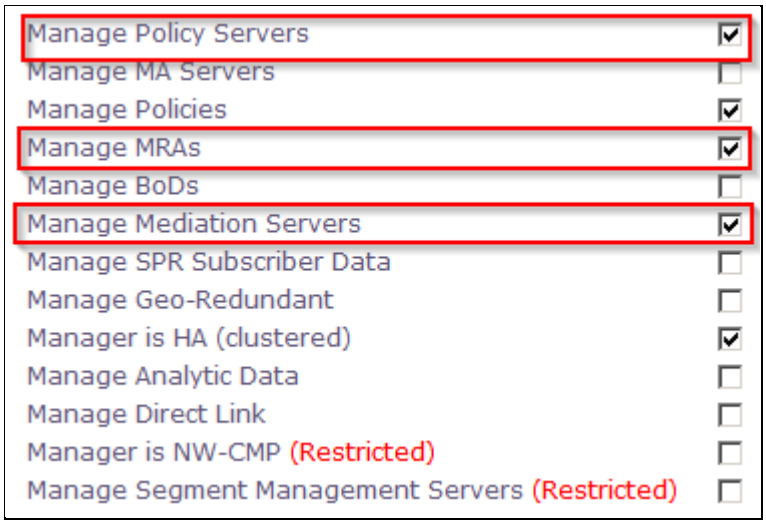
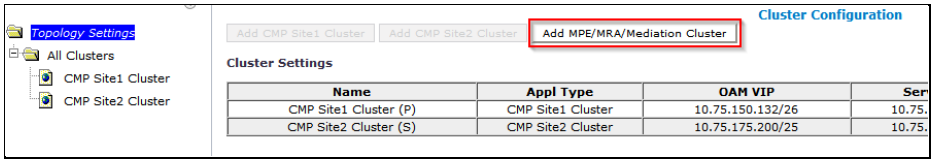
6.4.2 Setting Up a Non-CMP Cluster (MPE/MRA/Mediation)

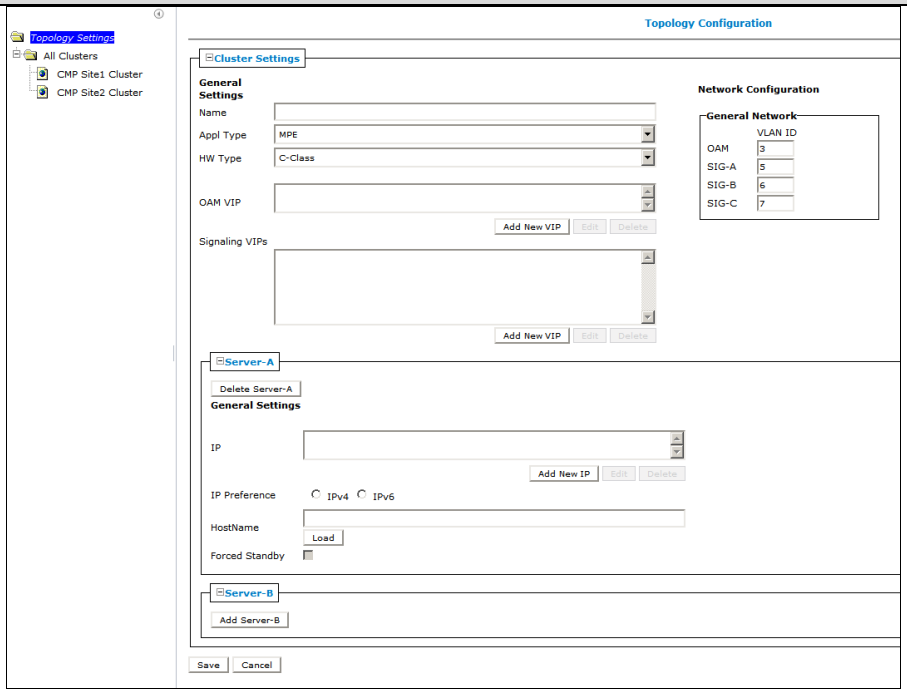
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

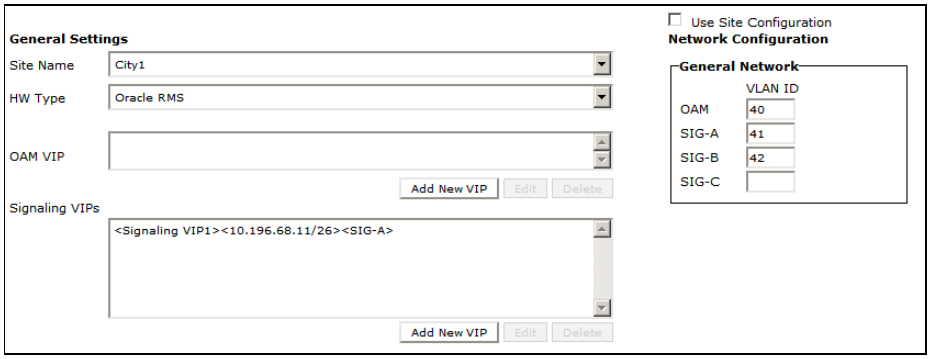
6.4.2: Setting Up a Non-CMP Cluster (MPE/MRA/Mediation)

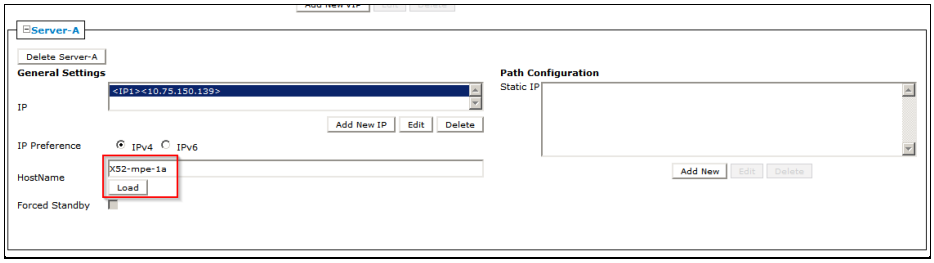
Step	Procedure	Details
1. ☐	**CMP GUI:** Login to CMP Server GUIs (using VIP)	1. From a browser, enter CMP Server VIP in Navigation string. **NOTE:** Only the following web browsers are supported in OCMP 12.3 - Mozilla Firefox® release 31.0 or later - Google Chrome version 40.0 or later  2. Login as admin (or a user with admin privileges)

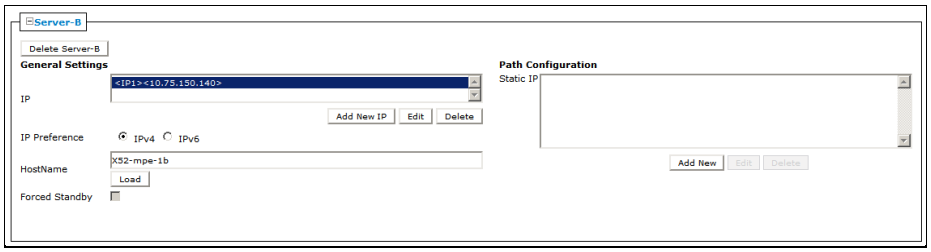
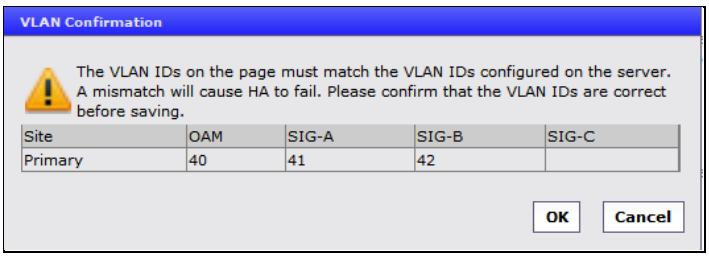
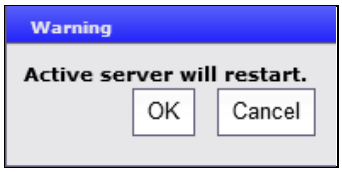
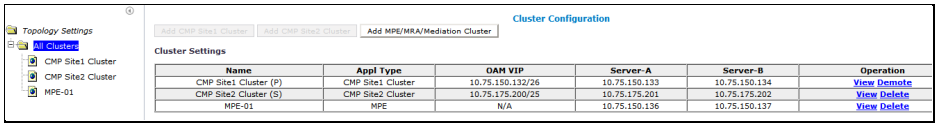
Step	Procedure	Details
2. ☐	**CMP GUI**: View Active Alarms	It is recommended to view the active alarms in the system before performing configuration work. Check clarm information and determine if any alarms present can affect configuration activies. • View alarms from CMP GUI upper right banner  • View alarms from **System Wide Reports → Active Alarms**.  ***IMPORTANT: In Policy 12.3.x, there is online help provided for alarm descriptions:*** • Go to **Alarms → Active** alarms, click the alarm ID to open the alarm description help page. • Go to **Help → Online Help**, and select **Troubleshooting Guide**. Search for the alarm ID.

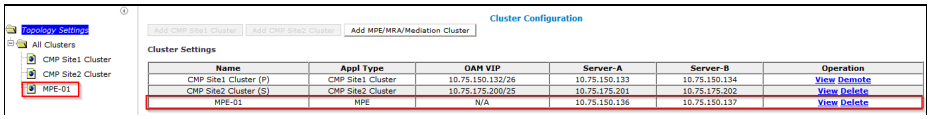
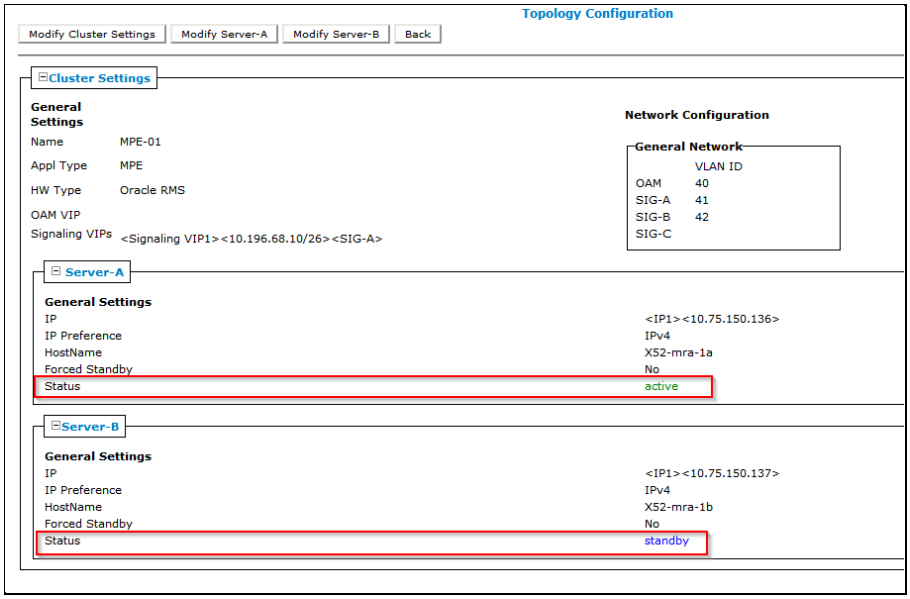
Step	Procedure	Details
3. ☐	Mode Configuration Considerations	The proper modes must be selected during the initial GUI configuration for all the options in this procedure to be available for configuration on the CMP. To add a non-CMP cluster, the following Mode options must be selected on the CMP: • MPE (Manage Policy Servers) • MRA (Manage MRAs) • Mediation (Manage Mediation Servers)  **NOTES:** • Mediation Servers are used with **Wireless-C** Mode enabled. This is a restricted setting. For further details on using the Wireless-C mode contact your Oracle support representative. Mediation Servers are not needed for most Wireless configurations. • If **Manage Georedundant** mode is selected, proceed to the next procedure 6.4.4 Setting Up a Georedundant Non-CMP Cluster (MPE/MRA/Mediation). Modes can be changed at a later time if needed, but the method to access this mode selection is not documented. Contact My Oracle Support if Mode selection is required to be changed after the initial configuration.
4. ☐	**CMP GUI:** Add MPE/MRA/Mediation Clusters	Navigate to **PLATFORM SETTINGS → Topology Settings**.  On the cluster Configuration page, click **Add MPE/MRA/Mediation Cluster**. **NOTE:** Mediation is only present if Manage Mediation Servers is selected. The procedure for adding an MPE, MRA, or Mediation cluster is the same except for selecting Appl Type which is MPE, MRA, or Mediation respectively. The Topology Configuration page opens:

Step	Procedure	Details
		
5. ☐	**CMP GUI:** Add MPE/MRA/Mediation 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, or Mediation cluster is the same except for selecting Appl Type which is MPE, MRA, or Mediation respectively. 1. 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** or **Mediation**. **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 ▪ Oracle RMS—Oracle Server X5-2 or Oracle Netra Server X5-2 ▪ RMS (rack-mounted server)—HP ProLiant DL380 Gen8 or Gen9 server ▪ VM (virtual machine) ▪ VM(Automated) (VM managed by NF Agent) 2. If you selected C-Class, C-Class (Segregated Traffic), or Oracle RMS: d. Enter the General Network—VLAN IDs.

Step	Procedure	Details
		e. Enter the OAM, SIG-A, and (optionally) SIG-B 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 **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 Host Name of Server-A is the IP address and Host Name used during the Initial Configuration of the server in section 6.1, Perform Initial Server Configuration of Policy Servers—platcfg. They 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 have defined. The CMP loads the hostname from the IP reachable server. This confirms network connectivity and minimizes the possibility of incorrectly defining the Host Name. To configure Server-A, in the Server-A section of the page: 3. (Required) Click **Add New IP** to enter the IP address. The Add New IP dialog box appears. 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

Step	Procedure	Details
		hexadecimal string format. 5. 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. 6. Enter the HostName of the server. This must exactly match the host name provisioned for this server (the output of the Linux command **`uname -n`**). **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 indicates 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: 7. (Required) Click **Add New IP** to enter the IP address. The Add New IP dialog box appears. 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 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. 10. Enter the HostName of the server.

Step	Procedure	Details
		This must exactly match the host name provisioned for this server (the output of the Linux command **`uname -n`**). **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 indicates 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:**  **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/Mediation Clusters	1. Click **Save** at 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 was added successfully, it is visible on the Cluster Configuration page. The Cluster Configuration page opens: 

Step	Procedure	Details
7. ☐	**CMP GUI:** Add MPE/MRA/Mediation Clusters	Confirm the cluster has been 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 has just been added.  The Topology Configuration opens for the Non CMP cluster. There should be an active and a standby server. It does not matter which server is active. If this is the case and there are no alarms, then the cluster has been successfully added. 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, Mediation servers being added to the topology, the status of these added servers show as offline and alarms are 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 have been added in the topology. In this case, further configuration cannot be performed until the network connectivty between the CMP and the target servers is available. Do not proceed. Return to this stepwhen 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 has been successfully added.
8. ☐	Repeat the previous step for additional clusters	A list of clusters to be configured can be added to this step as a reminder. The procedure for adding an MPE, MRA, or Mediation cluster is the same except for selecting Appl Type which is MPE, MRA, or Mediation respectively.

Step	Procedure	Details
9. ☐	If the CMP will Manage Remote sites, and these are not yet available.	If the CMP manages Remote sites, and the remote sites are not yet available. • a) Configure these clusters, but Return to the Verify Steps above after the connectivity has been established. • b) Configure these clusters at a later time when the connectivity is established.
---END OF PROCEDURE---		

6.4.3 Setting Up a Georedundant Site

This procedure creates Sites that are used if georedundant clusters are added to the CMP Topology. A georedundant cluster is associated with these Sites in the next procedure. If georedundant clusters are not needed then skip this procedure.

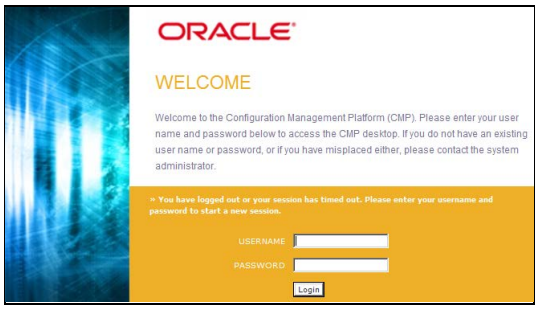
Prerequisites

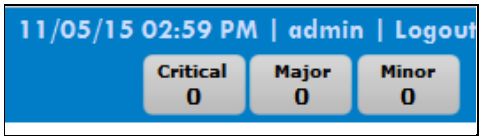
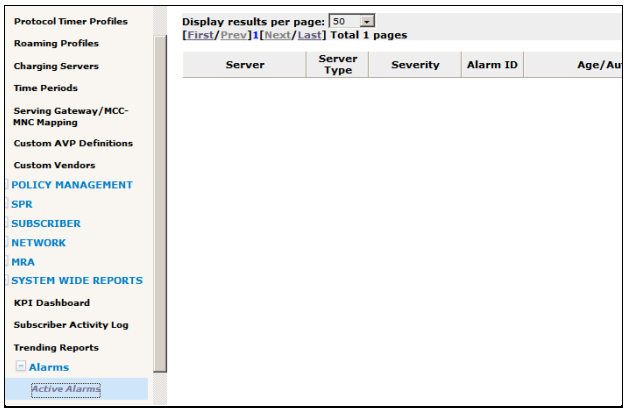
- Before beginning this procedure, verify that you have HTTP access to the CMP server.
- Names of Sites to be created

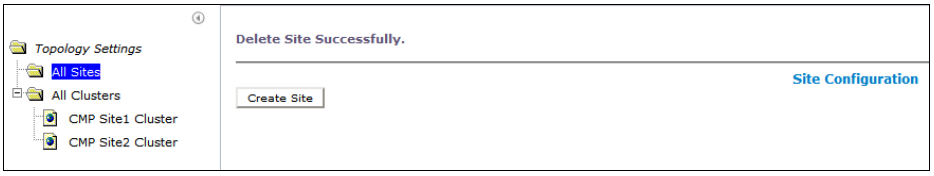
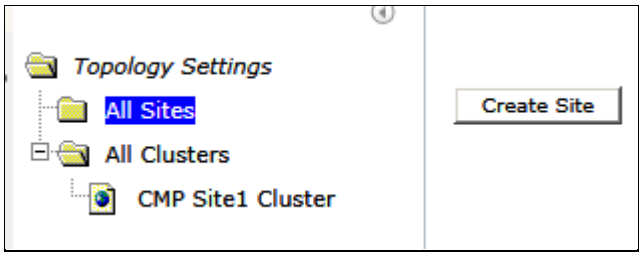
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

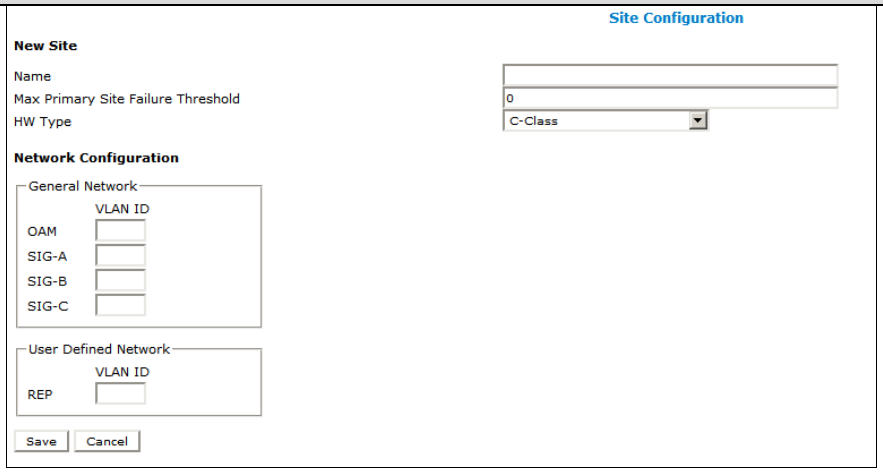
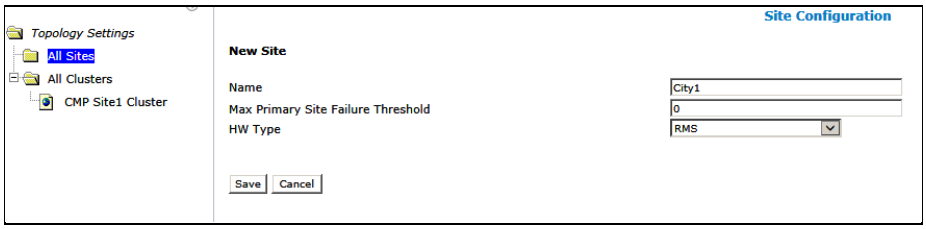
If this procedure fails, contact ORACLE TECHNICAL Services and ask for ASSISTANCE.

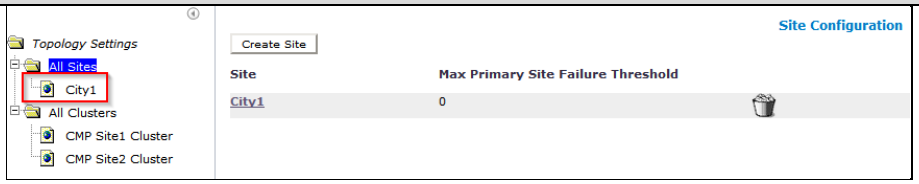
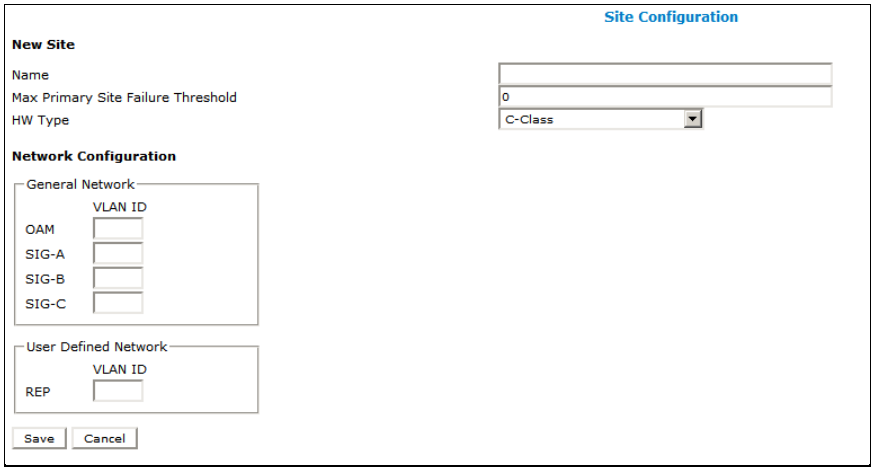
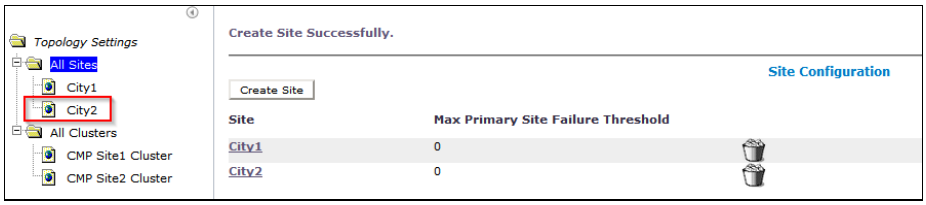
6.4.3: Setting Up a Georedundant Site

Step	Procedure	Details
1. ☐	**CMP GUI:** Login to CMP Server GUIs (using VIP)	1. From a browser, enter CMP Server VIP in Navigation string. **NOTE:** Only the following web browsers are supported in OCMP 12.3. - Mozilla Firefox® release 31.0 or later - Google Chrome version 40.0 or later  2. Login as admin (or a user with admin 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 alarm information and determine if any alarms present may affect configuration activies. • View alarms from CMP GUI upper right banner  • Navigate to **System Wide Reports → Active Alarms**.  ***IMPORTANT: In Policy 12.3.x, there is online help provided for alarm descriptions:*** • Go to **Alarms → Active** alarms, click the alarm ID to open the alarm description help page. • Go to **Help → Online Help**, and select **Troubleshooting Guide**. Search for the alarm ID.

Step	Procedure	Details
3. ☐	**CMP:** View Topology Settings	1. Navigate to **PLATFORM SETTINGS → Topology Settings**. 2. Confirm that All Sites are in the Topology Settings list.  **NOTE:** Sites may only be created when Manage Georedundant mode is enabled.  **NOTE:** If Manage Georedundant mode was not selected during initial configuration of the Site1 CMP cluster, the CMP modes can be changed if required, but the method to access this mode selection is not documented here. Contact My 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 a georedundant MPE, MRA, or mediation clusters and is not needed to add georedundant CMP cluster. If georedundancy is not anticpated, 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) - Oracle RMS (rack-mounted servers using tagged VLANs) - RMS (for a rack-mounted server) - VM (for a virtual machine) - VM (Automated) (for a VM managed by NF Agent) 4. If you selected C-Class, C-Class(Segregated Traffic), or NETRA, enter the General Network information. VLAN IDs. Enter the OAM, SIG-A, and (optionally) SIG-B 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. Name the new site and click **Save**.  The site is present in the Topology Settings menu

Step	Procedure	Details
		 6. Create a second site and click **Save**.  The site is listed in the Topology Settings menu. 
---END OF PROCEDURE---		

6.4.4 Setting Up a Georedundant Non-CMP Cluster (MPE/MRA/Mediation)

This procedure configures the management relationships between the CMP and other Georedundant non-CMP in Wireless Mode.

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

- MPE
- MRA
- Mediation

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 have been 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 has been completed

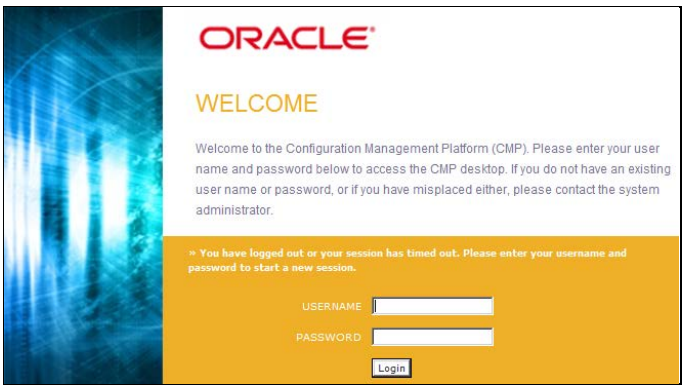
To complete this procedure, you need the following:

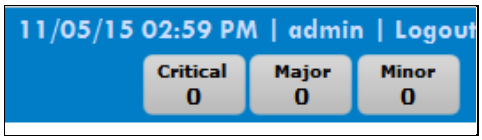
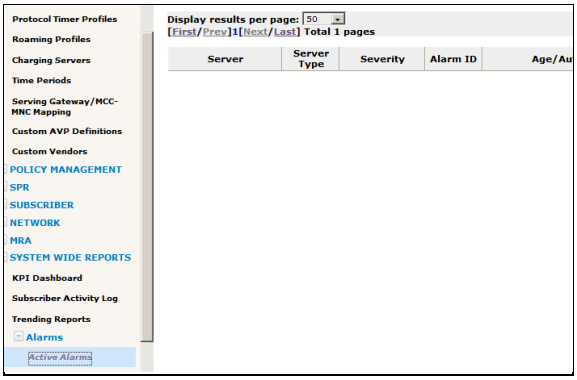
- HW Type—Determines whether VLANs are required. If you select c-Class, c-Class (segregated traffic), or Netra hardware, VLANs are required. For RMS hardware, VLANs are not required.
- OAM VIP (optional)—The IP address and netmask a CMP cluster uses to communicate with an MPE or MRA cluster.
- Signaling 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 will use 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.

