Oracle® COMMUNICATIONS

Policy Management
Bare Metal Installation Guide

Release 12.2

E82615-01
February 2017

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*.

TABLE OF CONTENTS

1. PREFACE 6
1.1 Related documents 7
1.2 Acronyms 8

1. PREFACE

This guide provides instructions for installing Oracle Communications Policy Management (also referred to as Policy Management) software for Wireless, Fixed Broadband and Cable networks 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/cd/E66963_01/index.htm

[11] E72271 - 12.2 Release Notes

[12] E66966 - Configuration Management Platform, Wireless User's Guide, Release 12.2

[13] E66967 - Configuration Management Platform, Cable User's Guide, Release 12.2

[14] E66965 - Platform Configuration User's Guide, Release 12.2

[15] E82607 - Network Impact Report

[16] E66971 - Policy Front End Wireless User's Guide

[17] E72270 - Mediation Server User's Guide

[18] E66972 - Bandwidth on Demand Cable User's Guide

[19] E66973 - Troubleshooting Reference

[20] E66969 - SNMP User's Guide

[21] E81791 - Licensing Information User Manual

[22] E61553 - Analytics Data Stream Wireless Reference

[23] E66970 - 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 and Terms

Term	Definition
BoD	Bandwidth on Demand — application manager within a cable network
CMP	Configuration Management Platform — component of a Policy Management system
Data Source	Interface that provides data to components
ECO	Engineering Change Order
FUP	Firmware Upgrade Pack
HP c-Class	HP blade server system
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
MA	Management Agent — one of the components in a cable network.
Mediation	Component that interfaces with SPR and Boss to process subscriber profile and service subscription data
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.)
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 – 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
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	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	Tekelec Virtualization Operating Environment – 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.
UDR	User Database Repository
XMI	External Management Interface — see OAM
XSI-1	External Signaling Interface 1 — see SIG-A

2. INSTALLATION OVERVIEW

This document describes how to install the 12.2 Policy Management application 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 executed to configure hardware to be 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
- Management Agent (MA) — an element in a cable network that collects network and topology information to make routing and policy decisions
- Bandwith on Demand (BoD) Application Manager — a required element in a cable network that manages subscriber resources and data
- 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 will be 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 will be required for initial configuration of systems. In this case, it is possible that firmware revisions may be 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 will be needed. This document assumes that all hardware meets Oracle specifications.

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

- For 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
- For Cable environment, a backplane network to connect two servers in an HA (High-Availability) configuration

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*" or Section 7, "*Configure Policy Application Servers in Cable 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, Wireless-C (see note), or Cable.
- Determine the names and addresses of network elements used in your network with which Policy Management will interact.
- Determine the names and addresses of external data sources used in your network with which the Policy Management software will interact; for example, subscriber profile repositories, on-line charging servers, and offline charging servers.
- Choose the Policy Management components you want to install.
- Install Policy Management software and any optional components.
- Configure each Policy Management component.

Note: Wireless-C supports a wireless system supporting 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 prior to being implemented 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 rather than actual subscriber data during testing.

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

See Section 4.0, "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 executes 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-12.2.0.0.0_65.1.0-x86_64.iso
- MPE: mpe-12.2.0.0.0_65.1.0-x86_64.iso
- MRA (PFE): mra-12.2.0.0.0_65.1.0-x86_64.iso
- MA: ma-12.2.0.0.0_65.1.0-x86_64.iso
- BoD: bod-12.2.0.0.0_65.1.0-x86_64.iso
- Mediation: mediation-12.2.0.0.0_65.1.0-x86_64.iso

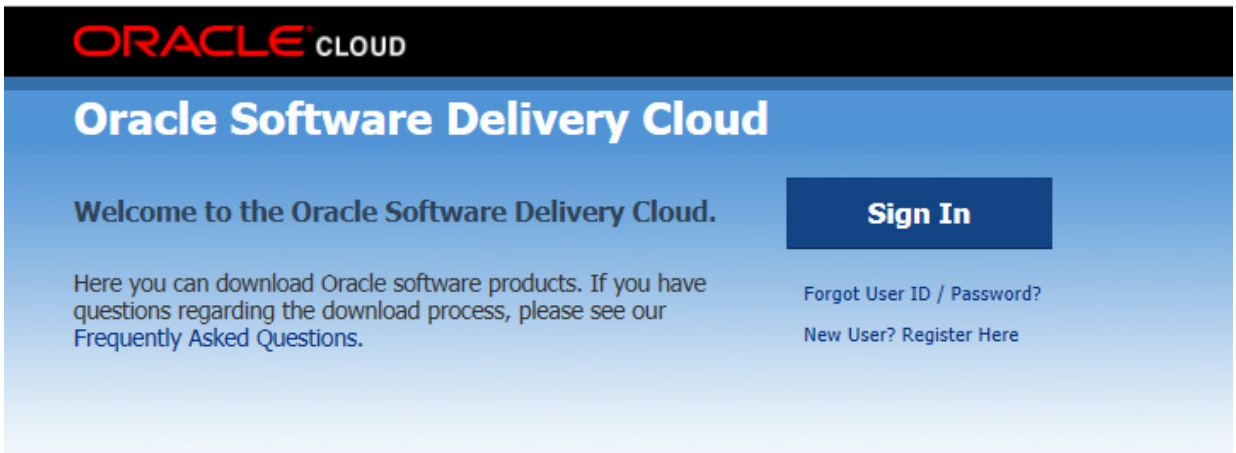
4.1.4 Acquiring Software

Customers:

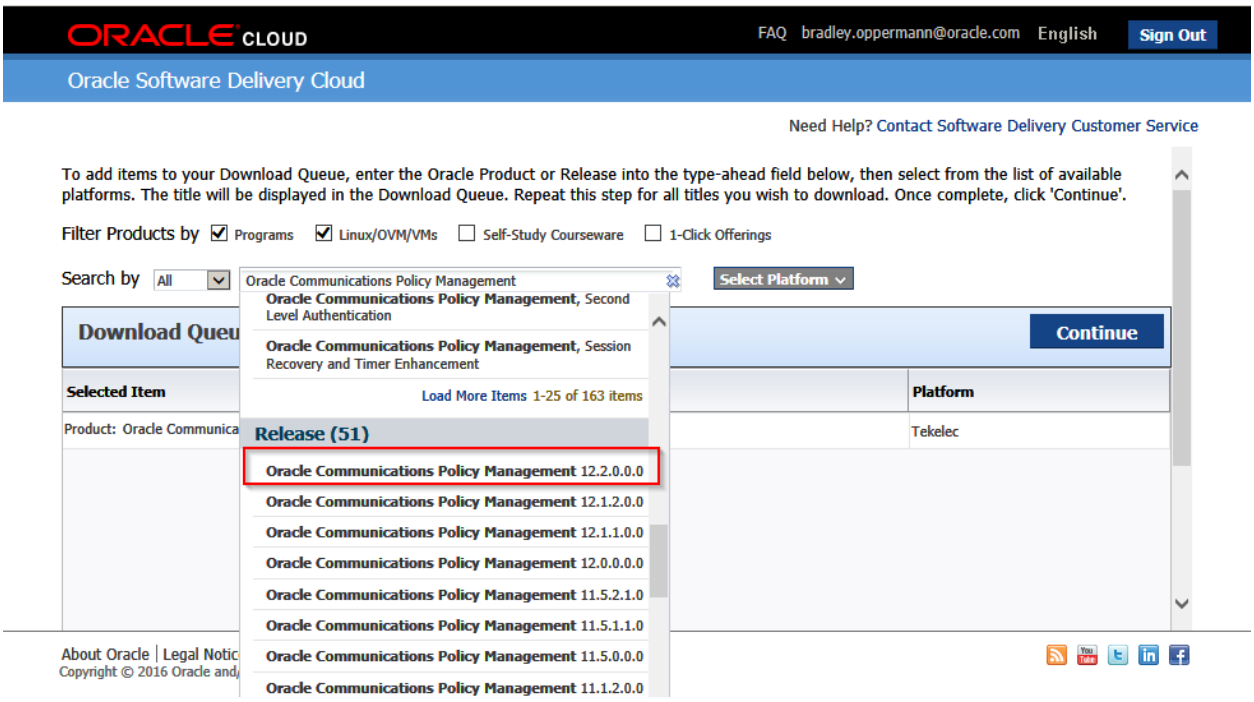
If you already have a commercial license you should download your software from the Oracle Software Delivery Cloud, which is specifically designed for customer fulfillment.

For patches, see My Oracle Support.

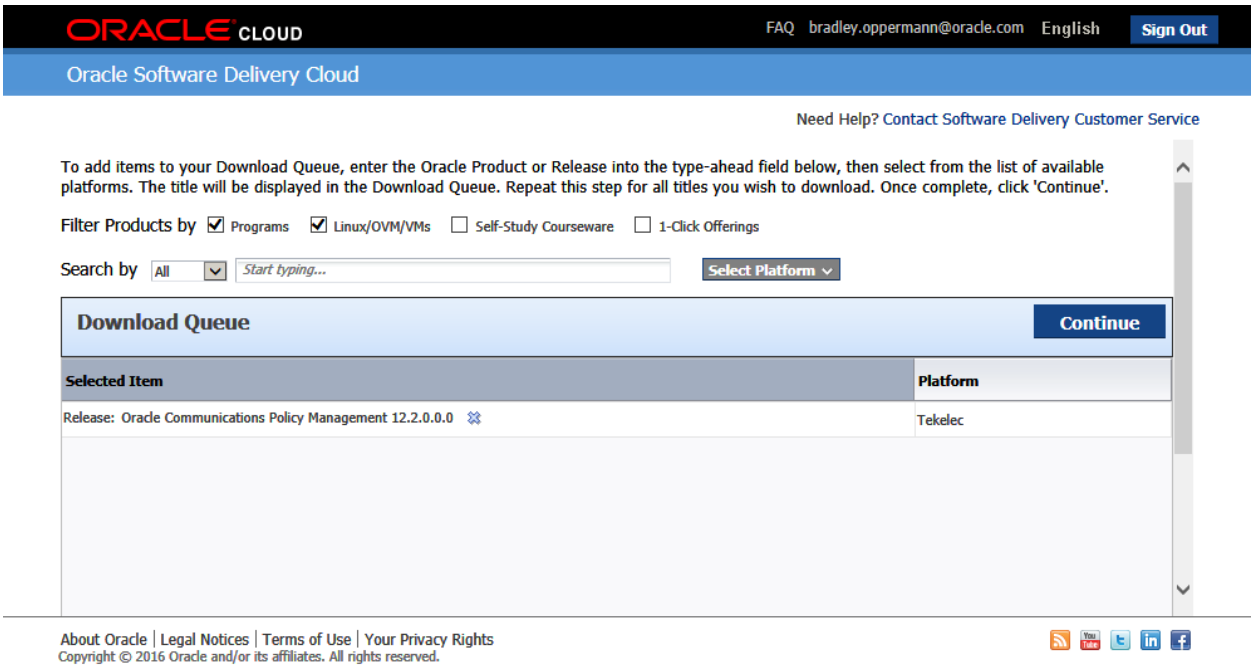
Note: The following is an example of downloading the Policy Management software.



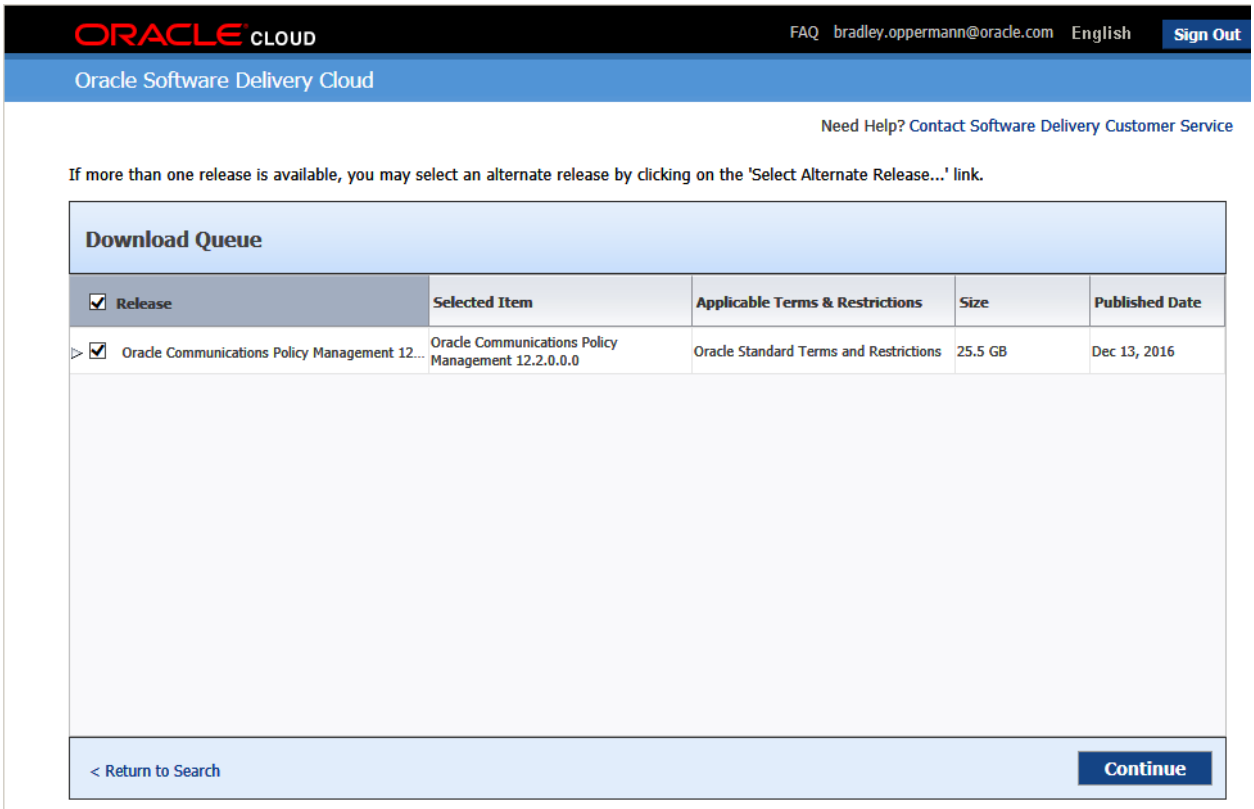
Set the "Search by" field to "Oracle Communications Policy Management" select "12.2.0.0.0"



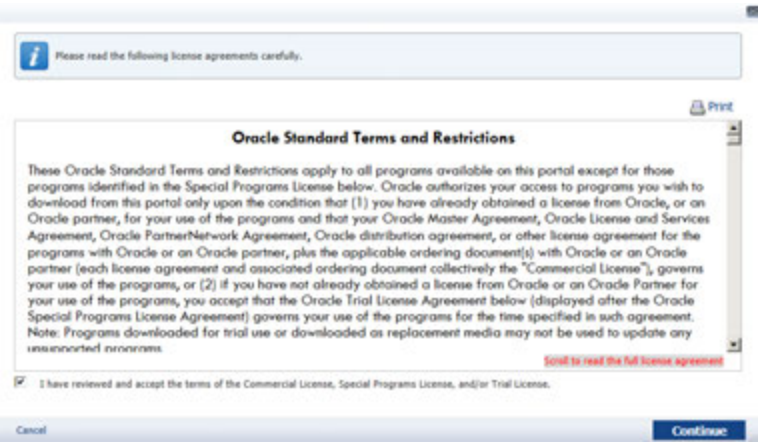
Choose Continue



Choose Oracle Communications Policy Management checkbox for 12.2.0.0.0 and Continue

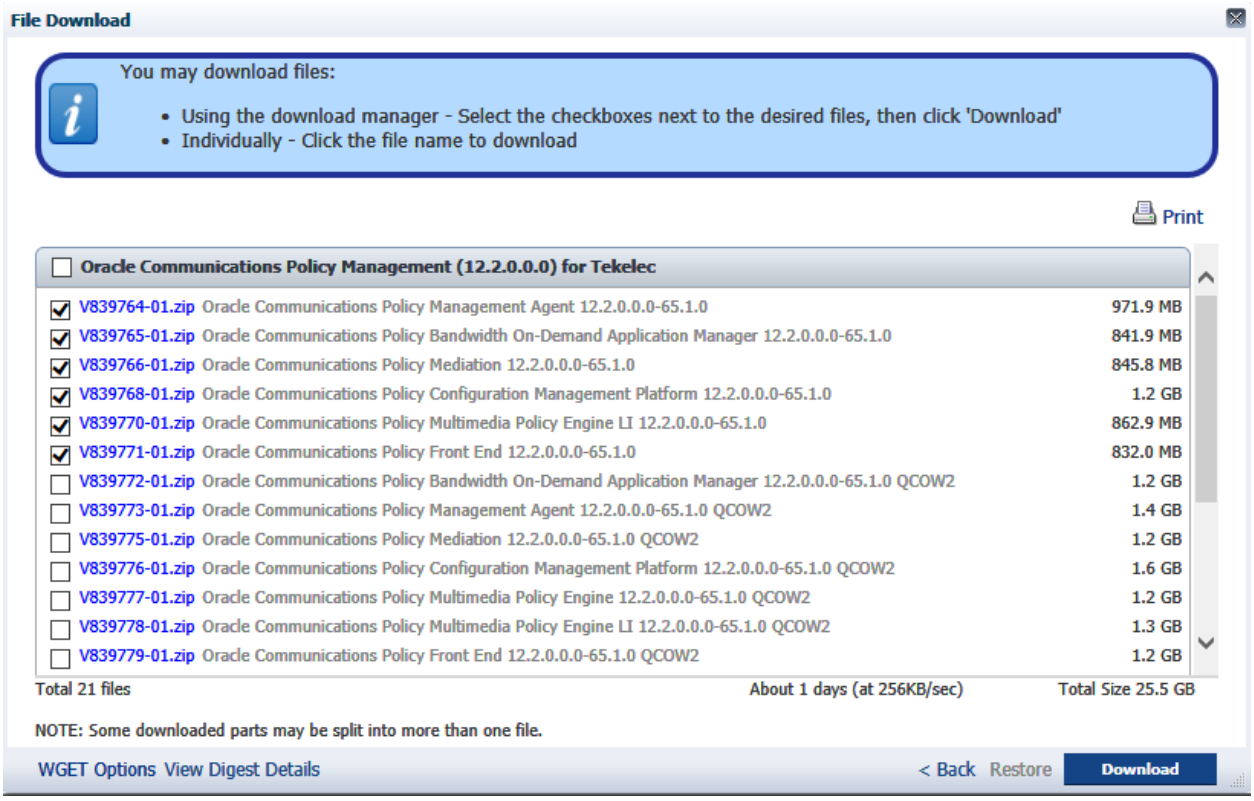


Confirm the License Agreement



Choose the required Software files in their .zip compressed format

Note: Choose "View Digest Details" in the lower left corner to see MD5sum and SHA-1 references



4.1.5 About Critical Patch Updates

Install all Oracle Critical Patch Updates as soon as possible. To download critical patch updates, find out about security alerts, and enable email notifications about critical patch updates, see *Oracle patch and security bulletins.*

4.1.6 Additional Software Requirements

For an HP c-Class hardware installation, the 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 may 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 (G6/G8/G9 RMS)
- HP c-Class server (BL460 G6/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 12.2 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* or *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 12.2, 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 will need 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/Passwords

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

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

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

- **admin** This is the default administrator user with all privileges.
- **operator** This is the default operator user with all privileges except user administration.
- **viewer** This is the default read-only user.

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

5. PREPARING THE SYSTEM ENVIRONMENT

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

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

To prepare and configure servers, you will also 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 server's serial console

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 its web GUI interface. You should now change the default password for the **root** account.

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

To change the password, while in the ILOM web interface, navigate to **ILOM Administration** > **User Management** > **User Accounts**. Select **Edit**, change the **root** account password, and 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 *10.3.3: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 will be 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)

5.1.5: IPM of Oracle X5-2 RMS Server

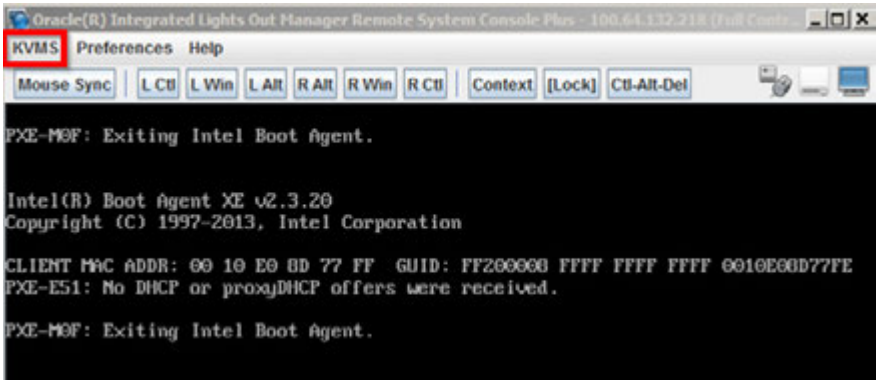
STEP #	This procedure will install system OS (IPM) of the server Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. **Needed material:** - TPD ISO image file to be used for virtual mount accessible on laptop or - USB device prepared with bootable version of TPD image IF THIS PROCEDURE FAILS, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1. ☐	Insert Bootable USB Media/mount TPD ISO	Create a bootable USB drive with the TPD ISO image file. Use the method provided in the "README.txt" file that is included with the downloaded Policy Software or other suitable method for creating a bootable USB device. There are several readily available utilities to achieve this. Then insert the USB drive locally into the server and reboot the server to the bootable USB device. Then proceed to Step 3 of this procedure if using this method If local access to the server is not available and network access to the 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 "8.1.2: Accessing the iLO VGA Redirection Window for Oracle RMS Servers" Login to iLOM web interface and Navigate to "System Information" → "Summary" then launch

5.1.5: IPM of Oracle X5-2 RMS Server

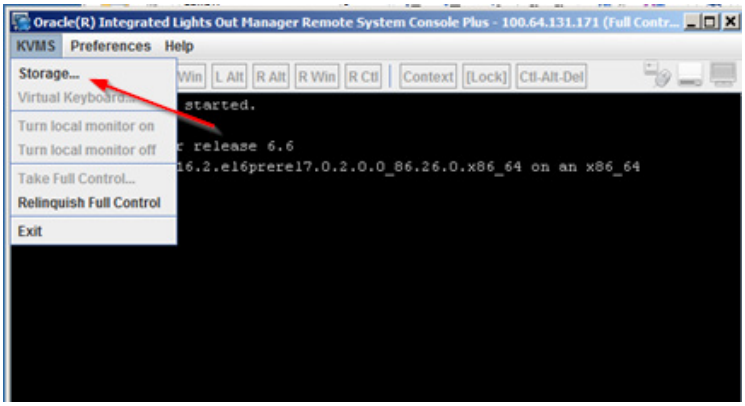
the remote console:

Note: This will launch the "video redirection" console which is preferred to perform these procedures

The iLOM remote system console will launch. If no OS has been previously installed something similar to the following will be presented:



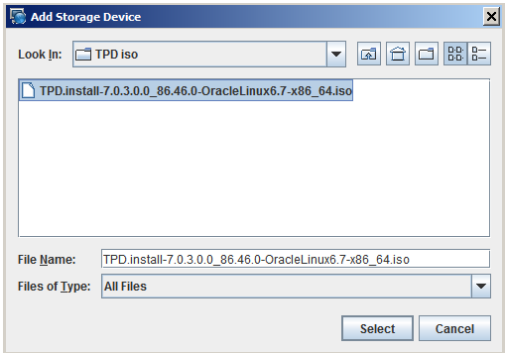
From "KVMS", click "Storage":



In the Storage devices form that opens up, click on the "Add" button.

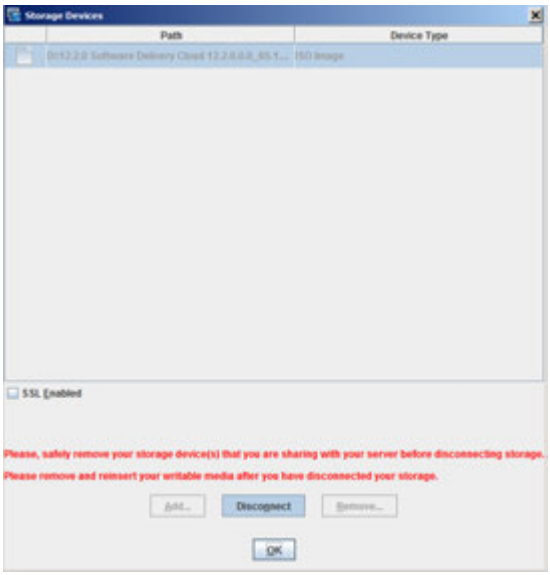
5.1.5: IPM of Oracle X5-2 RMS Server

Browse to ISO image file that will be mounted and click on “Select”.

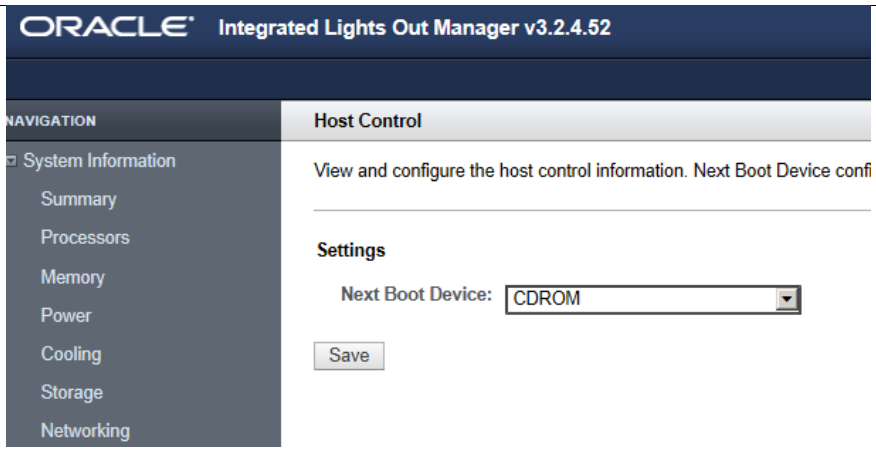


The Storage Devices form will now display the selected ISO image file. Highlight the file and the Connect option will now be available at the bottom of the form. Click on “Connect”. And then Confirm “OK”.

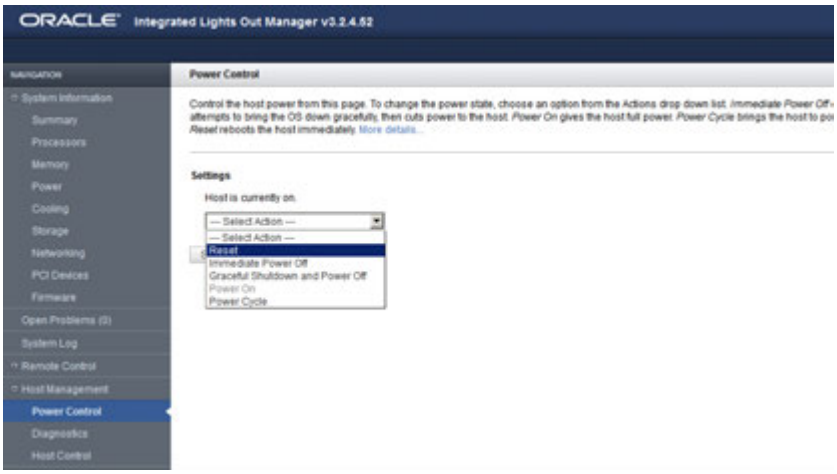
5.1.5: IPM of Oracle X5-2 RMS Server

		The Storage Devices will indicate that the ISO image has successfully mounted/connected. Leave this window open. 
2. ☐	**Console:** Boot server, wait for TPD boot: form	Return to the iLO summary page and navigate to Host Management -> Host Control  Change the drop down tab to <CDROM>. And click on "**save**". This will cause the server to boot to the virtually mounted ISO image from the previous steps.

5.1.5: IPM of Oracle X5-2 RMS Server



In the iLO Navigate to Host Management -> Power Control and select "Reset" from the drop down menu to reboot the server. Click on "Save" and the server will reboot to the mounted ISO image.

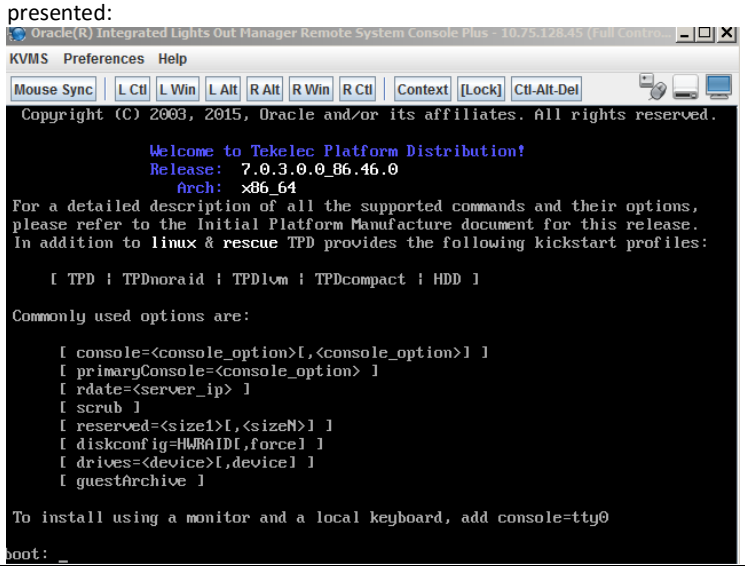


3. ☐

Console: Enter TPD boot: command with correct options

TPD install takes 20 – 40 minutes to complete

The server has now booted to the virtually mounted TPD ISO image and the following screen is presented:



5.1.5: IPM of Oracle X5-2 RMS Server

"**IPM**" the server using the following command at the boot prompt:

•boot: **TPDnoraid diskconfig=HWRAID,force console=tty0**

```
To install using a monitor and a local keyboard, add console=tty0

boot: TPDnoraid console=tty0 diskconfig=HWRAID,force
```

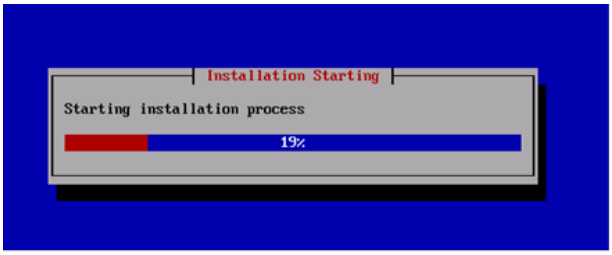
Note: If a direct connection to the serial console is being used for this step instead of the remote iLO console it is not necessary to include "console=tty0"

After the command has been entered press the carriage return and you will see something like the following screen indicating that the OS is installing

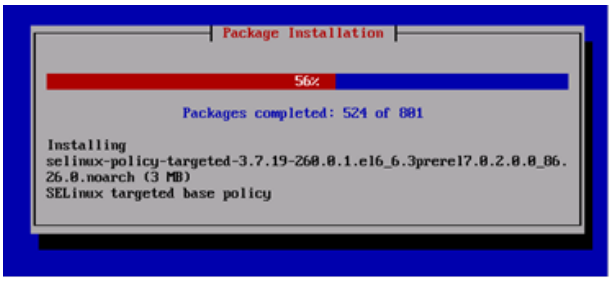
```
boot: TPDnoraid diskconfig=HWRAID,force console=tty0
Loading vmlinuz......
Loading initrd.img.......
```

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. Refer to TPD Initial Product Manufacture, Software Installation Procedure (Section 3.4)

The TPD installation takes 20-40 minutes to complete, starting with some checks then installation starts:



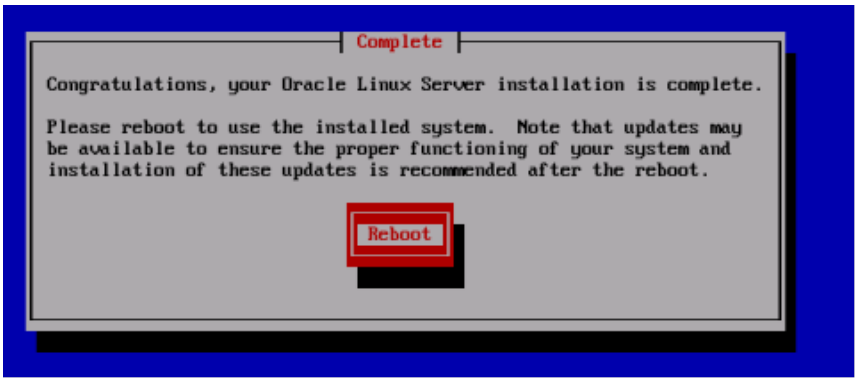
Then you will be able to monitor the packages installation progress:



Then post installation scripts kick off:

After IPM the process is completed, you are prompted to press **Enter** to reboot the server.

5.1.5: IPM of Oracle X5-2 RMS Server



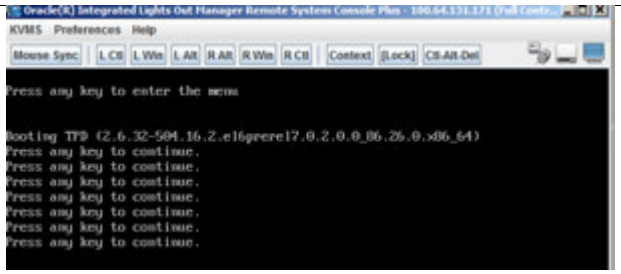
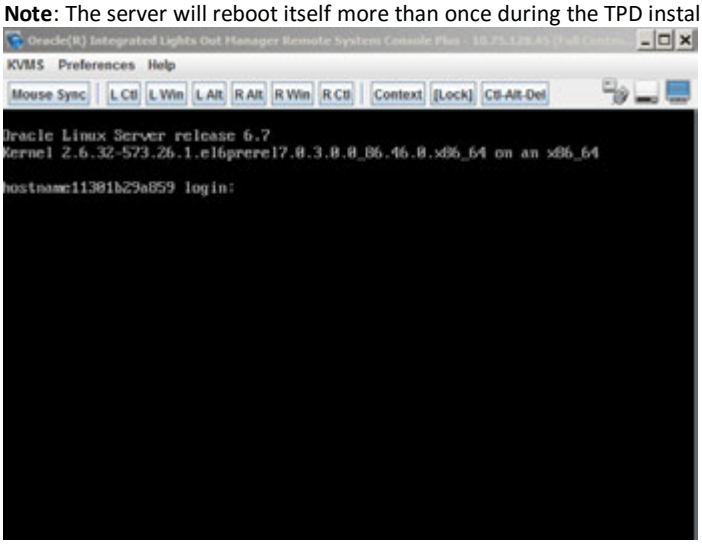
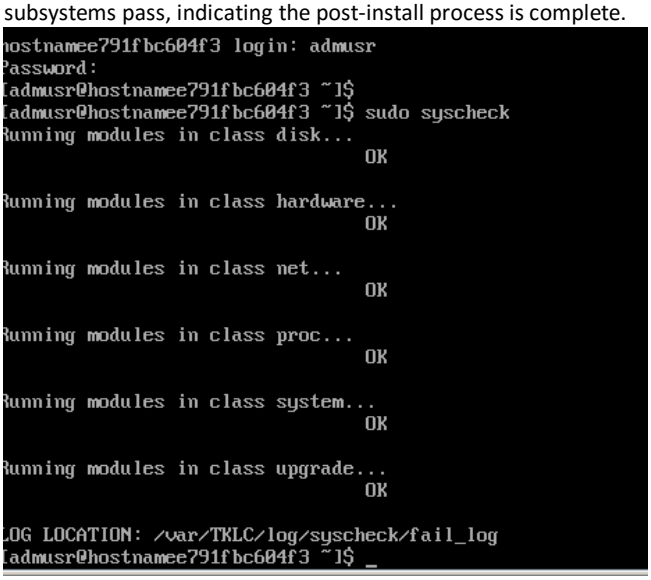
At this time the media can be disconnected. Using the iLOM's remote console, Add "Storage Devices" form, unmount the image from the ILOM remote console. Then highlighting the remote console dialog window press **Enter** to reboot the server as per the following steps. .

In the case a bootable USB device was used, remove the USB device

To unmount the ISO image file select the file and click on "Disconnect if the file was previously "connected"

Press **Enter** to boot the server from TPD and finish up the installation. The installed OS can be seen booting up

5.1.5: IPM of Oracle X5-2 RMS Server

		
4. ☐	**Console:** Login prompt	Once the server reboots, the login prompt is displayed. Login into the server with ***admusr.*** **Note**: The server will reboot itself more than once during the TPD installation process.  If no login prompt is displayed after waiting 15 minutes, contact Oracle Customer Support for assistance.
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 an "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.  If any of the modules return an error, do not continue; contact Oracle Customer Support and report the error condition.

5.1.5: IPM of Oracle X5-2 RMS Server

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 shot shows no errors returned which indicates the TPD installation process is successfully completed. If errors are found, contact Oracle Customer Support.
THIS PROCEDURE HAS BEEN COMPLETED		

5.1.6 Installing Policcy Management Software

5.1.6: Installing Policy Management Software

STE P #	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:** Two methods for installing the Policy Application are presented here. The 1st is to use a USB drive inserted locally into the server. This is the preferred method. The 2nd is to 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 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.	
1. ☐	Make the Policy Application ISO images available for installation	Copy the Policy Application ISO image file (CMP/MPE/MRA/BOD/MA/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, or

5.1.6: Installing Policy Management Software

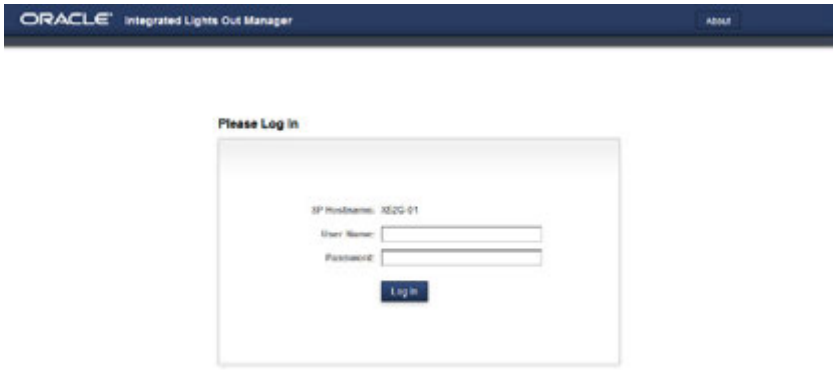
- using the Server iLO port and iLO Web Interface (to access Remote Console)

Proceed to step #2 of this procedure

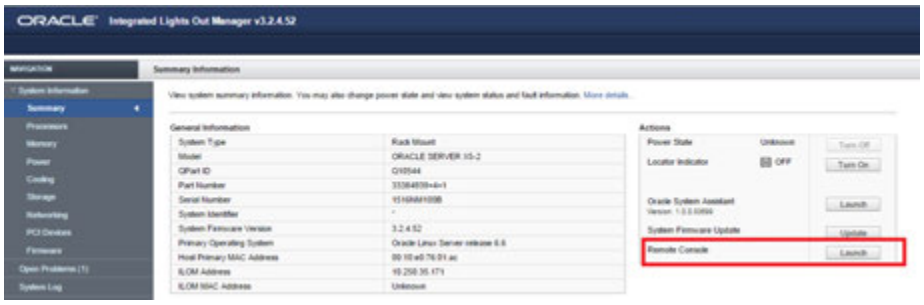
Or

If you are using the ILOM remote console and have the Policy Management software as an ISO image file, do the following:

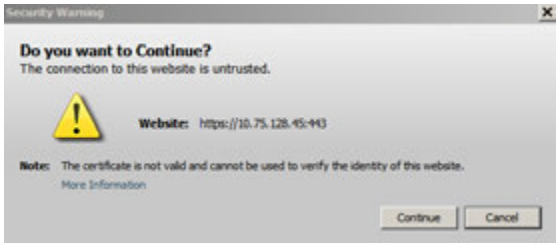
a. Open a browser, enter the URL of the ILOM system, and log in. For example:



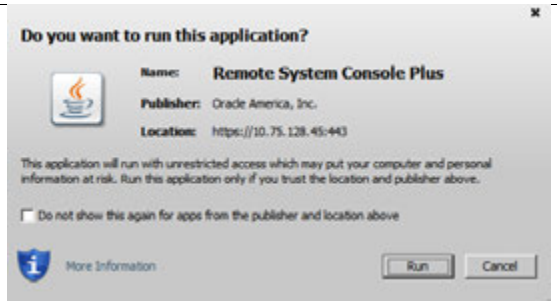
b. Select System Information > Summary. The Summary Information page opens. Under Actions, locate Remote Console and click Launch. For example:



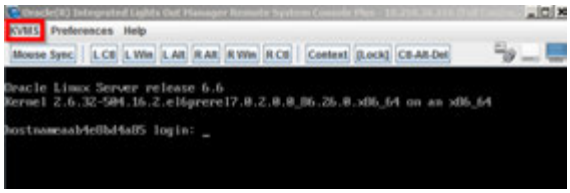
c. The ILOM remote system console starts. Select “continue” and “run” if needed.



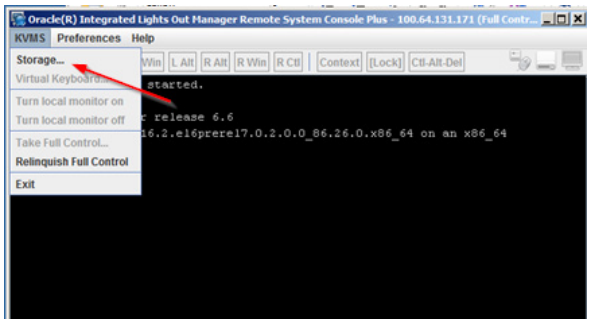
5.1.6: Installing Policy Management Software



d. Select KVMS > Storage. The Storage Devices window opens.



e. From “KVMS”, click “Storage”:

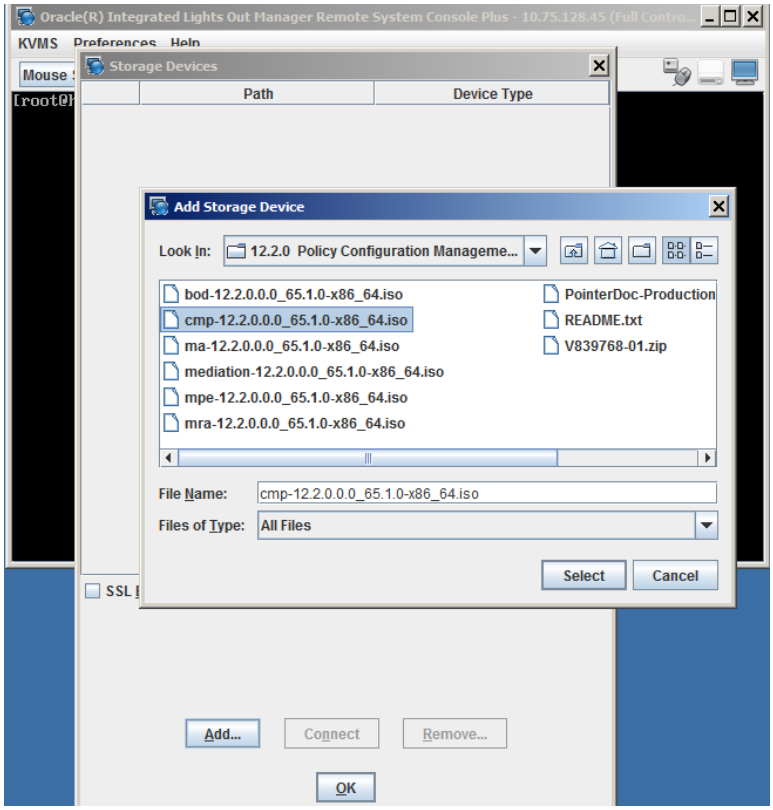


f. In the Storage Devices window, click Add... The Add Storage Device window opens.

5.1.6: Installing Policy Management Software

g. Browse to the ISO image file to mount and click Select.

Note: Make certain that the ISO image file selected (CMP/MPE/MRA/BOD/MA/MEDIATION) is the correct one for the target server according to the Policy Solution Design!



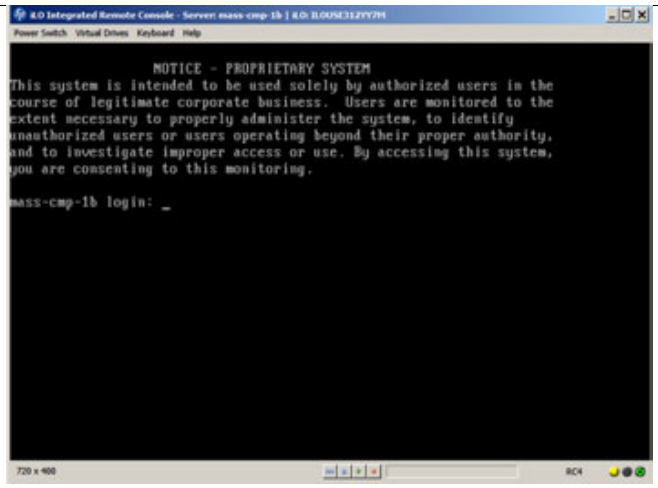
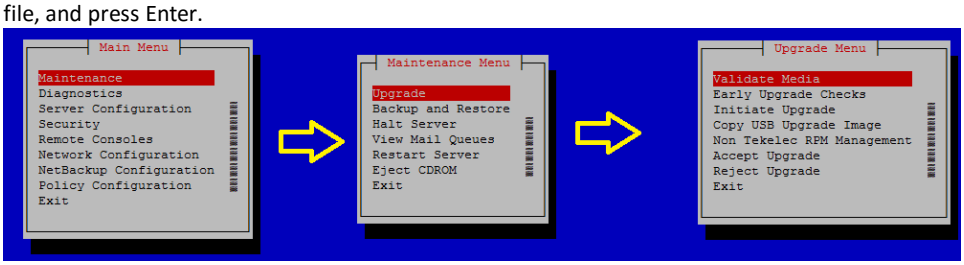
The Add Storage Device window closes, and the Storage Devices window displays the selected ISO image file.

h. Select the ISO image file. The Connect button, at the bottom of the form, becomes enabled. For example:

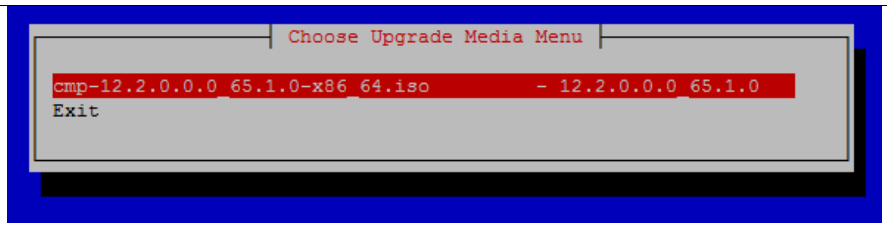
5.1.6: Installing Policy Management Software

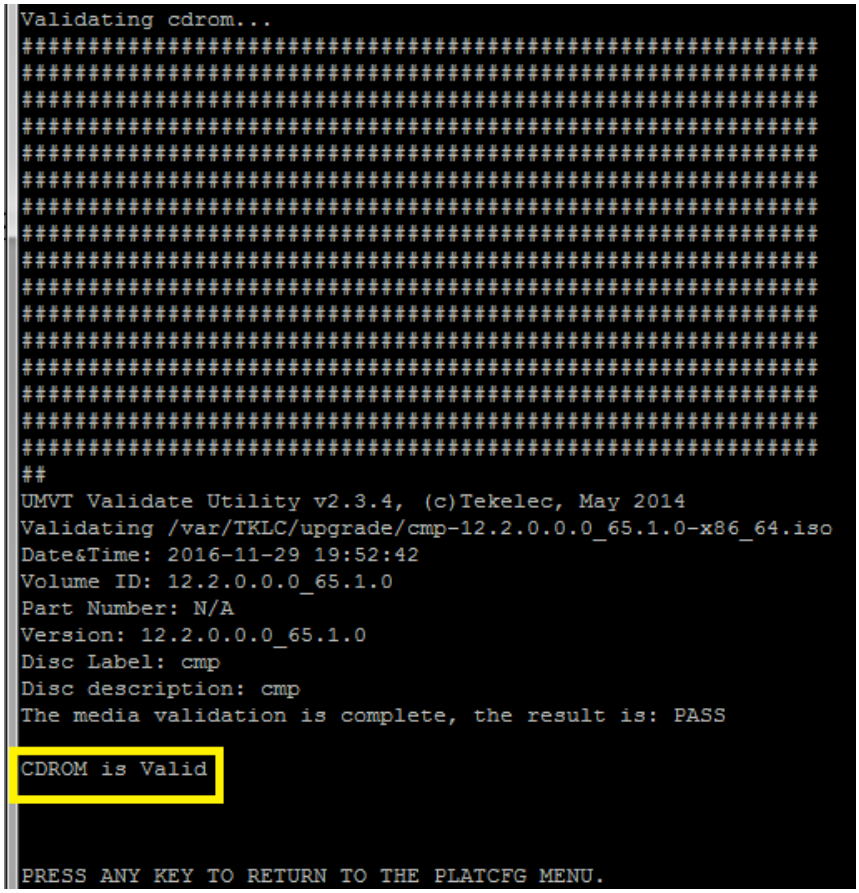
		 Click **Connect** and then **OK**. The Storage Devices window indicates that the ISO image file is successfully connected. For example:  Leave this window open.
2. ☐	**Console**: Login as <admusr>	Connect to the server console, either directly or remotely: • Directly — using a display and keyboard • Remotely — using the iLO Remote Console and the server iLO port Login as <admusr> if not already logged in.

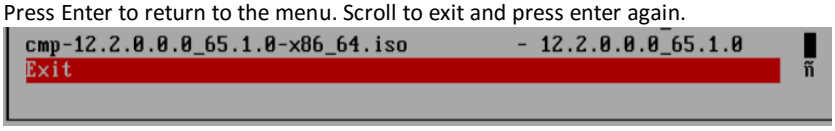
5.1.6: Installing Policy Management Software

		
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 [admusr@X52-cmp-2a ~]$ sudo getPlatRev 7.0.3.0.0-86.46.0
4. ☐	**Console:** run platcfg and validate the media	Enter the following command to start the Platform Configuration utility: #sudo su - platcfg The Platform Configuration Main menu opens. From the Main menu, navigate to Maintenance > Upgrade > Validate Media, select the ISO image file, and press Enter.  **Note:** Depending on the method used the platcfg utility will search for any mounted ISOs and if successful will display the Policy Application ISO image file to install For example:

5.1.6: Installing Policy Management Software

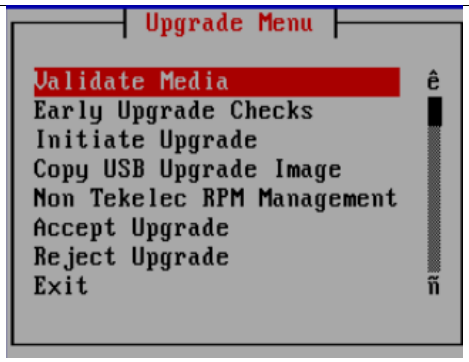
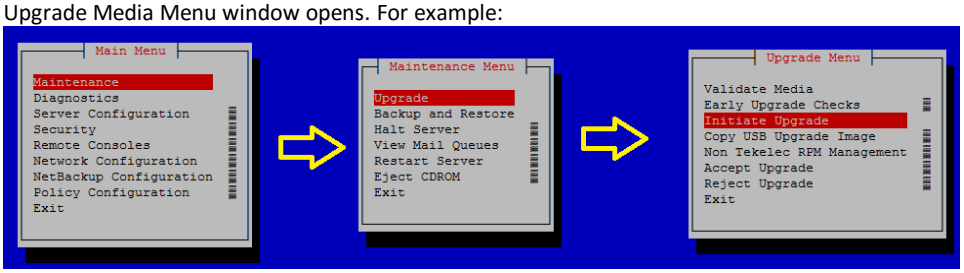
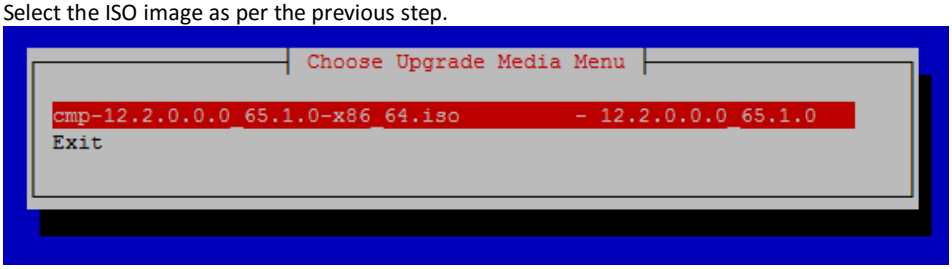
<table>
<tr>
<td></td>
<td></td>
<td>


Then choose the ISO image:
The utility displays “Validating media or cdrom”… and a series of hash marks (#) signs. When it finishes it displays information about the ISO image file and the message the CDROM or Media is Valid. The following example shows a successful validation:


</td>
</tr>
<tr>
<td>5.
☐</td>
<td>Console: verify platform revision</td>
<td>
Press Enter to return to the menu. Scroll to exit and press enter again.


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

5.1.6: Installing Policy Management Software

		
6. ☐	**Console:** Select ISO to install, and confirm Application install may take 20 Minutes – if installing with a virtual mount, it will take longer	From the Main menu, navigate to Maintenance > Upgrade > Initiate Upgrade. The Choose Upgrade Media Menu window opens. For example:  Select the ISO image as per the previous step.  **Note:** The server will reboot twice during the installation process, Do Not Remove the media at this time.

7. ☐	**Console:** Verify Policy install version	After the application has completed installation log back in to the command line as admusr and confirm the installed TPD platform version and the policy application version.
		
		$appRev
		`mass-cmp-1b login: admusr`
		`Password:`
		`Last login: Fri Jan 20 17:11:38 on tty1`
		`[admusr@mass-cmp-1b ~]$ appRev`
		`Install Time: Thu Jan 19 17:07:20 2017`
		`Product Name: cmp`
		`Product Release: 12.2.0.0.0_65.1.0`
		`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-12.2.0.0.0_65.1.0-x86_64.iso`
		`OS: OracleLinux 6.7`
		
		Verify:
		• TPD revision installed
		• Policy application installed and its revision

5.1.6: Installing Policy Management Software

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, BoD, MA, MEDIATION) on each server. For Wireless mode, proceed *to* *Section 6: Configure Policy Application Servers in Wireless Mode* For Cable mode, proceed *to* *Section 7: Configure Policy Application Servers in Cable Mode*
THIS PROCEDURE HAS BEEN COMPLETED		

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 server's serial console

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 now change the default password for the **root** account.