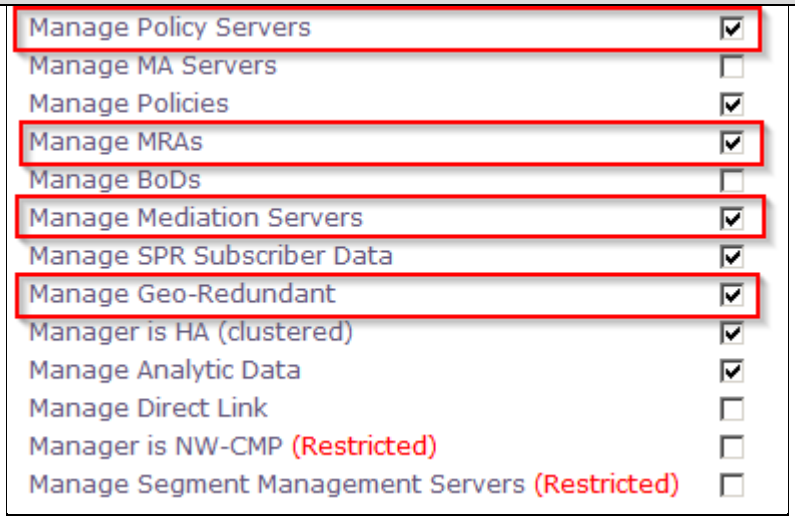
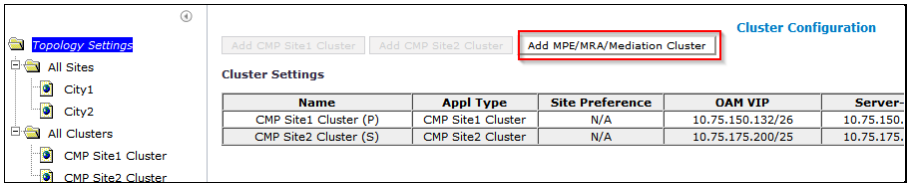
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

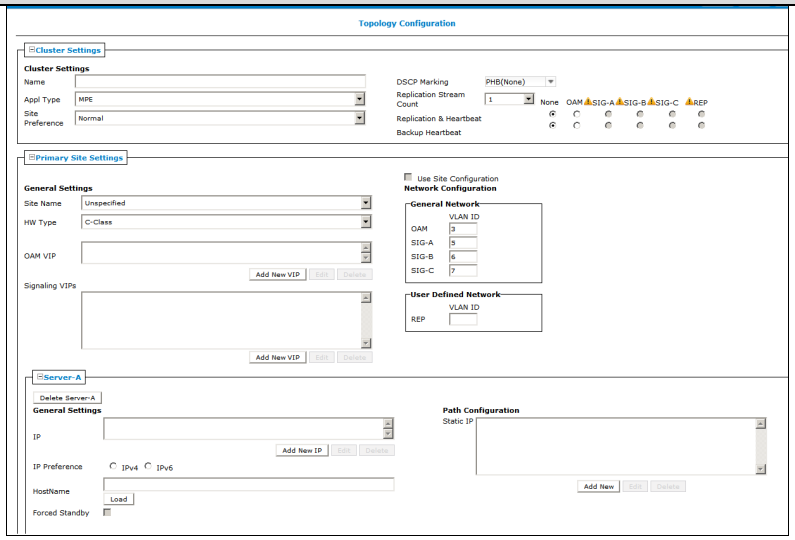
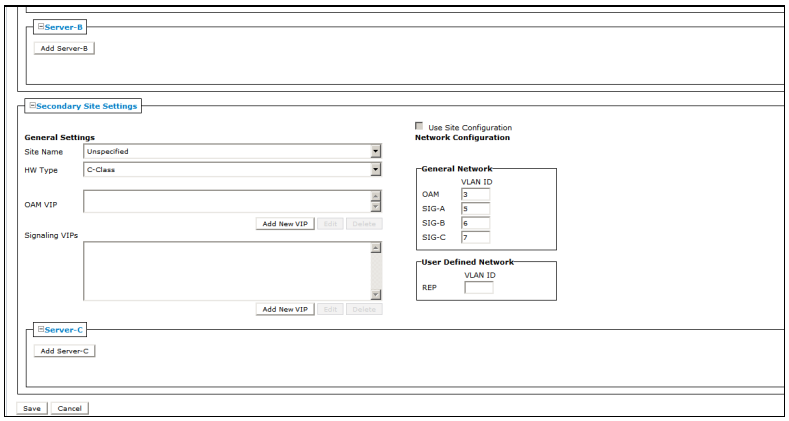
If this procedure fails, contact ORACLE TECHNICAL Services and ask for ASSISTANCE.

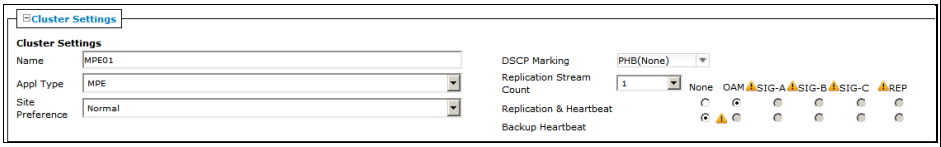
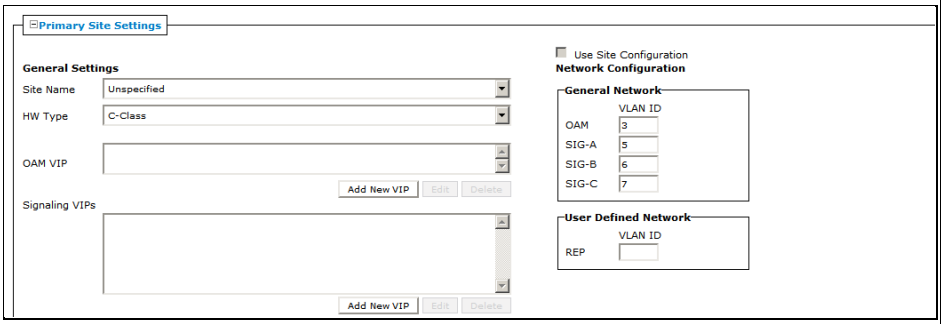
6.4.4: Setting Up a Georedundant Non-CMP Cluster (MPE/MRA/Mediation)

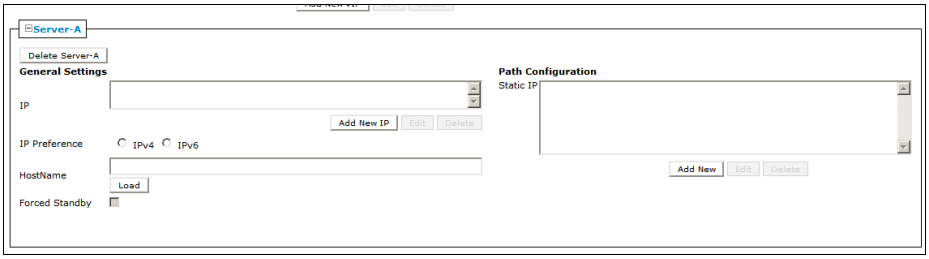
Step	Procedure	Details
1. ☐	**CMP GUI:** Login to CMP Server GUIs (using VIP)	1. From a browser, enter CMP Server VIP in Navigation string. **NOTE:** Only the following web browsers are supported in OCMP 12.3 - Mozilla Firefox® release 31.0 or later - Google Chrome version 40.0 or later  2. Login as admin (or a user with admin privileges).

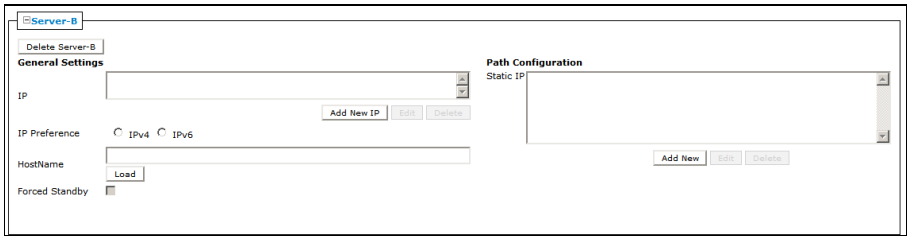
Step	Procedure	Details
2. ☐	**CMP GUI**: View Active Alarms	It is recommended to view the active alarms in the system before performing configuration work. Check alarm information and determine if any alarms present can affect configuration activies. View alarms from CMP GUI upper right banner  View alarms from **System Wide Reports → Active Alarms**.  ***IMPORTANT: In Policy 12.3.x, there is online help provided for alarm descriptions:*** • Go to **Alarms → Active** alarms, click the alarm ID to open the alarm description help page. • Go to **Help → Online Help**, and select **Troubleshooting Guide**. Search for the alarm ID.
3. ☐	Mode Configuration Considerations	The proper 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) • Mediation (Manage Mediation Servers) • Manage Georedundant

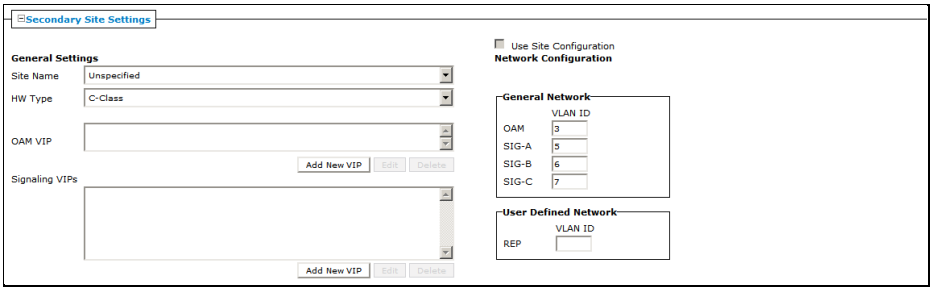
Step	Procedure	Details
		 **NOTES:** • Mediation Servers are used with **Wireless-C** mode enabled. This is a restricted setting. For further details on using the Wireless-C mode contact your Oracle support representative. • **Manage Geo-Redundant** mode provides the ability to configure Primary and Secondary sites as well as adding a Server-C (spare) to each non-CMP cluster in the Topology. Modes can be changed at a later time if needed, but the method to access mode selection is not documented here. Contact My Oracle Support if mode selection is required to be changed after the initial configuration.
4. ☐	**CMP GUI:** Add MPE/MRA/Mediation Clusters	1. Navigate to **PLATFORM SETTINGS → Topology Settings**.  2. On the *Cluster Configuration* page, click **Add MPE/MRA/Mediation**. **NOTE:** Mediation cluster is available if Manage Mediation Servers is selected in mode options. The procedure for adding an MPE, MRA, or Mediation cluster is the same except for selecting Appl Type which is MPE, MRA, or Mediation respectively. The *Topology Configuration* page opens.

Step	Procedure	Details
		  **NOTES:** • All Sites are listed in the Topology Settings menu. • Primary Site Settings and Secondary Site Settings are listed on the *Topology Configuration* page. • Server-C is listed in the Secondary Site Settings section of th page.
5. ☐	**CMP GUI:** Add MPE/MRA/Mediation 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 **+** (plus) 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, or Mediation cluster is the same except for selecting Appl Type which is MPE, MRA, or Mediation respectively. **Define the Cluster Settings** **Name** (required)—Name of the cluster. Enter up to 250 characters, excluding quotation marks(") and commas (,).

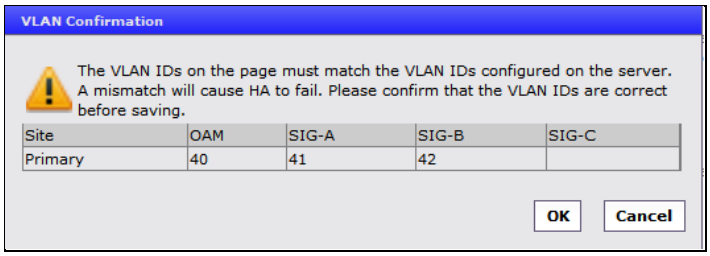
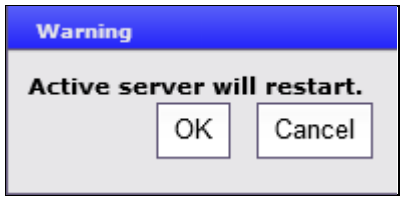
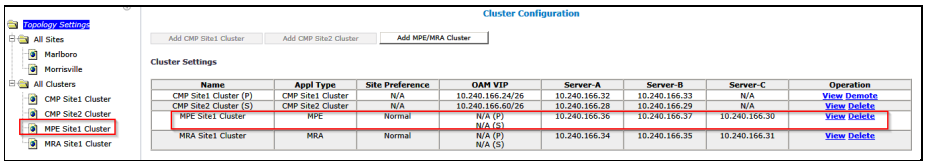
Step	Procedure	Details
		Appl Type—Select the type of server: **MPE** (default) **MRA** or **Mediation** **Site Preference**—NORMAL (default). **DSCP Marking**—PHB(None)is the default. **Replication Stream Count**—1 through 8. 1 is the default. **Replication and Heartbeat**—None is the default. OAM is 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 can be associated with a previously configured site in the drop down tab if this will be Georedundant 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 - Oracle RMS—Oracle Server X5-2 or Oracle Netra Server X5-2 - RMS (rack-mounted server)—HP ProLiant DL380 Gen8 or Gen9 server - VM (virtual machine) - VM(Automated) (VM managed by NF Agent) Define the network configuration if you selected C-Class, C-Class(Segregated Traffic), or Oracle RMS, enter the General Network—VLAN IDs. Enter the OAM, SIG-A, and (optionally) SIG-B 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 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 through 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-A in the Primary Site Settings section of the page.** **NOTE:** The IP address and Host Name of Server-A is the IP address and Host Name used during the initial configuration of the server from section 6.2 of this document. They must match exactly. If Server-A is network reachable from the CMP it is recommended that you click **Load** after the IP address and IP Preference have been 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 Host Name.  To configure Server-A, in the Server-A section of the page: 3. (Required) Click **Add New IP** to enter the IP address. The Add New IP dialog box 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. 5. 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.

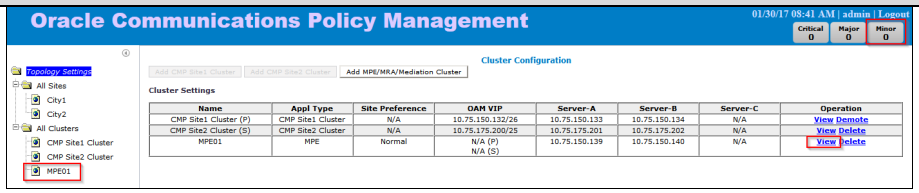
Step	Procedure	Details
		- If neither an IPv4 OAM IP nor a static IP address is defined, IPv4 cannot be selected. 6. Enter the HostName of the server. This must exactly match the host name provisioned for this server (the output of the Linux command **`uname -n`**). **NOTE:** If the server has a configured server IP, you can click **Load** to retrieve the remote server host name. If the retrieve fails, this indicates 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. 7. In the *Path Configuration* section, click **Add New** to add a Static IP. The *New Path* dialog box 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. f. Enter a Static IP address and Mask. g. 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** 8. 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: 9. (Required) Click **Add New IP** to enter the IP address. The Add New IP dialog box opens. 10. 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

Step	Procedure	Details
		hexadecimal string format. 11. 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. 12. Enter the HostName of the server. This must exactly match the host name provisioned for this server (the output of the Linux command **`uname -n`**). **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 indicates 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 is required. 13. In the *Path Configuration* section, click **Add New** to add a Static IP. The New Path dialog 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. a. Enter a Static IP address and Mask. b. Select the Interface: ▪ SIG-A ▪ SIG-B ▪ SIG-C ▪ REP ▪ BKUP **Define the Secondary Site Settings**  **Site Name**—Here the added server can be associated with a previously configured site in the drop down tab if this will be Georedundant topology. **HW Type**—Select the type of hardware: - C-Class (default)—HP ProLiant BL460 Gen8 server

Step	Procedure	Details
		- C-Class (Segregated Traffic) (a configuration where Signaling and other networks are separated onto physically separate equipment)—HP ProLiant BL460 Gen8 - Oracle RMS—Oracle Server X5-2 or Oracle Netra Server X5-2 - RMS (rack-mounted server)—HP ProLiant DL380 Gen8 or Gen9 server - VM (virtual machine) - VM(Automated) (VM managed by NF Agent) Define the network configuration if you selected C-Class, C-Class(Segregated Traffic), or Oracle RMS, enter the General Network—VLAN IDs. Enter the OAM, SIG-A, and (optionally) SIG-B virtual LAN (VLAN) IDs. VLAN IDs are in the range 1–4095. The default values are: • 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 through 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. 14. **Signaling VIPs** (Required) Click **Add New IP** to enter the IP address. The Add New IP dialog box opens. 15. 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. 16. 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. 17. Enter the HostName of the server. This must exactly match the host name provisioned for this server (the output of the Linux command `uname -n`). **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 indicates 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

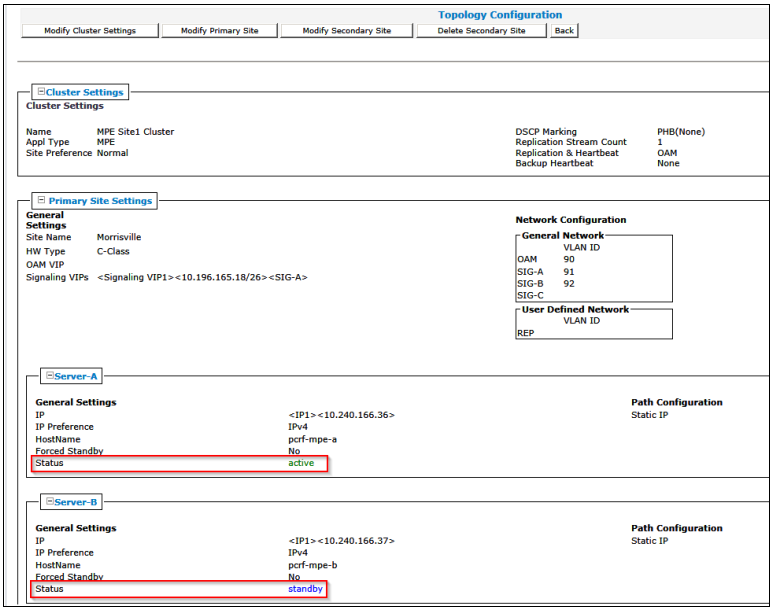
Step	Procedure	Details
		that may be required. 18. In the *Path Configuration* section, click **Add New** to add a Static IP. The *New Path* dialog box appears. **NOTE:** If an alternate replication path and secondary HA heartbeat path is used, a server Static. IP address must be entered in this field. a. Enter a Static IP address and Mask. b. Select the Interface: ▪ SIG-A ▪ SIG-B ▪ SIG-C ▪ REP ▪ BKUP **NOTE:** These settings are only an example of a likely configuration. An actual deployment will be specific to customer requirements.
6. ☐	**CMP GUI:** Add MPE/MRA/Mediation clusters	1. Click **Save** on 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 was added successfully, it is visible on the *Cluster Configuration* page. The *Cluster Configuration* page opens: 
7. ☐	**CMP GUI:** Add MPE/MRA/Mediation clusters	Confirm the cluster has been 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.

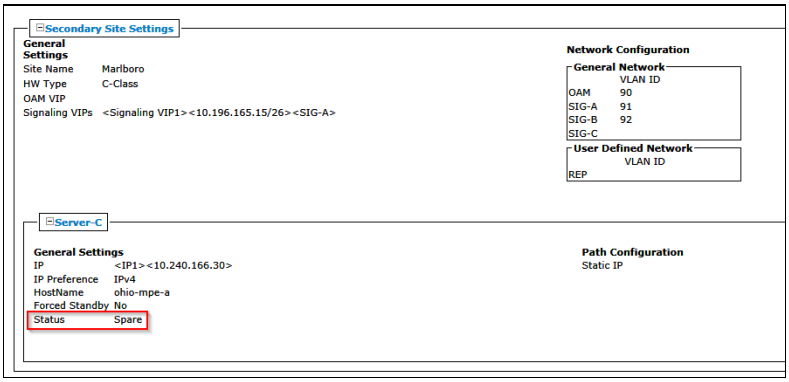
Step	Procedure	Details



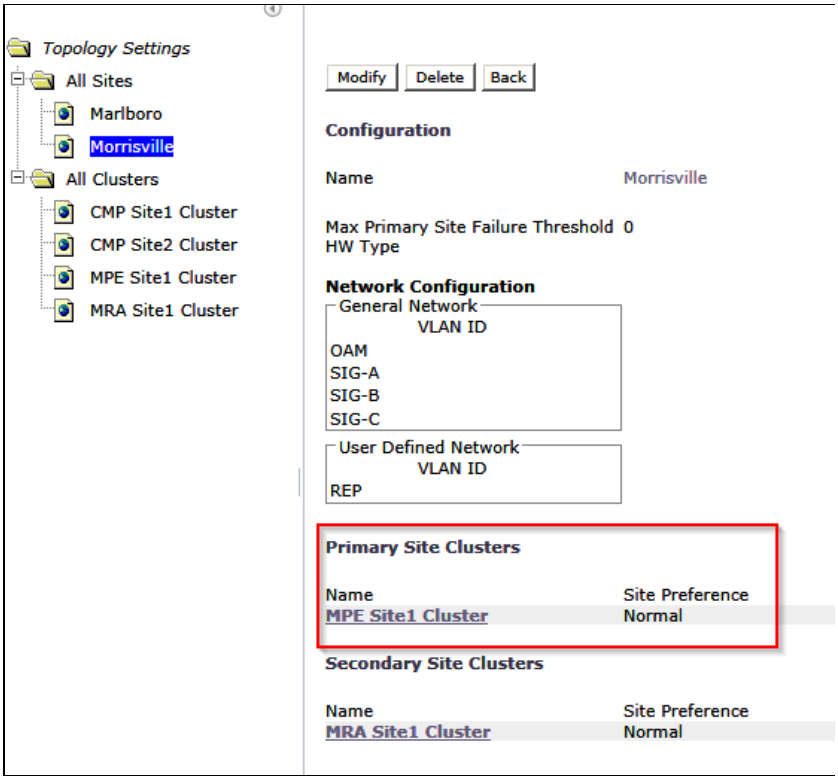
Server-A and Server-B should be active and standby. It does not matter which server is active. Spare-Server-C should show a staus of Spare. If this is the case, and there are no alarms, then the Georedundant cluster has been added successfully.

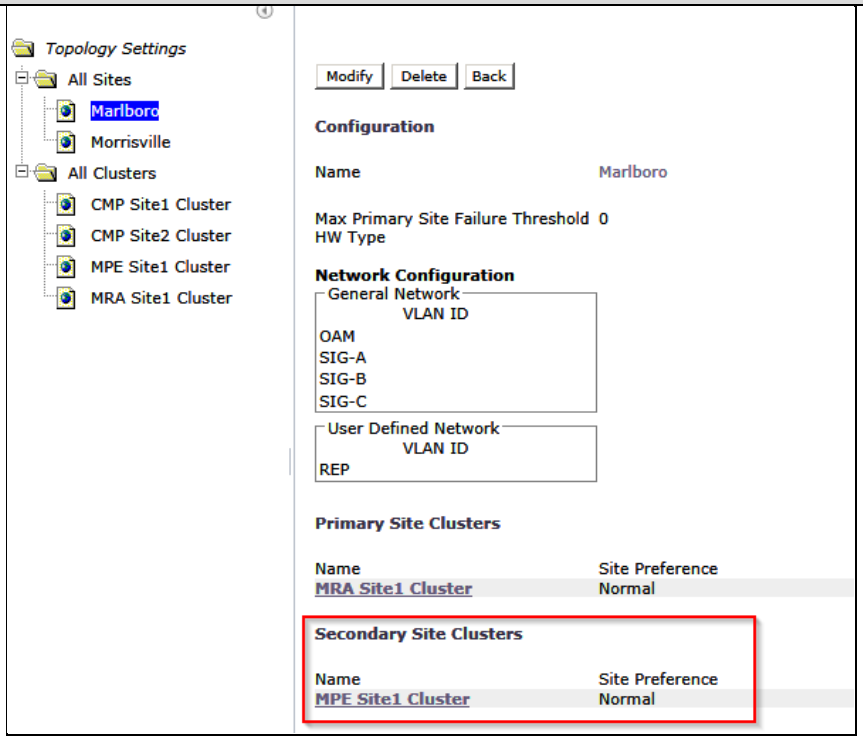
For Example:





NOTE: If the topology configuration is performed at a time when there is no network connectivity between the CMP and the MRA, MPE, Mediation servers being added to the topology, the status of these added servers shows as 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 have been added in the topology. In this case, no further configuration can be performed until the network connectivity between the CMP and the target servers is available. Do not proceed further. Return to this step at when the network connectivity from the CMP to the target servers is available. If the servers are

Step	Procedure	Details
		reachable then proceed to the next step. Confirm the added non-CMP clusters have been associated with the correct Site. Navigate to **Topology Settings→All Sites→**<*Site Name*>. **For example:** MPE Site1 Cluster is associated to the Morrisville Site as a Primary Site Cluster. This would be Server-A and Server-B.  Here MPE Site1 Cluster is associated to the Marlboro Site as a Secondary Site Cluster. This would be Server-C.

Step	Procedure	Details
		 The cluster has been successfully added.
8. ☐	Repeat the previous step for additional clusters	A list of clusters to be configured can be added to this step as a reminder. The procedure for adding an MPE, MRA, or Mediation cluster is the same except for selecting Appl Type which will be MPE, MRA, or Mediation respectively.
9. ☐	If the CMP manages remote sites, and they are not available.	If the CMP manages remote sites, and they are not available: • Configure the clusters, but return to the verify steps above after the connectivity has been established. • Configure the 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, and Mediation 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 previously 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 new 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 occur, perform this procedure again. The SSH provisioning utility rechecks the existing SSH key exchanges in the entire topology and provisions any key exchanges not yet run. You can run the command multiple times, even if keys were previously exchanged.

Prerequisites

- 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. Boxes have been provided for this purpose under 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:** Perform Key Exchanges on all servers	Use SSH to connect to the **active** server at the CMP Site 1 cluster as the user admusr.
		