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

To change the password, while in the ILO web interface, navigate to **ILOM Administration** > **User Management** > **User Accounts**. Select **Edit**, change the **root** account password, and 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 *8.3.1:BIOS Settings for HP Gen 8 Blade and Rackmount Servers* or *8.3.2: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 will be 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:

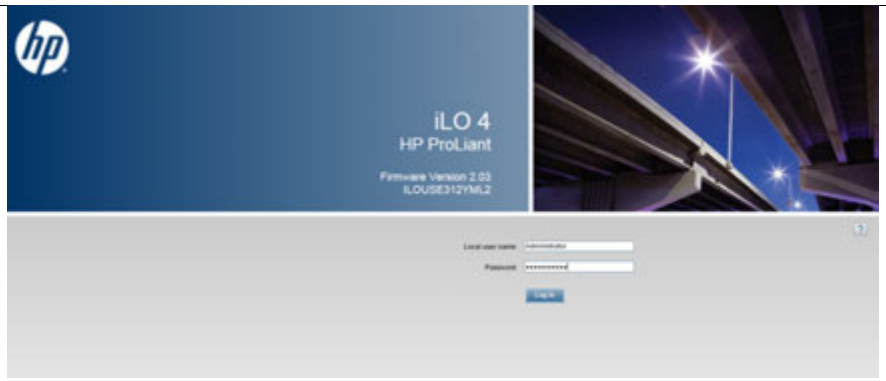
- TPD ISO image file (Section 4.1 Software Requirements)

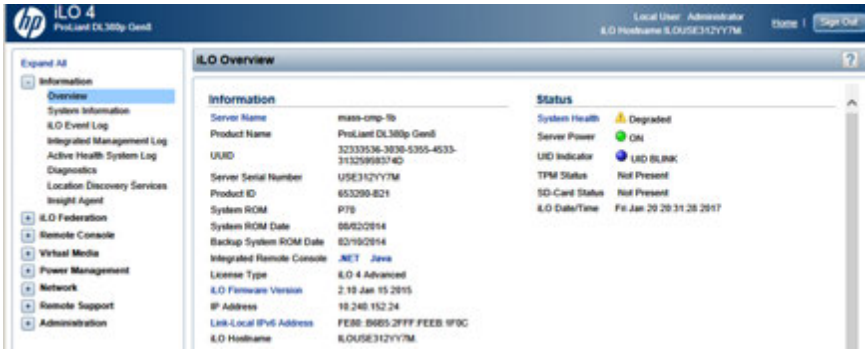
Additional information regarding the IPM install procedure is described in the *TPD Initial Product Manufacture, Software Installation Procedure* (Section 3.3)

5.2.5: IPM of a HP DL380 RMS Server

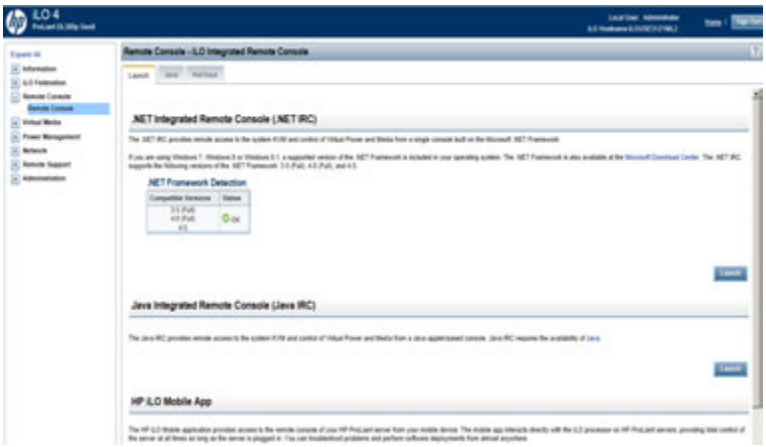
STEP #	This procedure will install system OS (IPM) of the server Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. **Needed material:** - TPD ISO image file to be used for virtual mount accessible on laptop or - USB device prepared with bootable version of TPD image IF THIS PROCEDURE FAILS, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1. ☐	Insert Bootable USB Media/mount TPD ISO	Create a bootable USB drive with the TPD ISO image file. Use the method provided in the "README.txt" file that is included with the downloaded Policy Software or other suitable method for creating a bootable USB device. There are several readily available utilities to achieve this. Then insert the USB drive locally into the server and reboot the server to the bootable USB device. Then proceed to Step 3 of this procedure if using this method If local access to the server is not available and network access to the iLO of the server has been enabled you can use the remote console capability of the HP iLO as per the following procedure See Section "8.1.2: 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: a. Open a browser, enter the URL of the iLO system (management_server_iLO_ip), and log in. For example:

5.2.5: IPM of a HP DL380 RMS Server





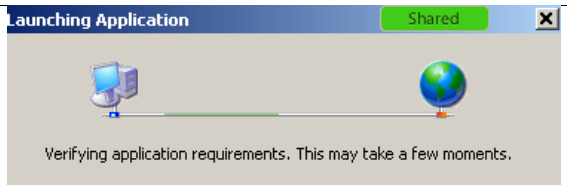
b. On the home page, select Remote Console > Remote Console. The Remote Console page opens. For example:



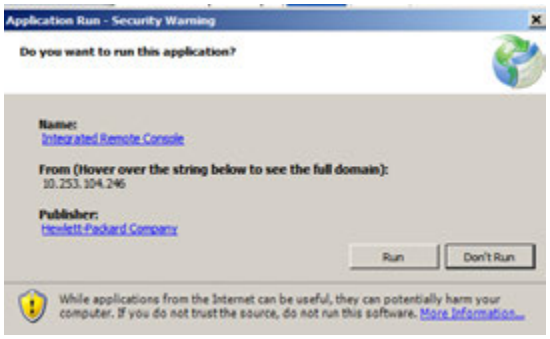
Note: When launching a remote console, the .NET application is compatible with a Windows browser; Java is compatible with both Windows and Firefox browsers.

c. 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:

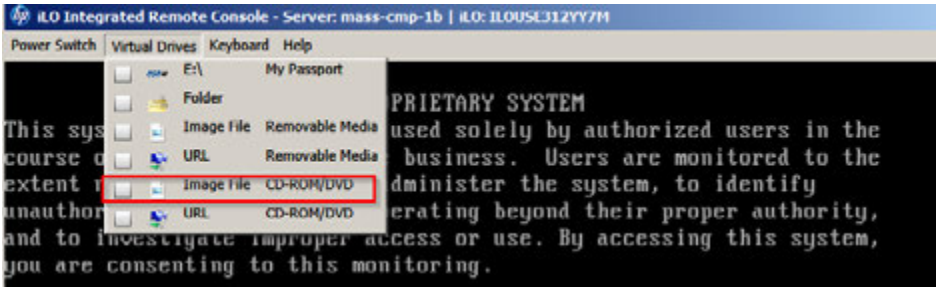
5.2.5: IPM of a HP DL380 RMS Server



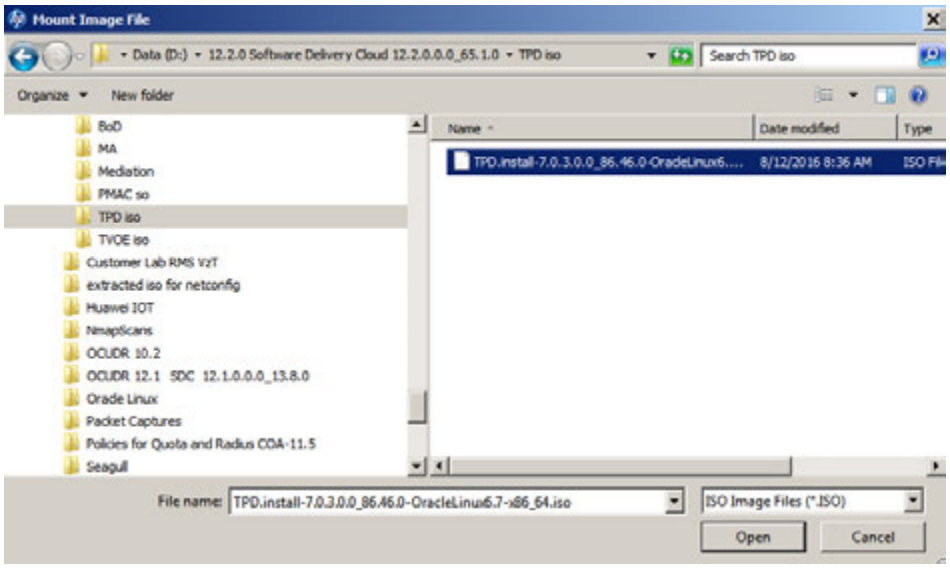
d. Click Run. The Remote Console window opens.



e. Select Virtual Drives > Image File CD-ROM/DVD, browse to the ISO image file location, and click Open. The ISO image file is mounted.

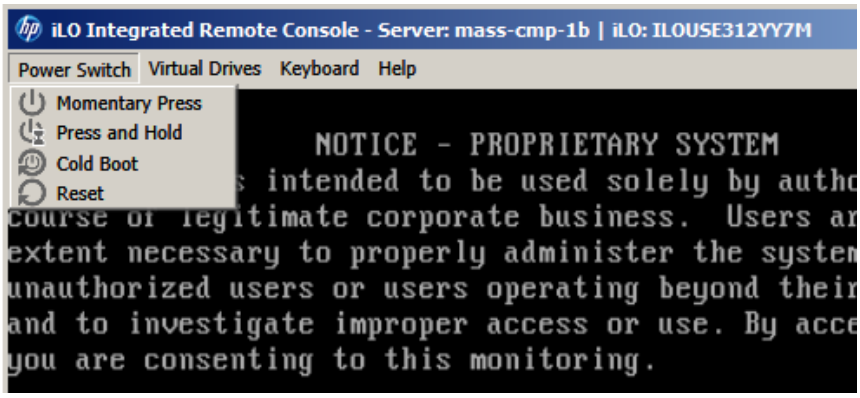


f. Select Image file CD-ROM/DVD and browse to the TPD ISO location then click open:

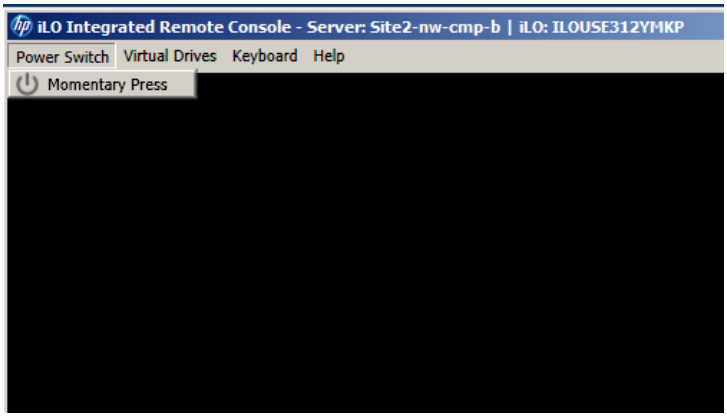


5.2.5: IPM of a HP DL380 RMS Server

g. Select Power Switch > Momentary Press. The server powers down.

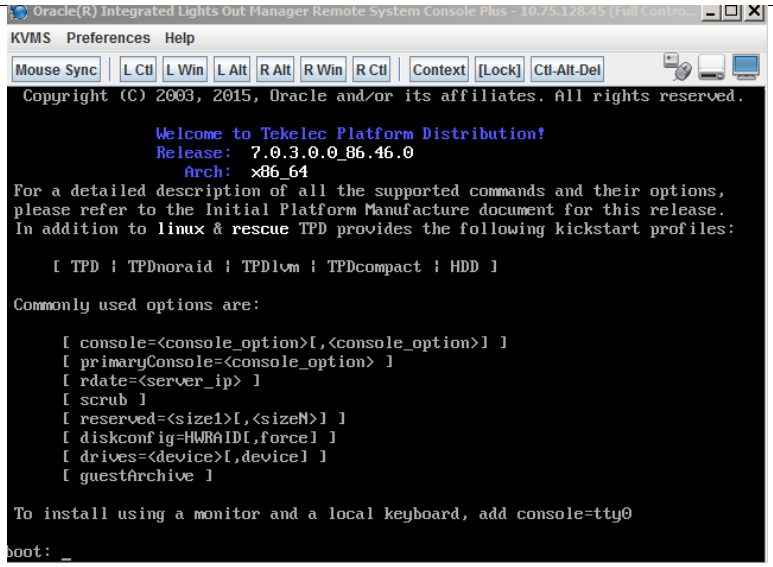


h. When the Power Switch options display the Momentary Press option, Click Momentary Press again.



i. The server starts, and upon completion of the boot process displays a screen similar to the following

5.2.5: IPM of a HP DL380 RMS Server

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


</td>
</tr>
<tr>
<td>2.
☐</td>
<td>**Console:** Enter TPD boot: command with correct options

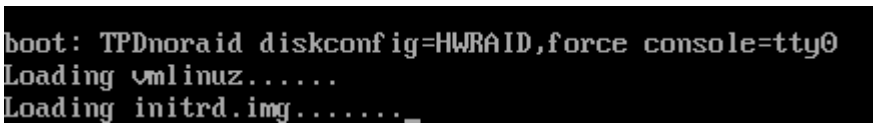
TPD install takes 20 - 40 minutes to complete</td>
<td>
Enter the following command at the boot prompt to initiate the initial product manufacture (IPM) process.

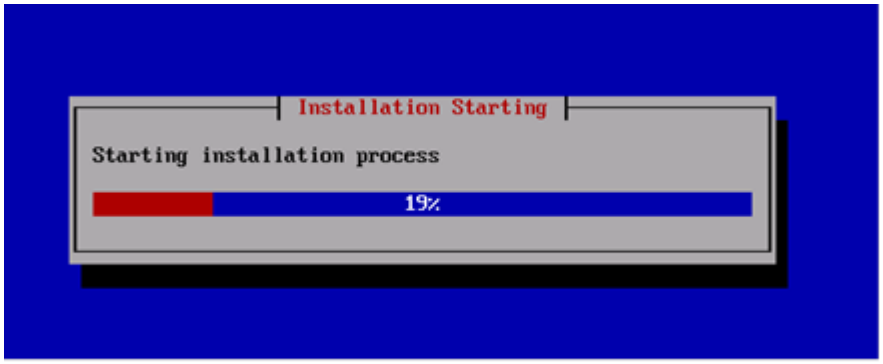
•boot: **TPDnoraid console=tty0 diskconfig=HWRAID,force**

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. Refer to *TPD Initial Product Manufacture, Software Installation Procedure* (Section 3.4)

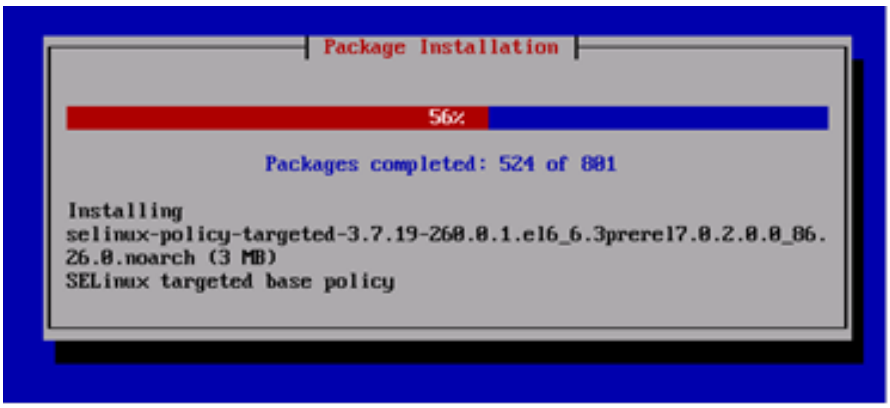
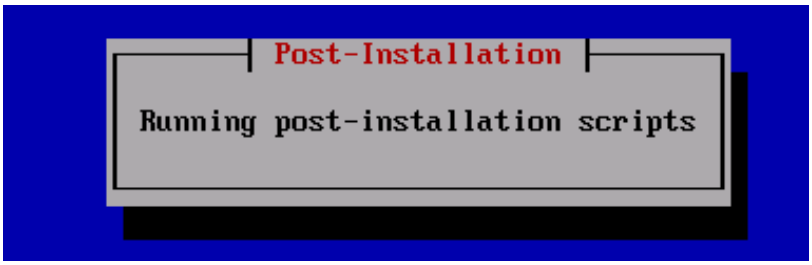
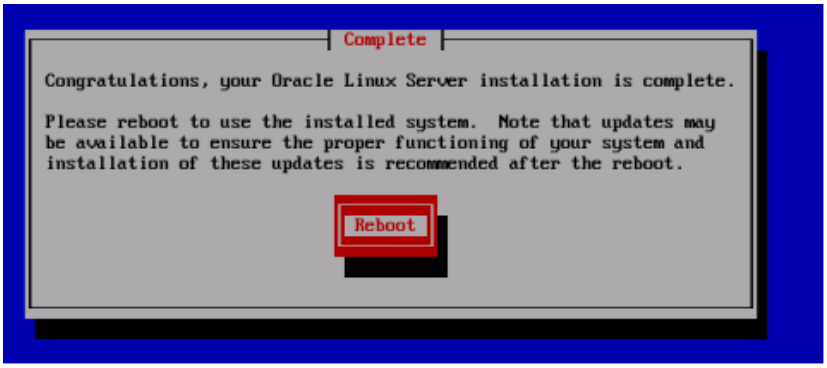
TPD installation takes 20–40 minutes. During this process you see in-progress windows similar to the following



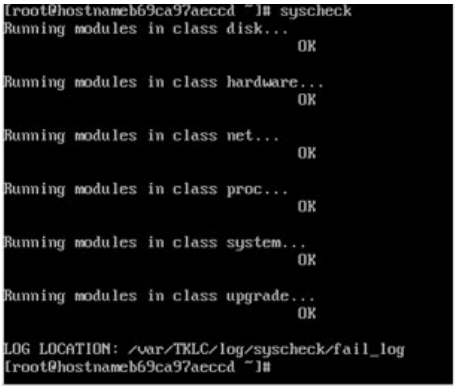


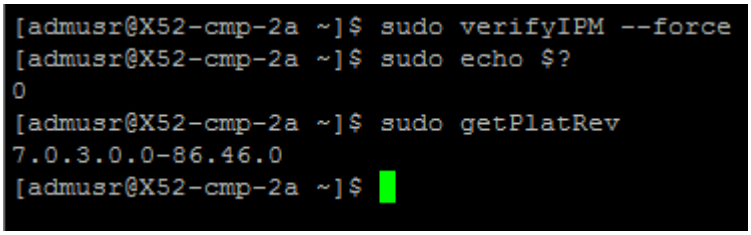
</td>
</tr>
</table>

5.2.5: IPM of a HP DL380 RMS Server

		Then you will be able to monitor the packages installation progress:  Then post installation scripts kick off:  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 will again boot to the bootable media.  When you see the Complete window, the IPM process is complete.
3. ☐	**Remove or unmount the installation media.**	In case installation is done remotely via iLO's remote console, unmount the image from the console's virtual drives menu (uncheck the image file option) then press **Enter** to reboot the server. In the case a bootable USB device was used, remove the USB device If you reboot the server without removing the installation media the server will again boot to the bootable media. If this happens, wait until you see the Complete window, remove the bootable image, and restart again.

5.2.5: IPM of a HP DL380 RMS Server

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	Once the server reboots, the login prompt is displayed. If no login prompt is displayed after waiting 15 minutes, contact Oracle Customer Support for assistance.
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.

THIS PROCEDURE HAS BEEN COMPLETED		

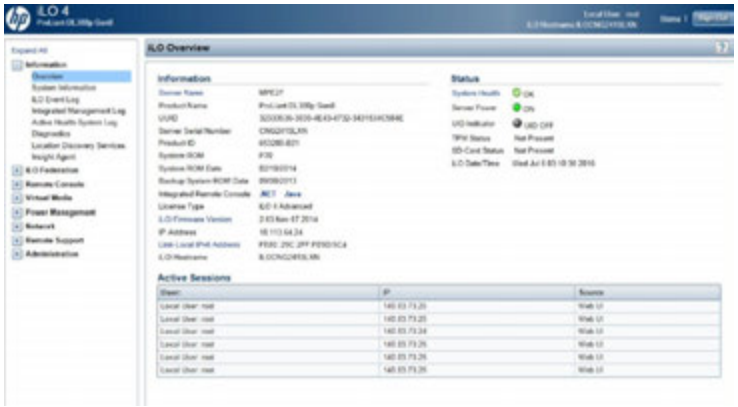
5.2.6 Installing Policy Management Software

5.2.6: *Installing Policy Management Software*

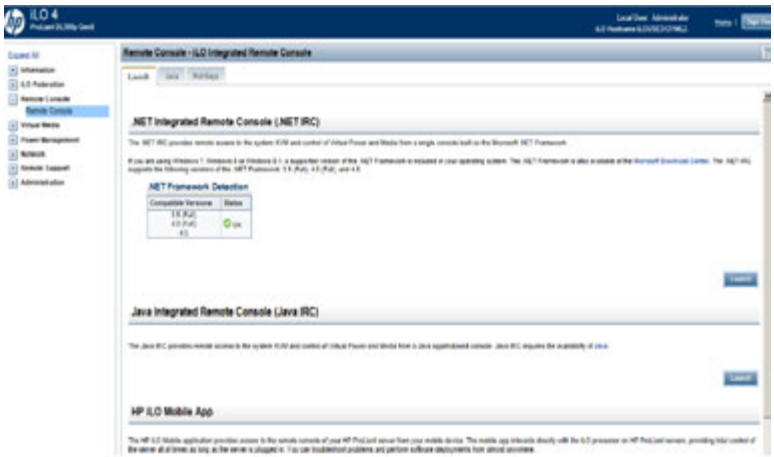
STEP #	This procedure will install the Policy Management Software. Prerequisites: Before beginning this procedure, you must have the following material and information: • The appropriate release and application package(s) of the Policy Management software, either on physical media to mount directly on 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:** Two methods for installing the Policy Application are presented here. The 1st is to use a USB drive inserted locally into the server. This is the preferred method. The 2nd is to 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 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. .	
1. ☐	Make the Policy Application ISO images available for installation	Copy the Policy Application ISO image file (CMP/MPE/MRA/BOD/MA/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, or - using the Server iLO port and iLO Web Interface (to access Remote Console) Proceed to step #2 of this procedure Or If you are using the iLO remote console and have the Policy Management software as an ISO image file, do the following to mount the ISO image file as a virtual drive: Note: This method is dependent on having a good network connection from the workstation where the ISO is located to the target server iLO. The browser used to attach the ISO and launch the server iLO remote console should be co-located with the ISO file repository. a. Open a browser, enter the URL of the iLO system (management_server_iLO_ip), and log in. For example: 

5.2.6: ***Installing Policy Management Software***

After login the iLO home screen presents.

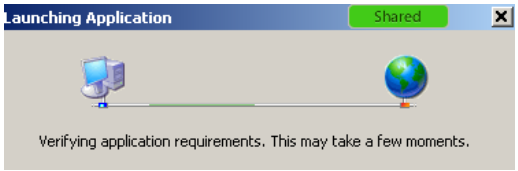


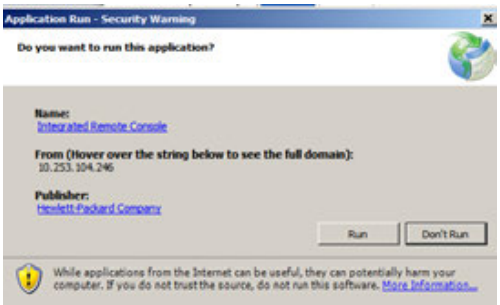
b. On the home page, select Remote Console. The Remote Console page opens. For example:



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

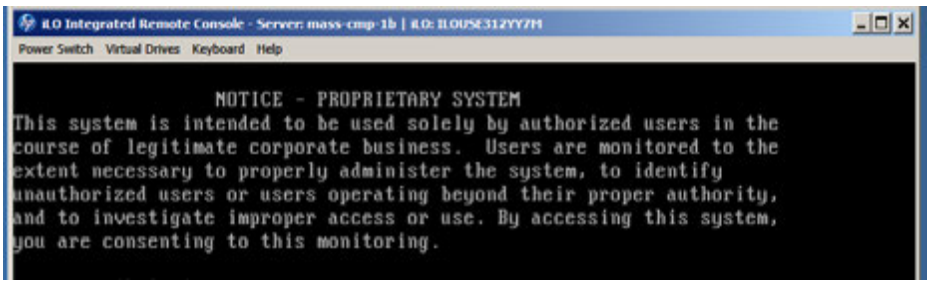
c. In the Java Integrated Remote Console section, click Launch. A security warning window opens, prompting for confirmation that you want to run the application. For example:



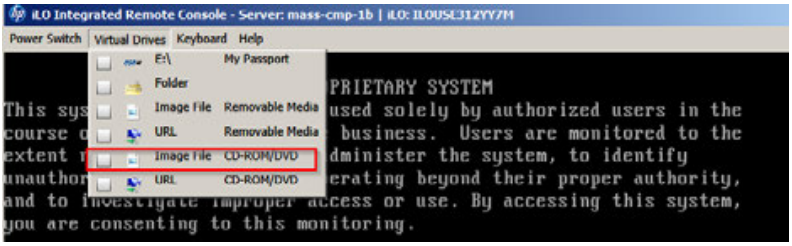


5.2.6: ***Installing Policy Management Software***

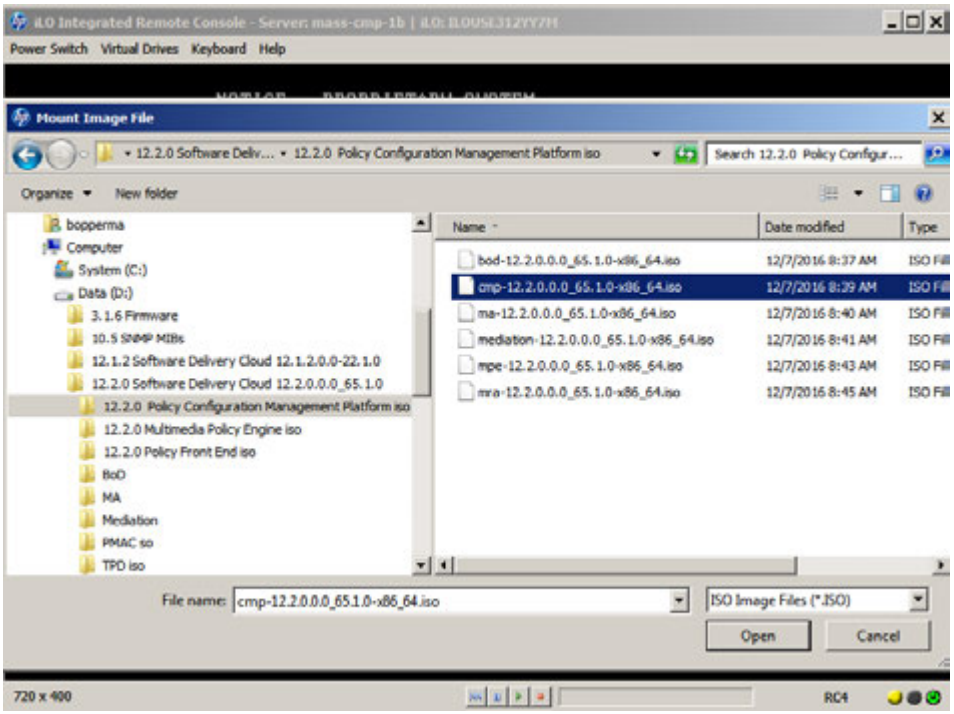
d. Click Run. The Remote Console window opens.



e. Select Virtual Drives > Image File CD-ROM/DVD, browse to the ISO image file location, and click Open. The ISO image file is mounted.

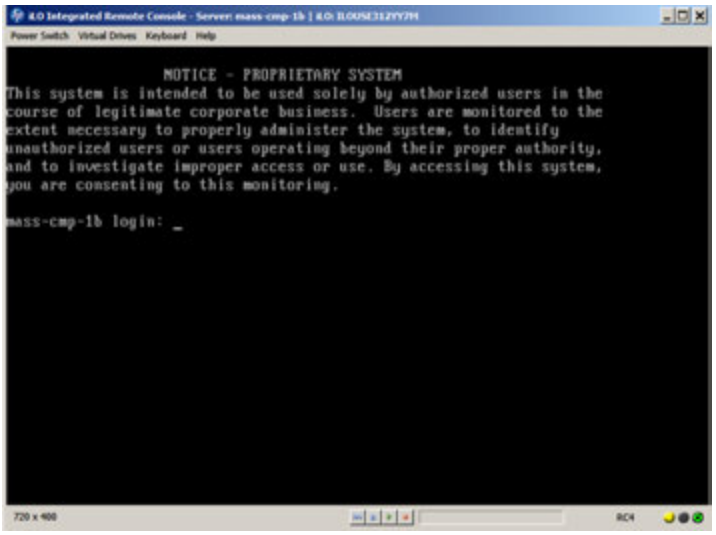
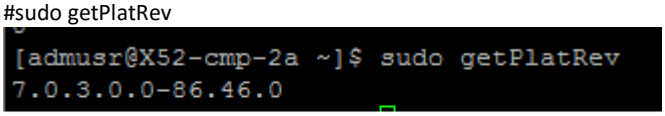
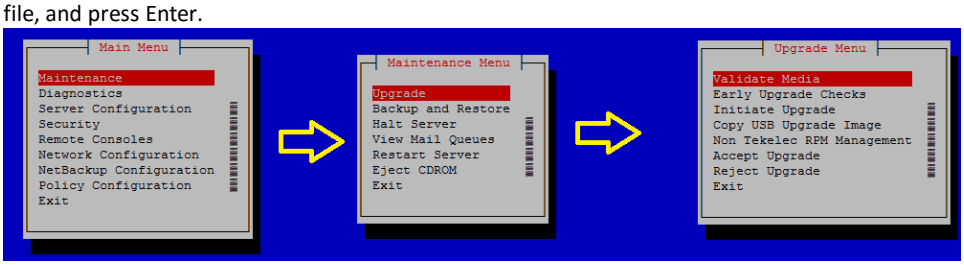


Note: Make certain that the ISO image file selected (CMP/MPE/MRA/BOD/MA/MEDIATION) is the correct one for the target server according to the Policy Solution Design!



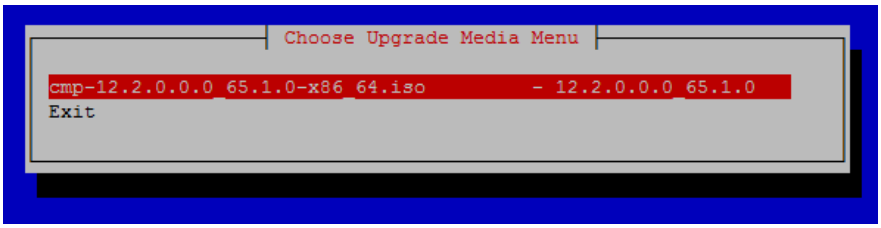
In this example the CMP ISO image has been selected. Click open to mount the required ISO image file, the screen will close (the ISO has mounted) and you will be returned to the CLI prompt of the remote console.

5.2.6: ***Installing Policy Management Software***

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> if not already logged in. 
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	Enter the following command to start the Platform Configuration utility: #sudo su - platcfg The Platform Configuration Main menu opens. From the Main menu, navigate to Maintenance > Upgrade > Validate Media, select the ISO image file, and press Enter.  **Note:** Depending on the method used the platcfg utility will search for any mounted ISOs and if successful will display the Policy Application ISO image file to install

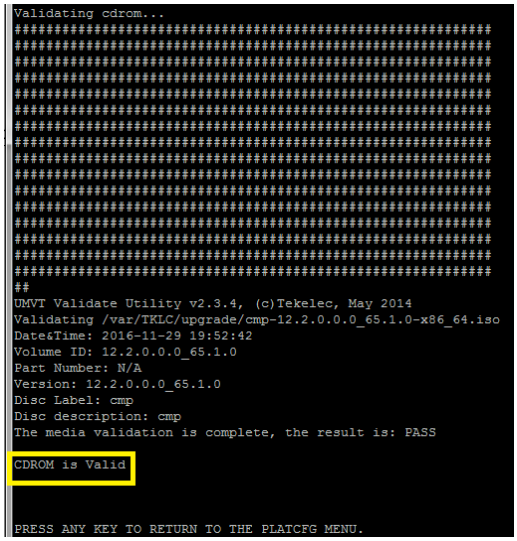
5.2.6: ***Installing Policy Management Software***

For example:



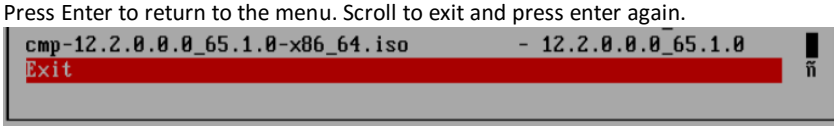
Then choose the ISO image and press enter:

The utility displays "Validating media or cdrom"… and a series of hash marks (#) signs. When it finishes it displays information about the ISO image file and the message the CDROM or Media is Valid. The following example shows a successful validation:

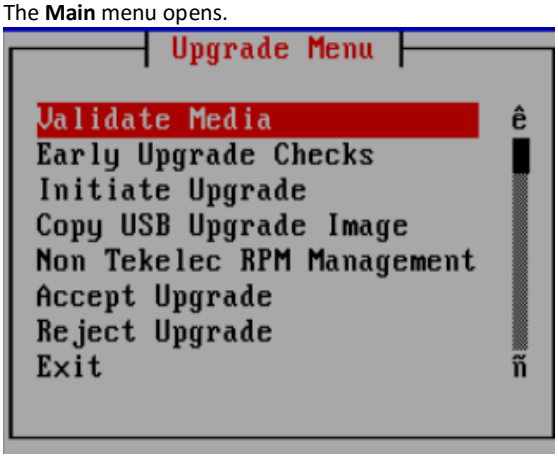


5. ☐ **Console:** verify platform revision

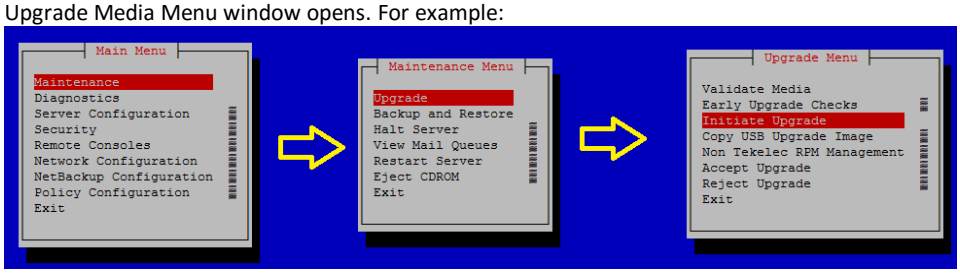
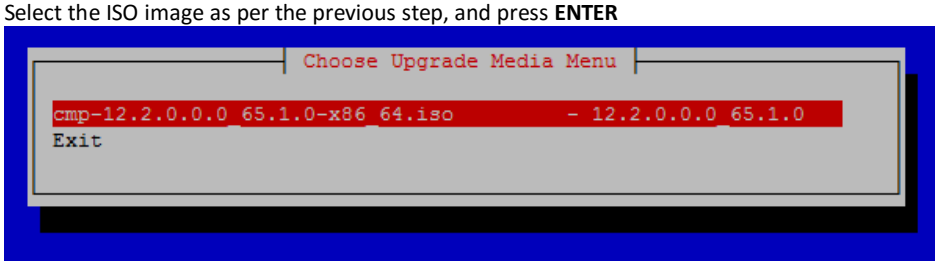
Press Enter to return to the menu. Scroll to exit and press enter again.



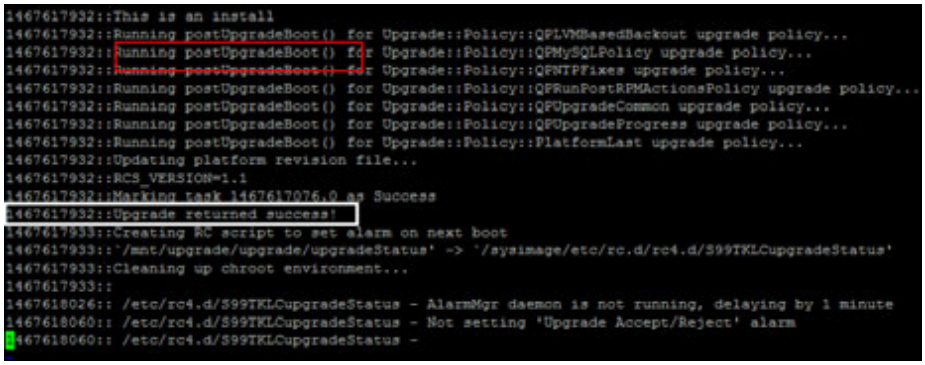
The **Main** menu opens.



5.2.6: ***Installing Policy Management Software***

6. ☐	**Console:** Select ISO to install, and confirm Application install may take 20 Minutes – if installing with a virtual mount, it will take longer	From the Main menu, navigate to Maintenance > Upgrade > Initiate Upgrade. The Choose Upgrade Media Menu window opens. For example:  Select the ISO image as per the previous step, and press **ENTER**  **Note:** The server will reboot twice during the installation process, Do Not Remove the media at this time.

7. ☐	**Console:** Verify Policy install version	After the application has completed installation log back in to the command line as admusr and confirm the installed TPD platform version and the policy application version.
		
		$appRev
		`mass-cmp-1b login: admusr`
		`Password:`
		`Last login: Fri Jan 20 17:11:38 on tty1`
		`[admusr@mass-cmp-1b ~]$ appRev`
		`Install Time: Thu Jan 19 17:07:20 2017`
		`Product Name: cmp`
		`Product Release: 12.2.0.0.0_65.1.0`
		`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-12.2.0.0.0_65.1.0-x86_64.iso`
		`OS: OracleLinux 6.7`
		
		Verify:
		• TPD revision installed
		• Policy 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: 

5.2.6: ***Installing Policy Management Software***

		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, BoD, MA, MEDIATION) on each server. For Wireless mode, proceed *to* *Section 6: Configure Policy Application Servers in Wireless Mode* For Cable mode, proceed *to* *Section 7: Configure Policy Application Servers in Cable Mode*
THIS PROCEDURE HAS BEEN COMPLETED		

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 will used for the Management Server.

Refer to *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 refer to 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 12.2, 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.*

Refer to *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 will configure initial OA settings using a configuration wizard. This procedure should be used for initial configuration only and should be executed 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 need to be configured

If the aggregation switches are provided by the customer, the user must ensure that the customer aggregation switches are configured as per requirements provided in the NAPD (CGBU_019407).

- Section 3.5.3 Configure OA Security

This procedure will disable telnet access to OA.

- Section 3.5.4 Upgrade or Downgrade OA Firmware

This procedure will update the firmware on the OA's.

- Section 3.5.5 Store OA Configuration on Management Server

This procedure will backup OA settings on the management server.

- Section 3.5.9 Updating IPv4 Addressing

This procedure will update the IP addressing for a C7000 enclosure.

Or

- Section 3.5.10 Updating IPv6 Addressing

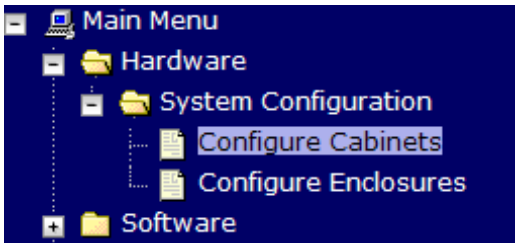
This procedure will update the IP addressing for a C7000 enclosure. It may be used to add IPv6 addresses and/or to edit existing IPv6 addresses.

- Section 3.5.11 Add SNMP Trap Destination on OA

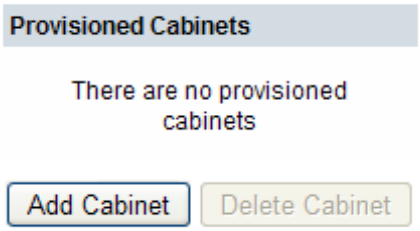
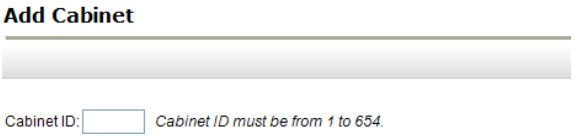
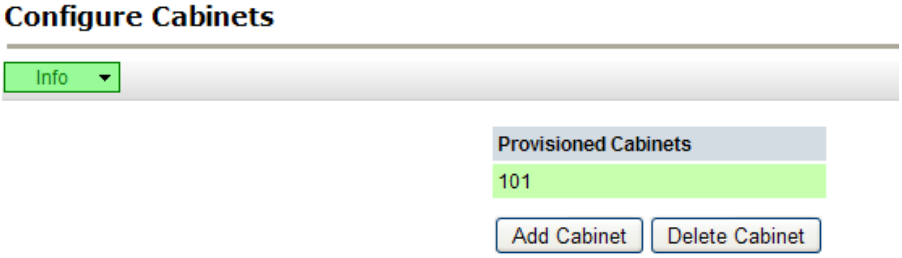
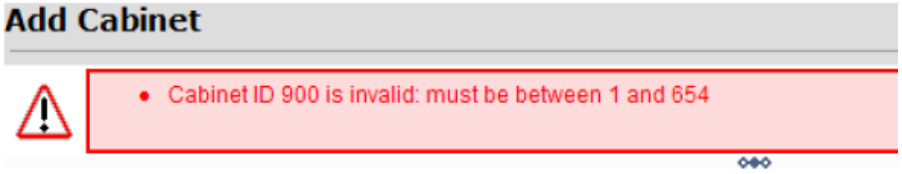
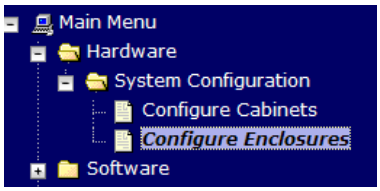
An SNMP trap destination must be added and configured using the Onboard Administrator (OA), or SNMP must be disabled.

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

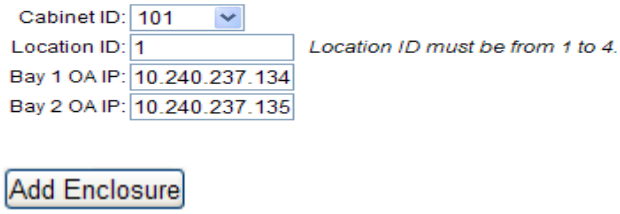
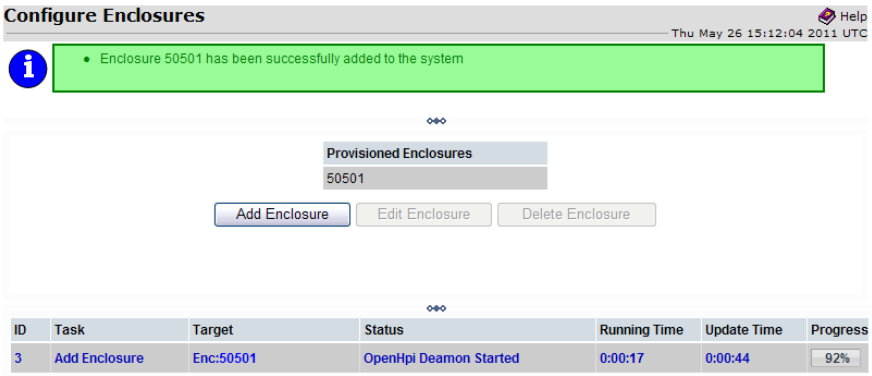
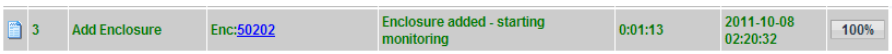
5.3.3: Adding the Cabinet and the Enclosure to PM&C

STEP #	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 will have 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.	
1. ☐	**PM&C GUI:** Login	Open web browser and enter: **https://<pmac_management_network_ip>** Log in as the pmacadmin user. 
2. ☐	**PM&C GUI:** Configure Cabinets	Navigate to **Main Menu** -> **Hardware** -> **System Configuration** -> **Configure Cabinets**. 

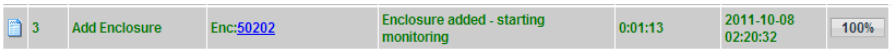
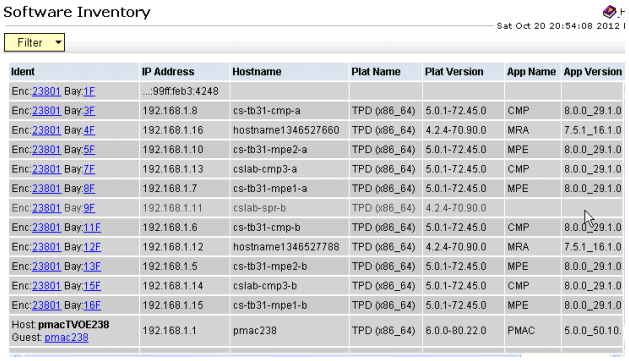
5.3.3: Adding the Cabinet and the Enclosure to PM&C

3. ☐	**PM&C GUI:** Add Cabinet	On the Configure Cabinets panel click on **Add Cabinet...** 
4. ☐	**PM&C GUI:** Enter Cabinet ID	Enter Cabinet ID and press **Add Cabinet**. 
5. ☐	**PM&C GUI:** Check errors	If no error is reported to the user you will see the following:  Or you will see an error message: 
6. ☐	**PM&C GUI:** Go to Configure HPC Enclosures	Navigate to **Main Menu** -> **Hardware** -> **System Configuration** -> **Configure Enclosures**. 

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

7. ☐	**PM&C GUI:** Go to Add Enclosure	On the Configure Enclosures panel click on **Add Enclosure...** 
8. ☐	**PM&C GUI:** Add Enclosure	On the Add Enclosure panel, enter the Cabinet ID, Location ID, and two OA IP addresses (the enclosure's active and standby OA). Then click on **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 will be combined to create a globally unique id for the enclosure (for example, an enclosure in cabinet 502 at location 1, will have an enclosure id of 50201). Enclosures are typically numbered from the bottom. i.e. Enclosure in the bottom of the cabinet is location = 1.
9. ☐	**PM&C GUI:** Monitor the Enclosure discovery status	When the task is complete, the text will change to green and the Progress bar will indicate "100%". 
10. ☐	**PM&C GUI:** Background Task monitoring	This page allows the user to monitor status updates:  **NOTE:** DO NOT click the ☒ button as this will delete the selected task from the Background Task Monitoring status screen.

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

11. ☐	**PM&C GUI:** Wait until the Add Enclosure task finishes	The color of the progress bar will change to green when complete:  3 | Add Enclosure | Enc:50202 | Enclosure added - starting monitoring | 0:01:13 | 2011-10-08 02:20:32 | 100% If the Add Enclosure task fails the Status will display information concerning the failed step and the color of the Progress bar will change to red.
12. ☐	**PM&C GUI:** Verify Software Inventory	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 will show blade server information. Example below:  Software Inventory Sat Oct 20 20:54:08 2012 Filter Ident | IP Address | Hostname | Plat Name | Plat Version | App Name | App Version Enc:23801 Bay:1F | ...:99ff:feb3:4248 Enc:23801 Bay:3F | 192.168.1.8 | cs-tb31-cmp-a | TPD (x86_64) | 5.0.1-72.45.0 | CMP | 8.0.0_29.1.0 Enc:23801 Bay:4F | 192.168.1.16 | hostname1346527660 | TPD (x86_64) | 4.2.4-70.90.0 | MRA | 7.5.1_16.1.0 Enc:23801 Bay:5F | 192.168.1.10 | cs-tb31-mpe2-a | TPD (x86_64) | 5.0.1-72.45.0 | MPE | 8.0.0_29.1.0 Enc:23801 Bay:7F | 192.168.1.13 | cslab-cmp3-a | TPD (x86_64) | 5.0.1-72.45.0 | CMP | 8.0.0_29.1.0 Enc:23801 Bay:8F | 192.168.1.7 | cs-tb31-mpe1-a | TPD (x86_64) | 5.0.1-72.45.0 | MPE | 8.0.0_29.1.0 Enc:23801 Bay:9F | 192.168.1.11 | cslab-spr-b | TPD (x86_64) | 4.2.4-70.90.0 Enc:23801 Bay:11F | 192.168.1.6 | cs-tb31-cmp-b | TPD (x86_64) | 5.0.1-72.45.0 | CMP | 8.0.0_29.1.0 Enc:23801 Bay:12F | 192.168.1.12 | hostname1346527788 | TPD (x86_64) | 4.2.4-70.90.0 | MRA | 7.5.1_16.1.0 Enc:23801 Bay:13F | 192.168.1.5 | cs-tb31-mpe2-b | TPD (x86_64) | 5.0.1-72.45.0 | MPE | 8.0.0_29.1.0 Enc:23801 Bay:15F | 192.168.1.14 | cslab-cmp3-b | TPD (x86_64) | 5.0.1-72.45.0 | CMP | 8.0.0_29.1.0 Enc:23801 Bay:16F | 192.168.1.15 | cs-tb31-mpe1-b | TPD (x86_64) | 5.0.1-72.45.0 | MPE | 8.0.0_29.1.0 Host: pmacTVOE238 Guest: pmac238 | 192.168.1.1 | pmac238 | TPD (x86_64) | 6.0.0-80.22.0 | PMAC | 5.0.0_50.10. NOTE: The procedure to configure the Enclosure switches, if they have not been previously configured, is yet to be performed.
THIS PROCEDURE HAS BEEN COMPLETED		

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:

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

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

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

3. 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

4. Copy the file to the following directory:

/usr/TKLC/smac/html/ilo_passwd

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

$ **sudo chmod 777 change_ilo_admin_passwd.xml**

6. Edit the file to update the *root password*, *iLO root password***,** and *iLO Administrator password* fields.

7. Make a temporary copy of the file in the following directory:

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

8. 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.

9. Log out from the active OA.

10. Delete the temporary copy of the file.

11. (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.

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

- For 4948 aggregation enclosure switches:
  - 4948_cClass_init.xml
  - 4948_layer2_configure.xml
  - 4948_layer3_configure.xml
  - 4948_RMS_init.xml
- For 4948E aggregation enclosure switches:
  - 4948E_cClass_init.xml
  - 4948E_layer2_configure.xml
  - 4948E_layer3_configure.xml
  - 4948E_RMS_init.xml
- For 6120XG enclosure switches:
  - 6120XG_init.xml
  - 6120XG_Single_configure.xml (for connections using a single 10 Gb/s copper uplink)
  - 6120XG_LAG_Uplink_configure.xml (for connections using a bundle of four 1 Gb/s copper uplinks)
  - 6120XG_TagCtl_Uplink_configure.xml (if the Control network will be VLAN tagged)
- For 6125XLG enclosure switches:
  - 6125XLG_init.xml
  - 6125XLG_Single_configure.xml (for connections using a single 10 Gb/s copper uplink)
  - 6125XLG_LAG_Uplink_configure.xml (for connections using a bundle of four 1 Gb/s copper uplinks)

Prerequisite:

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

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

The procedures to configure aggregation switches and enclosure switches using netConfig are described in the 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 need to confirm and update the BIOS boot order on the Policy Management servers.

Prerequisites:
Before beginning this procedure, you must have updated the firmware on the Policy Management servers.
To complete this procedure, you need the following information:

- The **root** password *root_password* (use the **root** account instead of the **Admin** account)
- You should not need to reset the date and time

The procedure for BIOS configuration are located in section *8.3.1:BIOS Settings for HP Gen 8 Blade and Rackmount Servers* or *8.3.2: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:

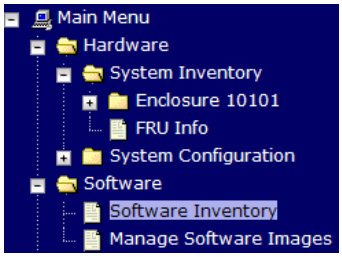
- Before beginning this procedure, you must have configured the PM&C application.
- To complete this procedure, you need the following:
  - TPD ISO image file.
  - Policy Management ISO image files (CMP, MPE, MRA, Mediation).

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

5.3.10: IPM Enclosure Blades Using the PM&C

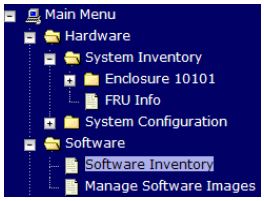
STEP #	This procedure will provide the steps to install TPD on Blade servers from PM&C. **Prerequisites**: Enclosures containing the blade servers targeted for IPM that have been configured. Appropriate version of TPD is previously added to the PM&C Software Image management. Check off (√) each step 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.	
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 will act as a DHCP server and provide control network addresses in the range of 192.168.1.3 – 254 to the blade servers in the managed cabinets/enclosures. PM&C always takes the address of 192.168.1.1. If the server has requested an IP address from PM&C, the IP address will appear in the "IP Address" column. TPD will always do this when a server blade is booted, and also periodically after this. 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. |				
---	---	---	---	---
Enc:801 Bay:6F	192.168.1.21	hostnameb9d92a84cefe	TPD (x86_64)	7.0.2.0.0-86.28.0
Enc:801 Bay:8F	192.168.1.16	hostname6de5d09f047e	TPD (x86_64)	7.0.2.0.0-86.28.0	 Porceed to the next step to IPM (install the OS) on the selected blade

5.3.10: IPM Enclosure Blades Using the PM&C

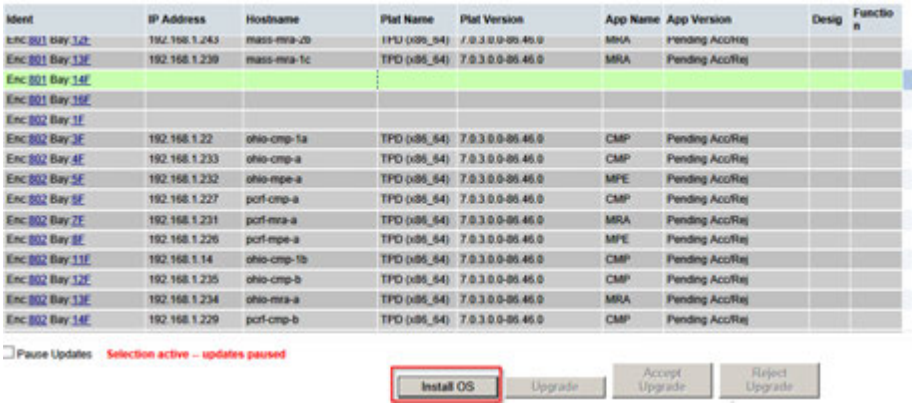
2. ☐

PM&C GUI: Initiate OS Install

Navigate to **Software** -> **Software Inventory**.