		Enter the command **sudo ha.mystate** to determine if 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 ~]$`

Step	Procedure	Details

2. ☐	**Ssh to CMP Site 1 active server:** Perfrom Key Exchanges to 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.
		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 **`SSH keys are OK`** message. 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. 4. ☐	**Ssh to CMP Site 1 active server:** Verify Key Exchanges to all servers	Enter the following command to verify that the keys are successfully exchanged: `$sudo qpSSHKeyProv.pl --check --verbose` You are prompted: The password of admusr in topology: 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 have been checked and have been exchanged successfully:

Step	Procedure	Details

```
[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: Adminstration 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 will follow 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 ILOM server or iLO remote console is available in case 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. You should perform this procedure only for the MPE and MRA servers, as the CMP system should retain the default route on the OAM interface.

6.7 Configure Policy Components

This section contains procedures to configure the Policy Servers to a minimum level to run a test call. Additional details can be found in the Configuration Management Platform Wireless User's Guide .

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 bring up a web browser GUI (http)
- MRA and MPE clusters have been added to the CMP Topology

NOTE: Only the following web browsers are supported in OCMP 12.3

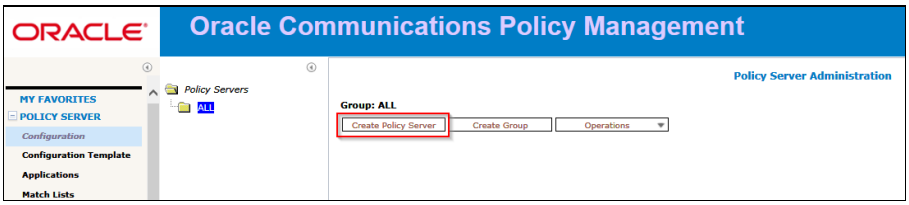
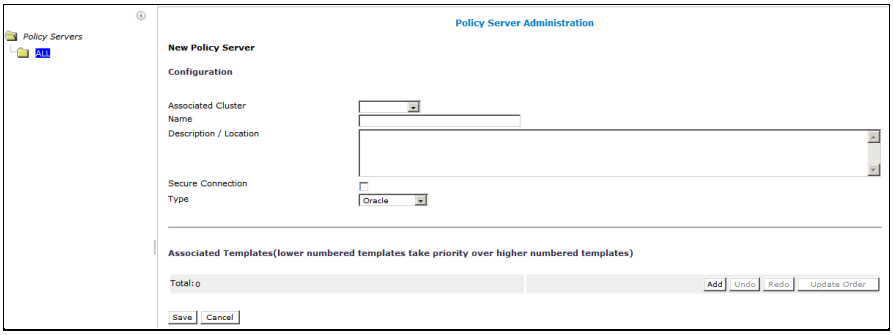
- Mozilla Firefox® release 31.0 or later

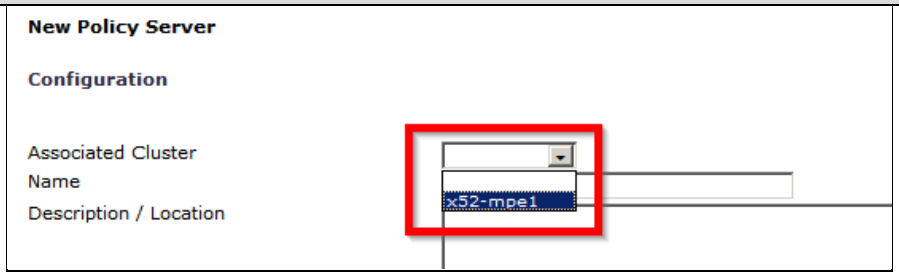
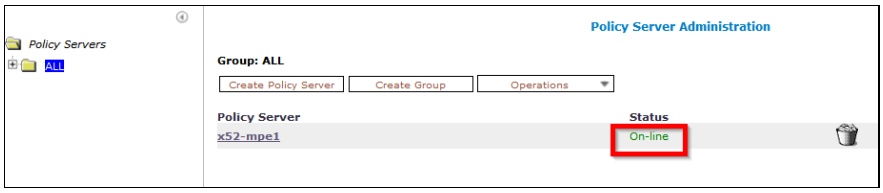
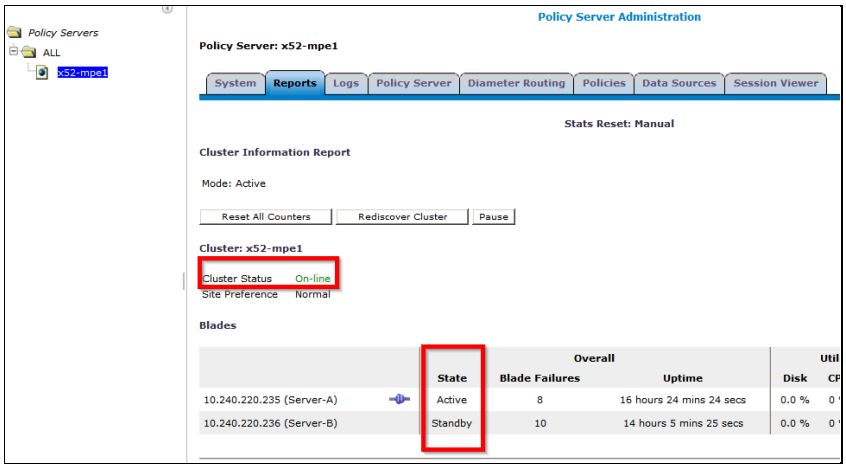
- Google Chrome version 40.0 or later

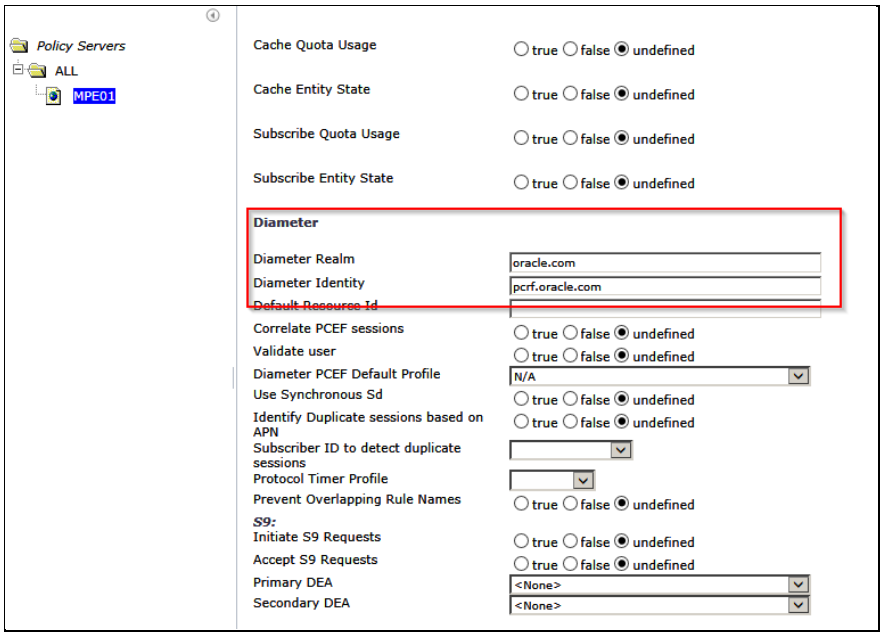
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

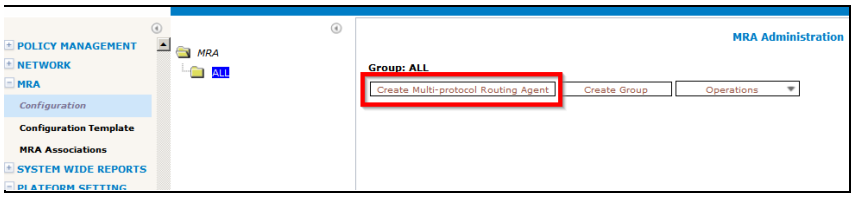
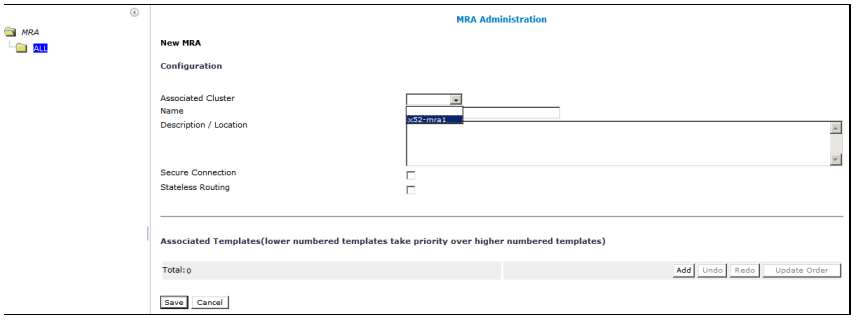
If this procedure fails, contact ORACLE TECHNICAL Services and ask for ASSISTANCE.

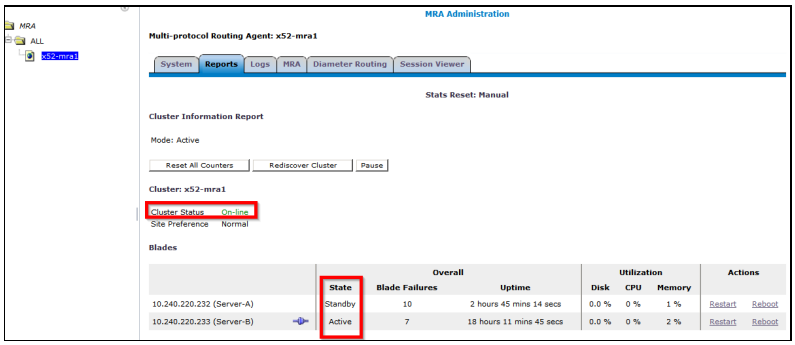
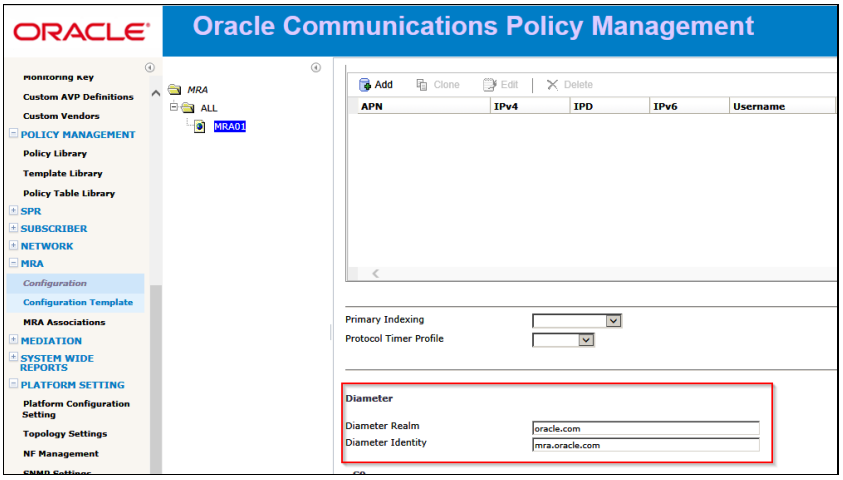
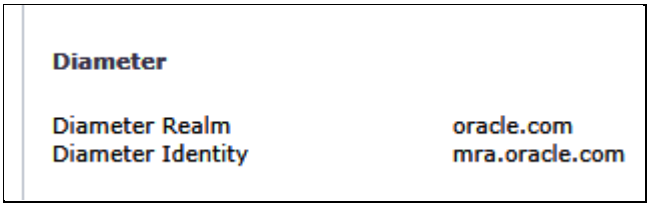
6.7.1: Adding MPE and MRA to the CMP Menu

Step	Procedure	Details
1. ☐	Create Policy Server in CMP GUI	1. Navigate to **Policy Server→ Configuration→ Policy Servers**.  2. Click **Create Policy Server** on the *Policy Server Administration* page.  3. Enter values for the configuration attributes: **Associated Cluster** (required)—Select the cluster with which to associate this MPE device. Configured MPE clusters are listed in Topology Settings. **Name**—Name of this MPE device. The default is the associated cluster name. **Description/Location** (optional)—Information that defines the function or location of this MPE device. **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. **Type**—Defines the policy server type: - Oracle (default) The policy server is an MPE device and can be fully 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. **NOTE:** When configuring an associated cluster, the list is only populated with MPE clusters that have been configured in the CMP Topology.

Step	Procedure	Details
		 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**.  2. Validate that MPE cluster status is On-line and that both Active and Standby servers displayed correctly.

Step	Procedure	Details
3. ☐	Diameter configuration of MPE	Navigate to **Policy Server → Configuration → MPE → Policy Server**. There are many configurations on Policy Server tab of a newly associated MPE. The most important is to define Diameter Realm and identity to allow Diameter connections.  To define these Diameter parameters, click **Modify** on the top of the page then enter the Diameter Realm and Identity for your network and 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: **Diameter** Diameter Realm — oracle.com Diameter Identity — pcrf.oracle.com Default Resource Id — <None> Correlate PCEF sessions — Yes Validate user — No Diameter PCEF Default Profile — <None> Use Synchronous Sd — No Identify Duplicate sessions based on APN — No Subscriber ID to detect duplicate sessions Prevent Overlapping Rule Names — false Protocol Timer Profile — undefined

Step	Procedure	Details
4. ☐	Create MRA in CMP GUI	1. Navigate to **MRA →Configuration→ ALL**.  2. Click **Create Multi-protocol Routing Agent** on the *MRA Administration* page.  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 Configured MRA status is On-line: 

Step	Procedure	Details
5. ☐	Check MRA cluster using the Reports tab	1. Navigate to **MRA → Configuration → MRA → Reports**.  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*>. It is important to define Diameter Realm and identity to enable Diameter messaging to function correctly:  2. To define these Diameter parameters, click the Modify on top of page then enter the Diameter Realm and Identity that your network uses and 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 will act as the Policy Front End, must be added to the MPE Pool on the MRA. If MPEs are not used in the Policy Solution this procedure can be skipped.

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

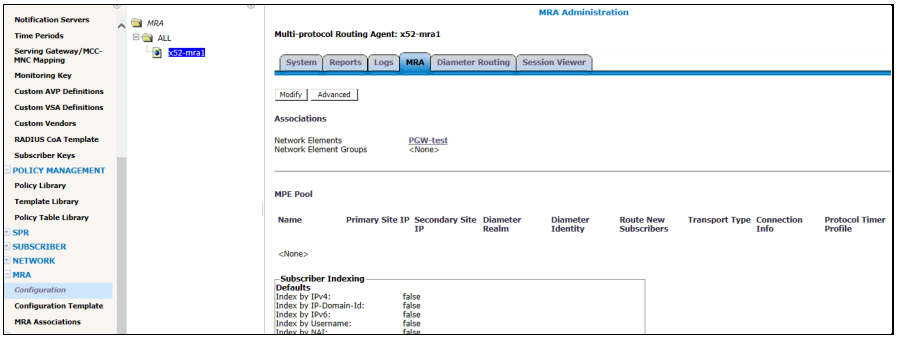
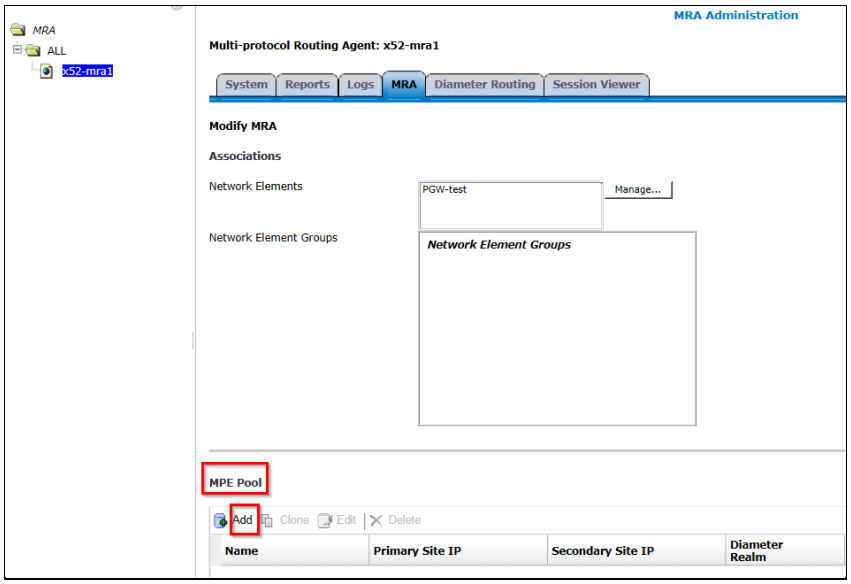
Prerequisite

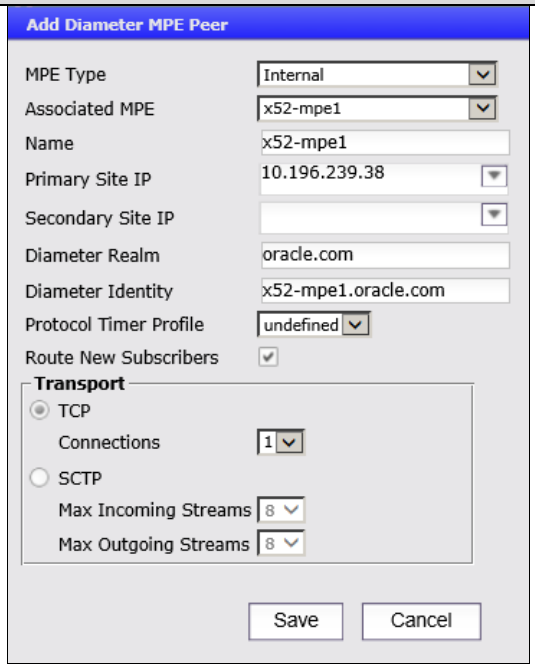
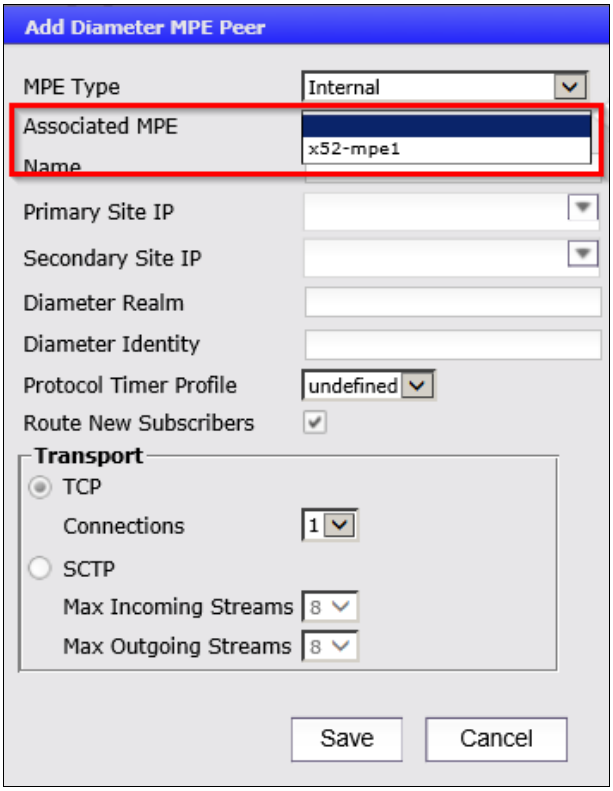
- Network access to the CMP OAM IP address, to bring up a web browser GUI (http)
- MRA and MPE clusters have been added to the CMP menu

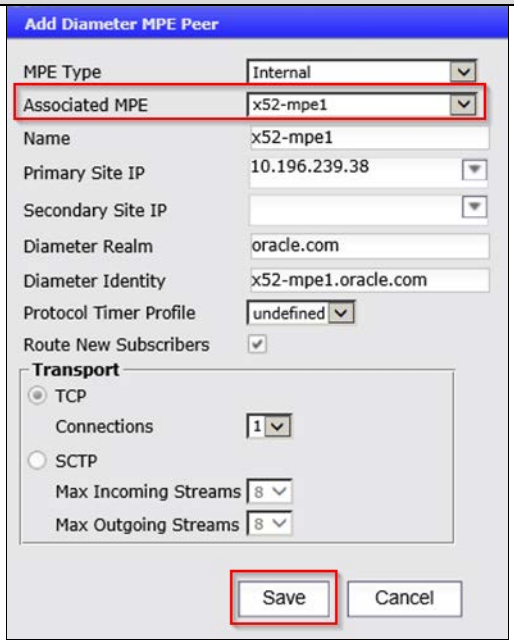
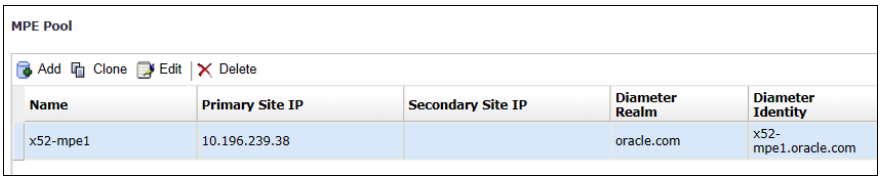
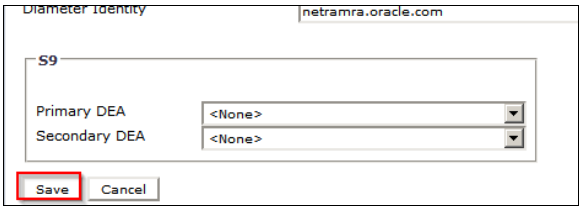
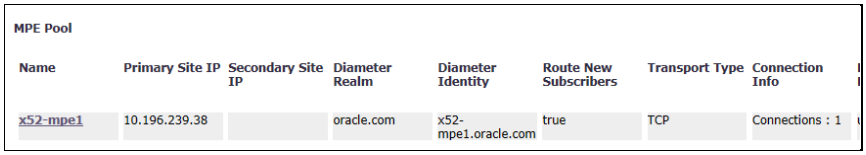
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

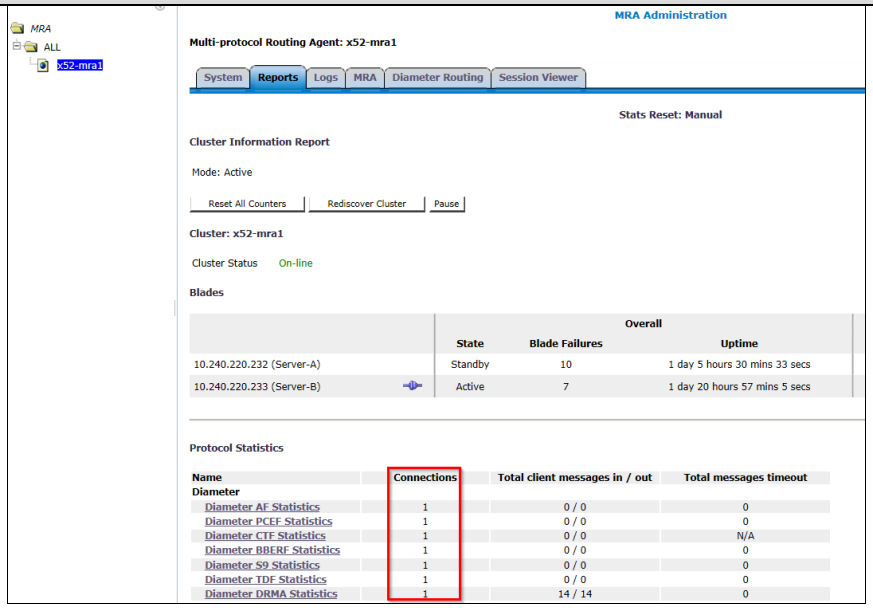
If this procedure fails, contact ORACLE TECHNICAL Services and ask for ASSISTANCE.

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

Step	Procedure	Details
1. ☐	Create Network Element in CMP GUI	1. Navigate to **MRA → Configuration →** <*MRA*> **→ MRA**.  2. Click **Modify** on the MRA Administration page. The MPE Pool configuration form opens.  3. Click **Add** under in the MPE Pool section. The Add Diameter MPE Peer form opens.

Step	Procedure	Details
		 4. Open the **Associated MPE** menu on the Add Diameter MPE Peer form. MPE clusters previously configured in the CMP topology and added to the CMP menu are listed.  5. Select an MPE cluster from the menu.

Step	Procedure	Details
		 6. The required fields auto-populate. Click **Save**. **NOTE:** The Diameter Realm and Diameter Identity must have been data-filled on the MPE. The added MPE cluster is listed in the MPE Pool.  7. Navigate to the bottom of the form and click **Save** again.  The added MPE cluster is listed in the MPE Pool.  8. Confirm the Diameter connection to the MPE from the MRA on the MRA Reports Navigate to **MRA → Configuration → MRA → Reports**.

Step	Procedure	Details
		 A 1401 Log can be noted in the MPE Trace Log that the Diameter connection between the MRA and the MPE has been 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 communicate with the Policy Server.

This procedure adds the Network elements that are configured in the CMP to define the External systems that the Policy Server will communicate with.

Prerequisite:

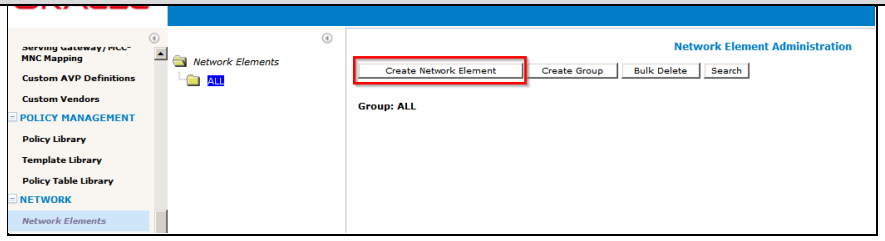
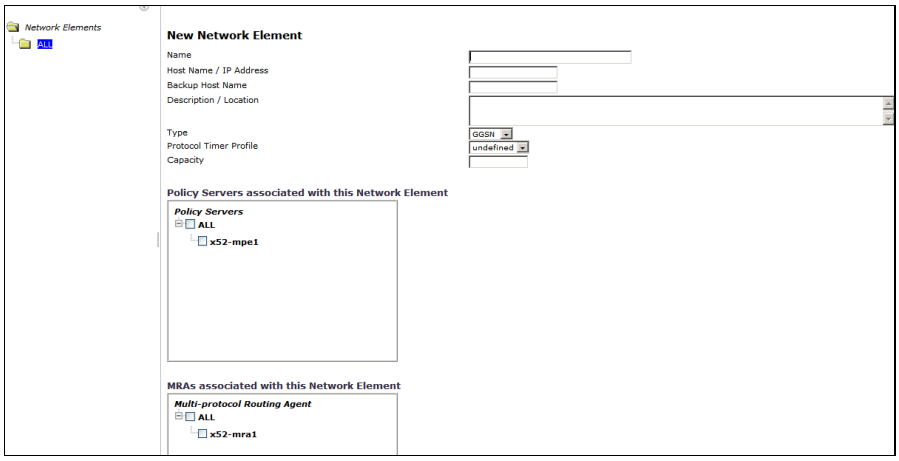
- Network access to the CMP OAM IP address, to bring up a web browser GUI (http)
- MRA and MPE clusters have been added to the CMP menu

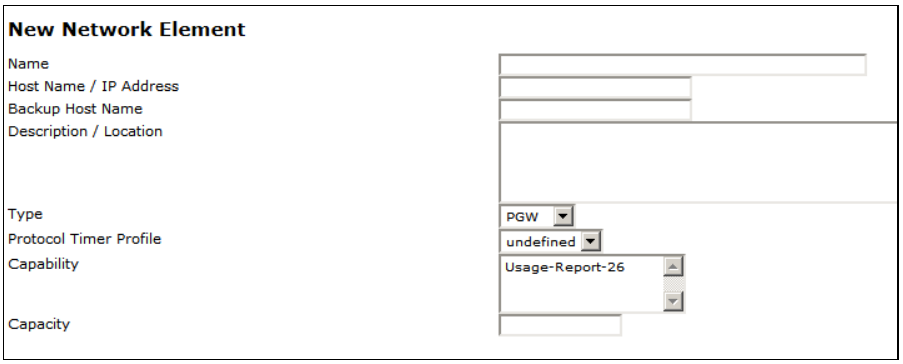
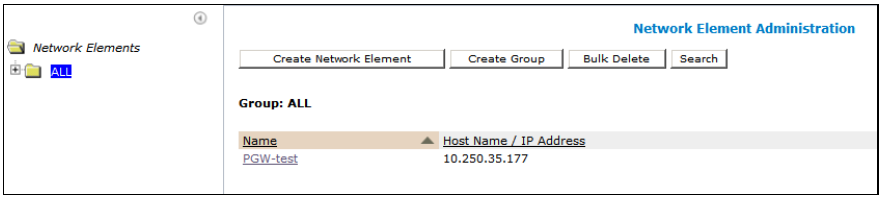
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

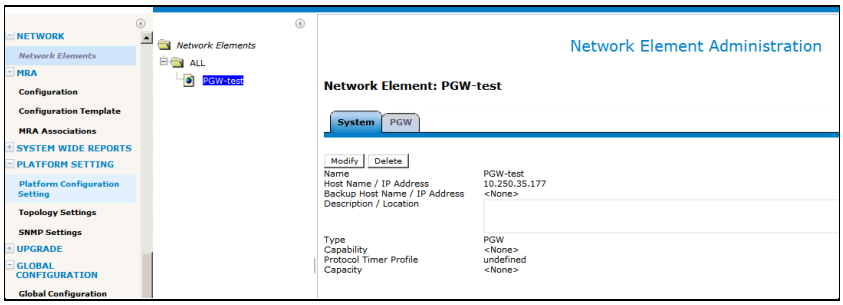
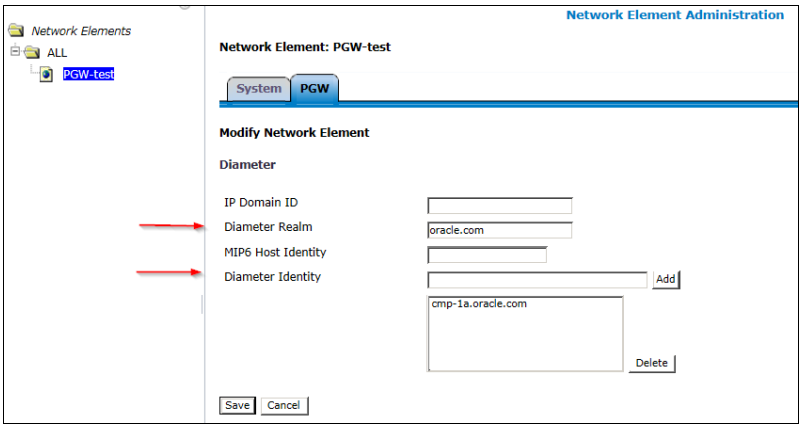
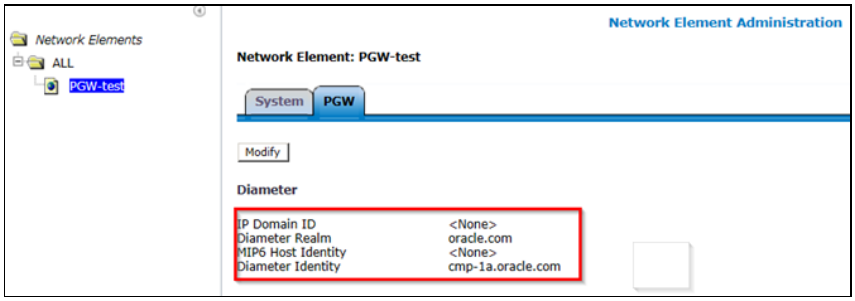
If this procedure fails, contact ORACLE TECHNICAL Services and ask for ASSISTANCE.

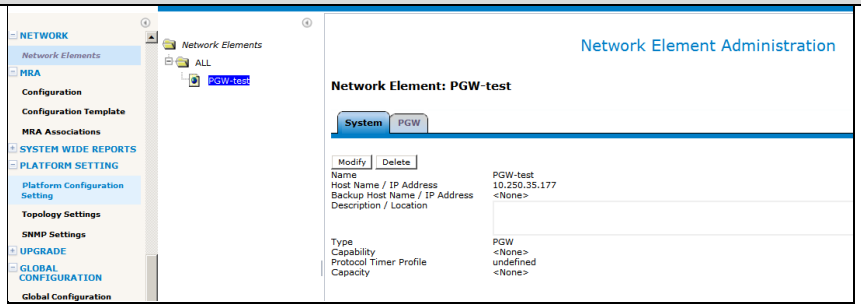
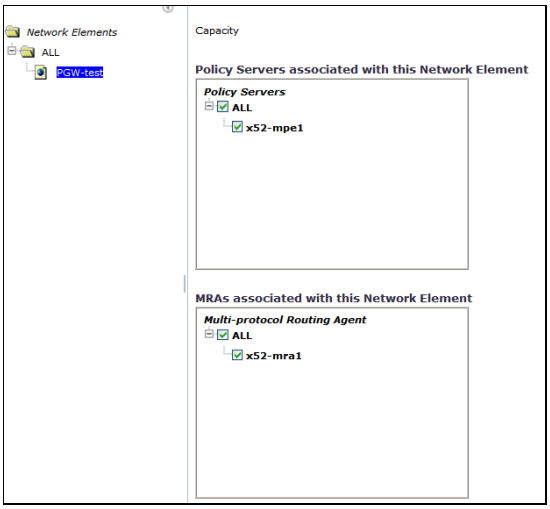
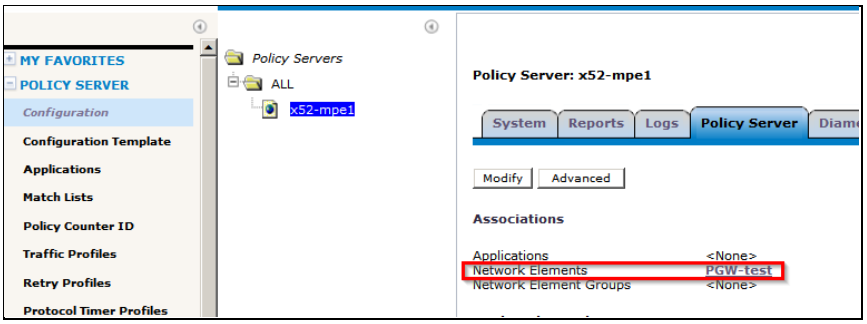
6.7.3: Define and Add Network Elements

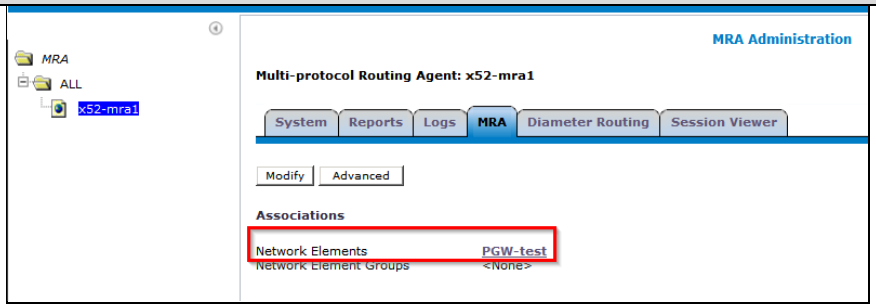
Step	Procedure	Details
1. ☐	Create Network Element in CMP GUI	1. Navigate to **Network→Network Elements→All**.

Step	Procedure	Details
		 2. Click **Create Network Element** on the Network Element Administration page:  3. Enter information for the network element: a. Name (required) The name you assign to the network element. b. Host Name/IP Address (required) Registered domain name, or IP address in IPv4 or IPv6 format, assigned to 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 **Radius-BNG**—RADIUS broadband network gateway **HSGW**—HRPD Serving Gateway

Step	Procedure	Details
		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 CMP Wireless User's Guide. g. **Capacity**—Not applicable. 4. Click **Save**. For this example a PGW Network Element has been defined.  5. After completing the form, click **Save**.  The Network Element has been created.

Step	Procedure	Details
2. ☐	Configure Network Element in CMP GUI	1. Navigate to **Network→Network Elements→<***Network Element entity***>**.  The 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 must have connectivity to the Policy Management System. In addition, the Network Element must have a Diameter Identity assigned that is used to authenticate the Diameter connection from the Network Element. 2. Click **PGW** of the Network Element to assign the Diameter Identity that will be used to authenticate to the Policy Management System. 3. Click **Modify**.  **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 will be used to establish a Diameter connection to the Policy Management System. 4. When you finish, click **Save**. 
3. ☐	Deploy Network	1. Navigate to **Network→Network Elements →<***Network Element entity***>**.

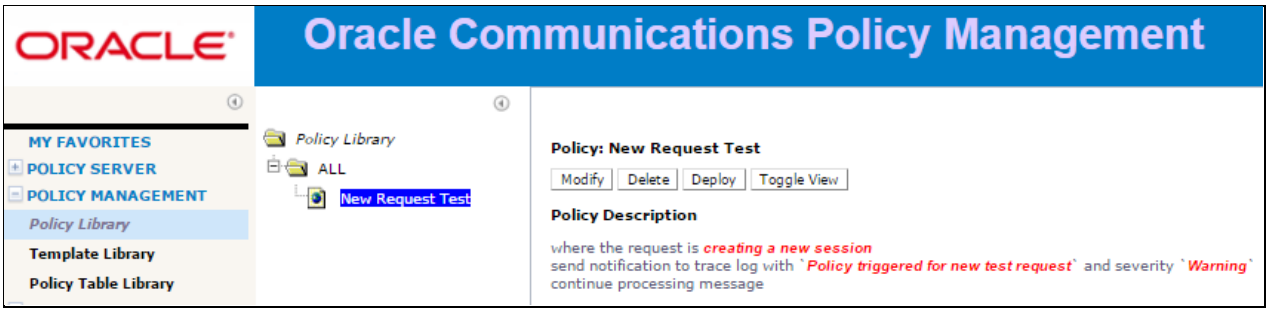
Step	Procedure	Details
	Element in CMP GUI	 2. Click **Modify** on the Network Element Administration page and check the boxes as appropriate to deploy the network element to the MPE and MRA if present.  3. Click **Save**. 4. Navigate to **Policy Server →Configuration→** <*MPE*> **→Policy Server**.  5. Confirm the deployed Network Element is associated with the MPE. Navigate to **MRA →Configuration→**<*MRA*> **→MRA**.

Step	Procedure	Details
		 6. Confirm the deployed Network Element is associated with the MRA.
---END OF PROCEDURE---		

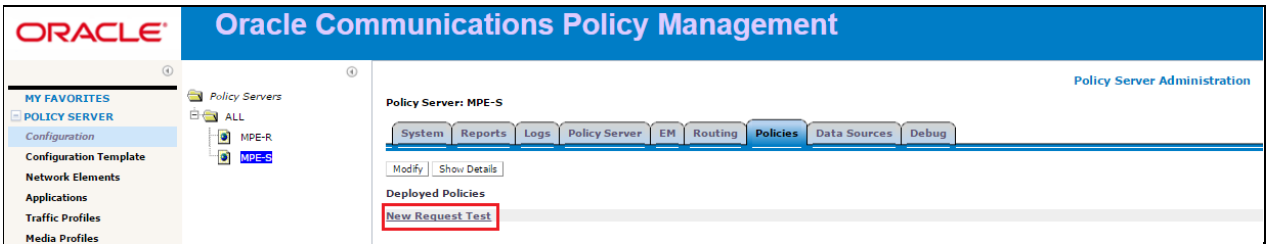
6.8 Load Policies and Related Policy Data

This step is optional. Policies are not required to process a test call but for the purpose of verification, a basic policy can be 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 can be used to confirm session creation for a test call by viewing the trace logs on the MPE that processes the test call.

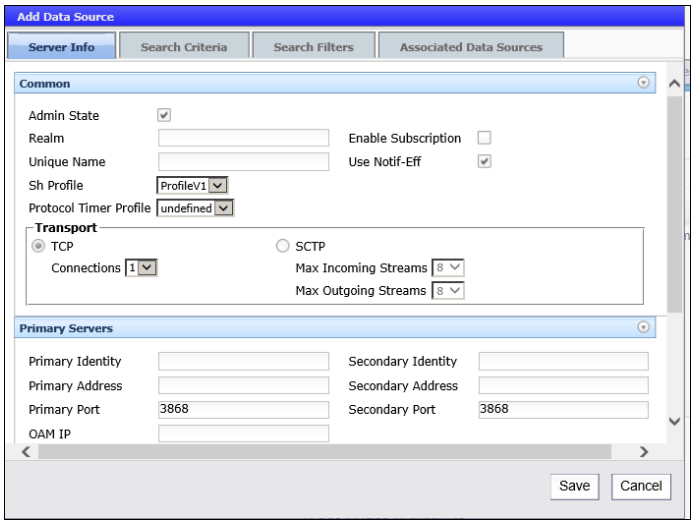


NOTE: This policy must be deployed to the relevant MPE that processes Diameter session requests. Deployed policies can be verified from the Policies tab of the MPE that processes the test request:

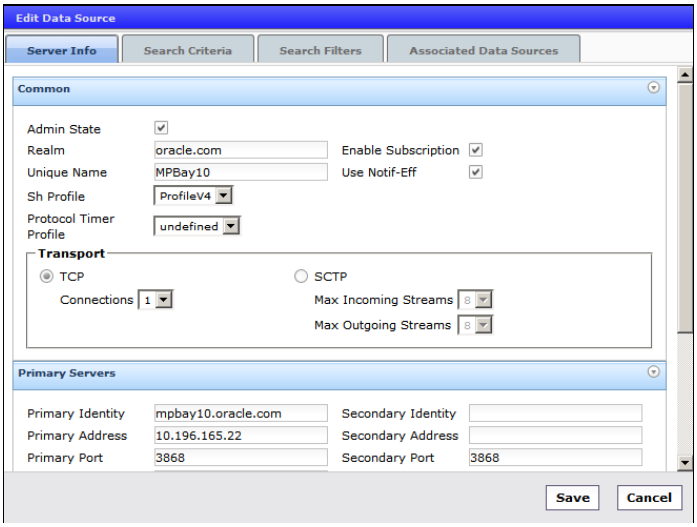


6.9 Add a Data Source

This step is optional. When the test call is received by the MPE, the MPE can be configured to perform a Subscriber lookup to an appropriately configured Subscriber Database. See the CMP Wireless User's Guide for more information.



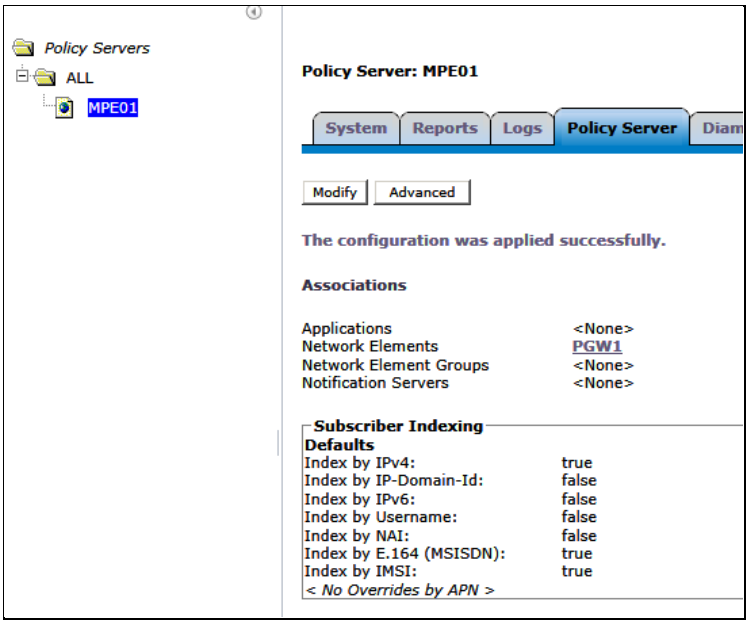
Here is a sample configuration. This form will be specific to the customer site.



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 initiates from the network element that has been created. For example, a PGW (Packet Gateway) first establishes a Diameter connection with the PCRF and then initiates 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** 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 (alarms) are being delivered to the customer Network Management centers. These are outside the scope of this document, but also must be planned and performed.

Reference the following document for information on configuring SNMP:

SNMP User's Guide 12.3

Additional Procedures can be referenced from the following documents:

Platform Configuration User's Guide Release 12.3

CMP Wireless User's Guide 12.3

Changes in the behavior of Release 12.3 are documented in the Oracle® Communications Policy Management Release Notes Release 12.3

Behavior Modifications

- Removal of Manual Statistics Mode (Statistics Mode Unification)—ER 22534128

  As of this release, the manual statistics mode is no longer available. The default and only available mode in this release is interval mode statistics. In prior releases, manual stats mode is the default.

- Firewall Enabled by Default—ER 22536198

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

7. SUPPORTING PROCEDURES

The following procedures may be referenced during installation.

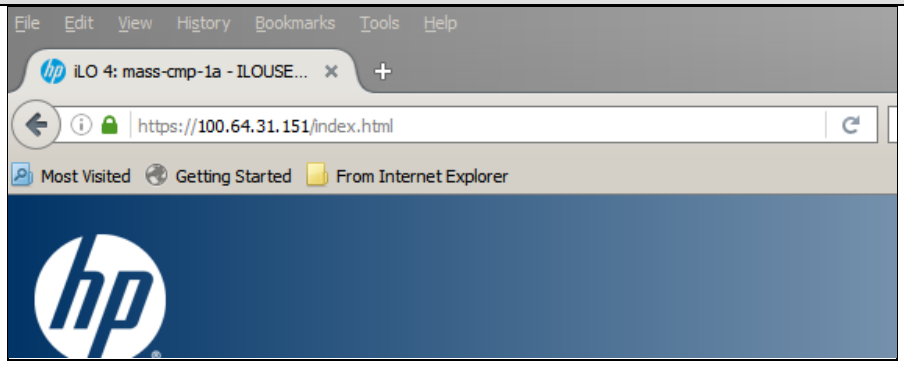
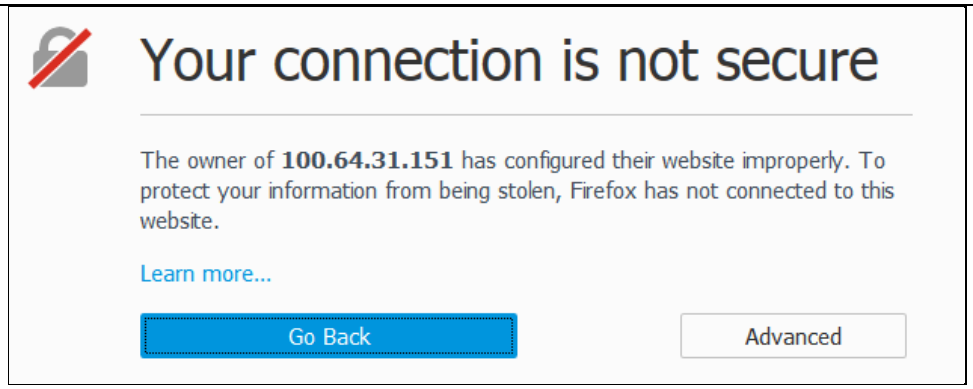
7.1 Accessing the iLO VGA Redirection Window

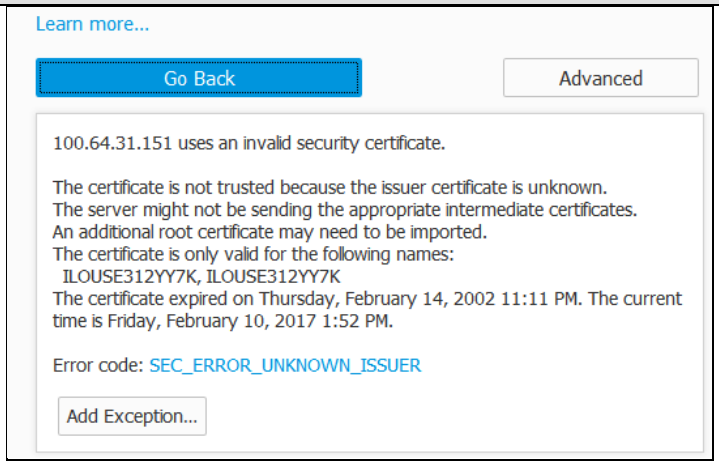
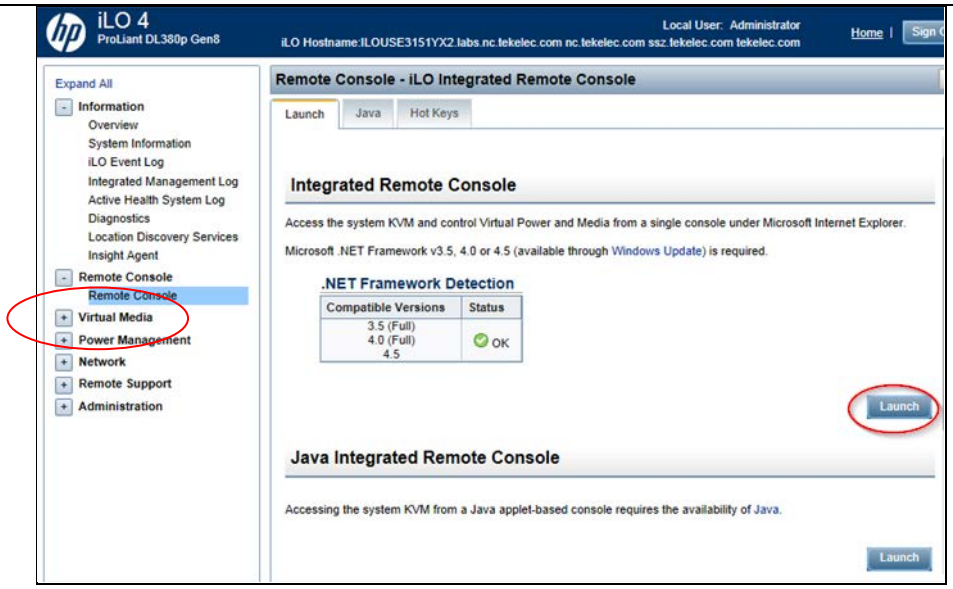