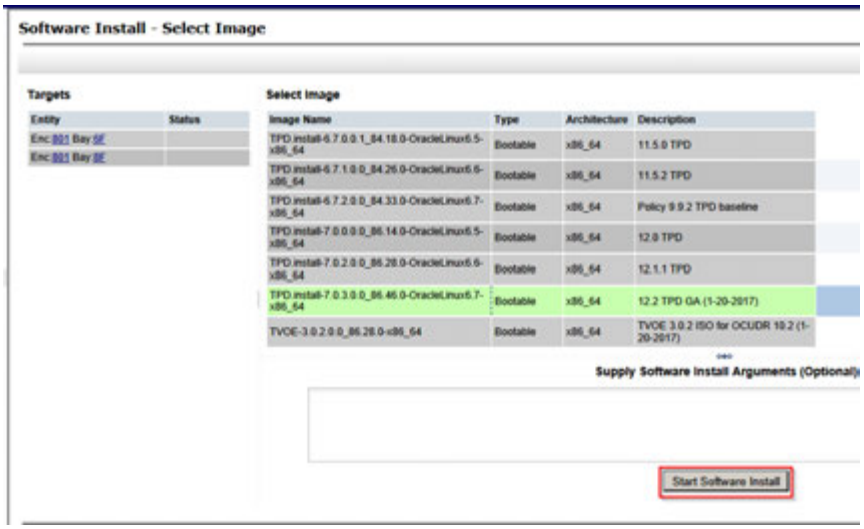


Select the servers you want to IPM with a bootable TPD ISO image file and select Install OS button. If you want to install the same OS image to more than one server, you may select multiple servers by clicking multiple rows individually. Selected rows will be highlighted in green.



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

After selecting "Install OS" the Software Install –Select Image screen appears:



Any bootable images in the PM&C repository will present. Choose the correct bootable image to proceed with the OS installation of the selected blade and click on "**Software Start Install**".

5.3.10: IPM Enclosure Blades Using the PM&C

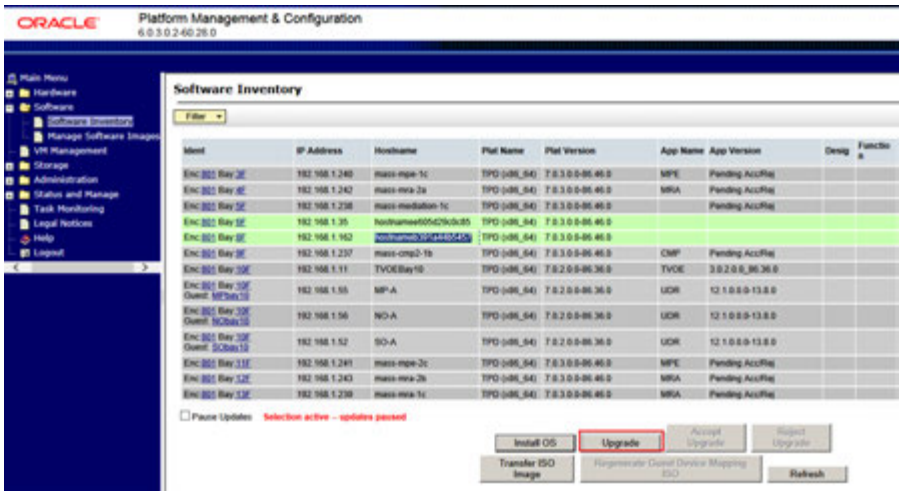
3. ☐	**PM&C GUI:** Monitor OS Install	Navigate to **Main Menu** > **Task Monitoring** to monitor the progress of the OS Installation background task. A separate task will appear for each blade affected.  When the installation is complete, the task will change to green and the Progress bar will indicate "100%". | ID | Task | Target | Status | State | Running Time | Start Time | Progress | | 970 | Install OS | Enc:801 Bay:8F | Done: TPD.install-7.0.3.0.0_86.46.0-OracleLinux6.7-x86_64 | COMPLETE | 0:21:52 | 2017-01-29 18:12:34 | 100% | | 969 | Install OS | Enc:801 Bay:6F | Done: TPD.install-7.0.3.0.0_86.46.0-OracleLinux6.7-x86_64 | COMPLETE | 0:23:00 | 2017-01-29 18:12:33 | 100% | NOTE: if the OS Install step fails, then it may be that the Control Network is not correctly established, and troubleshooting will be required.
THIS PROCEDURE HAS BEEN COMPLETED		

5.3.11 Install Policy Management Software on Blades using PM&C

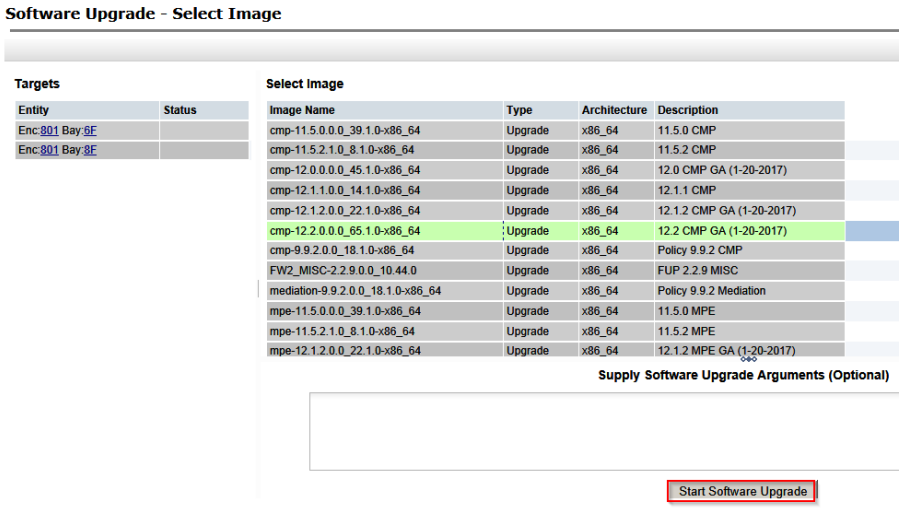
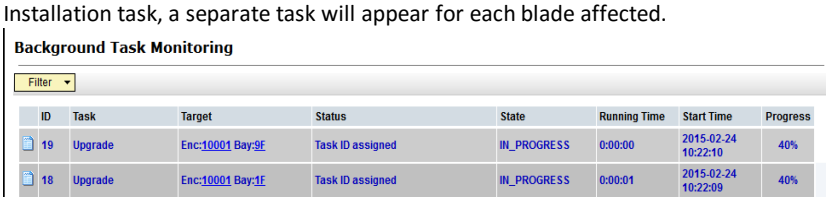
5.3.11: Install the Policy Management Application Software on Blades using PM&C

STEP #	This procedure will 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 will run which Policy Management application. IF THIS PROCEDURE FAILS, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ASSISTANCE.

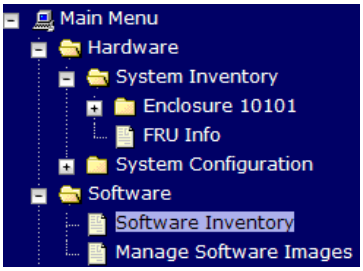
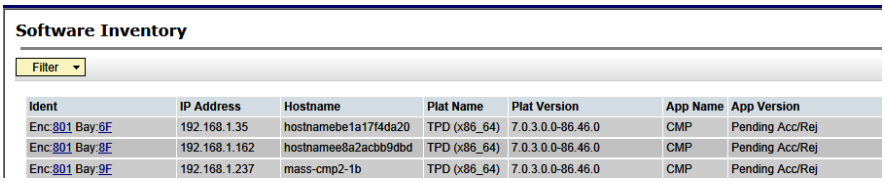
5.3.11: Install the Policy Management Application Software on Blades using PM&C

1. ☐	**PM&C GUI:** Login	Open web browser and enter: **http://<management_network_ip>** Login as PM&C admin user. 
2. ☐	**PM&C GUI:** Select Servers for Application install	Navigate to **Software** -> **Software Inventory**.  Select the servers on which the application is to be installed. If you want to install the same application image to more than one server, you may select multiple servers by clicking multiple rows individually. Selected rows will be highlighted in green. **Note:** After the TPD OS has been installed the system will assign a given hostname. **Note:** 8 is the maximum number to be selected at one time. Click on **Upgrade**

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

3. ☐	**PM&C GUI:** Initiate Application Install	The Software – Upgrade Page presents. The left side of this screen shows the servers to which the Application Software will be applied. From the list of available images presented, select the correct version and Application Software Package (CMP/MRA/MPE/Mediation) according to the system design.  Click on **Start Software Upgrade**, a confirmation window will pop up, click on **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 will appear for each blade affected.  When the installation is complete, the task will change to green and the Progress bar will indicate "100%". 
5. ☐	**REPEAT the above steps for each Application**	**Repeat steps 3 and 4 for each Application beings installed at the site.**

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

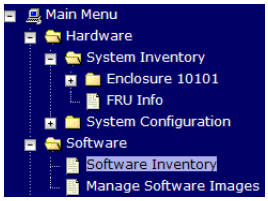
6. ☐	**Verify Application installations-Accept Upgrade**	Navigate to **Software** -> **Software Inventory**.  At this point, all the target servers have had their correct applications newly installed and the AppVersion appears as **Pending Acc/Reject**.  **Software Inventory** Filter Verify the App Name shows the correct name (CMP/MPE/MRA/Mediation) for each server on which the Applications are now installed. Also confirm the correct Enclosure and Bay position. Confirm all assignments are per the design. Now select the servers you wish to "Accept Upgrade". The Accept Upgrade" button will now be available to press. Confirm you wish to accept the Upgrade.

Ident	IP Address	Hostname	Plat Name	Plat Version	App Name	App Version
Enc:801 Bay:6F	192.168.1.35	hostnamebe1a17f4da20	TPD (x86_64)	7.0.3.0.0-86.46.0	CMP	Pending Acc/Rej
Enc:801 Bay:8F	192.168.1.162	hostnamee8a2acbb9dbd	TPD (x86_64)	7.0.3.0.0-86.46.0	CMP	Pending Acc/Rej
Enc:801 Bay:9F	192.168.1.237	mass-cmp2-1b	TPD (x86_64)	7.0.3.0.0-86.46.0	CMP	Pending Acc/Rej

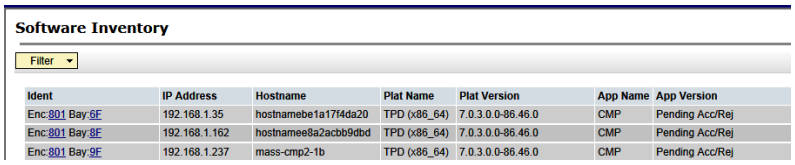
5.3.11: Install the Policy Management Application Software on Blades using PM&C

7. ☐ **Verify Application installations-Accept Upgrade**

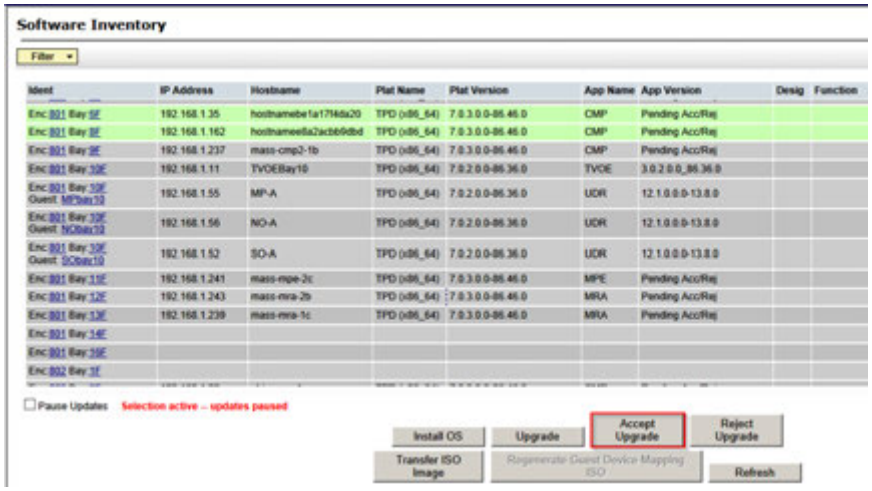
Navigate to **Software** -> **Software Inventory**.

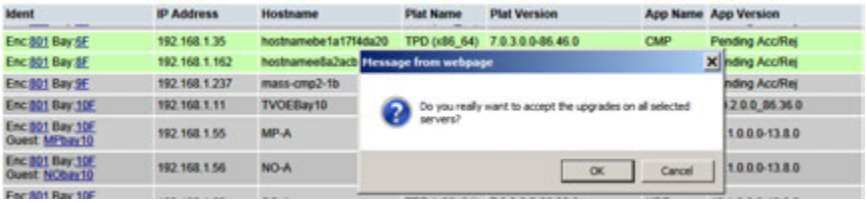


At this point, all the target servers have had their correct applications newly installed and the AppVersion appears as **Pending Acc/Reject**.



Verify the App Name shows the correct name (CMP/MPE/MRA) for each server on which the Applications are now installed. Also confirm the correct Enclosure and Bay position. Confirm all assignments are per the design. Now select the servers you wish to "Accept Upgrade". The Accept Upgrade" button will now be available to press. Confirm you wish to accept the Upgrade.





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

8. ☐	**Verify Application Installations**	Navigate to **Software** -> **Software Inventory**. **Software Inventory** Filter Ident | IP Address | Hostname | Plat Name | Plat Version | App Name | App Version Enc:801 Bay:6F | 192.168.1.35 | hostnamebe1a17f4da20 | TPD (x86_64) | 7.0.3.0.0-86.46.0 | CMP | 12.2.0.0.0_65.1.0 Enc:801 Bay:8F | 192.168.1.162 | hostnamee8a2acbb9dbd | TPD (x86_64) | 7.0.3.0.0-86.46.0 | CMP | 12.2.0.0.0_65.1.0 You can now confirm that the “App Version” column no longer displays the “Pending Acc/Rej” status but rather shows the correct Application Version.
THIS PROCEDURE HAS BEEN COMPLETED		

6. CONFIGURE POLICY APPLICATION SERVERS IN WIRELESS MODE

The following procedures configure the Policy Management Application and establish the network relationships, to a level that 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 within 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

Configuration Management Platform Wireless User's Guide Release 12.2

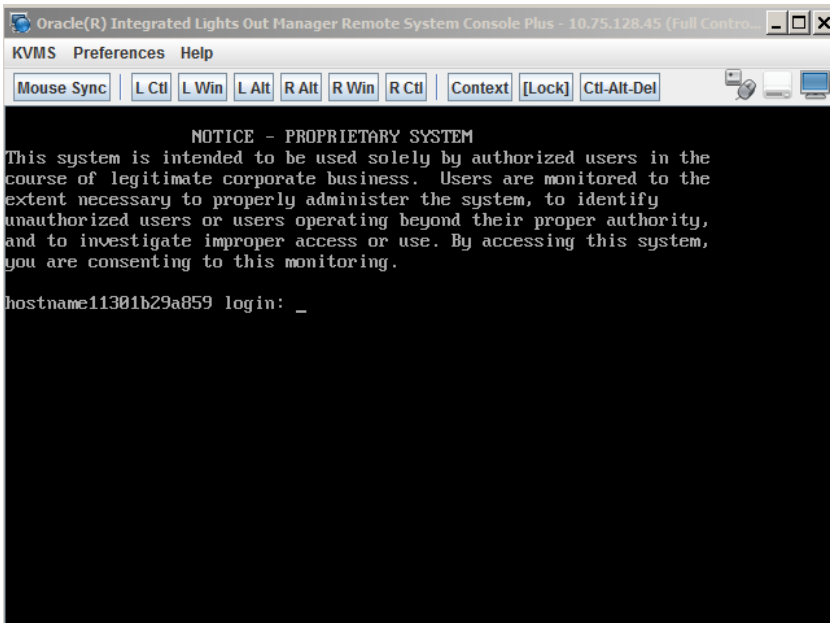
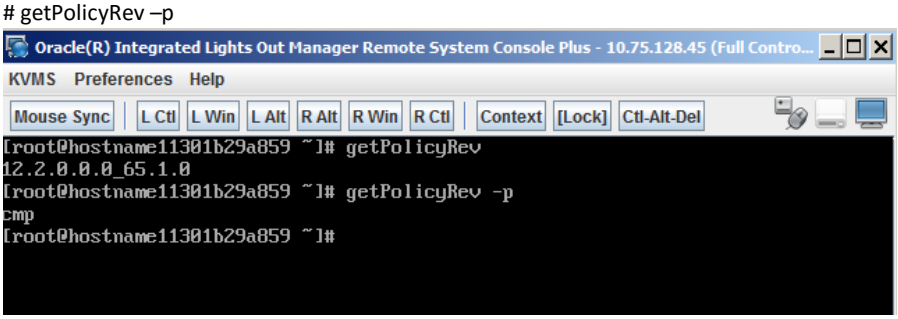
Platform Configuration User's Guide Release 12.2

6.1 PERFORM INITIAL SERVER CONFIGURATION OF POLICY SERVERS - PLATCFG

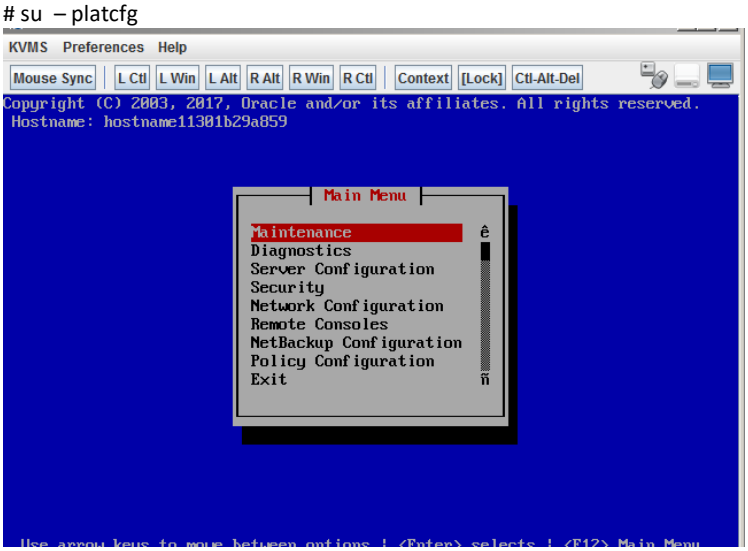
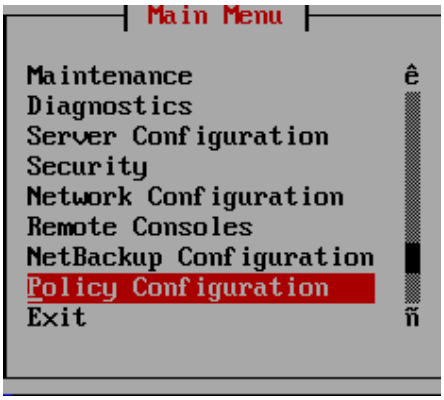
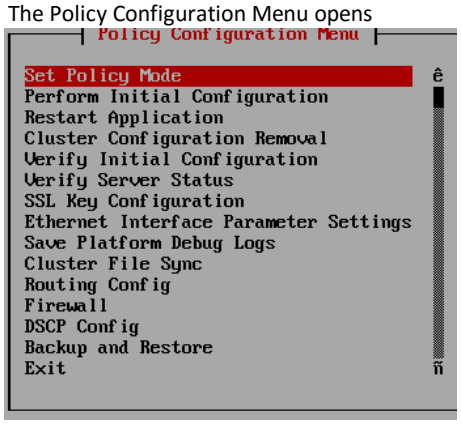
6.1: Perform Initial Server Configuration of Policy Servers - Platcfg

STEP #	
	You must configure the operation, administration, and management (OAM) network address of the server, as well as related networking. Execute the referenced procedure on every server in the Policy Management network. **Prerequisites:** To complete this procedure, you need the following information: • This procedure assumes that you are using Policy Management in a Wireless or Wireless-C (Wireless with Mediation). • You need to know whether or not the server has an optional Ethernet Mezzanine card installed. • Hostname — the unique hostname for the device being configured. • OAM Real IP IPv4 Address — the IP address that is permanently assigned to this device. • OAM Default IPv4 Route — the default route of the OAM network. The MPE and MRA system may move the default route to the SIG-A interface once 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 once 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. IF THIS PROCEDURE FAILS, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ASSISTANCE.

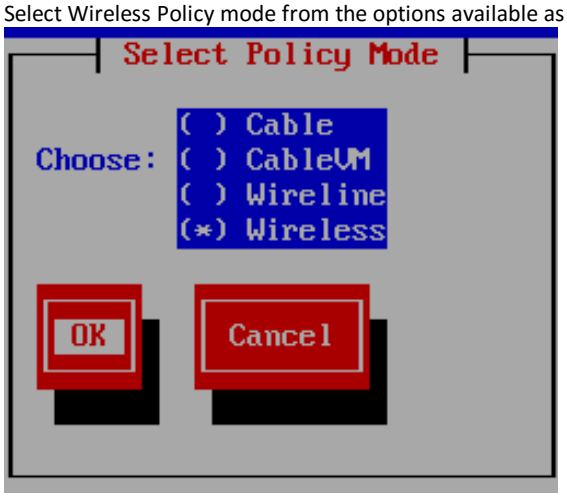
6.1: Perform Initial Server Configuration of Policy Servers - Platcfg

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 8:Accessing the iLO VGA Redirection Window 
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 will be either cmp, mpe, mra or mediation

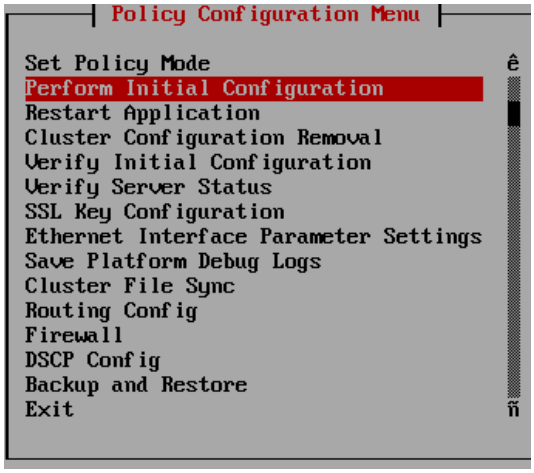
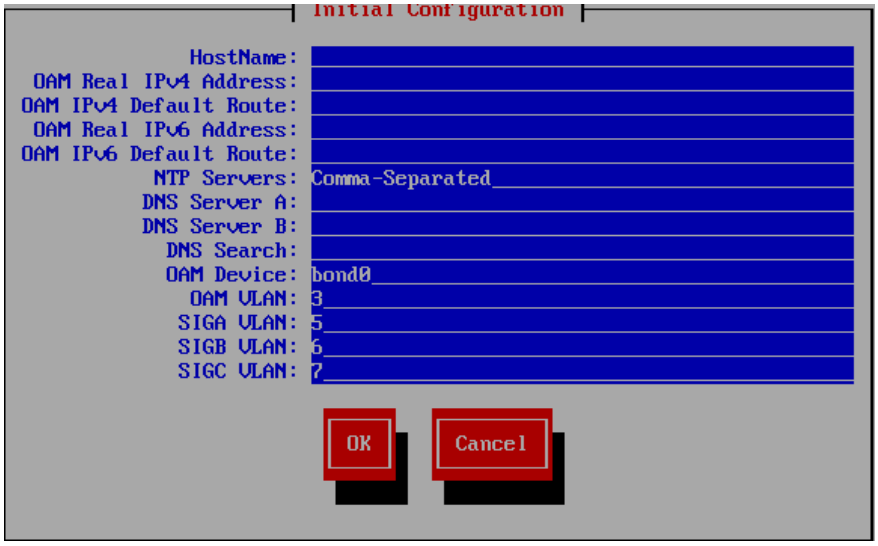
6.1: Perform Initial Server Configuration of Policy Servers - Platcfg

3. ☐	**Remote Console:** Login to platcfg	a) Run platcfg tool by executing the following command # su – platcfg  The platcfg tool opens b) Select : Policy Configuration  The Policy Configuration Menu opens 

6.1: Perform Initial Server Configuration of Policy Servers - Platcfg

4. ☐	**Remote Console**: Set Policy Mode	a) Set Policy Mode from the "Select Policy Mode" menu Select Wireless Policy mode from the options available as shown below:  b) Select: OK Wireless is the default configuration, if the "Current Policy Mode is "Wireless" prompt is not presented then the Wireless Mode will be set. c) Select : Yes  Depending on the hardware configuration you may be presented with a "Select Network Layout" screen. Refer to Configuration Management Platform Wireless User's Guide Release 12.2 (Setting Policy Management Mode) for further detail. In the case the "Select Network Layout" screen is not presented you will be returned to the Policy Configuration Menu.

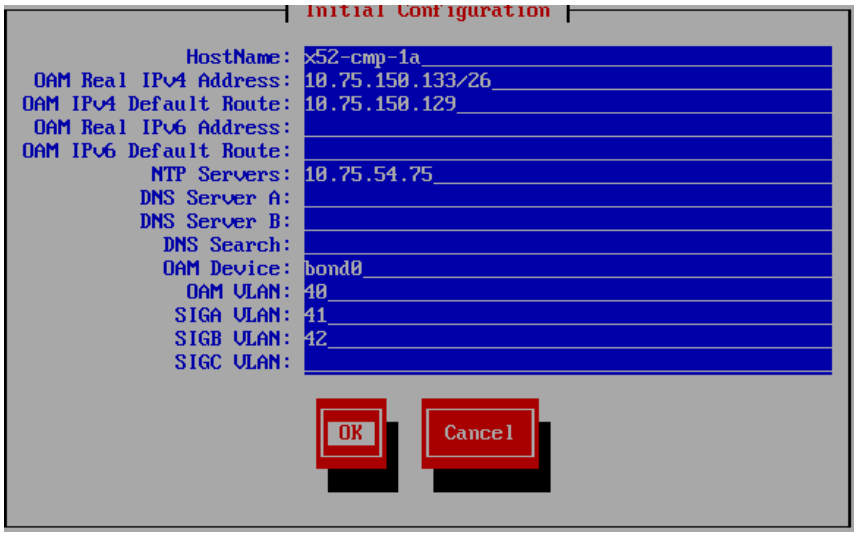
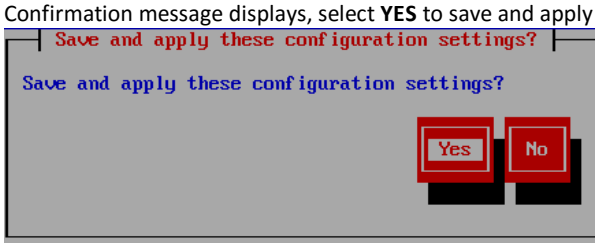
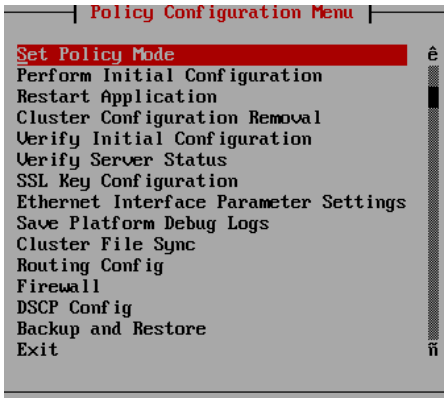
6.1: Perform Initial Server Configuration of Policy Servers - Platcfg

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

6.1: Perform Initial Server Configuration of Policy Servers - Platcfg

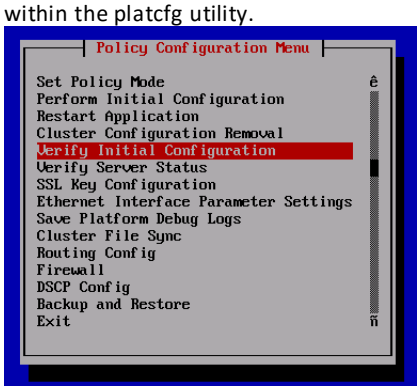
6. ☐	**Remote Console:** Perform Initial Configuration	Enter the configuration values and then select **OK**, where: • **HostName**--The unique name of the host for the device being configured. • **OAM Real IP Address**--The IP address that is permanently assigned to this device. • **OAM Real IPv4 Address**--The 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). **Note:** All of the fields listed above are required, except for fields *DNS Server* and *DNS Search*, which are optional but recommended. **Note:** Every network service and IP flow that is supported by IPv4 is now supported by IPv6. Either interface or a combination of the two can be configured.