7.1.1 Accessing the iLO VGA Redirection Window for HP Servers

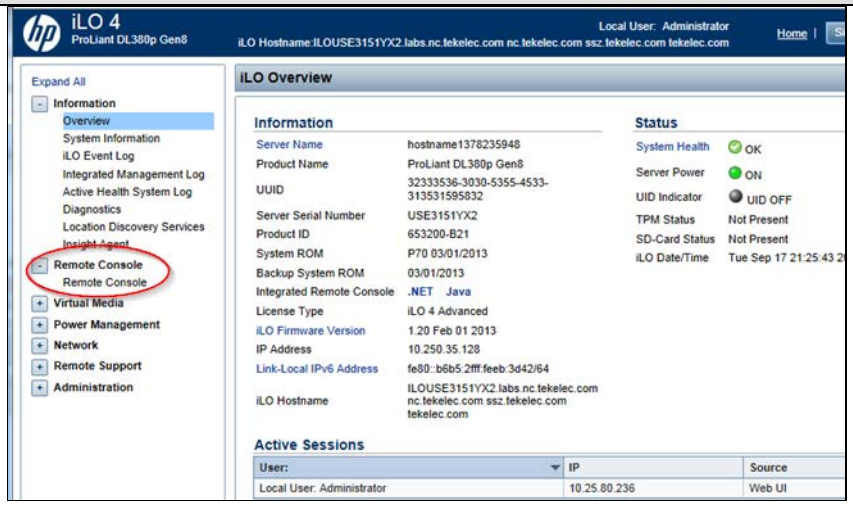
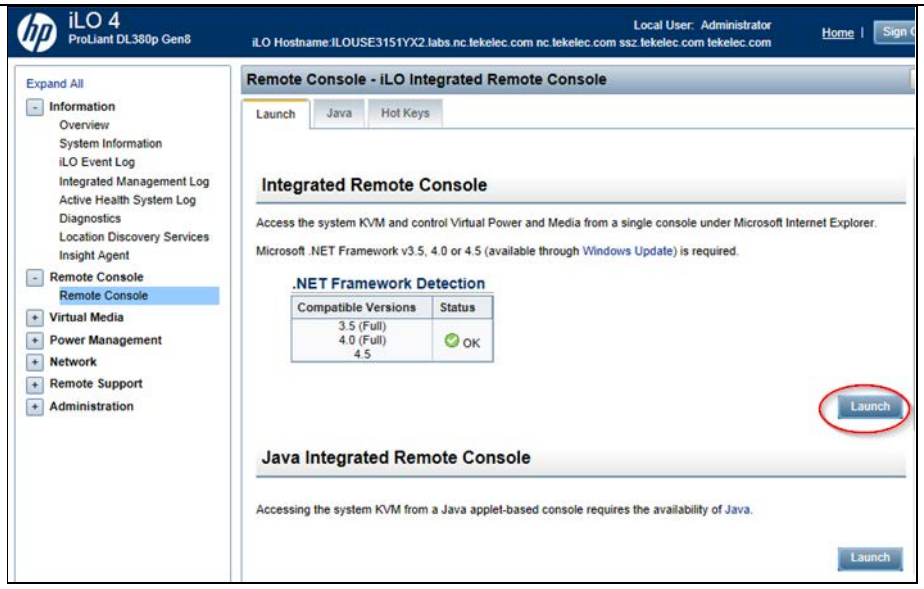
This procedure may very slightly depending on which type of browser is used. If security certificates are installed on the client browser, the security exceptions are not encountered.

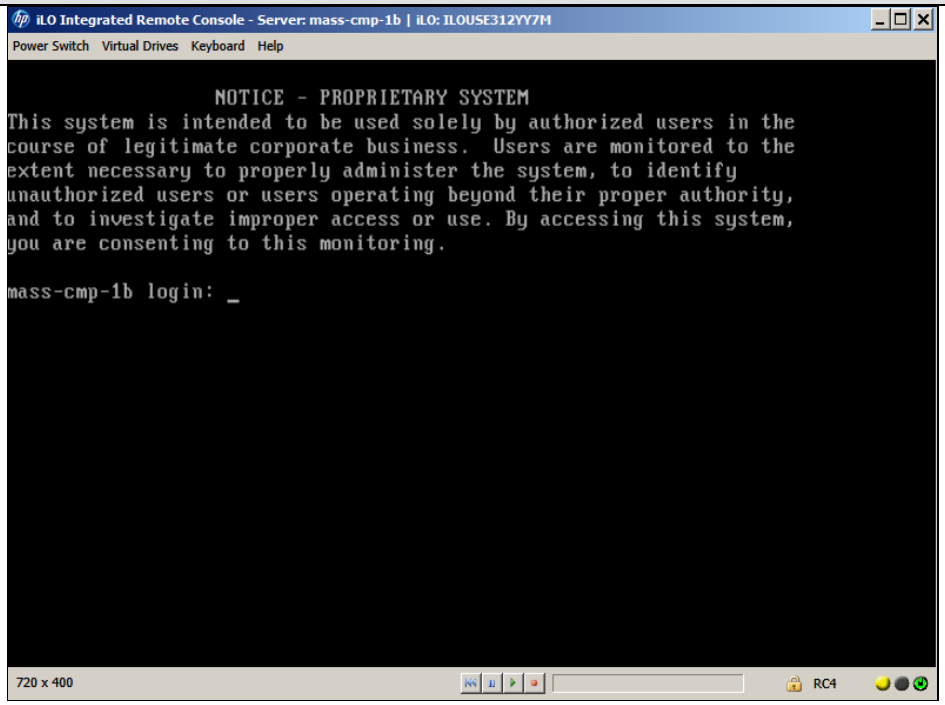
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

7.1.1: 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 warning message will be displayed regarding the Security Certificate.	

Step	Procedure	Result
3. ☐	1. Click **Advanced**. 2. Click **Add Exception.** 3. Click **Confirm Security Exception**.	
4. ☐	Login to the iLO console as Administrator.	
5. ☐	The adminstation page is displayed. Expand the Remote Console in the left pane of the page.	

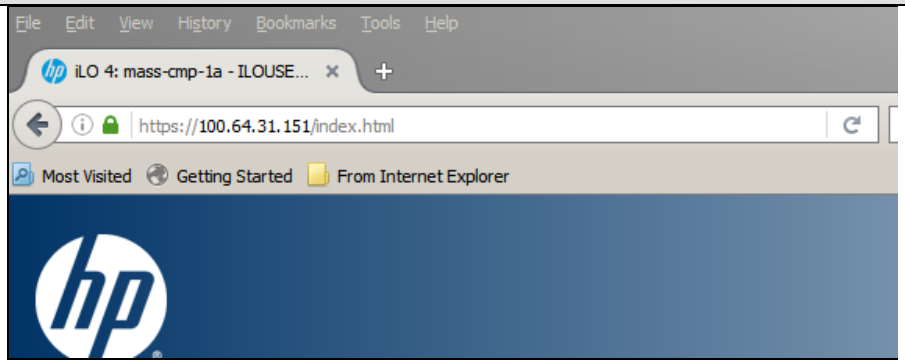
Step	Procedure	Result
6. ☐	The Remote Console tab is expanded Click **Remote Console** option	
7. ☐	The Remote Console GUI is displayed Click **Launch** for Integrated Remote Console.	

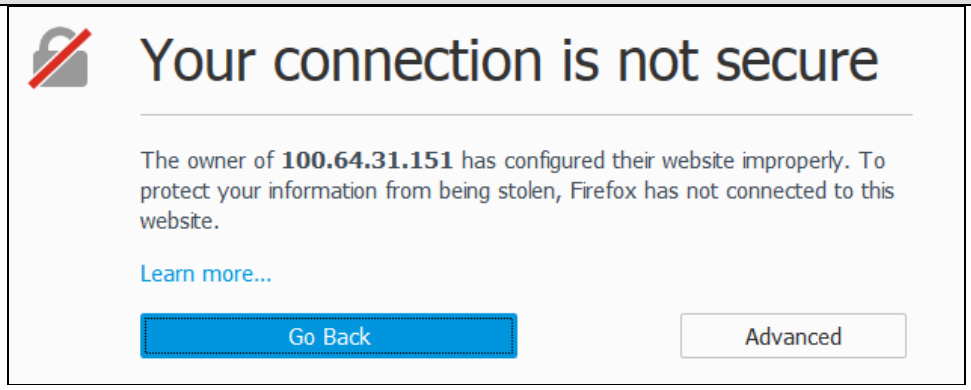
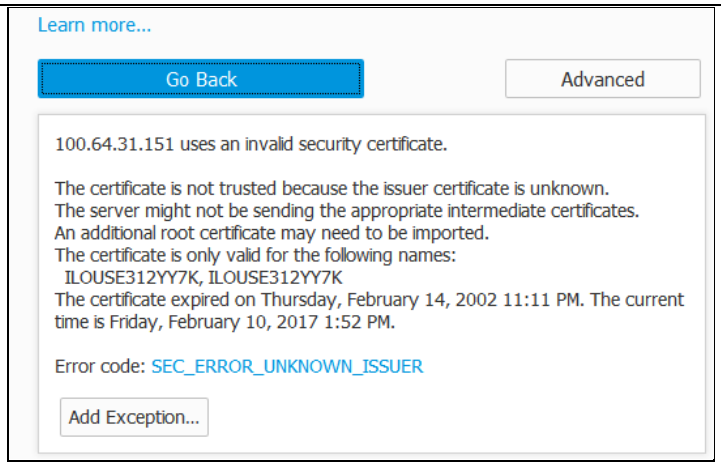
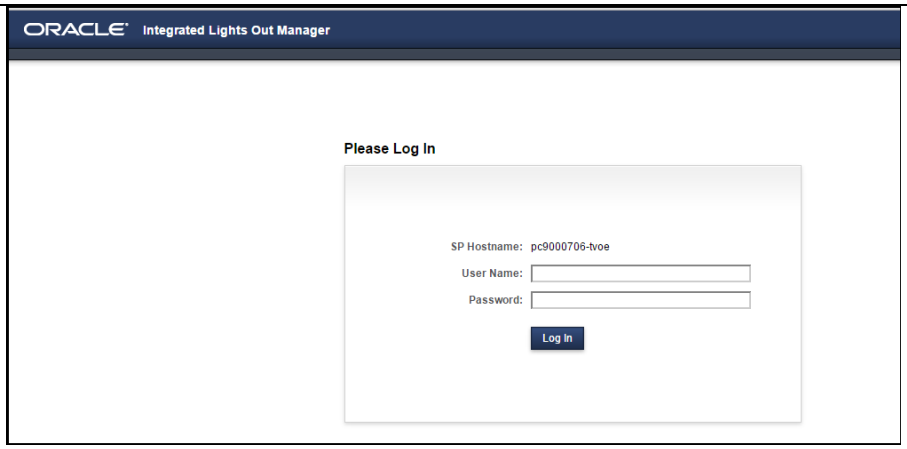
Step	Procedure	Result
8. ☐	The iLO Console window is displayed.	
---END OF PROCEDURE---		

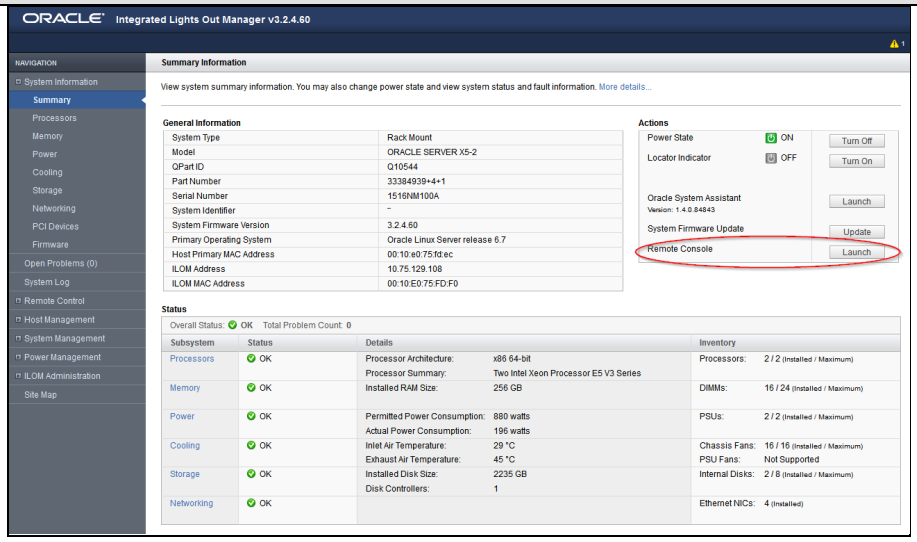
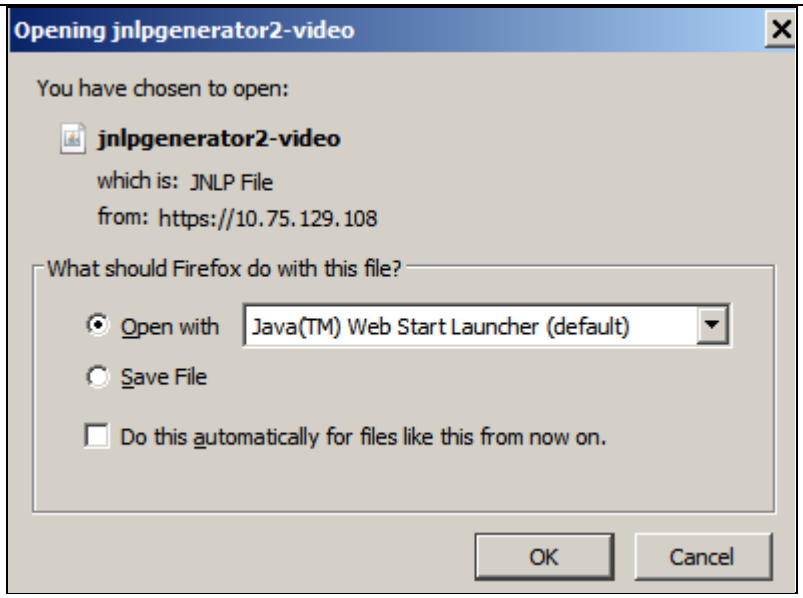
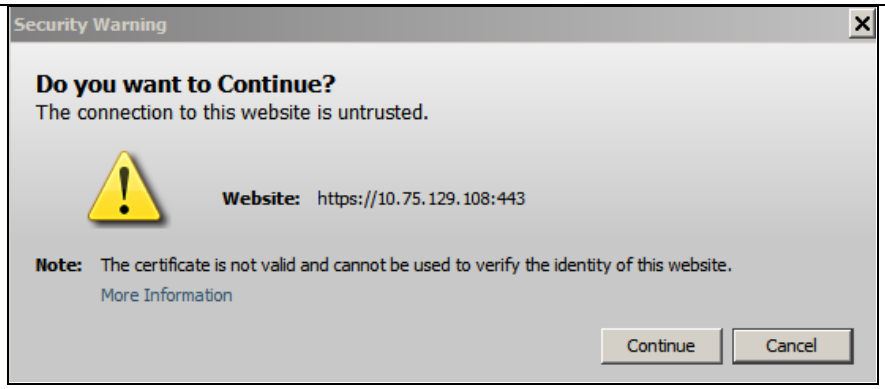
7.1.2 Accessing the ILOM VGA Redirection Window for Oracle RMS Servers

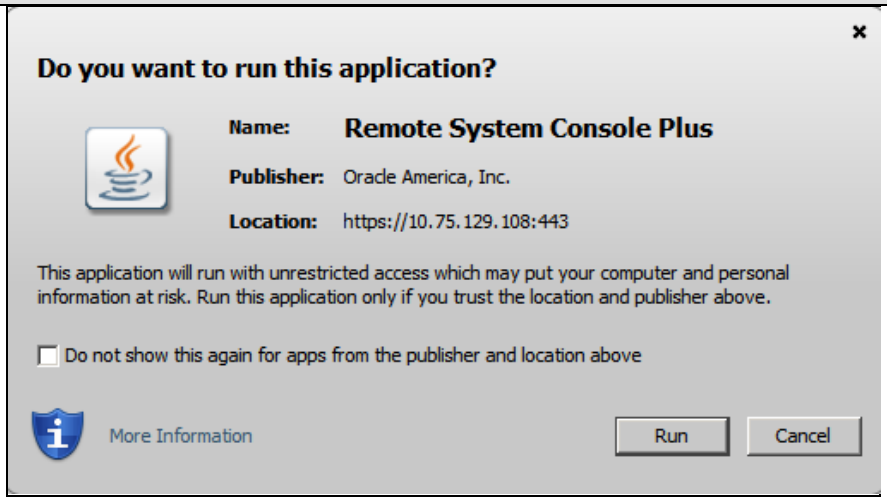
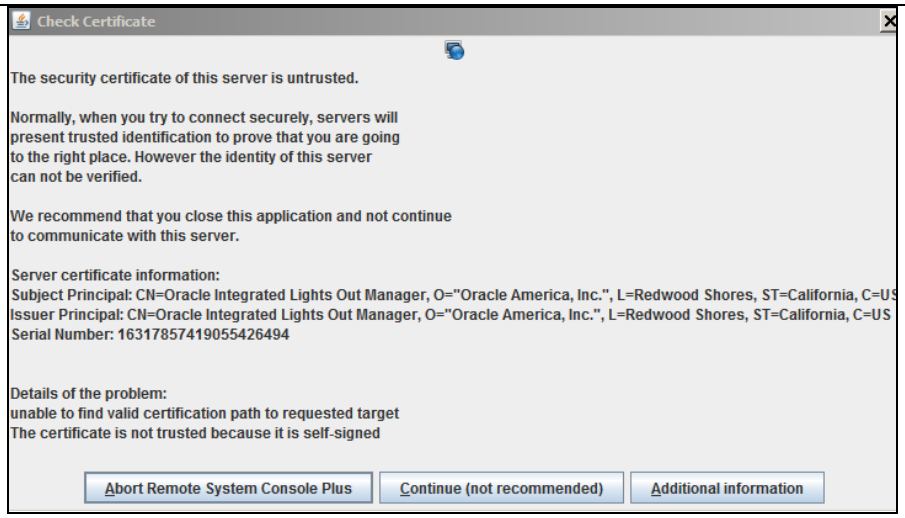
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

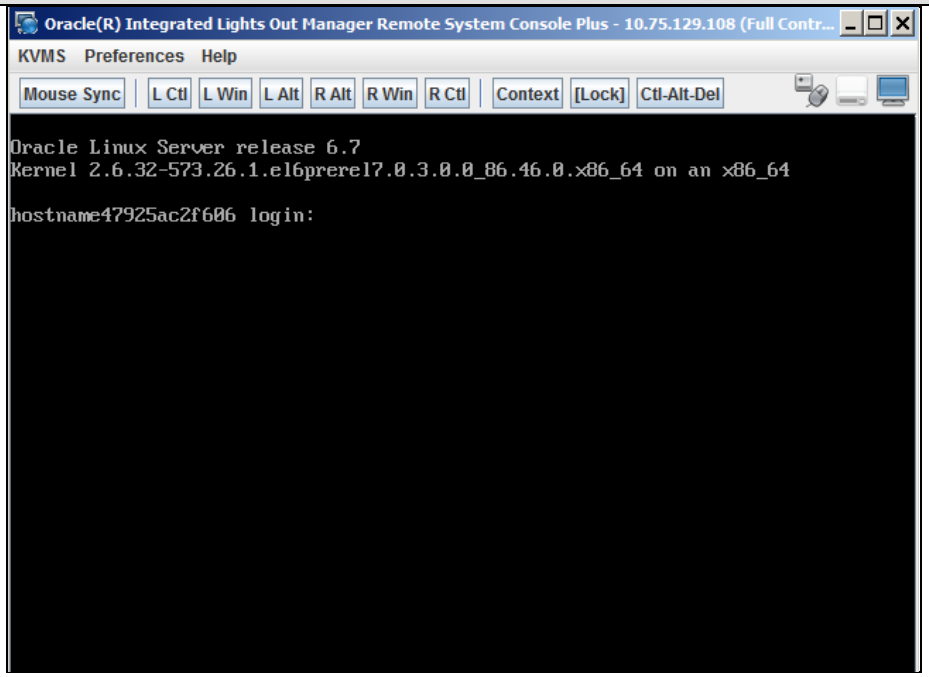
7.1.2: Accessing the ILOM VGA Redirection Window for Oracle RMS Servers

Step	Procedure	Result
1. ☐	Launch an approved web browser and connect to the iLO interface **NOTE:** Always use `https://` for iLO GUI access.	

Step	Procedure	Result
2. ☐	The first time the web browser connects to the iLO a warning message is displayed regarding the Security Certificate.	
3. ☐	1. Click **Advanced**. 2. Click **Add Exception**. 3. Click **Confirm Security Exception**.	
4. ☐	Login to the iLO console as Administrator.	

Step	Procedure	Result
5. ☐	The admin GUI is displayed. Click **Launch** for Remote Control from the right side of the page.	
6. ☐	Open Java Web Start when prompted.	
7. ☐	Click **Continue** if prompted.	

Step	Procedure	Result
8. ☐	Click **Run** if prompted.	
9. ☐	Click **Continue** if prompted.	

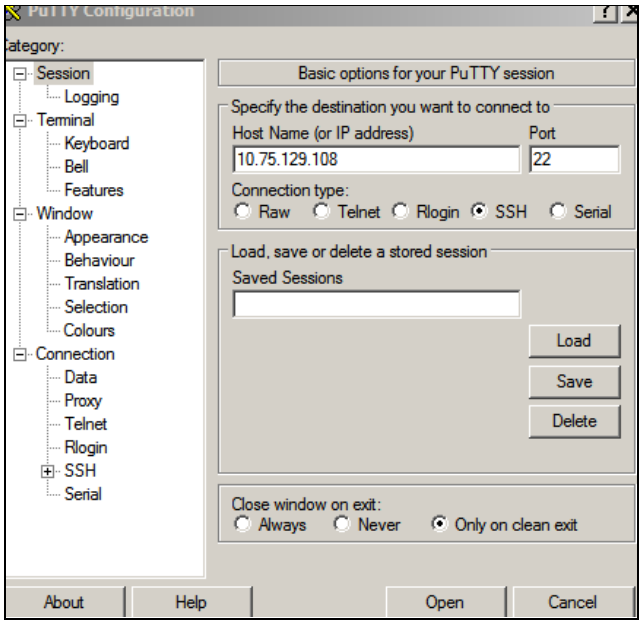
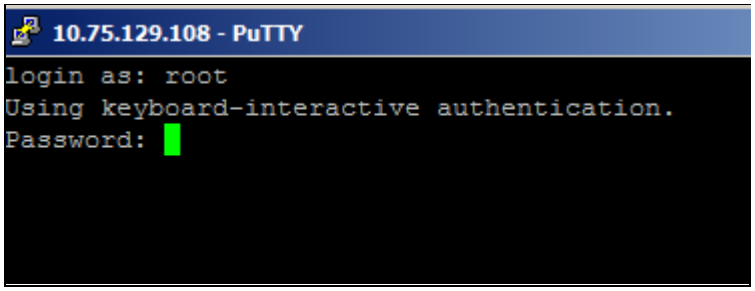
Step	Procedure	Result
10. ☐	The iLO Console window opens.	
---END OF PROCEDURE---		

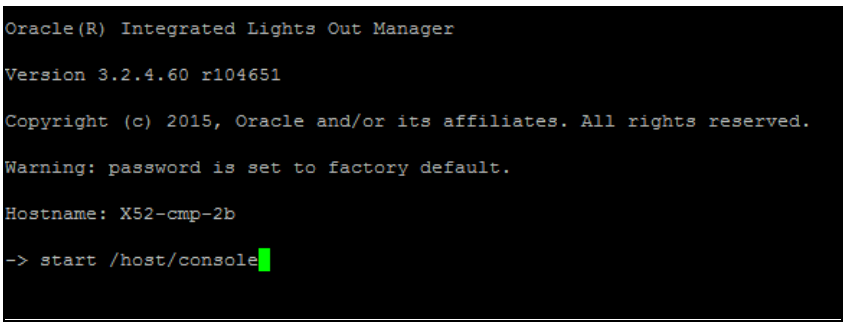
7.1.3 Accessing the ILOM Console for Oracle RMS Servers using SSH

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

7.1.3: Accessing the iLO Console for Oracle RMS Servers

Step	Procedure	Details

1. ☐	Login to the Server ILOM console with the **ssh** command.	Using putty or something similar-open an ssh session to ILOM of the target server using the ILOM IP address:
		 
		
		`login as: root`
		`Password:<root_password>`
		 

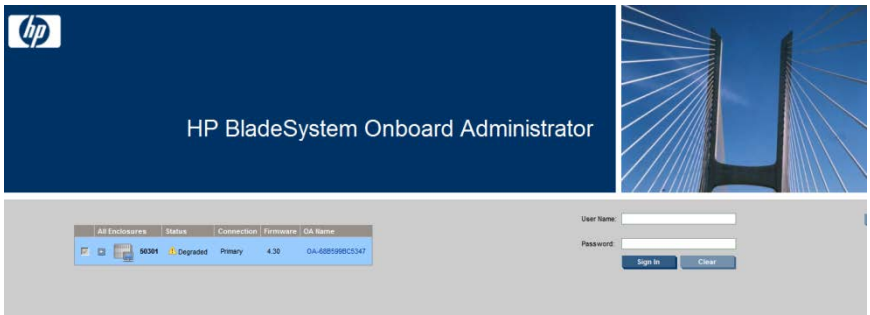
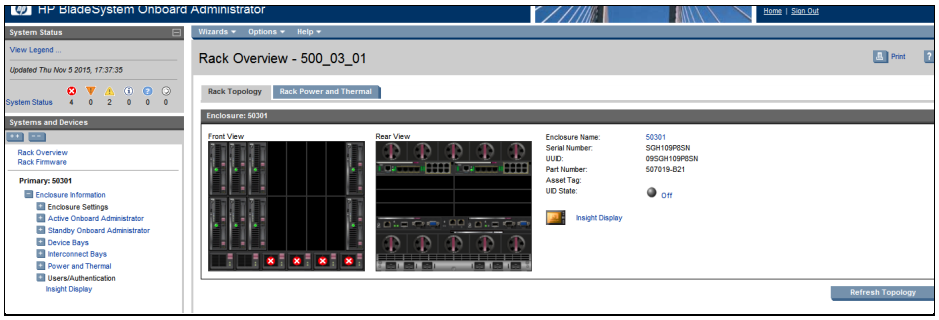
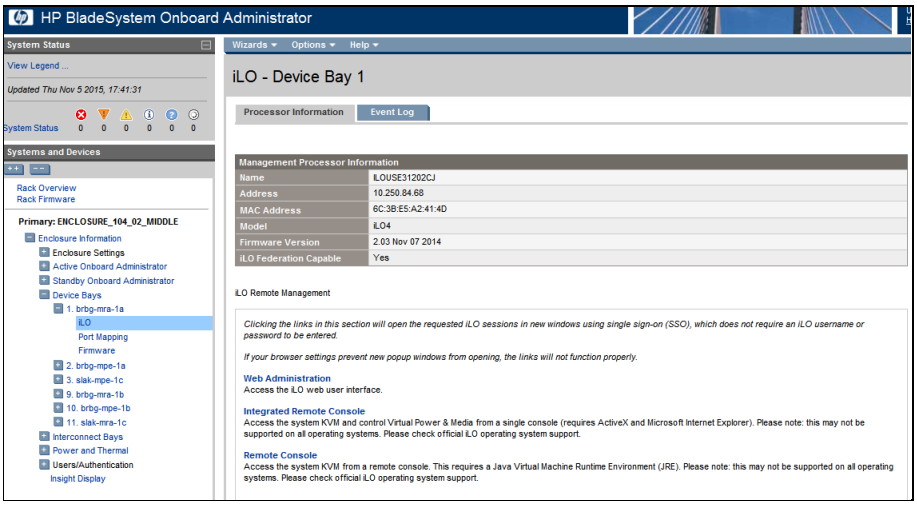
2. ☐	From the ILOM prompt:	Enter `start /host/console` at the → prompt to login into the server console. 

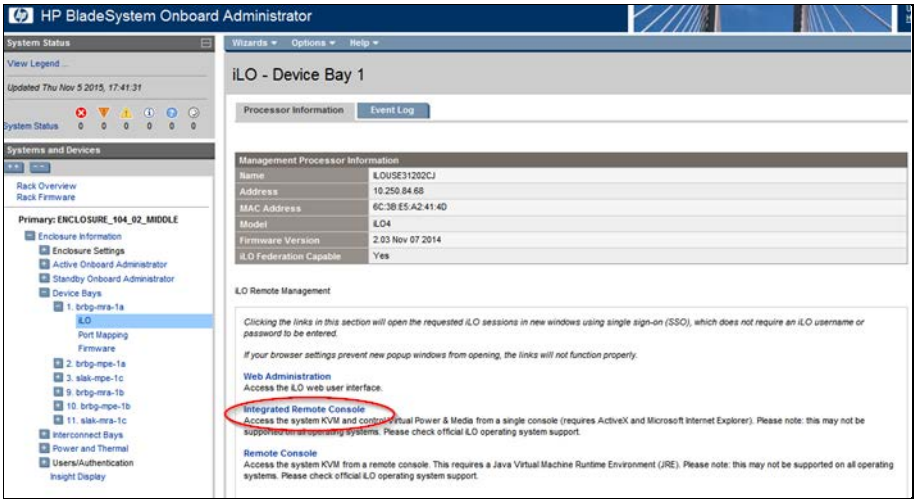
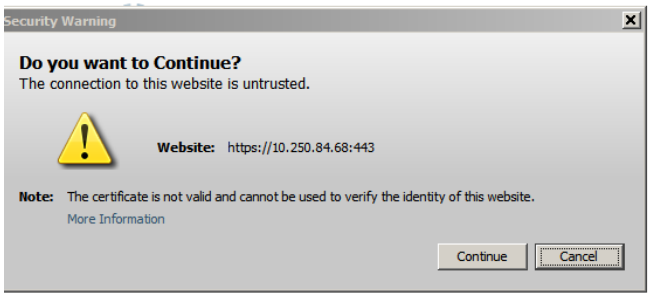
Step	Procedure	Details
3. ☐	From the ILOM prompt:	1. Answer `y` to confirm login to the console. `-> start /host/console` `Are you sure you want to start /HOST/console (y/n)? y` The prompt responds with the **`Serial Console Started`** message. `Serial console started.  To stop, type ESC (` 2. Press **Enter** to get the server prompt of the installed operating system. `Serial console started.  To stop, type ESC (` `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-2b login:` 3. Login to the server with the admusr user or any other appropriate login. `login: admusr` `Password:` `Last login: Wed Feb 8 15:28:10 from 10.154.117.232` `[admusr@X52-cmp-2b ~]$` **NOTE:** To exit the console press **Esc (** `Serial console started. To stop, type ESC (`
---END OF PROCEDURE---		

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

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

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

Step	Procedure	Details
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. 
3. ☐	**Web Browser:** Open the iLO form for the server blade you wish to connect to	1. From the navigation pane, select **Device Bays.** 2. Click the expand buttonfor the device. 3. Click the iLO link. 

4. ☐	**Web Browser:** Click the remote Console link	Click the **Remote Console** link, and a browser window opens.  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.  You must click **Continue** or **Yes** to proceed.
5. ☐	**Web Browser**	After a few moments, the *iLO Intergrated Remote Console* window opens. 
---END OF PROCEDURE---		

7.2 Mounting Media (Image Files)

7.2.1 Mounting Physical Media (RMS only)

This procedure contains steps to mount electronic and physical media on HP rack mount servers.

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

7.2.1: Mounting Physical Media on HP Rack Mount Servers

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

2. ☐	1. Access the command prompt.
	2. Log into the server as the root user.
		`CentOS release 5.6 (Final)`
		`Kernel 2.6.18-238.19.1.el5prerel5.0.0_72.22.0 on an x86_64`
		`hostname1260476221 login: root`
		`Password: <root_password>`

3. ☐	**HP Server:** Insert the USB flash drive containing the server configuration file into the USB port on the front panel of HP Server.	 **Figure 1 -HP DL380 Front Panel: USB Port**

4. ☐	**HP Server:** Output similar to that shown on the right will appear as the USB flash drive is inserted into the HP Server front USB port.
	Press **Enter** to return to the command prompt.
		`[root@hostname1260476099 ~]# sd 3:0:0:0: [sdb] Assuming drive cache: write through`
		`sd 3:0:0:0: [sdb] Assuming drive cache: write through <ENTER>`
		`[root@hostname1260476099 ~]#`

Step	Procedure	Details

5. ☐	**HP Server:** Verify that the partition of the USB flash drive has been mounted by the OS: Search **df** for the device named in the output of the previous step.	`[root@hostname1260476099 ~]# df |grep sdb`
		`/dev/sdb1  2003076  82003068 1% /media/sdb1`
		`[root@hostname1260476099 ~]#`

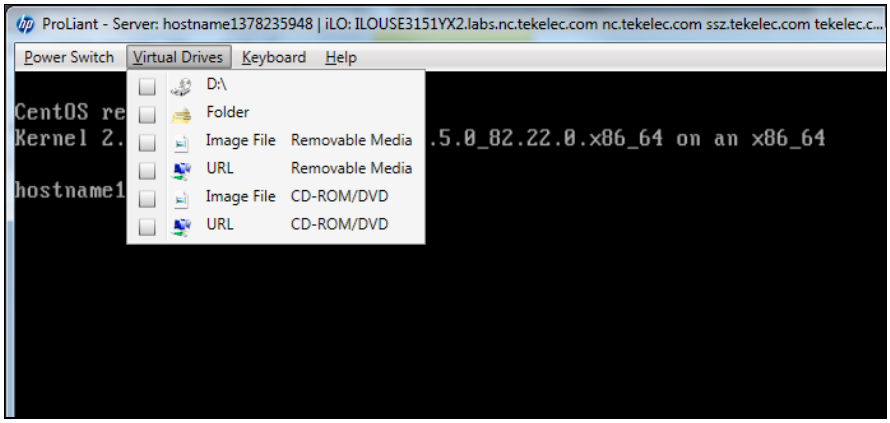
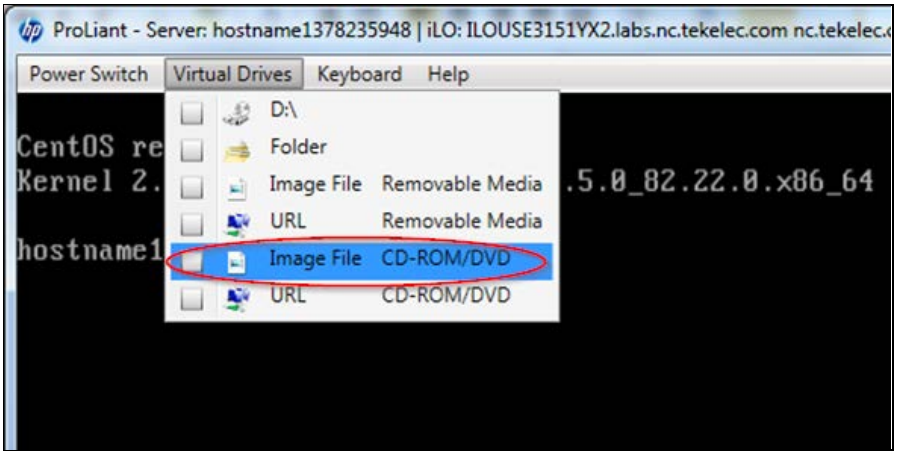
6. ☐	**HP Server:** USB media may be accessed via the path shown	`[root@hostname1260476099 ~]# cd /media/sdb1` `[root@hostname1260476099 ~]#`