6.1: Perform Initial Server Configuration of Policy Servers - Platcfg

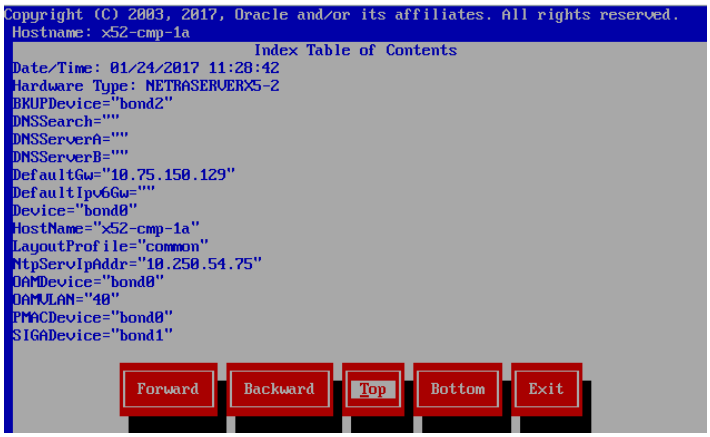
7. ☐	**Remote Console:** Perform Initial Configuration	**For example:**  When finished completing the form, select **OK** to save and apply the configuration. At this point the screen pauses for approximately a minute. This is normal behavior. Confirmation message displays, select **YES** to save and apply the configurations.  The platcfg form will process the configuration of the server, and then it will return to the platcfg menu. 

6.1: Perform Initial Server Configuration of Policy Servers - Platcfg

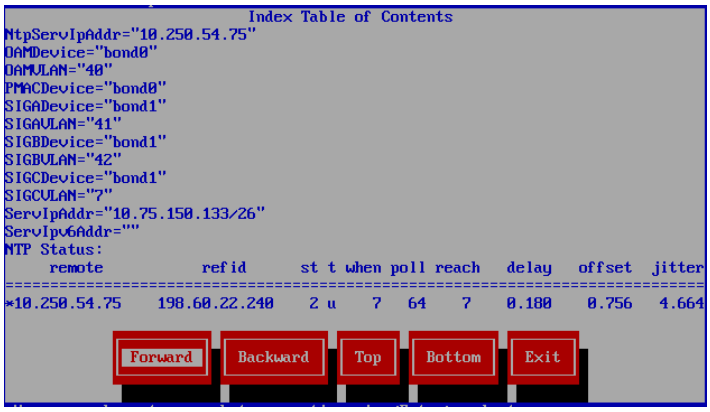
8. ☐	**Remote Console:** Verify Initial Configuration	From the main menu navigate to **Policy Configuration -> Verify Initial Configuration** from within the platcfg utility.



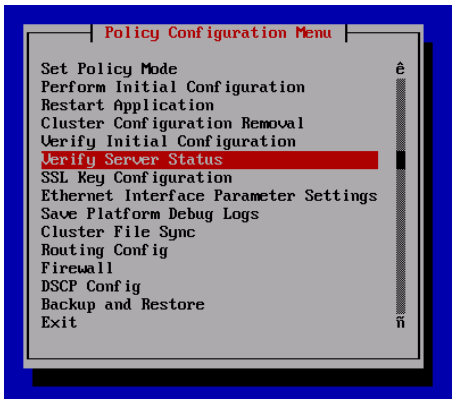
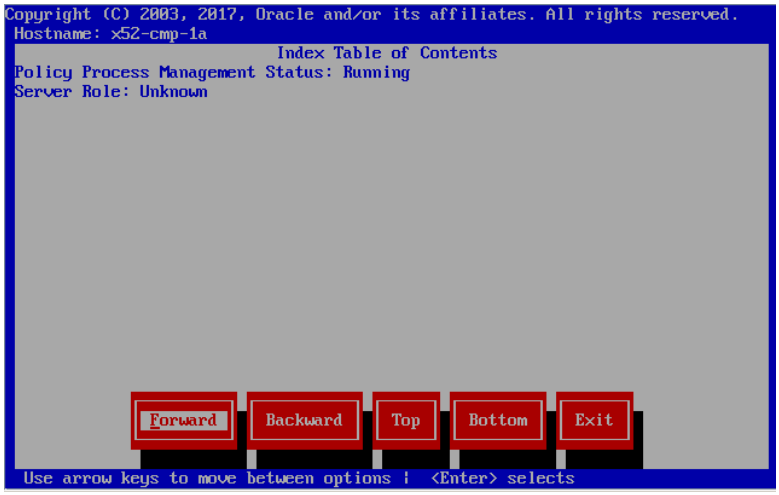
A display similar to the following is shown.



Note: The NTP status may not have updated. This is normal behavior. You may need to press the Forward button to view the NTP status.



6.1: Perform Initial Server Configuration of Policy Servers - Platcfg

9. ☐	**Remote Console:** Verify Server Status	Exit from this screen and select Verify Server Status:  The server should be in a running state. For example:  Note: At this point in the installation procedure the Server Role will be “Unknown”. “Unknown” is a valid state during initial configuration because the cluster has not yet been formed. Press “Exit” repeatedly until completely exiting the platcfg utility. You will be returned back to Linux prompt screen.

6.1: Perform Initial Server Configuration of Policy Servers - Platcfg

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** In case 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. Execute ip -4 addr (IPv4) or ip -6 addr (IPv6) to confirm the IP addresses configured during the initialization are present.

6.1: Perform Initial Server Configuration of Policy Servers - Platcfg

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 "*" sign besides the NTP server Ip indicates the NTP server is in sync. In case the sign is not there, you may try manually to sync with NTP server through the following steps: # **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 ntpdate has a bad response, follow up to get the needed networking, firewalls and permissions to solve this connectivity issue with the NTP server. **NOTE**: '*ntpdate*' is an emergency utility; use only when you see significant time difference between system and the actual time.
12. ☐	**Repeat on remaining servers**	Repeat this procedure on all Policy components' servers that are planned for service. If solution is geo-redundant, this procedure need to be performed on site1 and site2 Policy servers
THIS PROCEDURE HAS BEEN COMPLETED		

6.2 PERFORM INITIAL CONFIGURATION OF THE POLICY SERVERS - CMP GUI

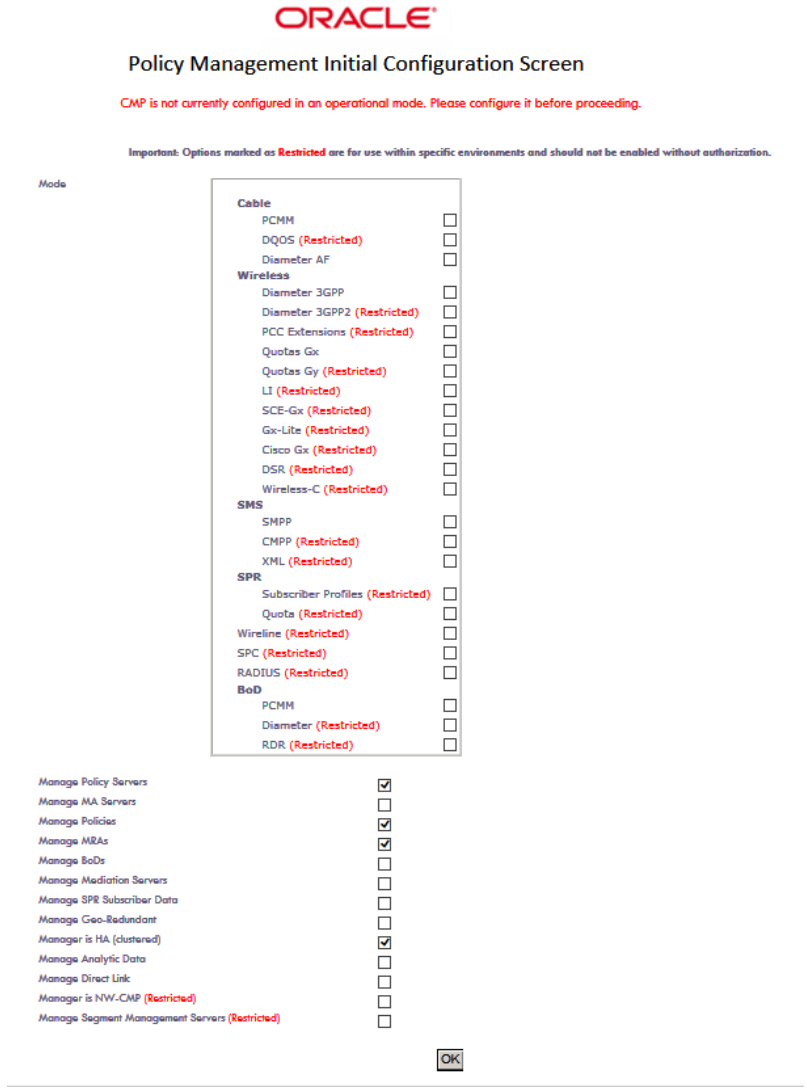
This procedure will perform initial configuration of the CMP GUI on a newly installed environment.

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

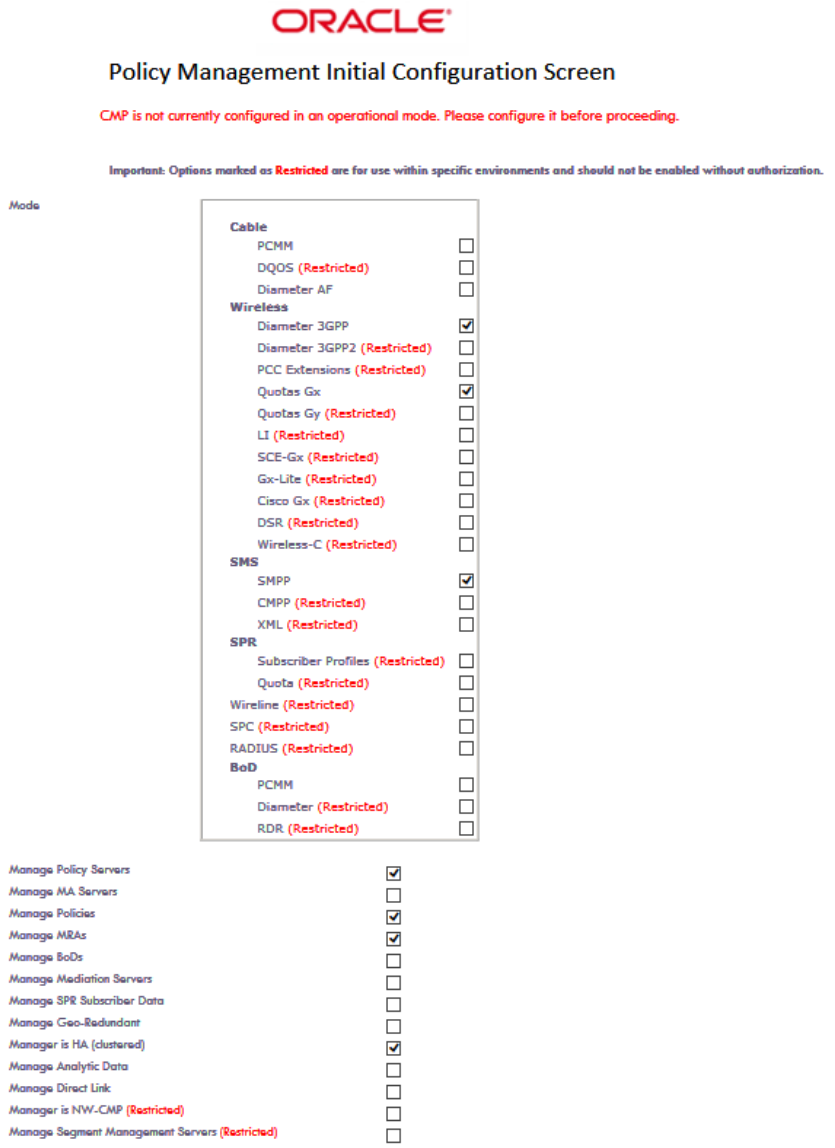
6.2: Perform Initial Configuration of the Policy Servers - CMP GUI

STE P #	This procedure will configure 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..	
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 will be located at Site1. If this is not geo-redundant solution there will be no 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 1st selected CMP	Once connected to the CMP GUI for the 1st time the , the user will be prompted to configure operation mode settings for the system, which define what functionality will be configurable from the CMP GUI. The selection depends on the customer deployment. The Policy Management Initial Configuration Screen presents as follows:

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

		 [Note: modes can be changed at a later time if needed, but the method to access to this mode selection is not documented.] Contact Oracle Support if Mode selection is required to be changed after the initial configuration.
3.	**CMP GUI:** Set CMP Mode in 1st selected CMP	Below is an example of a configuration that will provide basic functionality for a Policy 12.2.x Wireless solution. The wireless mode of operation will have already been confirmed in earlier procedures. (Checkboxes are for example only). For greater detail refer to **the Configuration Management Platform Wireless User's Guide** – CMP Modes section

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



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.

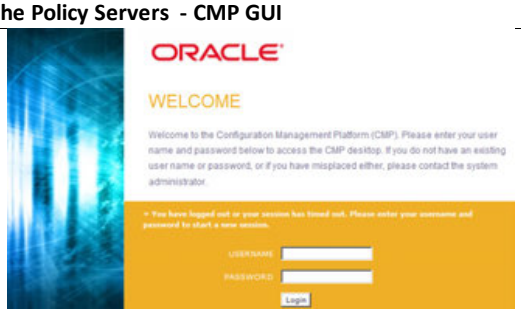
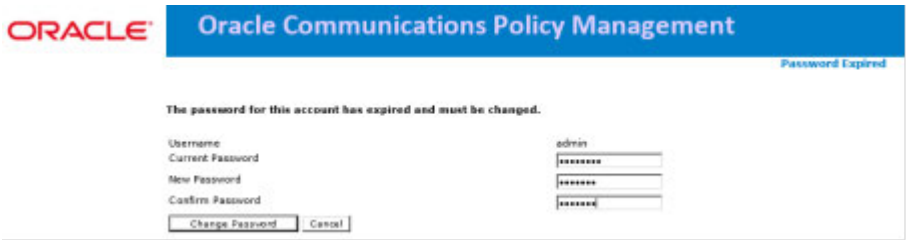
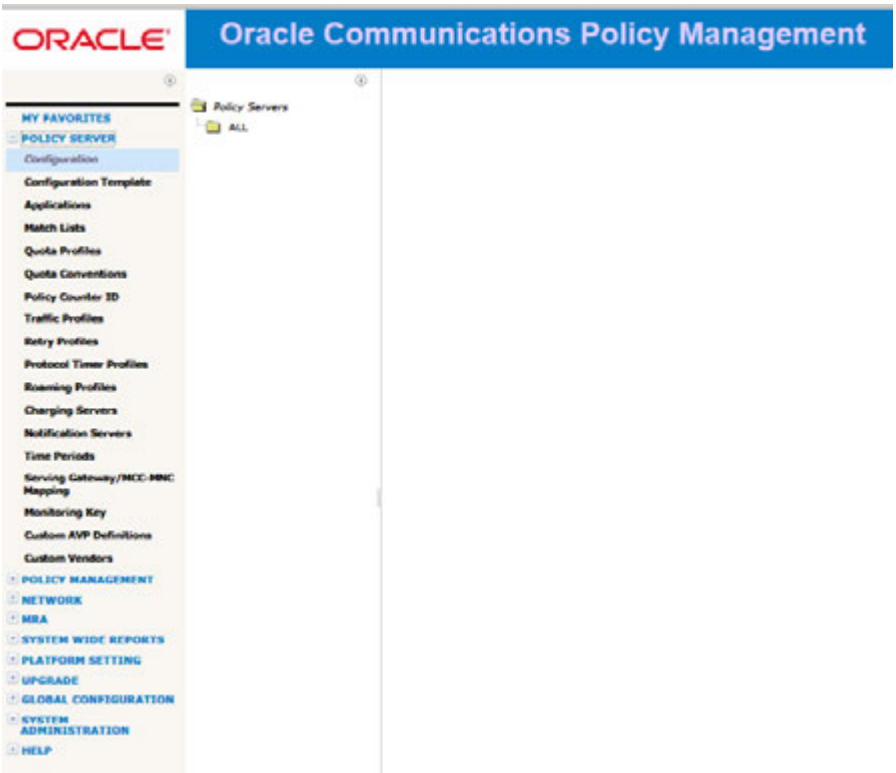
For a Wireless network:

- Wireless: Diameter 3GPP
- Quotas Gx
- Manage Policy Servers
- Manage Policies
- Manage MRAs
- Manage Geo-Redundant
- Manager is HA (clustered)

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

		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/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 will perform 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 Oracle Support for additional Information. ***Manage Policy Servers*** & ***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*** & ***Manager is S-CMP*** are specific to a "Tiered CMP System" deployment. Refer to Configuration Management Platform Wireless User's Guide for the procedure to deploy a Tiered CMP System. **Note:** The mode selections on this form depend on the customer deployment and should conform with the engineering team responsible for the planned Policy Management Solution deployment.
4. ☐	**CMP GUI:** Login to CMP GUI	After finishing the policy mode selection and pressing "OK", login screen below would be displayed:

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

		
5. ☐	**CMP GUI:** Set admin password	Initial, default login is admin/policies After login, the system will prompt the user to change the admin password.  Enter the default old password then the new password twice and press “Change Password” button.
6. ☐	**CMP GUI:** Verify that the CMP GUI is displayed, with expected menus.	

THIS PROCEDURE HAS BEEN COMPLETED

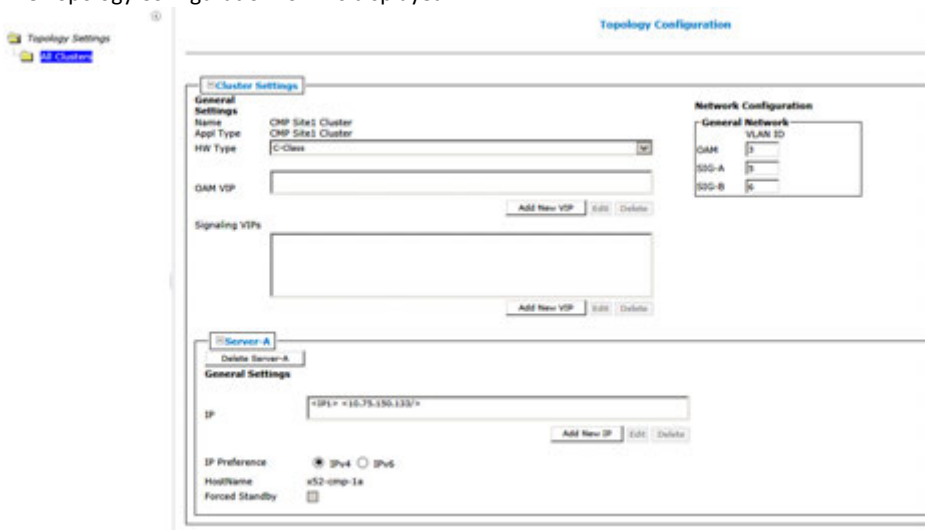
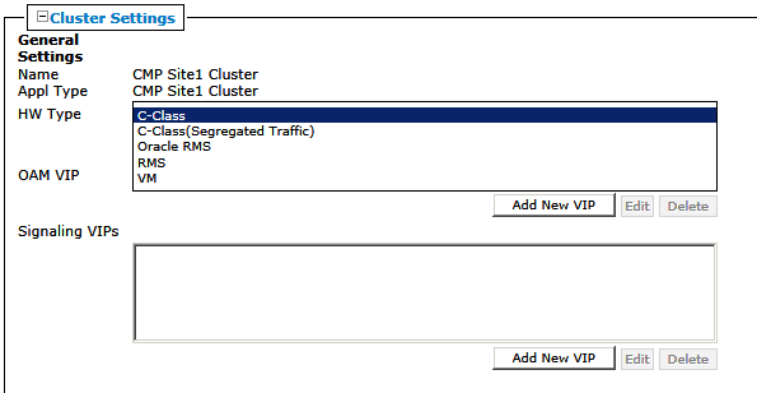
6.3 CMP SITE1 CLUSTER CONFIGURATION

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

6.3: CMP Site1 Cluster Topology Configuration

STEP #	You must configure the active site (Site 1) CMP cluster. Note: In a deployment that has Geo-Redundant CMP servers (that is, CMP servers at two different sites), the other pair of CMP servers will be added to the network topology using the CMP server at Site 1. The CMP Site 1 cluster will push the configuration to the Site 2 (Geo-Redundant) CMP servers later. **Prerequisites:** To complete this procedure, you need the following information: • OAM VIP — IP address and netmask for the cluster VIP address on the OAM network. • Hostname — The names you choose for each server in the cluster. • Signaling VIPs (optional) — Up to four IPv4 or IPv6 addresses and netmasks of the signaling VIP addresses. For each, select None, SIG-A, SIG-B, or SIG-C to indicate whether the cluster will use 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.	
1. ☐	**CMP GUI**: View Topology Settings	**Note:** Only the following Web Browsers are supported in Oracle Communications Policy Management 12.2 • Mozilla Firefox® release 31.0 or later • Google Chrome version 40.0 or later • *Internet Explorer in not supported for this procedure **Select: Menu → Platform Settings → Topology Settings → all clusters** The initial form will open, and display a message that initial configuration detected and CMP Site 1 Cluster should be added.

6.3: CMP Site1 Cluster Topology Configuration

2. ☐	**CMP GUI:** Add CMP Site 1 Cluster – **Server A**	Select the button to "**Add CMP Site 1 Cluster**". The Topology Configuration form is displayed.  In this form, the CMP cluster can be given a name, and certain characteristics of the cluster are defined. This form will define a VIP address to be assigned to the active server in the cluster. Complete the form according to the system design. <u>Define the "Cluster Settings"</u> Select the "**HW Type"** from the list 

6.3: CMP Site1 Cluster Topology Configuration

Available options are:

- C-Class (default) – HP Enterprise ProLiant BL460 Gen6/Gen8/Gen9 server
- C-Class (Segregated Traffic) (a configuration where Signaling and other networks are separated onto physically separate equipment) – HP Enterprise ProLiant BL460 Gen6/Gen8/Gen9
- Oracle RMS (rack-mounted servers using tagged VLANs)
- RMS (for a rack-mounted server not using VLANs)
- VM (virtual machine)

If you selected C-Class, C-Class (Segregated Traffic), or Oracle RMS, enter the General Network - VLAN IDs.

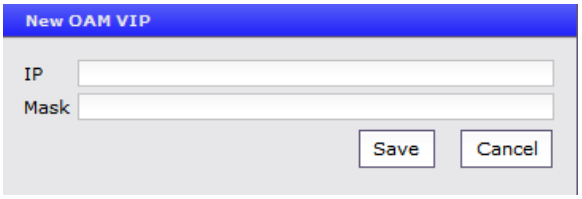
Enter the **OAM**, **SIG-A**, and (optionally) SIG-B virtual LAN (VLAN) IDs.

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

- OAM – 3
- SIG-A – 5
- SIG-B – 6

Select OAM VIP "**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.

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** will be the IP address and Host Name used during the "Initial Configuration" of the server from section 6.1 of this document. They must match exactly. If Server-A is network reachable from the CMP it is recommended to use the "load" button once the IP address and IP Preference have been defined. The CMP will attempt to load the hostname from the ip reachable server. This will not only confirm network connectivity but will also minimize the possibility of th incorrectly defining the Host Name.

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

a) (Required) To enter the IP address, click Add New IP.

6.3: CMP Site1 Cluster Topology Configuration

The Add New IP dialog box appears.

1. 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.

2. Select the IP Preference: IPv4 or IPV6.

The server will preferentially use 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.

b) Enter the HostName of the server.

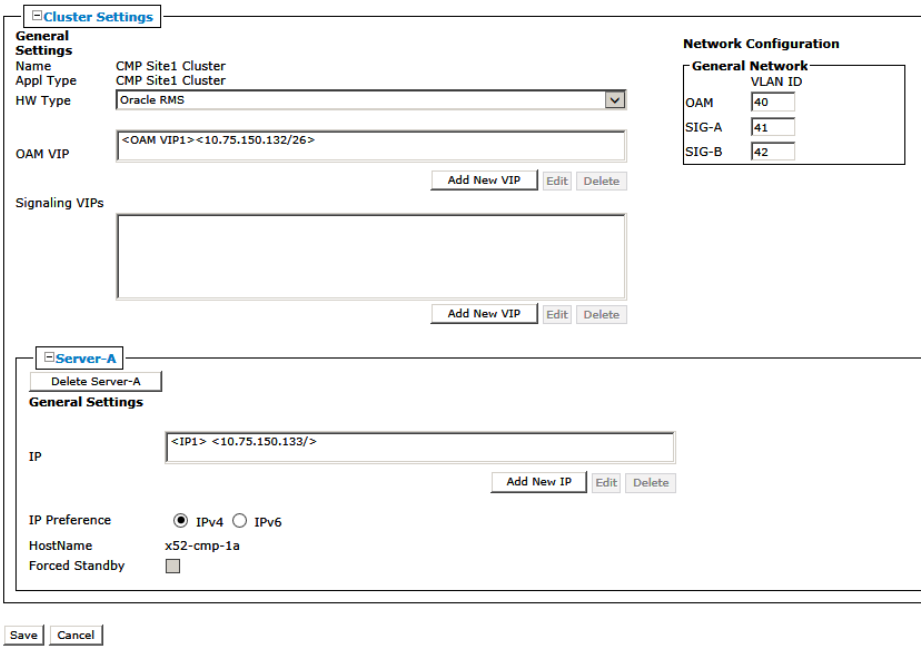
This must exactly match the host name provisioned for this server (the output of the Linux command uname –n).

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 a sign that the ip address configured is not accessible across the network. Alternately, you may enter the host name manually but it is recommended to do any network troubleshooting that may be required.

Server-A example:

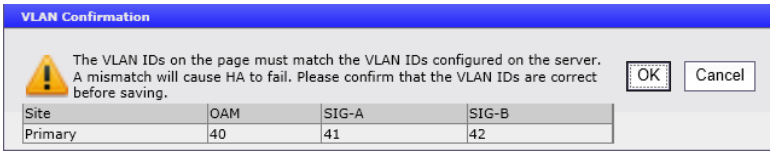
Topology Configuration of the HW Type “Oracle RMS” example:

6.3: CMP Site1 Cluster Topology Configuration

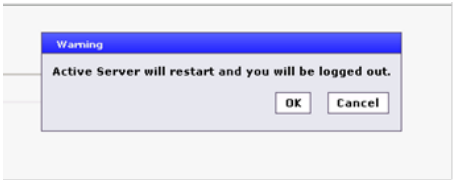


When done, **Save** the form and select **OK .**

If the configuration contains VLAN IDs you will be prompted to confirm the VLAN IDs.