7. ☐	**HP Server:** When you are finished using the mounted drive, remove the USB flash drive from the USB port on the front panel of the server.	 **Figure 2 -HP DL380 Front Panel: USB Port**
---END OF PROCEDURE---		

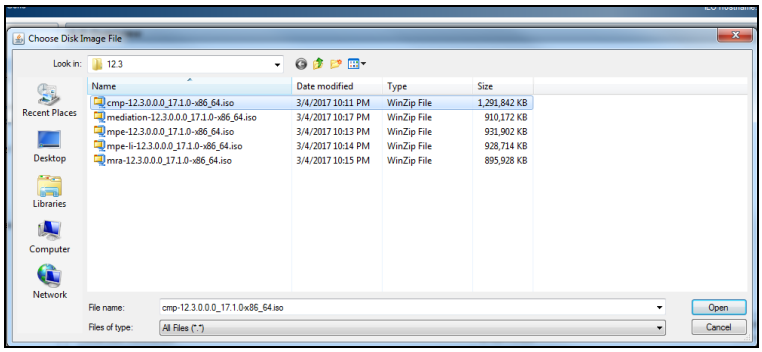
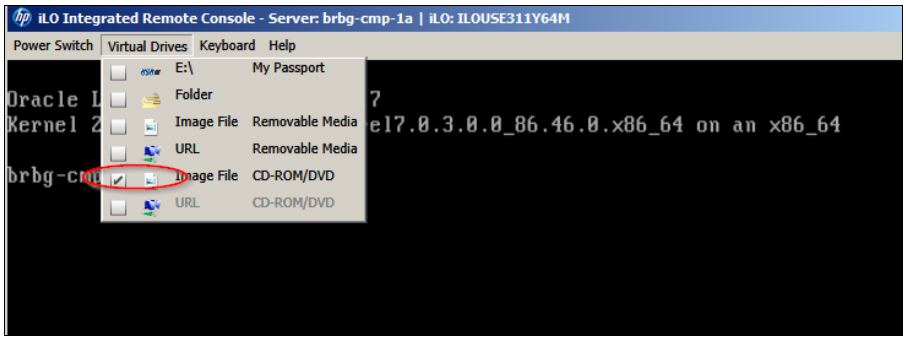
7.2.2 Mounting Virtual Media on HP Servers

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

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

7.2.2: Mounting Virtual Media on HP Rack Mount Servers

Step	Procedure	Details
1. ☐	Access the ILO VGA for the server.	Connect to the ILO VGA server using the access method described Section 7.1.1
2. ☐	**ILO Remote Console:** Select **Virtual Drives** from the top menu bar.	
3. ☐	**HP Server:** Select from the menu options: **Image File CD-ROM/DVD** to access a bootable iso image file on your laptop client machine. **URL CD-ROM/DVD** to access a bootable iso image file on the network.	Select **Image File CD-ROM/DVD**. 

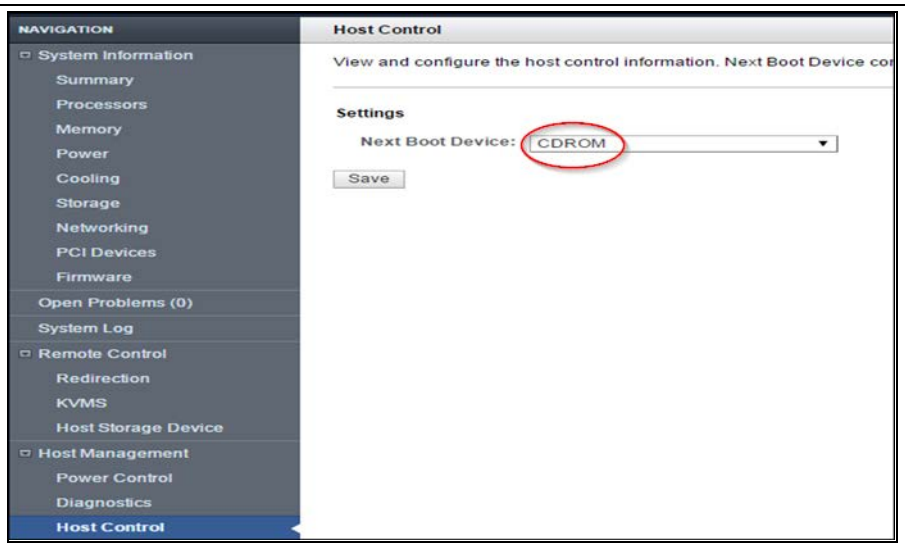
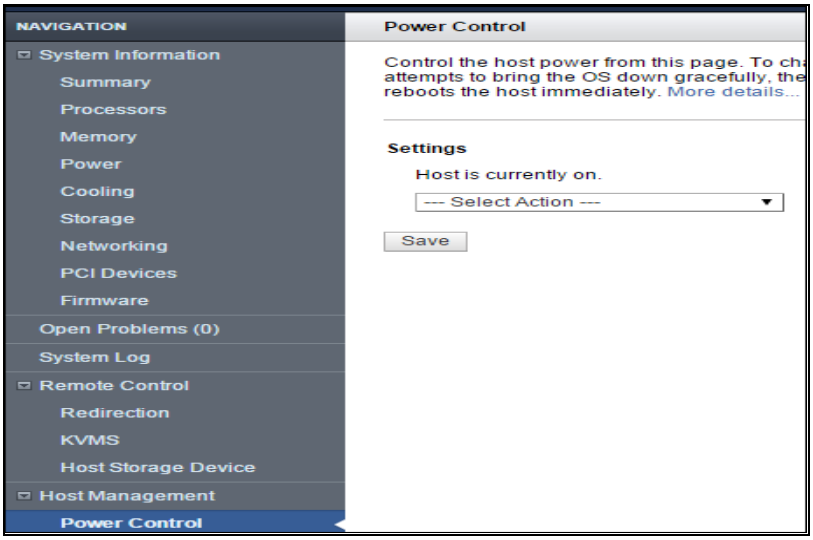
Step	Procedure	Details
4. ☐	**HP Server:** Select an image file to mount	A window opens to browse the client workstation or laptop.  Select the image file and click **Open**.
5. ☐	**HP Server:** Confirm the target image file has been mounted	Return to the Virtual Drives menu and the **Image File CD-ROM/DVD** option is checked indicating that the image file has been mounted. 
---END OF PROCEDURE---		

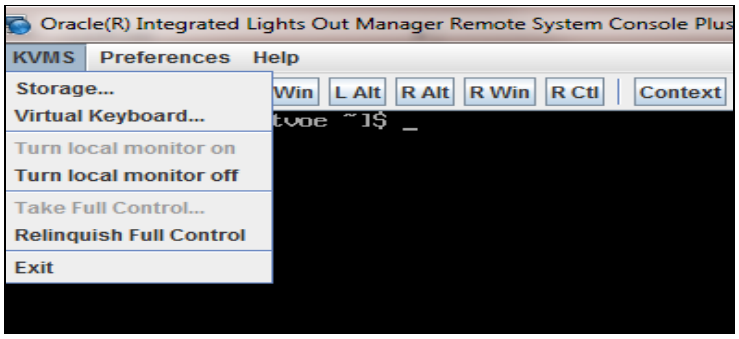
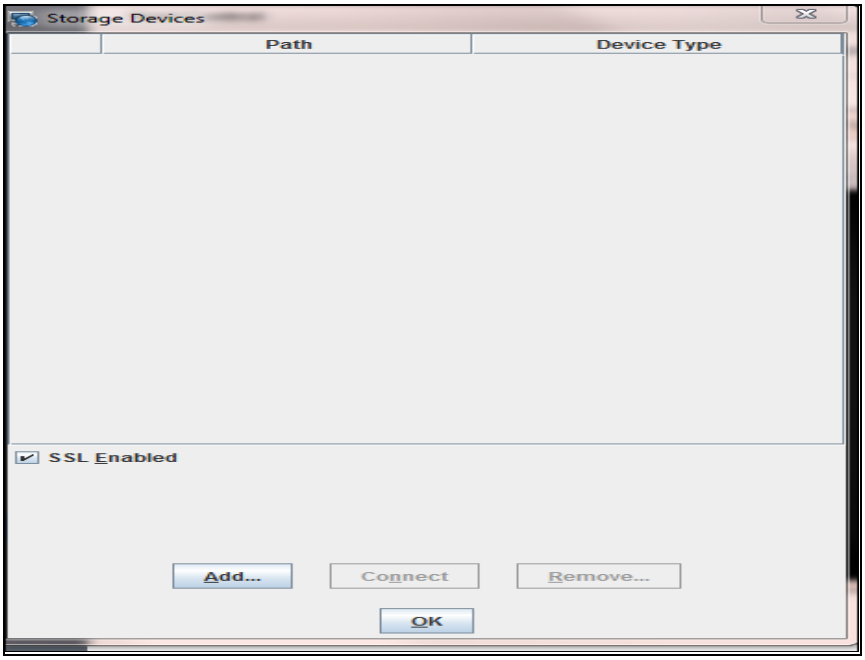
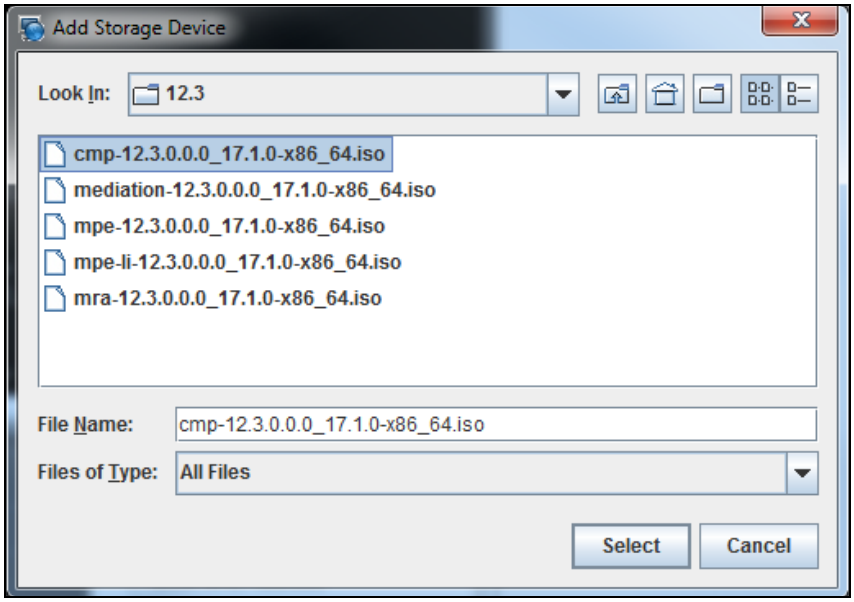
7.2.3 Mounting Virtual Media on Oracle RMS Servers

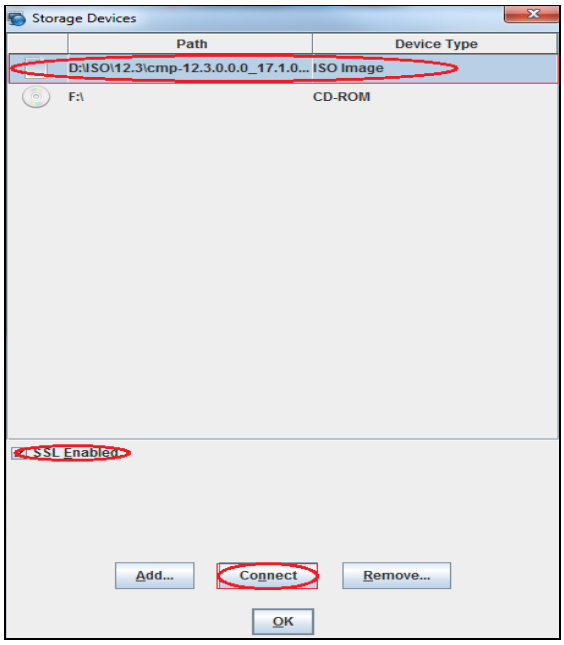
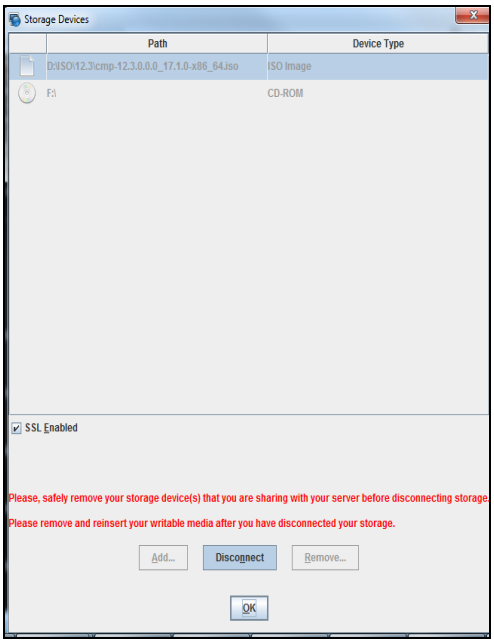
This procedure mounts the virtual media on Oracle RMS servers via the ILOM, for ISO access or other file transfer.

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

7.2.3: Mounting Virtual Media on Oracle RMS Servers

Step	Procedure	Details
1. ☐	Access the ILO VGA for the server.	Connect to the ILO VGA for the server using the access method described in Section 7.1.2.
2. ☐	**ILO Admin GUI:** Change the Next Boot Device. 1. Select **Host Management → Host Control**. 2. Select **CDROM** from the Next Boot Device list. 3. Click **Save**.	
3. ☐	**ILO Admin GUI:** 1. Go to **Host Management → Power Control**. 2. Verify that Host is currently on. **NOTE:** If it is turned off, turn it back on.	

Step	Procedure	Details
4. ☐	**ILO Remote Console:** 1. Select **KMVS → Storage** from the top menu bar. 2. Click **Add** near the bottom of the next page.	 
5. ☐	**ILO Remote Console:** Select the Image File from files on your laptop or desktop client machine.	

Step	Procedure	Details
6.	**ILO Remote Console:** 1. Select the ISO file. 2. Uncheck **SSL Enabled** before connecting to the TVOE ISO file. 3. Click **Connect**. 4. Click **OK.**	 
---END OF PROCEDURE---		

7.3 Hardware Setup (Bios Configuration)

Reference material:

TPD Initial Product Manufacture, Release 6.7.2+

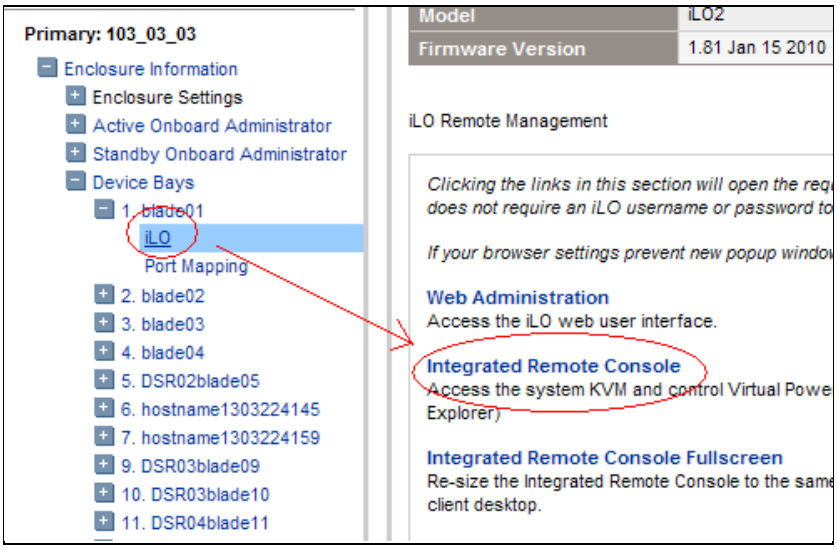
Tekelec Platform 7.0.x Configuration Guide

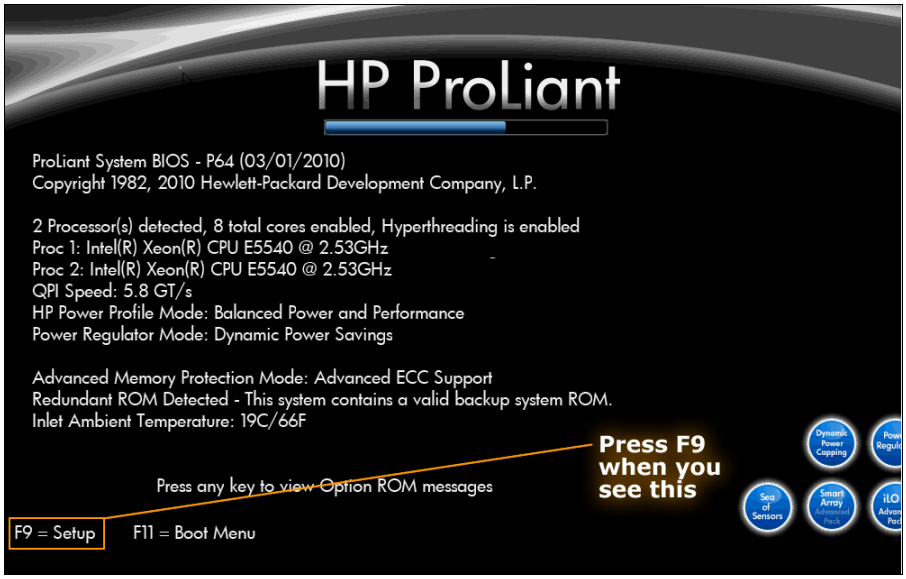
7.3.1 BIOS Settings for HP Gen 8 Blade and Rack Mount Servers

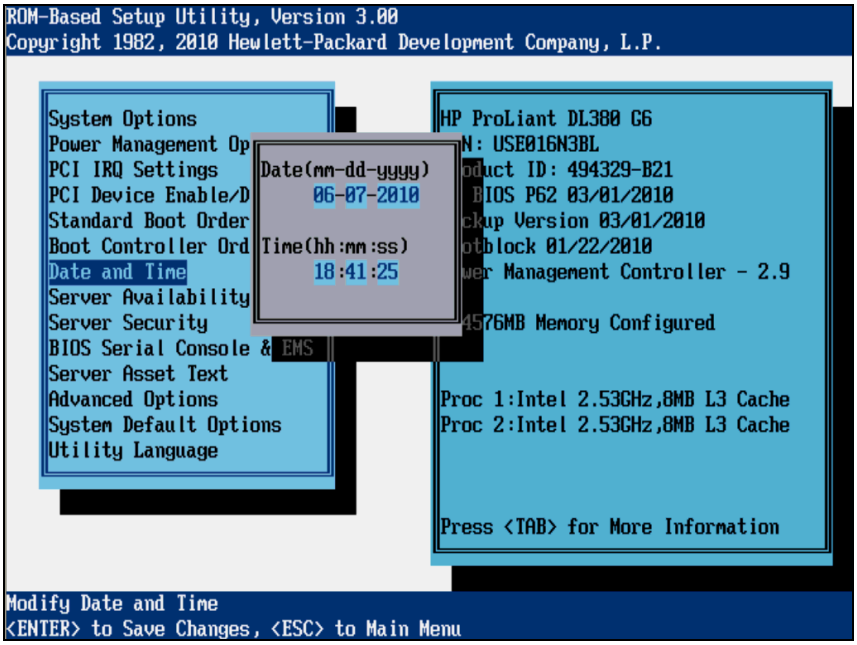
This procedure configures HP BIOS settings for Gen 8 Blade and RMS.

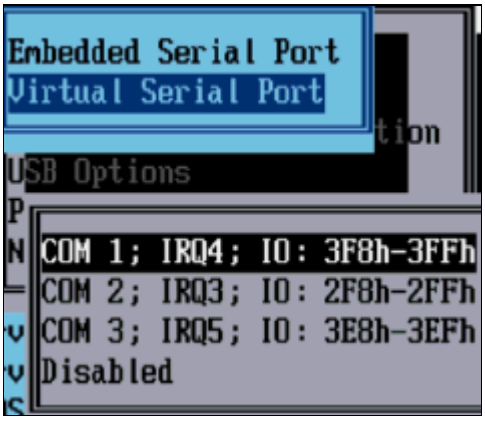
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

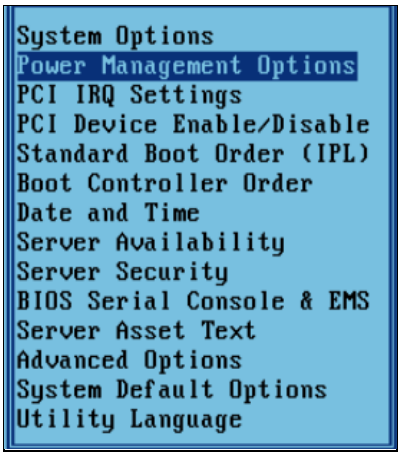
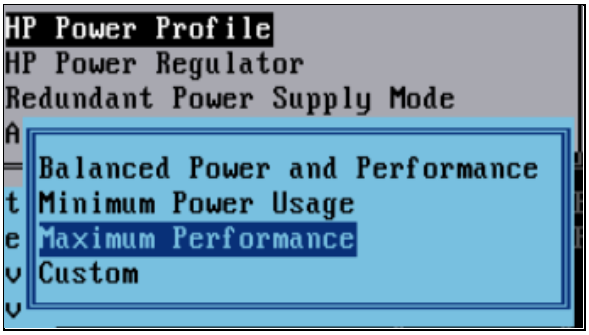
7.3.1: BIOS Settings for HP Gen 8 Blade and Rack Mount Servers

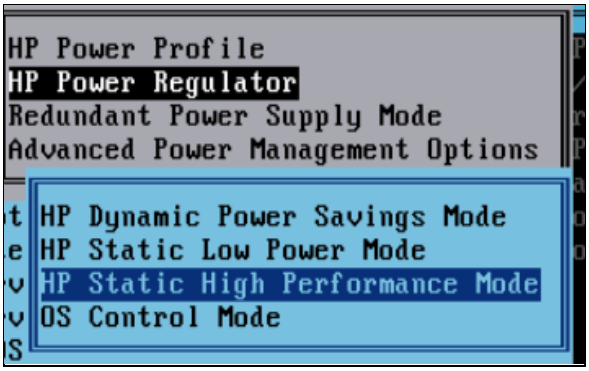
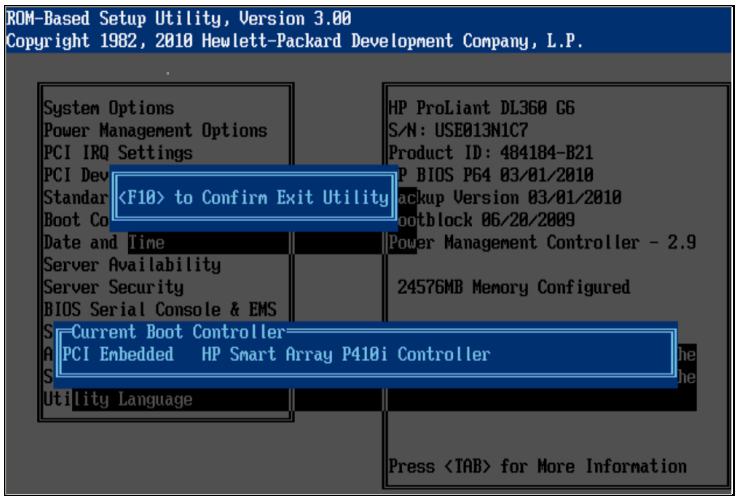
Step	Procedure	Details
1. ☐	Access the console for the HP server.	Connect to the console for the server using one of the access methods described in Section 7.1.1.
2. ☐	Access the console for the HP server according to its hardware type.	For Rack Mount Servers (RMS), connect to the console for the server 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.

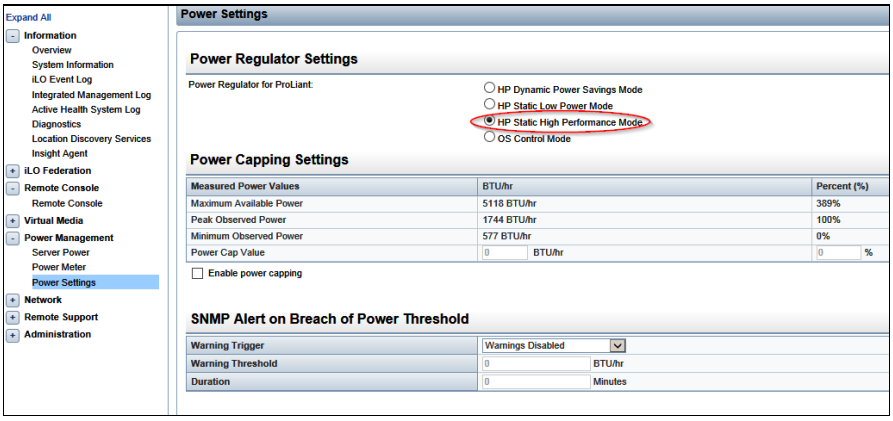
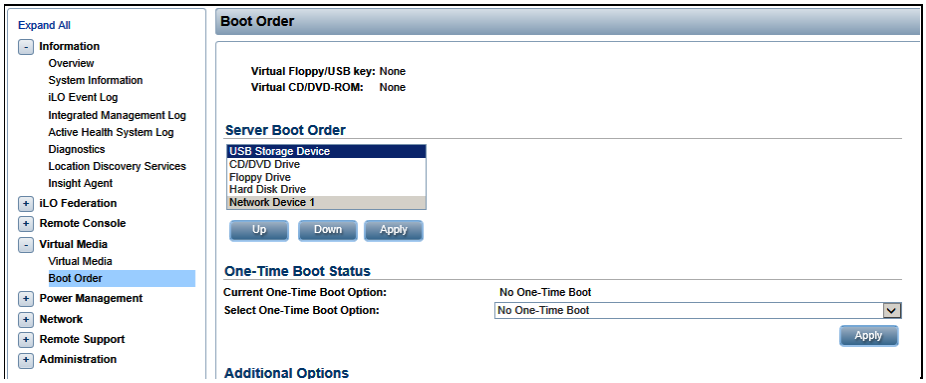
Step	Procedure	Details
3. ☐	Access the Server BIOS	Reboot the server. • For Blade and RMS: This can be achieved by selecting **Cold Boot** from the **Power Management → Server Power** menu of the Integrated Console. • For RMS: This can also be achieved by pressing and holding the power button until the 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 page, press **F9** to access the BIOS setup page. You may be required to press **F9** two or three times. The **`F9=Setup`** changes to **`F9 Pressed`** after it is accepted.  **Expected Result:** ROM-Based Setup Utility is accessed and the *ROM-Based Setup Utility* menu displays.

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

Step	Procedure	Details
5. ☐	**(RMS Only)** Configure iLO serial port settings	For RMS only, the serial ports on HP DL360 G8 rack mount servers must 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 has not been completed correctly and the server rebooted, the `syscheck -v hardware serial` test fails. 1. Select **System Options** and press **Enter**. 2. Select **Serial Port Options** and press **Enter**. 3. Change Embedded Serial Port to COM2 and press **Enter**.  4. Change Virtual Serial Port to COM1 and press **Enter**.  5. Press Esc two times.

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** and press **Enter**.  2. Select **HP Power Profile** 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. Still in the **Power Management Options** Select **HP Power Regulator** option and press **Enter**. **NOTE:** A note may appear to say certain processors support only one power state. If this appears, press **Esc** to clear it. Change setting to 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.

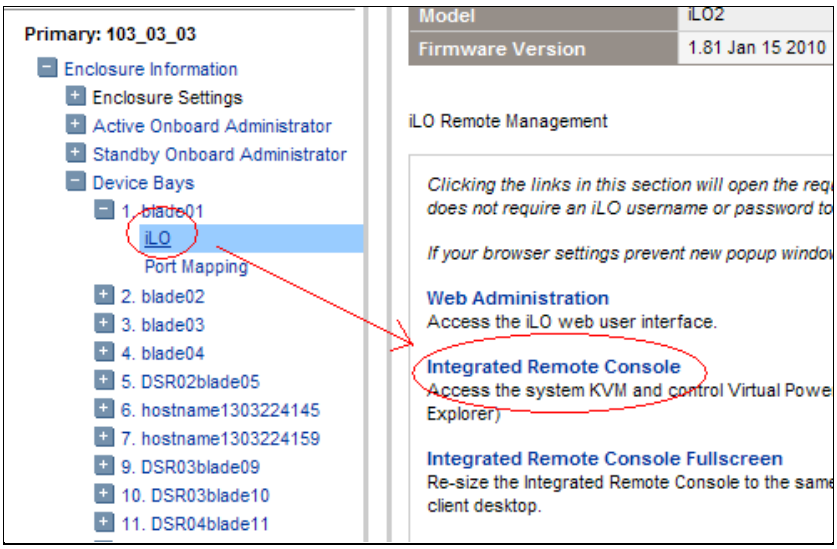
Step	Procedure	Details
9. ☐	Confirm the Power Regulator setting for the HP server.	If not connected to the iLO for the server, connect using 7.1.1 Accessing the iLO VGA Redirection Window for HP. From the iLo on the HP server: 1. Navigate to **Power Management → Power Settings**. 2. Confirm Power Regulator 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 should look like the above snapshot unless the customer has specified otherwise.
---END OF PROCEDURE---		

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

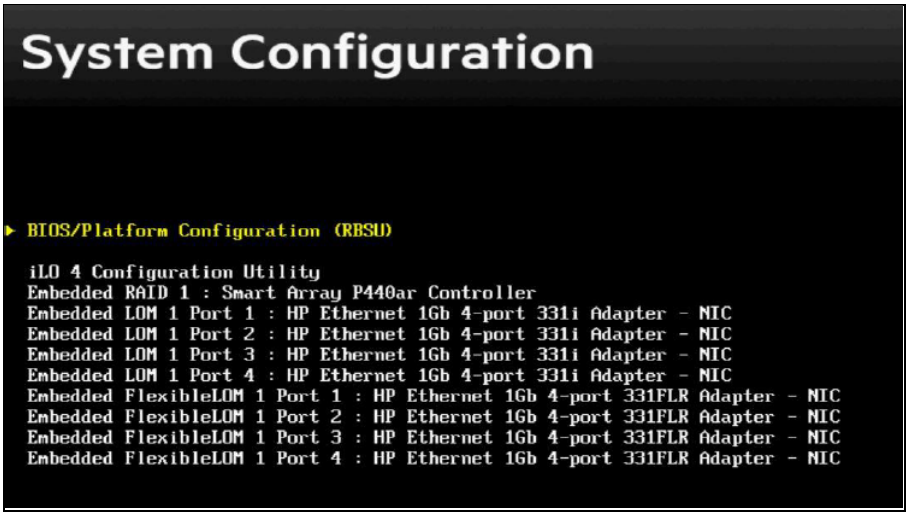
This procedure configures BIOS settings for HP hardware.

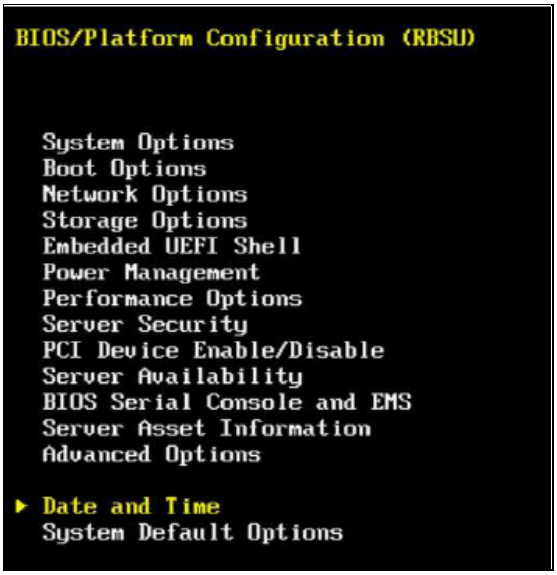
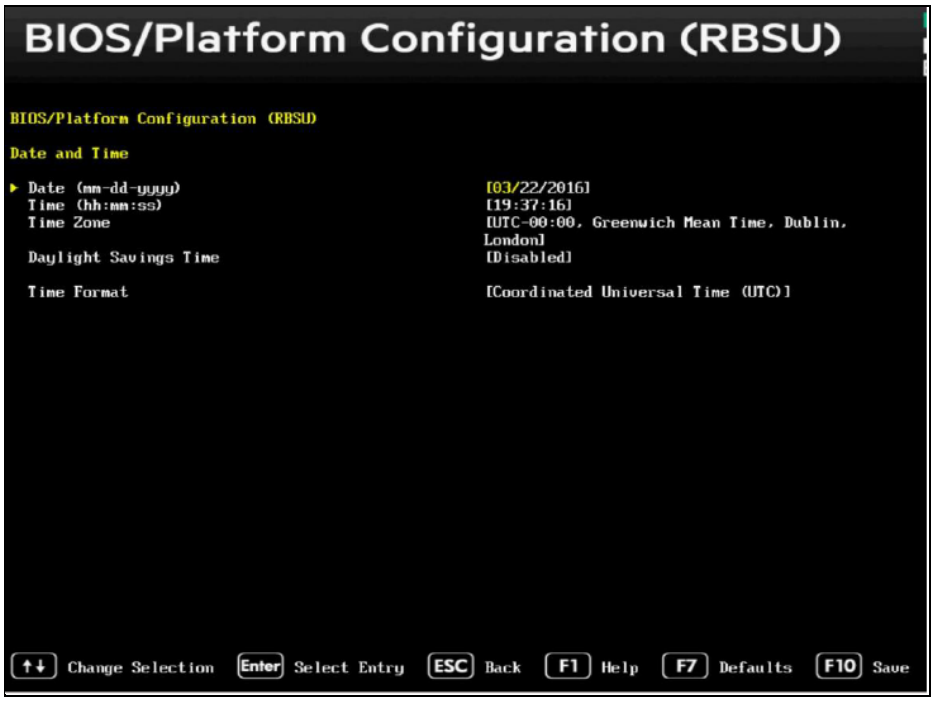