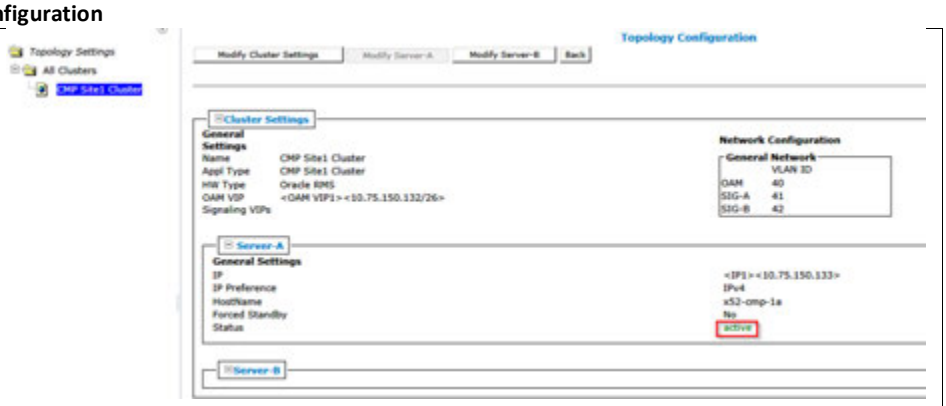
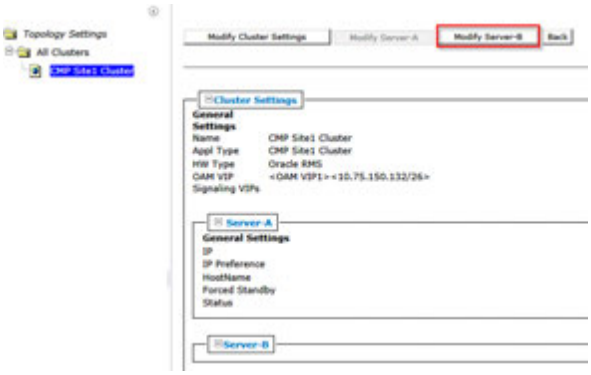
Then the following confirmation prompt appears. Click <OK>



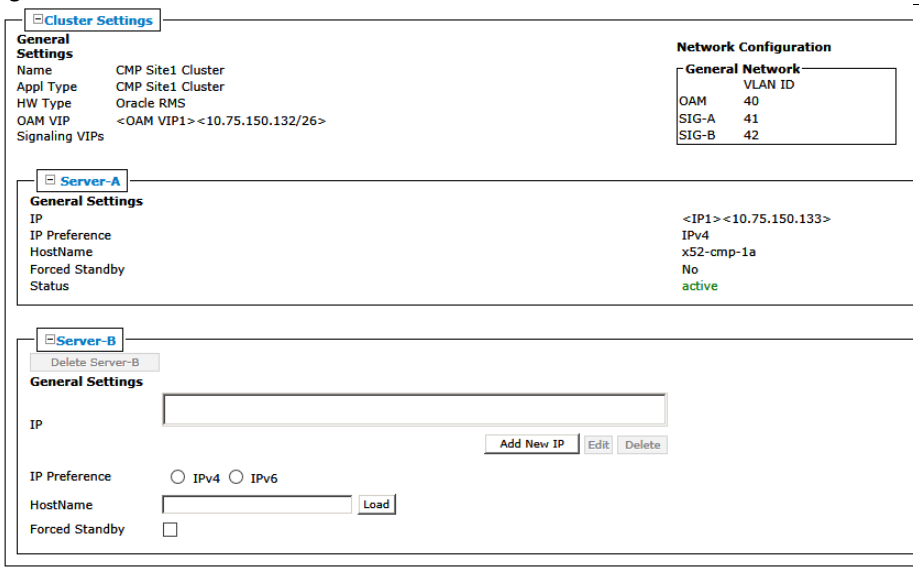
At this point you will be logged out of CMP GUI.

3. ☐	**CMP GUI**: Login using the CMP cluster VIP.	After the Topology Configuration is saved, the CMP VIP address will be taken by the Active CMP server of the cluster. This may take a minute. Login to the CMP GUI using the VIP address, then navigate to **Platform Settings →Topology Settings → all clusters → CMP Site1 Cluster**

6.3: CMP Site1 Cluster Topology Configuration

		 Verify the configured CMP server is now in "Active" state
4 ☐	**SSH to CLI**: If the CMP VIP is not available	SSH to the CMP Real IP address of the CMP server to confirm the server role is "active" as shown below # ha.mystate root@Site1-CMP-A:~ [root@Site1-CMP-A ~]# ha.mystate resourceId role node subResources lastUpdate DbReplication Active A3134.062 0 1008:174816.643 VIP Active A3134.062 0 1008:174816.644 QP Active A3134.062 0 1008:174816.645 DbReplication_old OOS A3134.062 0 1008:174806.315 [root@Site1-CMP-A ~]# NOTE: "DbReplication_old" with role "OOS" is not an indication of a problem and can be ignored. It is still possible to login to the CMP server with its Real IP address, if needed, to verify that the Topology Configuration was done correctly.
5 ☐	**CMP GUI:** Modify CMP Site 1 Cluster – add Server B	*Modify CMP Site 1 Cluster – add Server B* Select: **Menu →Platform Settings → Topology Settings** Select View for **CMP Site 1 Cluster** Select **Modify Server B**  The Topology Configuration now presents Server-B for configuration.

6.3: CMP Site1 Cluster Topology Configuration



<u>Define the settings for **Server-B** in the Server-B section of the page</u>

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

a) (Required) To enter the IP address, click Add New IP.

The Add New IP dialog box appears.

1. 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.

2. Select the IP Preference: IPv4 or IPV6.

The server will preferentially use 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.

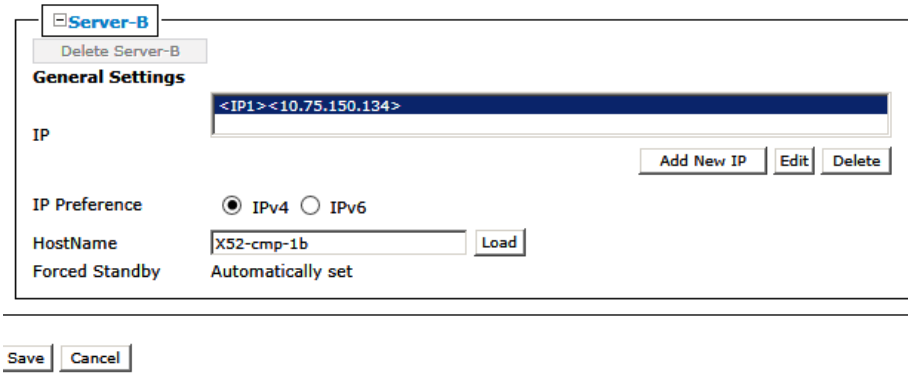
b) Enter the HostName of the server.

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

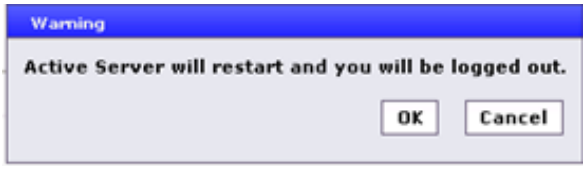
Note: If the server has a configured server IP, you can click Load to retrieve the remote server host name. If the retrieve fails, this a sign that the ip address configured is not accessible across the network. Alternately, you may enter the host name manually but it is recommended to do any network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

Example of Site1 CMP Cluster Server B Topology Configuration

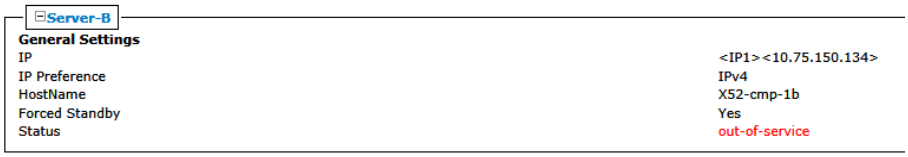
6.3: CMP Site1 Cluster Topology Configuration



a. Select "save" then "OK" on the following confirmation message.



The server status will be "out-of-service" for few minutes and that is expected until the cluster forms.

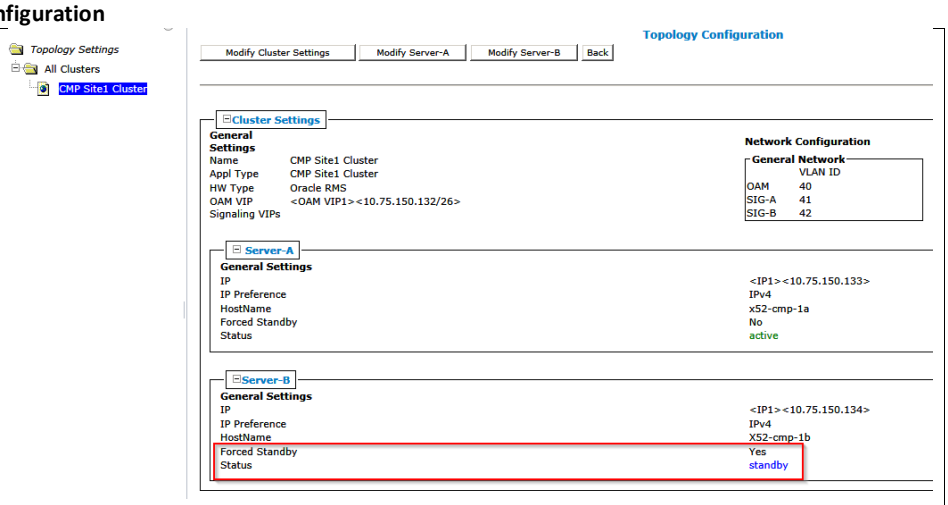


Note: Wait for any Alarms, such as the following, to clear. This takes about 5 minutes

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

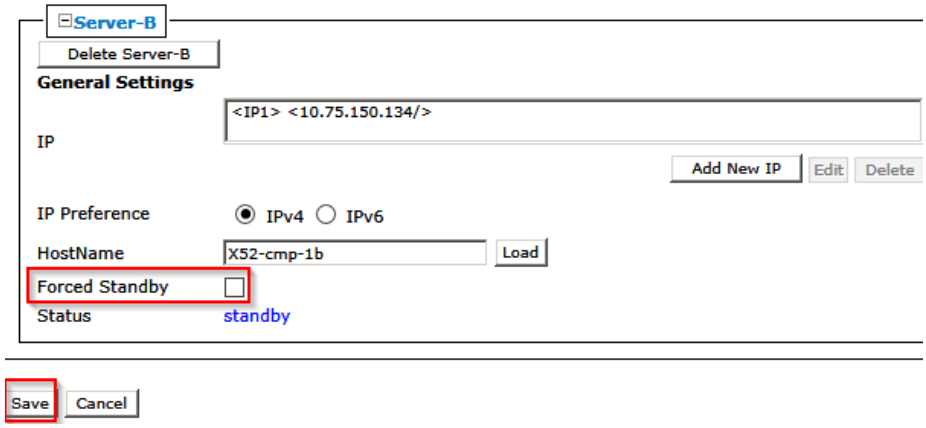
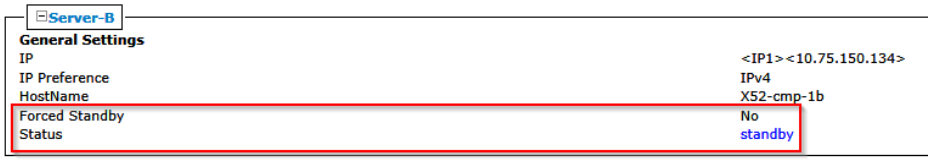
6. ☐	**CMP GUI:** Verify Server B is added	Refresh the CMP GUI screen: **Menu → Topology → CMP Site 1 Cluster**

6.3: CMP Site1 Cluster Topology Configuration

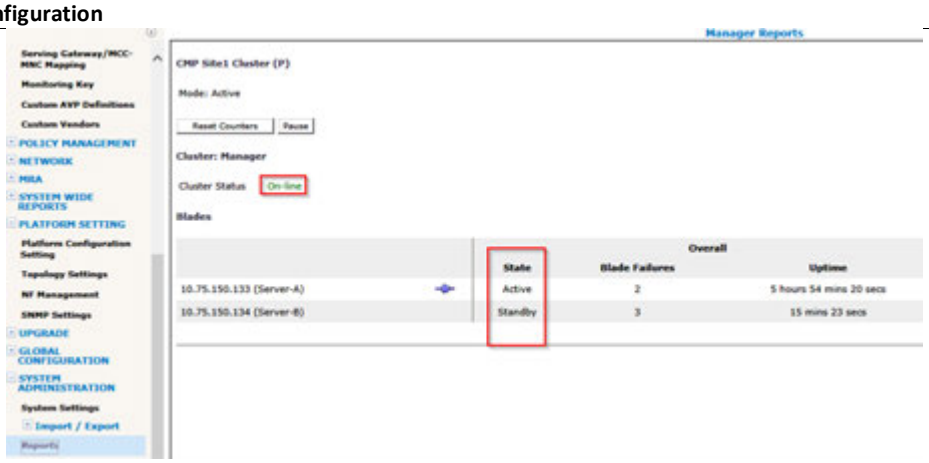
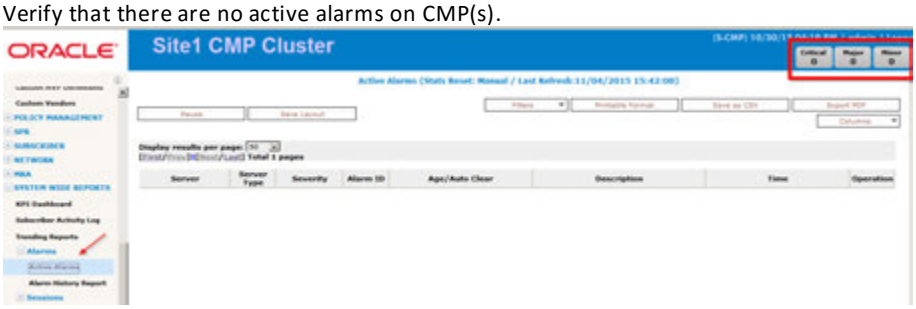
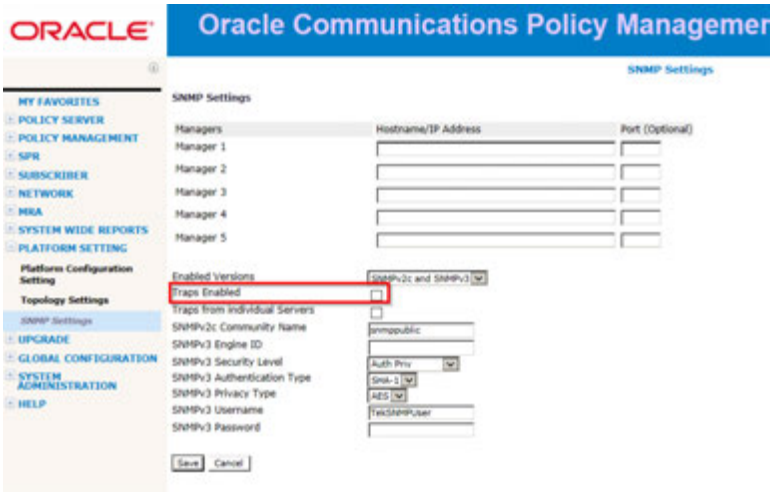


Verify status is:

- Forced Standby = yes (automatically set upon entering CMP Server-B information)
- Status = **standby** (after refreshing the page)

7. ☐	**CMP GUI:** Remove Force Standby on Server B	Click **Modify Server-B** button and uncheck "**Force Standby"**, then click **Save** when finished and **OK** to the following confirmation message:  Verify status becomes: • Forced Standby = no • Status = Standby 
8. ☐	**CMP GUI:** Verify CMP cluster	**SYSTEM ADMINISTRATION → Reports** Verify both CMP servers are present , with one "Active" and the other in "standby" status and also the status of the cluster is "On-line":

6.3: CMP Site1 Cluster Topology Configuration

		
9. ☐	**CMP GUI:** Verify CMP cluster	**SYSTEM WIDE REPORTS → Active Alarms** Verify that there are no active alarms on CMP(s). 
10. ☐	**CMP GUI:** Add SNMP Servers	**PLATFORM SETTING → SNMP Settings** Make the appropriate configuration for SNMP destination, version and community string and then select save.  NOTE: De-select the checkbox for “traps enabled” until ready to go live.

THIS PROCEDURE HAS BEEN COMPLETED

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.

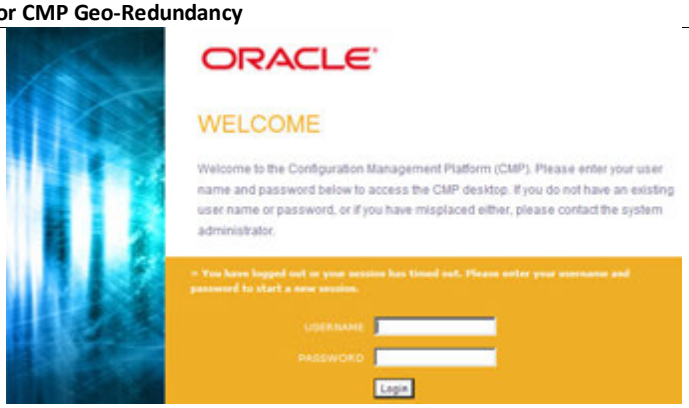
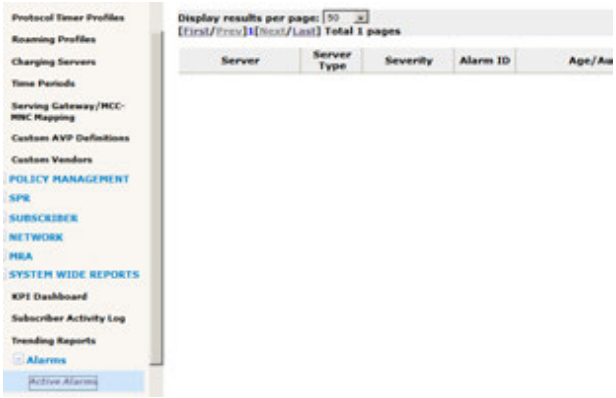
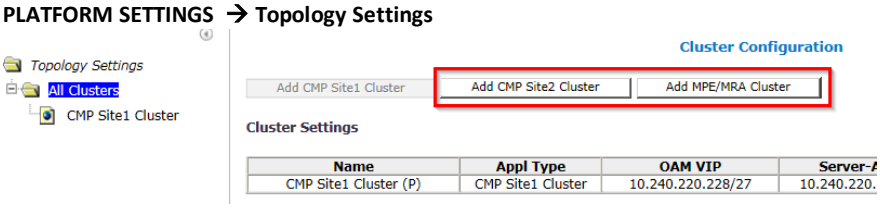
Note: For the full management relationships to be established, certain IP network services must be allowed between the CMP Site 1 cluster and the other clusters in the network. Incorrectly configured firewalls in the network can cause the management relationships to fail and alarms to be raised at the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

6.4.1 Adding a CMP Site2 Cluster for CMP Geo-Redundancy

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

STEP #	This procedure will configure a Geo-Redundant CMP Site2 Cluster. After this procedure a Site2 CMP Cluster will be 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 Geo-Redundant 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.	
1. ☐	**CMP GUI:** Login to CMP Server GUIs (using VIP)	From Browser, enter CMP Server VIP in Navigation string. **Note:** Only the following Web Browsers are supported in OCMP 12.2 • Mozilla Firefox® release 31.0 or later • Google Chrome version 40.0 or later *Internet Explorer in not supported for this procedure

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

		 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 activities.  View of Alarms from CMP GUI upper right banner  View of Alarms from System Wide Reports -> Active Alarms IMPORTANT: In Policy 12.2.x, there is On-line help provided for Alarm descriptions. In the Alarm views, click on the alarm Id to open the Alarm description help page. Alternatively, from the Menu select On-Line Help, and select Troubleshooting Guide. Search this for the Alarm Id.
3. ☐	**CMP:** View Topology Settings	**PLATFORM SETTINGS → Topology Settings**  The Topology Settings screen allows for the selection of adding a CMP Site2 Cluster (used for CMP Cluster Geo-Redundancy) or adding an (MPE/MRA) Cluster. **Note:** Adding a CMP Site2 Cluster does not require the "Manage Geo-Redundant" mode option to be selected. This option is for adding Geo-Redundant MPE/MRA/Mediation clusters.

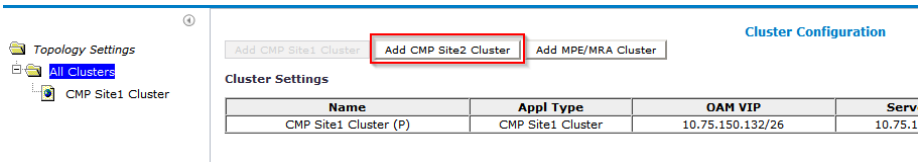
6.4.1: Adding a CMP Site2 Cluster for CMP Geo-Redundancy

4. ☐

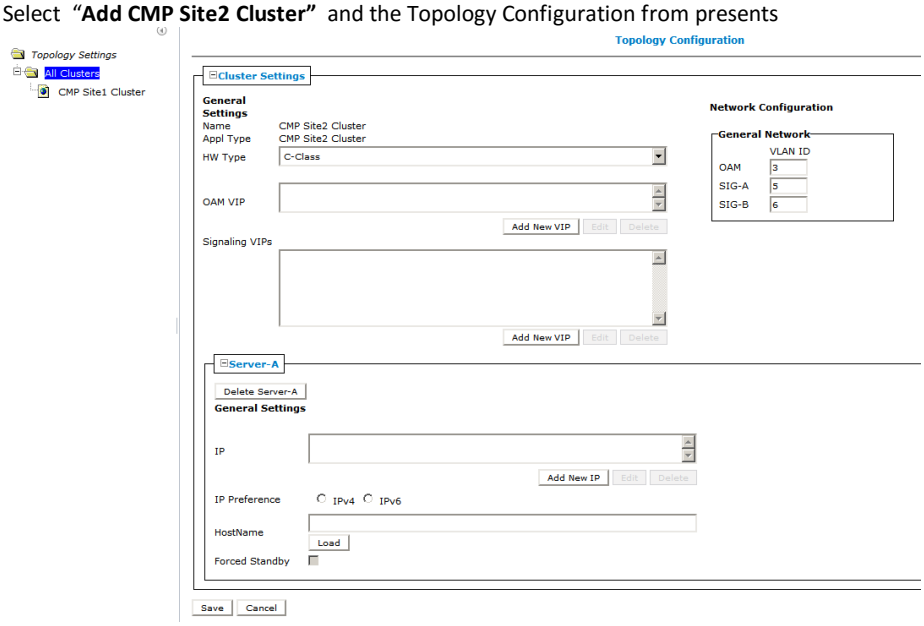
CMP GUI: Add Site 2 CMP Cluster

Adding a CMP Site2 CMP cluster is optional. If the Policy Management Solution design calls for "Geo-Redundant" CMP clusters, the "Site 2 CMP Cluster" must be configured from the "CMP Site1 Cluster" GUI.

PLATFORM SETTINGS →Topology Settings



Select "**Add CMP Site2 Cluster**" and the Topology Configuration from presents



Complete the form according to the system design.

<u>Define the "Cluster Settings"</u>

Select the "**HW Type**" from the list.

Available options are:

- C-Class (default) – HP Enterprise ProLiant BL460 Gen6/Gen8/Gen9 server
- C-Class (Segregated Traffic) (a configuration where Signaling and other networks are separated onto physically separate equipment) – HP Enterprise ProLiant BL460 Gen6/Gen8/Gen9
- Oracle RMS (rack-mounted servers using tagged VLANs)
- RMS (for a rack-mounted server not using VLANs)
- VM (virtual machine)

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.

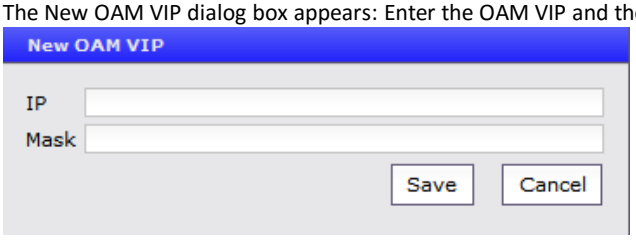
6.4.1: Adding a CMP Site2 Cluster for CMP Geo-Redundancy

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

- OAM – 3
- SIG-A – 5
- SIG-B – 6

Select OAM VIP "**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.

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.

<u>Define the settings for **Server-A** in the Server-A section of the page</u>

The "**IP**" address and "**Host Name**" of **Server-A** will be the IP address and Host Name used during the "Initial Configuration" of the server from section 6.1 of this document. They must match exactly. If Server-A is network reachable from the CMP it is recommended to use the "load" button once the IP address and IP Preference have been defined. The CMP will attempt to load the hostname from the IP reachable server. This will not only confirm network connectivity but will also minimize the possibility of incorrectly defining the Host Name.

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

a) (Required) To enter the IP address, click Add New IP.

The Add New IP dialog box appears.

1. 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.

2. Select the IP Preference: IPv4 or IPV6.

The server will preferentially use 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.

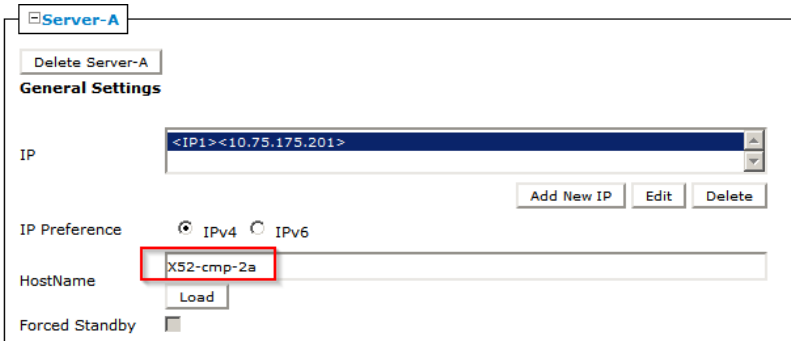
6.4.1: Adding a CMP Site2 Cluster for CMP Geo-Redundancy

b) Enter the HostName of the server.

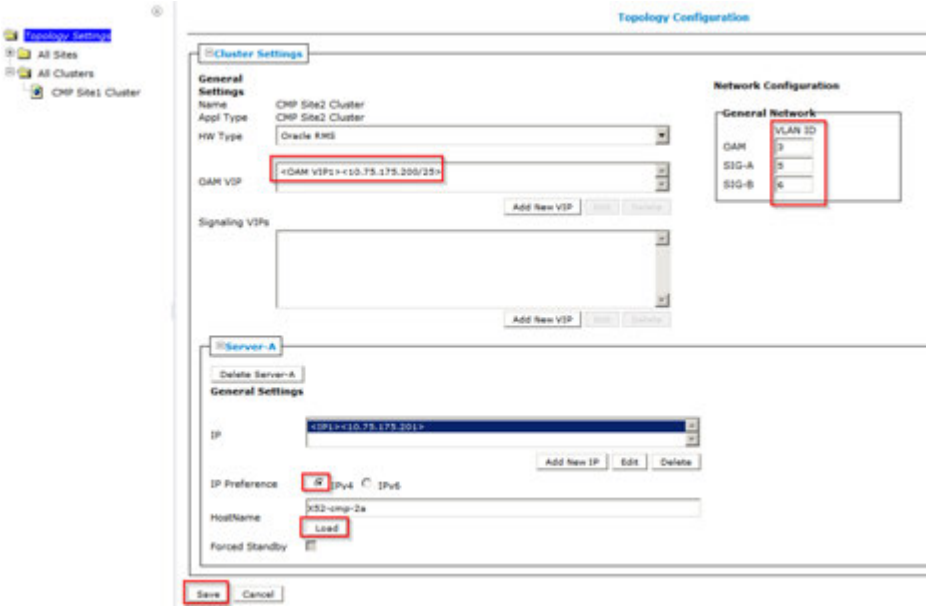
This must exactly match the host name provisioned for this server (the output of the Linux command uname –n).