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

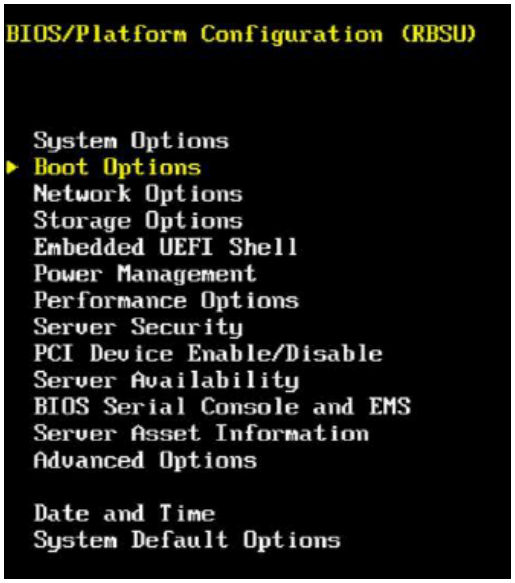
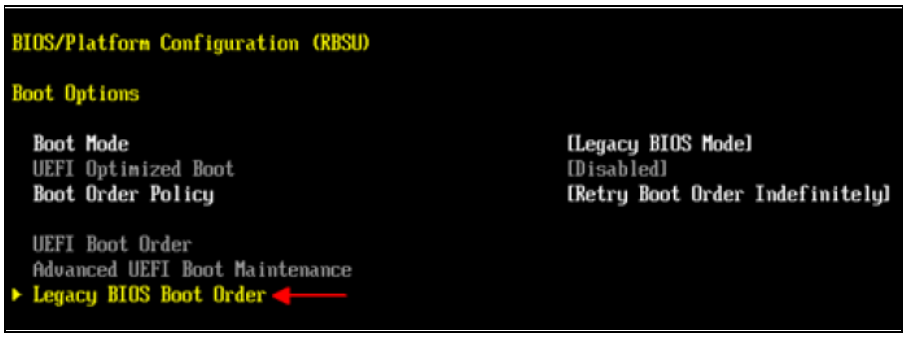
7.3.2 BIOS Settings for HP Gen 9 Blade and Rack Mount Servers

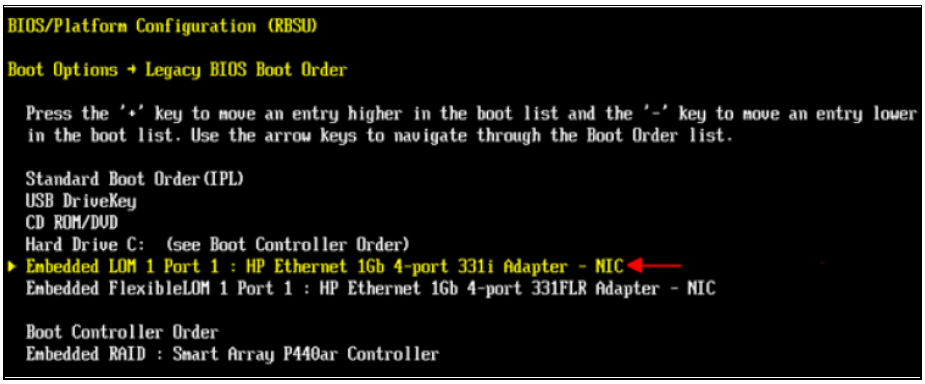
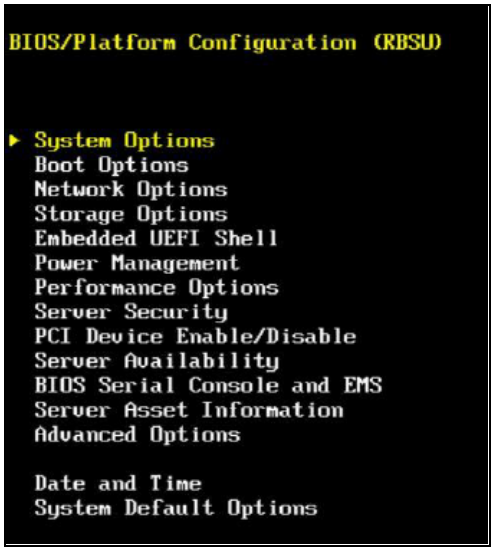
Step	Procedure	Details
1. ☐	Access the console for the HP server.	Connect to the console for the server using one of the access methods described in Section 7.1.1
2. ☐	Access the console for the HP server according to its hardware type	For Rack Mount Servers (RMS), connect to the console for the server 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. 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 instructions.

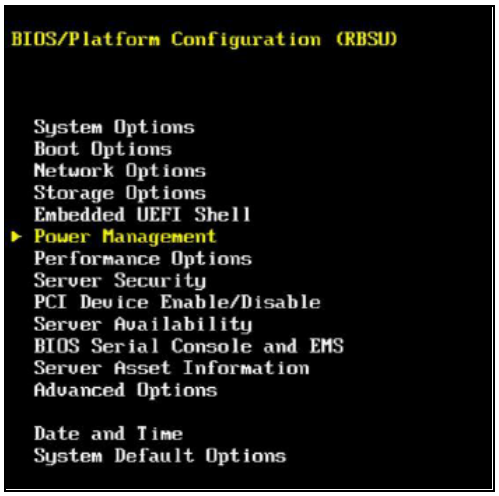
Step	Procedure	Details
3. ☐	Access the Server BIOS	Reboot the server. • For Blade and RMS: This can be achieved by selecting **Cold Boot** from the **Power Management → Server Power** menu of the Integrated Console. • For RMS: This can be achieved by pressing and holding the power button until the server 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 page, press **F9** to access the BIOS setup page. You may be required to press **F9** two to three times. The **`F9=Setup`** changes to **`F9 Pressed`** after it is accepted.  **Expected Result:** *System Utilities* page displays.

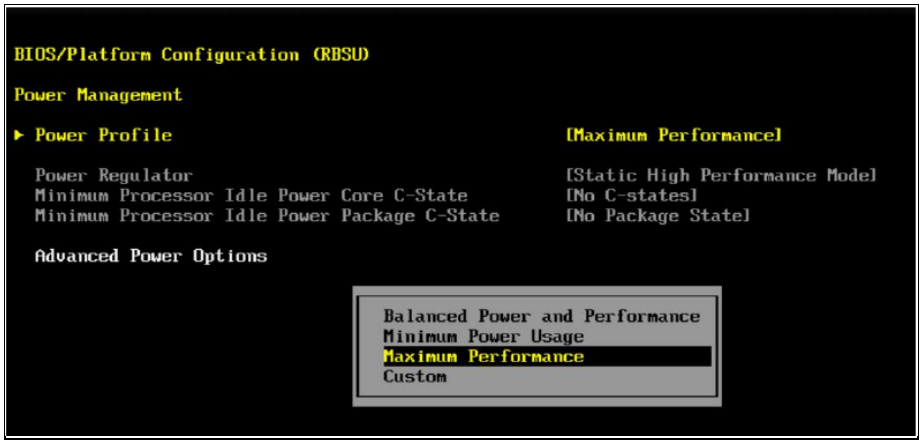
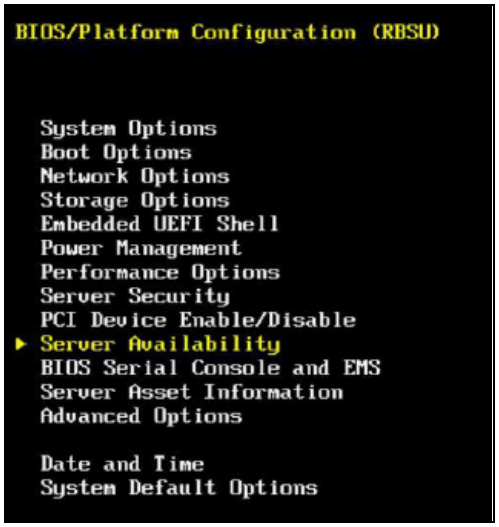
Step	Procedure	Details
4. ☐	System Utilities Configuration	From the *System Utilities* page, select **System Configuration**, then click Enter. 
5. ☐	System Utilities Configuration	From the *System Configuration* page, select **BIOS/Platform Configuration (RBSU)**, and click **Enter**. 

Step	Procedure	Details
6. ☐	System Utilities Configuration	From the *Bios/Platform Configuration* page, select **Date and Time** and press **Enter**. 
7. ☐	System Utilities Configuration	1. From the *Date and Time* list, set: a. Date and Time to the correct UTC (Greenwich Mean Time) b. Time Zone to UTC c. Time Format to Coordinated Universal Time (UTC) 2. Press **F10** to save your changes. 3. Press **Esc** to return to the *Bios/Platform Configuration* page. 

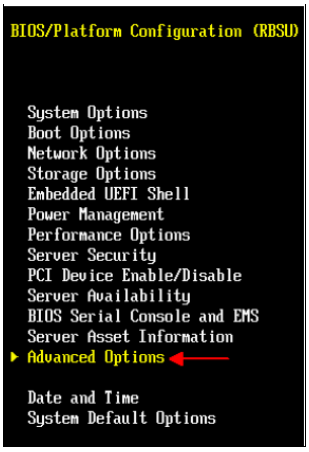
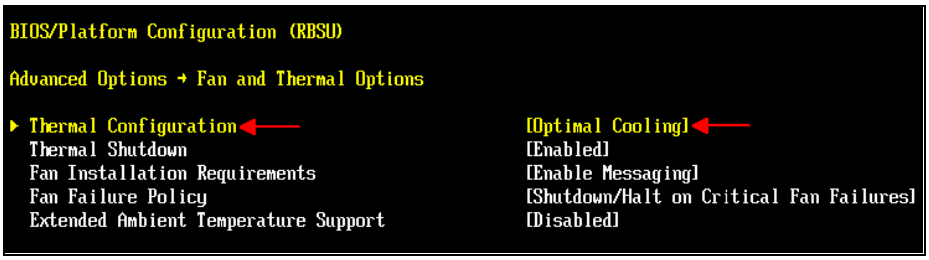
Step	Procedure	Details
8. ☐	System Utilities Configuration	From the *Bios/Platform Configuration* page, select **Boot Options** and press **Enter**. 
9. ☐	System Utilities Configuration	1. From the *Boot Options* list, set: a. Boot Mode to Legacy BIOS Mode b. UEFI Optimized Boot to Disabled c. Boot Order Policy to Retry Boot Order Indefinitely. 2. Press **F10** to save your changes. 3. Select the Legacy BIOS Boot Order option and press **Enter**. 

Step	Procedure	Details
10. ☐	System Utilities Configuration	1. From the *Legacy BIOS Boot Order Option* page, 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 press **F10** to save your changes. 2. Press **Esc** to return to the *Boot Options* page. 
11. ☐	System Utilities Configuration	1. Press **Esc** again to return to the *Bios/Platform Configuration* page. 2. Select **System Options.** 3. Press **Enter**. 

Step	Procedure	Details
12. ☐	System Utilities Configuration	From the *System Options* page, select **Serial Port Options** and press **Enter**. 
13. ☐	System Utilities Configuration	1. From the *Serial Port Options* page, set: a. Embedded Serial Port to **COM2.** b. Virtual Serial Port to **COM1.** 2. Press **F10** to save your changes. 3. Press **Esc** twice to return to the *Bios/Platform Configuration* page. 
14. ☐	System Utilities Configuration	1. From the *Bios/Platform Configuration* page. 2. Select **Power Management**. 3. Press **Enter**. 

Step	Procedure	Details
15. ☐	System Utilities Configuration	1. From the *Power Management* page, set **Power Profile to Maximum Performance**. 2. Press **F10** to save your changes. 3. Press **Esc** to return to the *Bios/Platform Configuration* page. 
16. ☐	System Utilities Configuration	From the *Bios/Platform Configuration* page, select **Server Availability** option and press **Enter**. 

Step	Procedure	Details
17. ☐	System Utilities Configuration	From the *Server Availability* page, set ASR Status to **Enabled**. BIOS/Platform Configuration (RBSU) Server Availability ▸ ASR Status [Enabled] ASR Timeout [10 Minutes] Wake-On LAN [Enabled] POST F1 Prompt [Delayed 20 seconds] Power Button Mode [Enabled] Automatic Power-On [Always Power on] Power-On Delay [No Delay]
18. ☐	System Utilities Configuration	Set POST F1 Prompt to **Delayed 20 seconds**. BIOS/Platform Configuration (RBSU) Server Availability ASR Status [Enabled] ASR Timeout [10 Minutes] Wake-On LAN [Enabled] ▸ POST F1 Prompt [Delayed 20 seconds] Power Button Mode [Enabled] Automatic Power-On [Always Power on] Power-On Delay [No Delay]
19. ☐	System Utilities Configuration	Set Power-On Delay to **No Delay**. BIOS/Platform Configuration (RBSU) Server Availability ASR Status [Enabled] ASR Timeout [10 Minutes] Wake-On LAN [Enabled] POST F1 Prompt [Delayed 20 seconds] Power Button Mode [Enabled] Automatic Power-On [Always Power on] ▸ Power-On Delay [No Delay]

Step	Procedure	Details
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* page. 
21. ☐	System Utilities Configuration	From the *Bios/Platform Configuration* page, 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* page.  4. Press **Esc** to return to the *System Utilities* page.

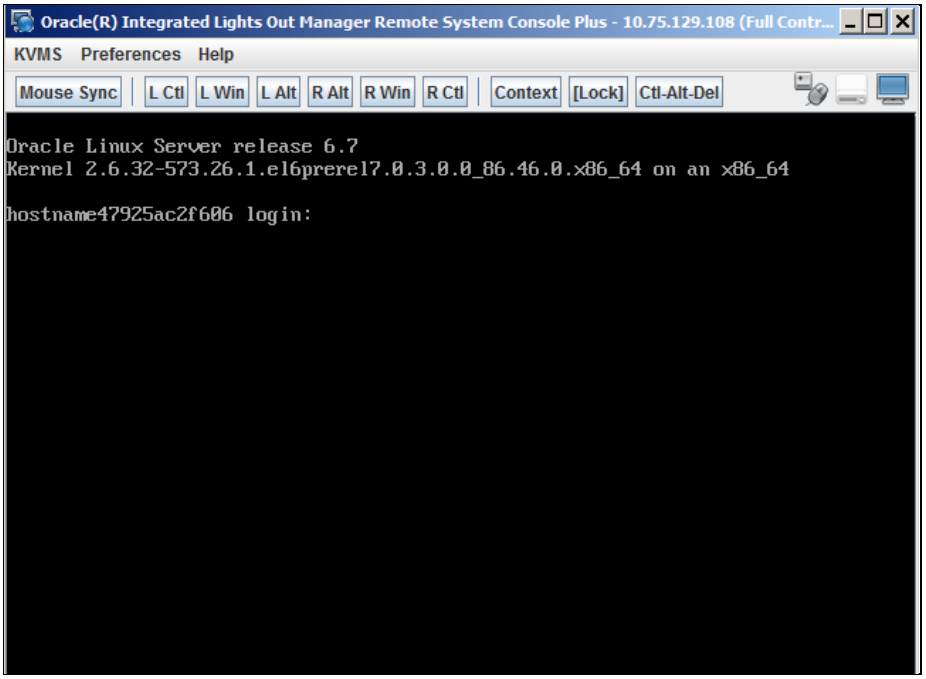
Step	Procedure	Details
---END OF PROCEDURE---		

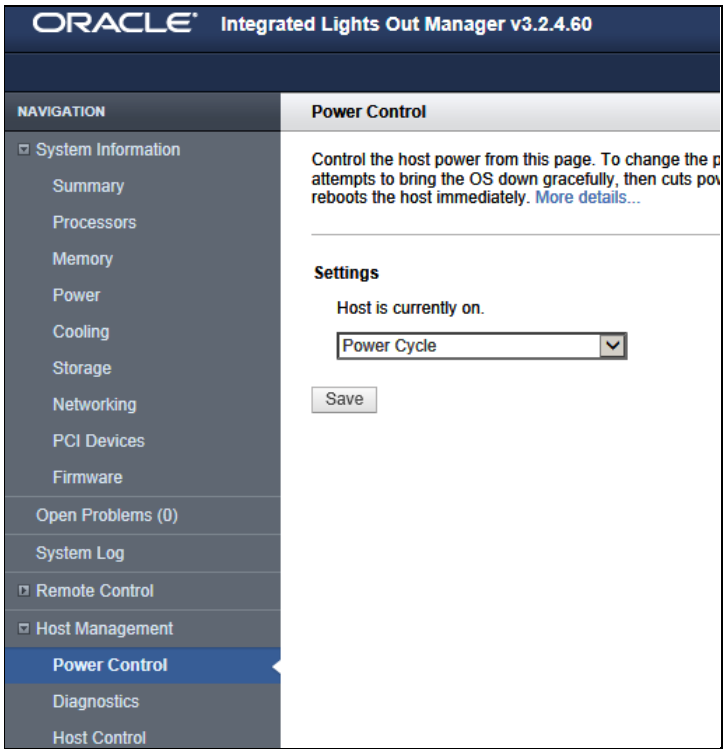
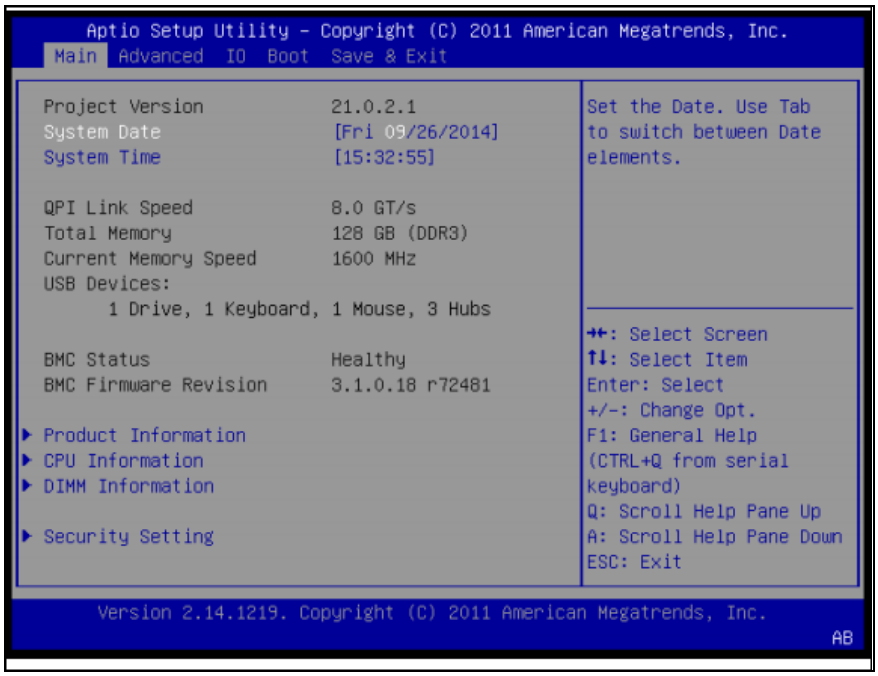
7.3.3 BIOS Settings for Oracle RMS Servers

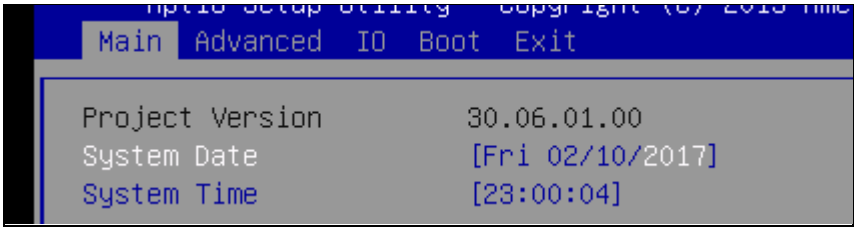
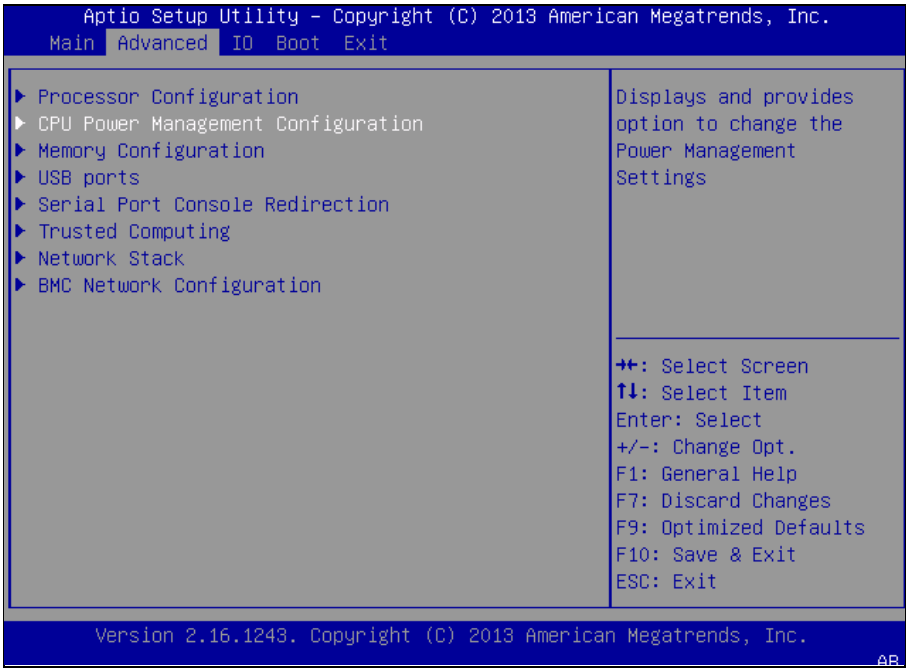
This procedure configures BIOS settings for Oracle Rack Mount Servers hardware.

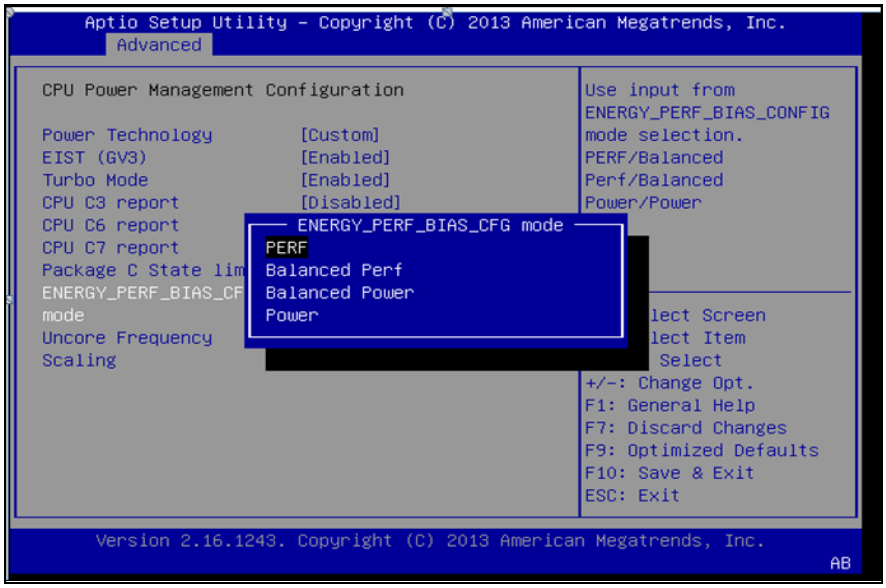
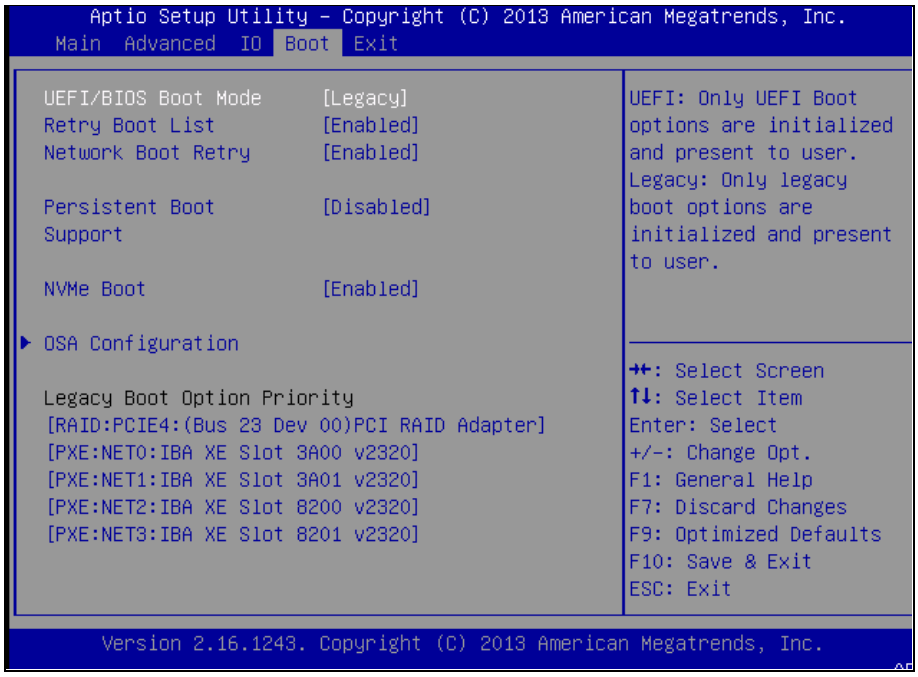
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

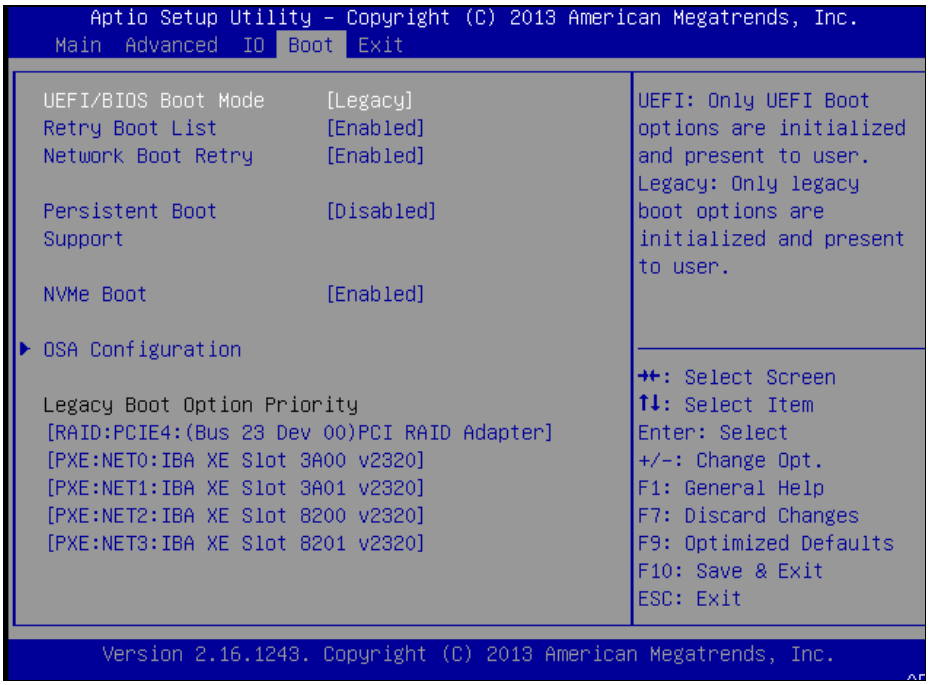
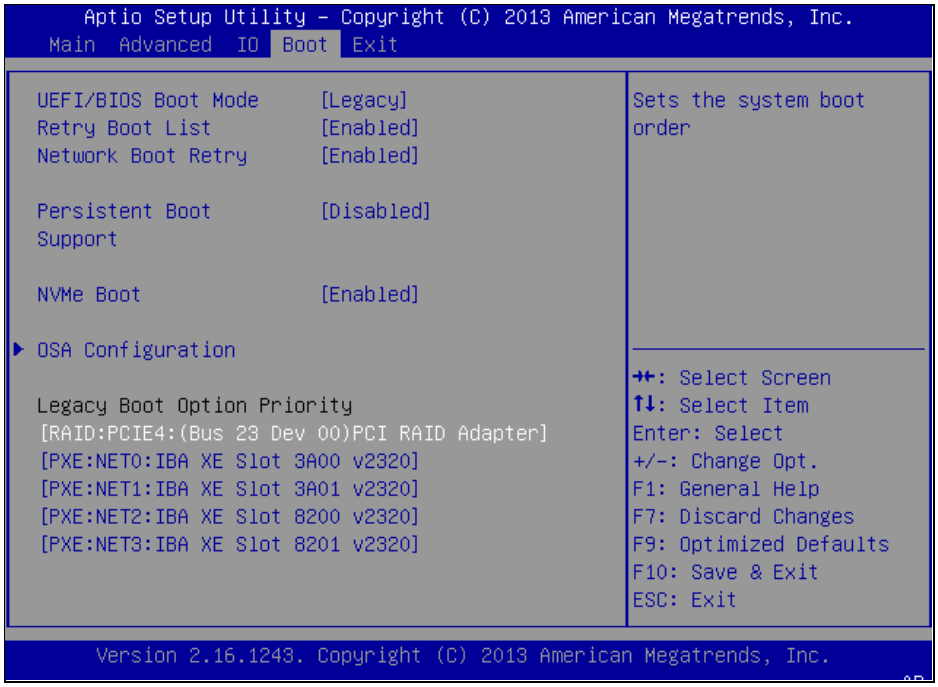
7.3.3: BIOS Settings for Oracle Rack Mount Servers

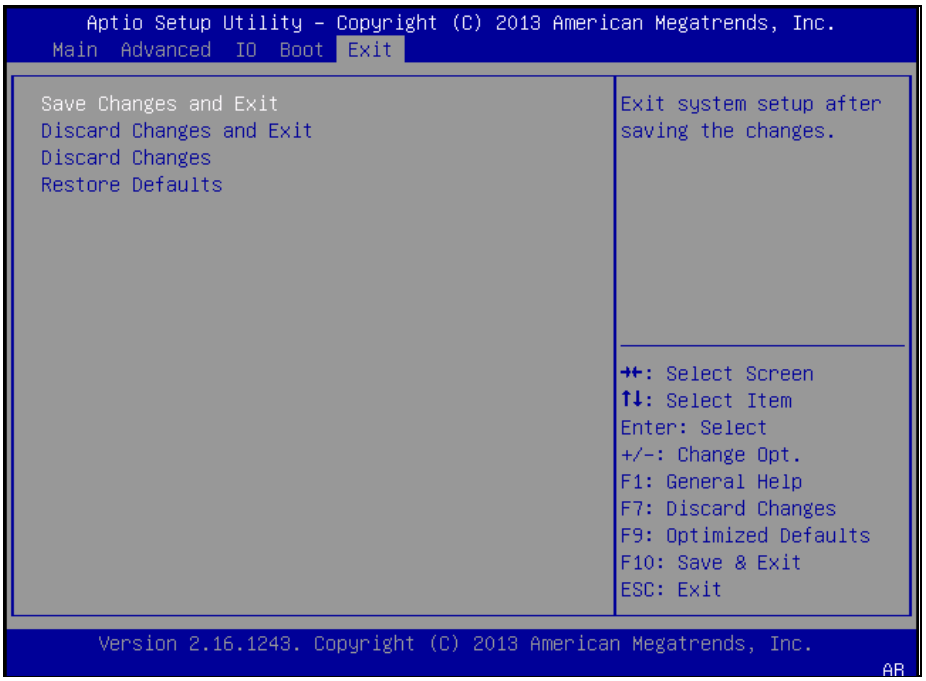
Step	Procedure	Details
1. ☐	Access the console for the Oracle server.	Connect to the console for the Oracle server as per Section 7.1.2. 

Step	Procedure	Details
2. ☐	Reboot the server from the ILOM	1. Navigate to **Host Management→Power Control.** 2. Select **Power Cycle** in the settings 3. Click **Save** to reboot the server. 
3. ☐	Console for the Oracle server. Reboot the server and press **F2** .	After the server is powered on, press **F2** when prompted to access the Setup Utility. 

Step	Procedure	Details
4. ☐	Console for the Oracle server.	Select **System Date** and press **Enter** to move forward and set the server date and time to GMT (Greenwich Mean Time). 
5. ☐	Console for the Oracle server	Navigate to the **Advanced → CPU Power Management Configuration**. 

Step	Procedure	Details
6. ☐	Console for the Oracle server.	1. From the CPU Power Management Configuration page, scroll to **ENERGY_PERF_BIAS_CFG**. 2. If Energy Performance is not set to PERF, select **PERF** and press **Enter**. 
7. ☐	Console for the Oracle server.	Select **Boot**. 

Step	Procedure	Details
8. ☐	Oracle console server	Select **Boot**. 
9. ☐	Oracle console server	Under Legacy Boot Option Priority, verify the RAID Adapter is listed first. If not, highlight it and press + (plus) to move it to the top of the list. 

Step	Procedure	Details
10. ☐	Oracle console server	Go to the Exit menu. Select **Save Changes and Reset**. 
---END OF PROCEDURE---		

7.3.4 Configuring CPU Power Limit on Netra X5-2 Servers

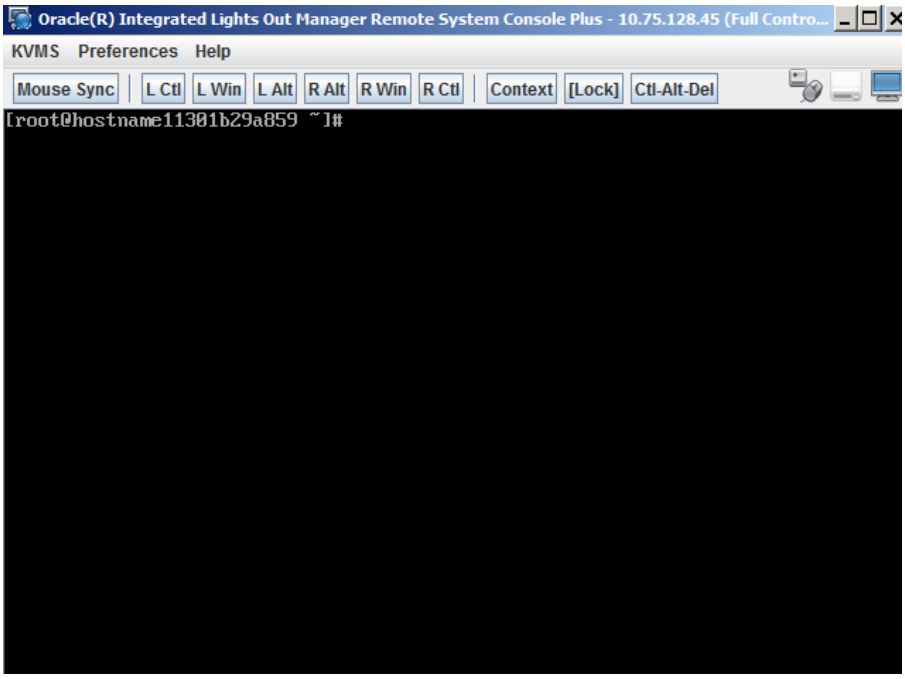
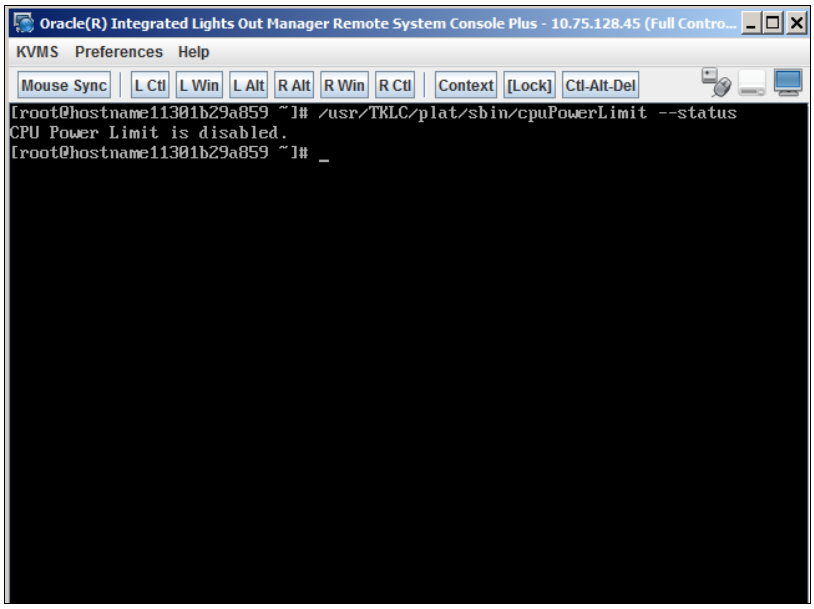
To meet NEBS requirements, the Netra X5-2 server has an option in the BIOS to set a CPU Power Limit. When the CPU Power Limit is enabled the server is in NEBS mode, and this function reduces the CPU power to 120 watts from the maximum 145 watts to prevent CPU throttling. By default TPD sets this option to disabled during IPM of a Netra X5-2 server, but this value can be changed after IPM by using the cpuPowerLimit utility. The cpuPowerLimit utility has four options: enable, disable, status, and check. After using the cpuPowerLimit utility to change the value of CPU Power Limit the server must be rebooted for the change to take effect. When running the utility it is important to note that is it reading and writing to the current BIOS values and can take 10-30 seconds to complete each action.

This procedure configures the CPU Power Limit for Netra X5-2 Servers

NOTE: This procedure is performed after the Platform software has been installed.

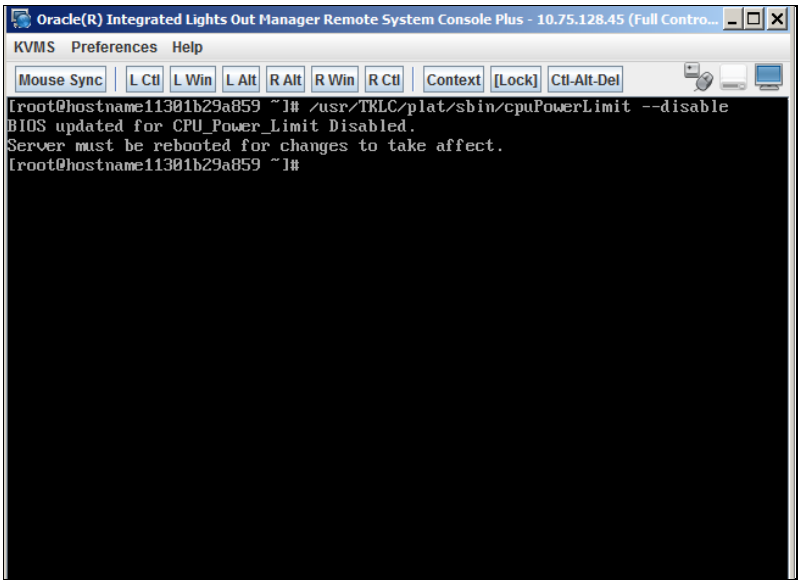
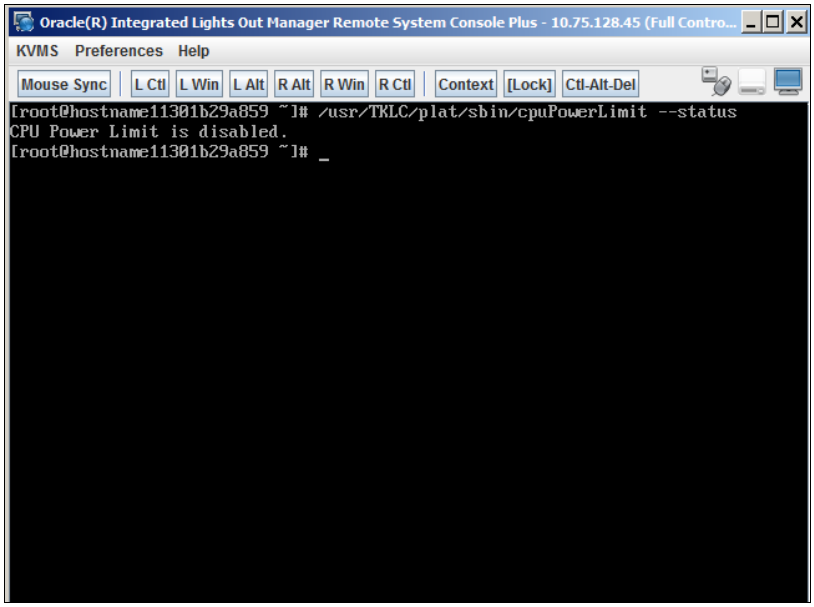
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

7.3.4: Configuring CPU Power Limit on Netra X5-2 Servers

Step	Procedure	Details
1. ☐	Access the console for the Oracle server.	Connect to the console for the server as instructed in Section 7.1.2:Accessing the iLO VGA Redirection Window for Oracle RMS Servers. 
2. ☐	Remote Console command line: check settings	To check the current setting of CPU Power Limit in the BIOS run: `/usr/TKLC/plat/sbin/cpuPowerLimit -status`  CPU Power Limit is disabled

Step	Procedure	Details

3. ☐	Remote Console command line: enable settings	1. To enable CPU Power Limit after IPMing a Netra X5-2 server log into the server as root and run:
		`/usr/TKLC/plat/sbin/cpuPowerLimit -enable`
		`[root@X52-mpe-1a ~]# /usr/TKLC/plat/sbin/cpuPowerLimit -enable`
		`BIOS updated for CPU_Power_Limit Enabled.`
		`Server must be rebooted for changes to take affect.`
		`[root@X52-mpe-1a ~]#`
		2. Reboot the server for the setting to take effect.
		`[root@X52-mpe-1a ~]# /usr/TKLC/plat/sbin/cpuPowerLimit -status`
		`CPU Power Limit is enabled.`
		`[root@X52-mpe-1a ~]#`

Step	Procedure	Details
4. ☐	Remote Console command line: disable settings	To disable CPU Power Limit log into the server as root and run: `/usr/TKLC/plat/sbin/cpuPowerLimit -disable`  Reboot the server for the new setting to take effect.  CPU_PowerLimit Disabled
---END OF PROCEDURE---		

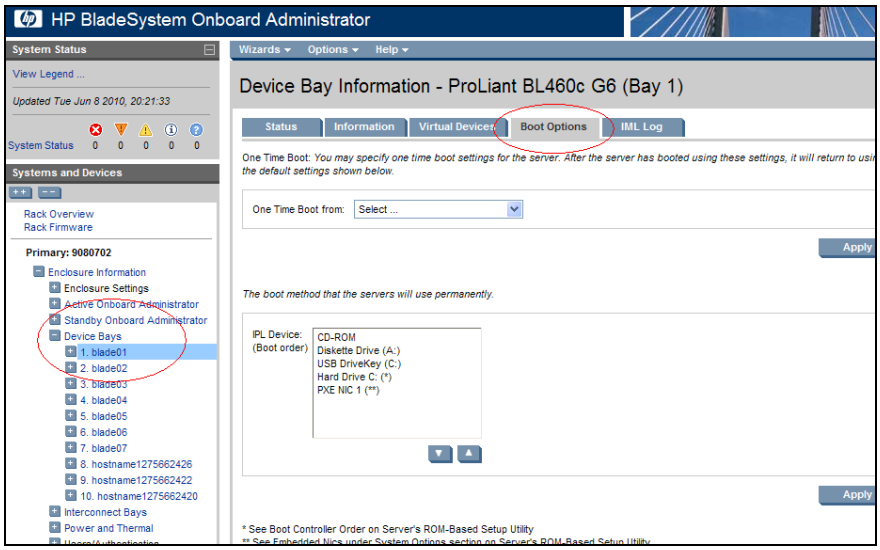
7.3.5 Using c-Class Enclosure OA to Update BIOS Settings for the Application Blade

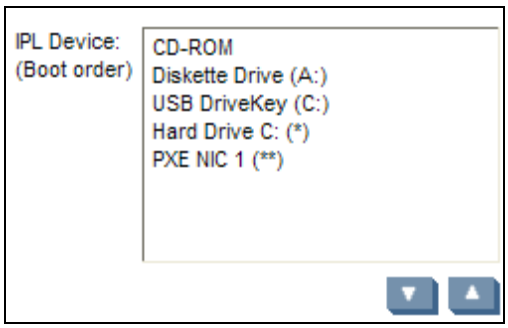
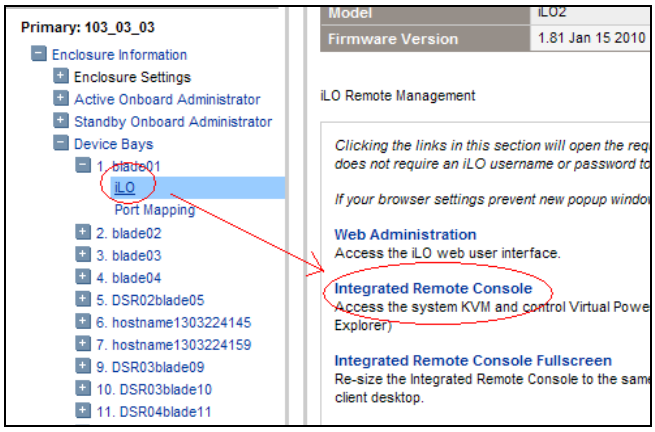
This procedure confirms and update the BIOS configuration on Blade servers using the C-Class enclosure OA.

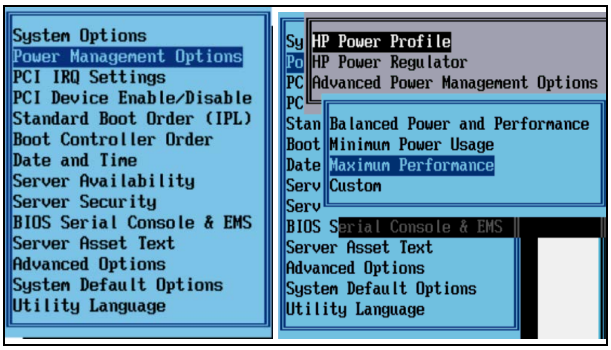
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

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	Open your web browser and navigate to the OA IP address Login to HP OA as Administrator. Original password is on paper card attached to each OA.
2. ☐	**OA:** Navigate to device Bay Settings	1. Navigate to **Enclosure Information → Device Bays → <*Blade 1*>.** 2. Click **Boot Options**. 

Step	Procedure	Details
3. ☐	**OA:** Verify/update Boot device Order	Verify that the Boot order is: **CD-ROM** **Diskette Drive (A:)** **USB DriveKey (C:)** **Hard Drive C: (*)** **PXE NIC 1 (**)** If it is not, use the up and down arrows to adjust the order, 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.
5. ☐	**OA:** restart the blade and access the bios	1. If you are prompted with a certificate security warning, click **Continue**. 2. After a prompt is displayed, login onto the blade using the root username. 3. After you are 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).

Step	Procedure	Details
6. ☐	**OA:** Update bios settings	1. Scroll down and click **Power Management Options** and press **Enter** 2. Select **HP Power Profile** and press **Enter** 3. Scroll down and click **Maximum Performance** and press **Enter**  4. Press **Esc** twice to return to exit the BIOS setup screen and press **F10** to confirm Exiting the utility. The blade reboots.s
7. ☐	**OA:** Repeat for the remaining blades	Repeat Steps 2 through 6 for the remaining blades. After you are finished, 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 you purchased your servers from Oracle, they will have the latest revisions available at the time of shipment. If the installation is HP c-Class then the OA (Online Administrator) GUI will have a summary of the firmware revisions of all the equipment in the c-Class enclosure. (It will generally 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 correctly. Back up the final switch configuration to PM&C so that it can be restored in a repair operation. Also, make note if the netConfig files are not used for the restore operation (because you made switch 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 will 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 correct 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.

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 the following sequence on the Support telephone menu:

1. Select **2** for New Service Request
2. Select **3** for Hardware, Networking and Solaris Operating System Support
3. Select one of the following options:
    a. For technical issues such as creating a new Service Request (SR), select **1.**
    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.