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 a sign that the IP address configured is not accessible across the network. Alternately, you may enter the host name manually but it is recommended to do any network troubleshooting that may be required

For example: Here the HostName has been populated by clicking on the "load" button.

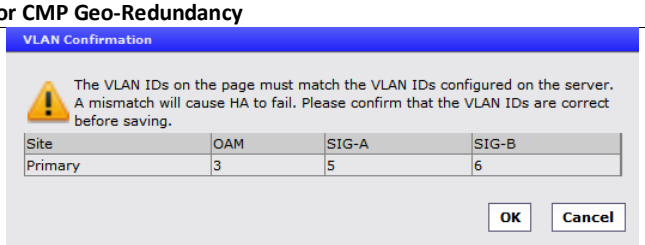


An example of the completed form for HW Type "Oracle RMS".



"**Save**" the completed form and confirm the VLAN IDs if needed

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



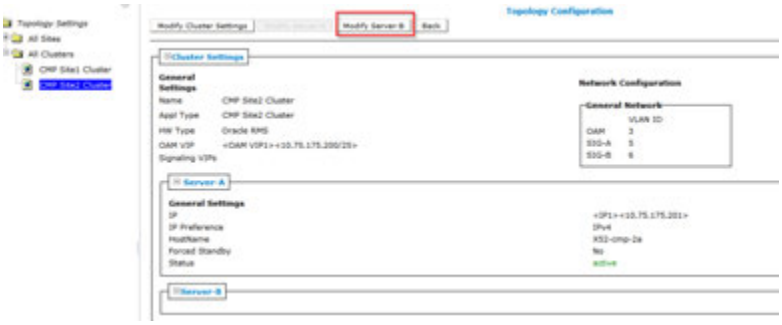
There will be a transition period and some alarms that will clear after a few minutes while the "Site1 CMP Cluster" configures the GeoRedundant "CMP Site2 Server-A". When complete the Geo-Redundant "CMP Site2 Cluster" is now visible in **PLATFORM SETTINGS →Topology Settings**

Note: For further detail of regarding the relationship between the **Primary Site1 CMP Cluster (P)** and the Site2 CMP Cluster (S) refer to [Configuration Management Platform Wireless User's Guide]

Confirm the newly added "Site2 CMP Cluster" Server-A is "active".

PLATFORM SETTINGS →Topology Settings→CMP Site2 Cluster

Note: Server-B is now visible and will be used for the next step

5. ☐	**CMP GUI:** Add Site 2 CMP Cluster	CMP-Site2 Cluster will need Server-B added to complete the cluster configuration. From the "Topology Setting" menu click on CMP Site2 Cluster. Click on "Modify server-B". 

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

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:

a) (Required) To enter the IP address, click Add New IP.

The Add New IP dialog box appears.

1. 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.

2. Select the IP Preference: IPv4 or IPV6.

The server will preferentially use the IP address in the specified format for communication.

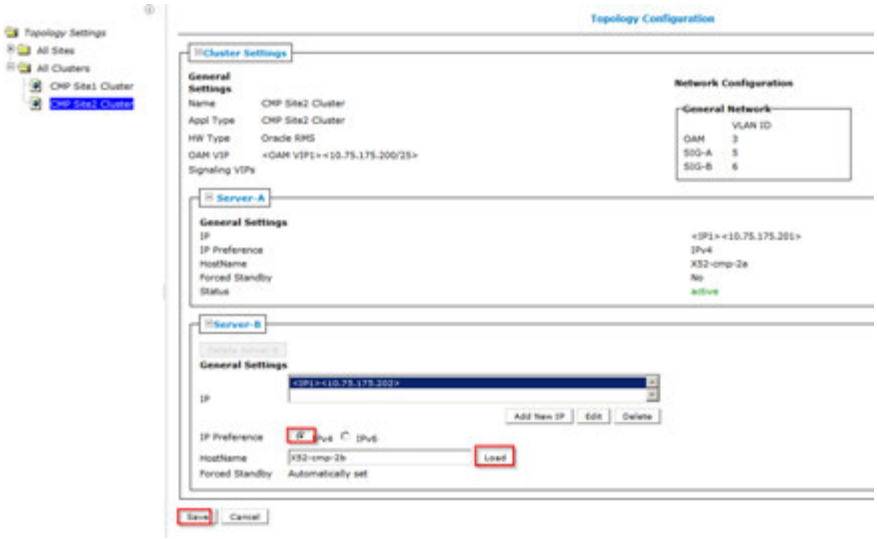
- If neither an IPv6 OAM IP nor a static IP address is defined, IPv6 cannot be selected.
- If neither an IPv4 OAM IP nor a static IP address is defined, IPv4 cannot be selected.

b) 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 a sign that the IP address configured is not accessible across the network. Alternately, you may enter the host name manually but it is recommended to do any network troubleshooting that may be required.

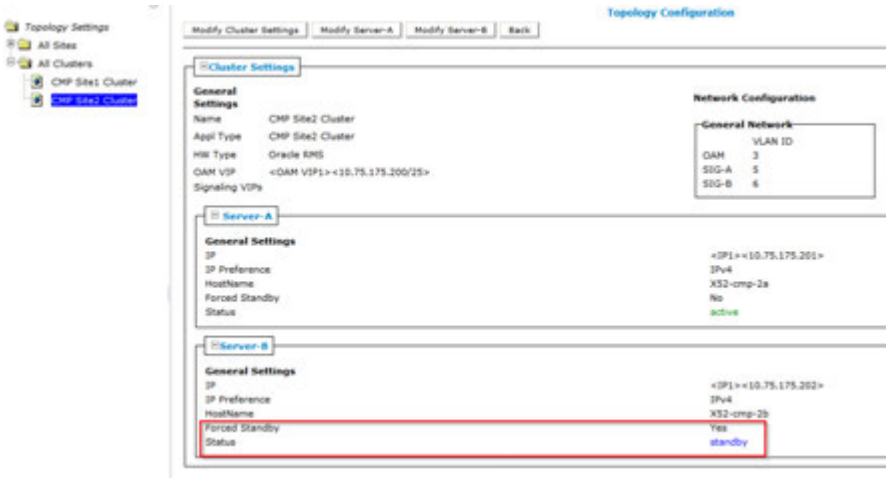
For example:



There will be a transition period and several alarms that will clear after a few minutes while the Site1 CMP Cluster configures the GeoRedundant CMP Site2 Server-B. Wait for all the alarms to clear and then then confirm that Server B in the CMP Site2 Cluster is now *standby*.

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

PLATFORM SETTINGS →Topology Settings→CMP Site2 Cluster

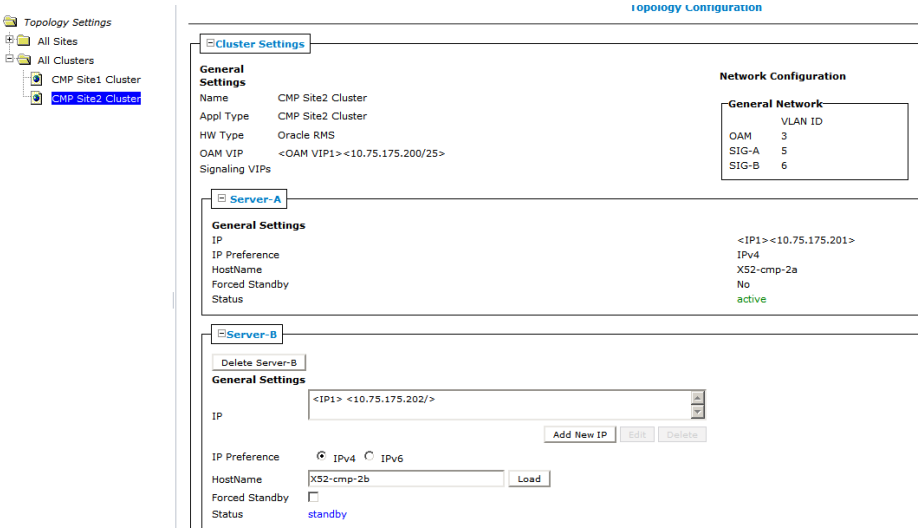


Note: Forced Standby of Server-B status is Yes.

6. ☐

CMP GUI: Clear "Forced Standby" – Server-B

From the Topology Settings" menu select the CMP Site2 Cluster and click on the "Modify Server-B" again to **uncheck** the "Forced Standby" state of "Server-B" by unchecking the "Forced Standby" box. "**Save**" the configuration.



The Geo-Redundant Site2 cluster confugration has been completed. The CMP Site1 Cluster will be marked with a (P) for primary and the CMP Site2 Cluster wiil be marked with an (S) for secondary.

PLATFORM SETTINGS →Topology Settings→

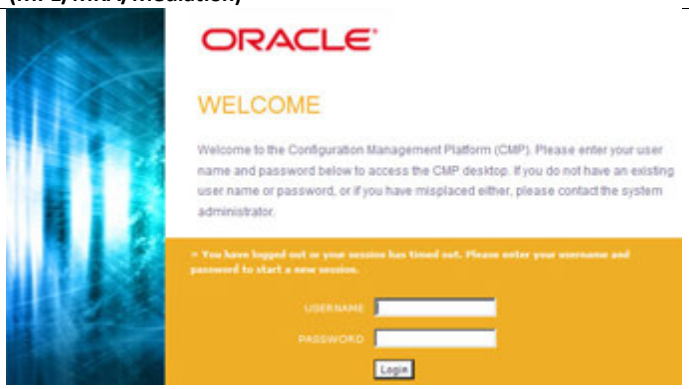
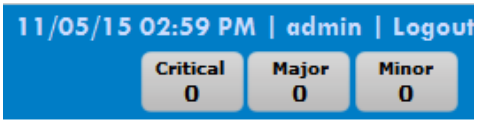
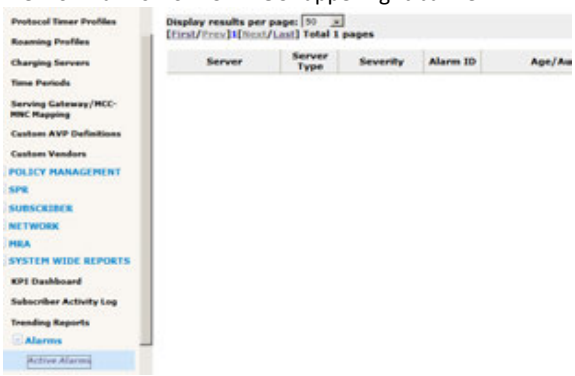
THIS PROCEDURE HAS BEEN COMPLETED

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

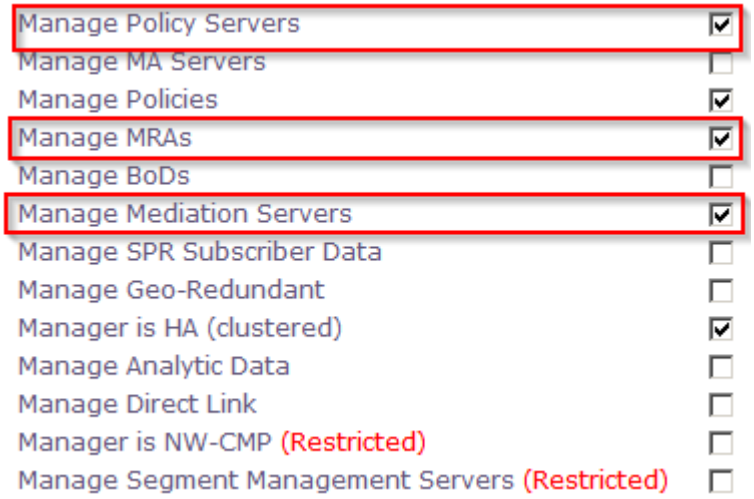
6.4.2: Setting Up a Non-CMP Cluster (MPE/MRA/Mediation)

STEP #	This procedure will configure the management relationships between the CMP and other Non-CMP clusters in Wireless Mode. A non-CMP cluster includes one of the following server types: • MPE • MRA • 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. 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.	
1. ☐	**CMP GUI:** Login to CMP Server GUIs (using VIP)	From Browser, enter CMP Server VIP in Navigation string. **Note:** Only the following Web Browsers are supported in OCMP 12.2 • Mozilla Firefox® release 31.0 or later • Google Chrome version 40.0 or later *Internet Explorer in not supported for this procedure

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

		 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 activities.  View of Alarms from CMP GUI upper right banner  View of Alarms from System Wide Reports -> Active Alarms IMPORTANT: In Policy 12.2.x, there is On-line help provided for Alarm descriptions. In the Alarm views, click on the alarm Id to open the Alarm description help page. Alternatively, from the Menu select On-Line Help, and select Troubleshooting Guide. Search this for the Alarm Id.
3. ☐	**Mode Configuration Considerations**	The 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)

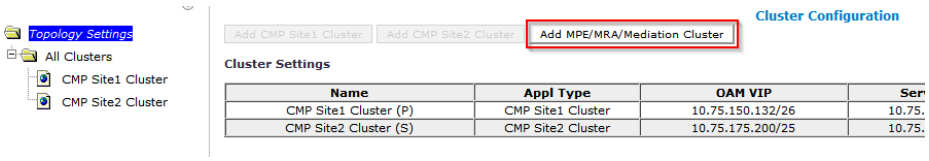
6.4.2: Setting Up a Non-CMP Cluster (MPE/MRA/Mediation)

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


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 Geo-Redundant” mode is selected proceed to the next procedure 6.4.4: Setting Up a 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 Oracle Support if Mode selection is required to be changed after the initial configuration.
</td>
</tr>
<tr>
<td>4.
☐</td>
<td>**CMP GUI:** Add MPE/MRA/Mediation Clusters</td>
<td>
PLATFORM SETTINGS → Topology Settings



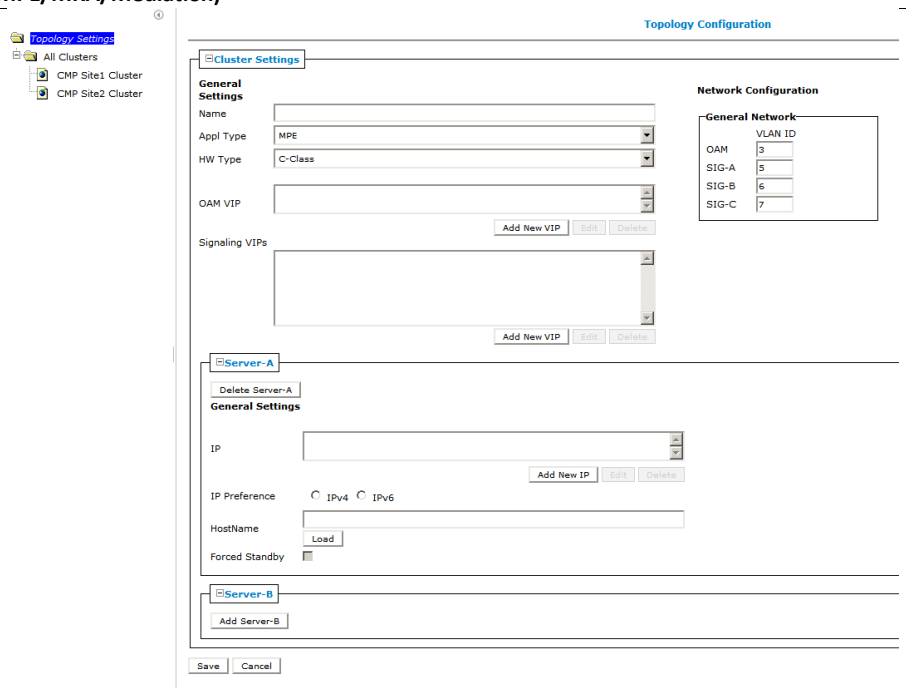
On the cluster Configuration page select “**Add MPE/MRA/Mediation**”

Note: Mediation will only be present if “Manage Mediation Servers” was selected.

- 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.

The Topology Configuration page presents:
</td>
</tr>
</table>

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

		
5. ☐	**CMP GUI:** Add MPE/MRA/Mediation Clusters	Complete the form according to the system design. It is allowed to 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 will be MPE/MRA or Mediation respectively. <u>Define the "Cluster Settings"</u> **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 Gen6/Gen8 server • C-Class (Segregated Traffic) (a configuration where Signaling and other networks are separated onto physically separate equipment) – HP ProLiant BL460 Gen6/Gen8 • Oracle RMS – Oracle Server X5-2 or Oracle Netra Server X5-2 • RMS (rack-mounted server) – HP ProLiant DL360 Gen6 or HP ProLiant DL380 Gen8/Gen9 server • VM (virtual machine) • VM(Automated) (VM managed by NF Agent) If you selected C-Class, C-Class (Segregated Traffic), or Oracle RMS, enter the General Network

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

- 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

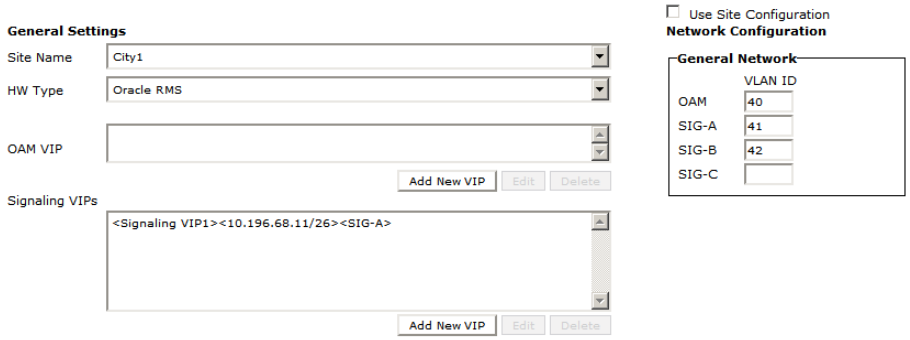
OAM VIP — The OAM VIP is not typically used for Non-CMP clusters. The Real IP address is used by the CMP to communicate with the Non-CMP cluster.

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:



<u>Define the settings for **Server-A** in the Server-A section of the page</u>

The "**IP**" address and "**Host Name**" of **Server-A** will be the IP address and Host Name used during the "Initial Configuration" of the server from section 6.1 of this document. They must match exactly. If Server-A is network reachable from the CMP it is recommended to use the "load" button once the IP address and IP Preference have been defined. The CMP will attempt to load the hostname from the IP reachable server. This will not only confirm network connectivity but will also minimize the possibility of incorrectly defining the Host Name.

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

a) (Required) To enter the IP address, click Add New IP.

The Add New IP dialog box appears.

1. 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.

2. Select the IP Preference: IPv4 or IPV6.

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

The server will preferentially use the IP address in the specified format for communication.

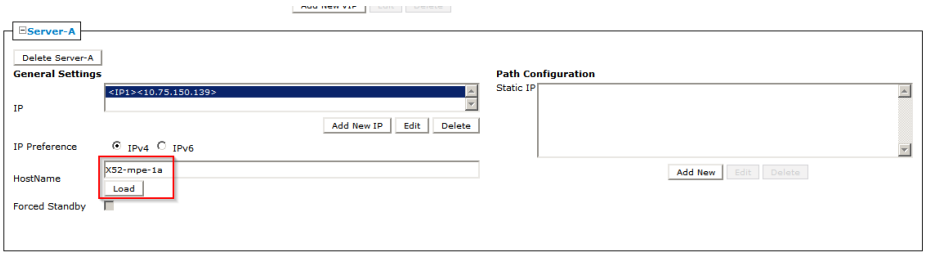
- If neither an IPv6 OAM IP nor a static IP address is defined, IPv6 cannot be selected.
- If neither an IPv4 OAM IP nor a static IP address is defined, IPv4 cannot be selected.

b) 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 a sign that the IP address configured is not accessible across the network. Alternately, you may enter the host name manually but it is recommended to do any network troubleshooting that may be required.

For example:



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:

a) (Required) To enter the IP address, click Add New IP.

The Add New IP dialog box appears.

1. 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.

2. Select the IP Preference: IPv4 or IPV6.

The server will preferentially use the IP address in the specified format for communication.

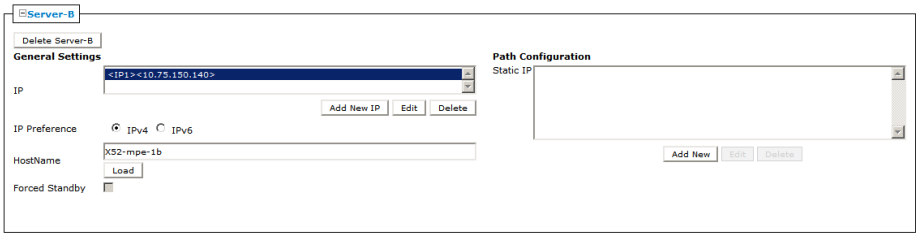
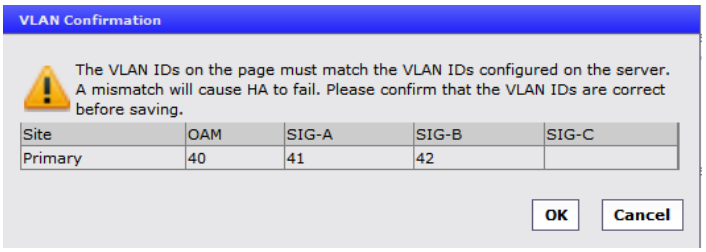
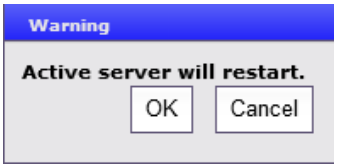
- If neither an IPv6 OAM IP nor a static IP address is defined, IPv6 cannot be selected.
- If neither an IPv4 OAM IP nor a static IP address is defined, IPv4 cannot be selected.

b) Enter the HostName of the server.

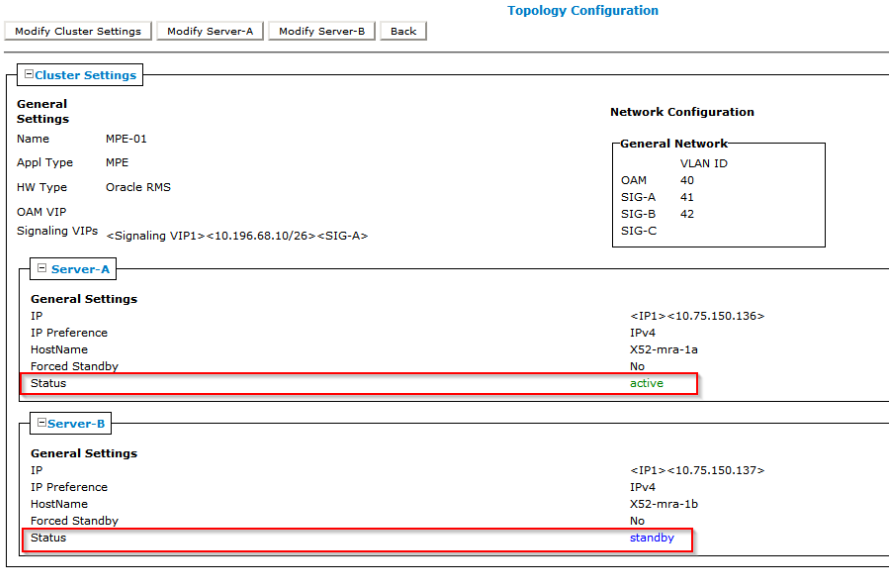
This must exactly match the host name provisioned for this server (the output of the Linux command uname –n).

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 a sign that the IP address configured is not accessible across the network. Alternately, you may enter the host name manually but it is recommended to do any network troubleshooting that may be required.

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

		For example:  **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	"**Save**" the Topology Configuration from the bottom of the Topology Configuration page. Confirm the VLAN configuration if the hardware type requires VLANs  Click <**OK**> to confirm  If the cluster has been added successfully it will now be visible on the Cluster Configuration page. The Cluster Configuration page presents: 
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 on "View" for the Cluster that has just been added 

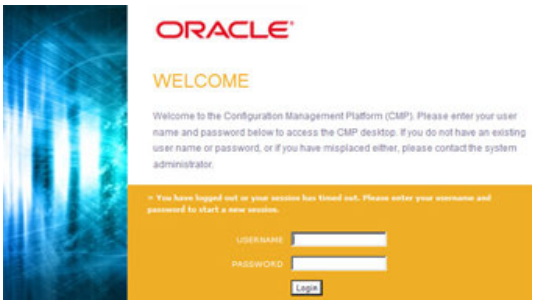
6.4.2: Setting Up a Non-CMP Cluster (MPE/MRA/Mediation)

		The "Topology Configuration presents" for the newly 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 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 newly added servers will show as "offline" and alarms will be generated due the offline state. These alarms will persist until such time as the servers become reachable from the CMP. The CMP will continually retry connecting to the servers that have been newly added in the topology. In this case no further configuration can be performed until the network connectivty between the CMP and the target servers is available. Do not proceed further but rather return to this step at such time the network connectivty from the CMP to the target servers is available. If the servers are reachable then proceed to the next step. The new cluster has now 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 will Manage Remote sites, and these are not yet available.**	If the CMP will Manage Remote sites, and these are not yet available. a) Configure these clusters, but Return to the Verify Steps above after the connectivity has been established. -- OR –- b) Configure these clusters at a later time when the connectivity is established.

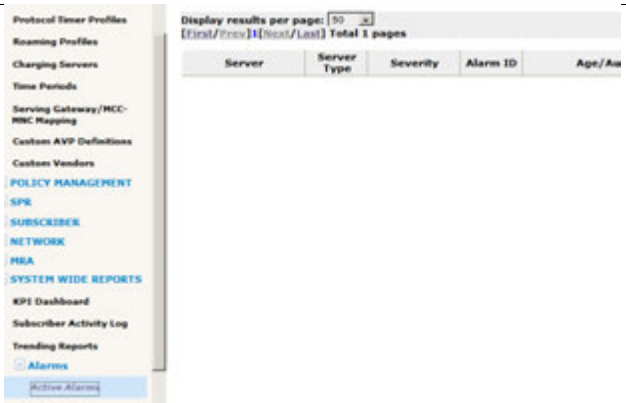
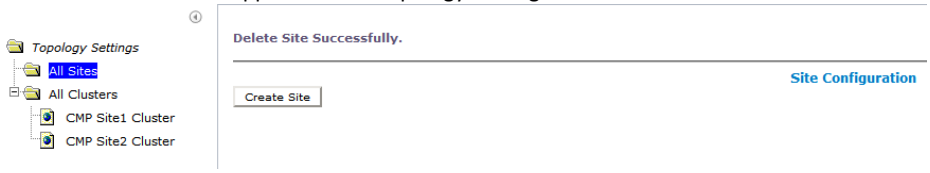
THIS PROCEDURE HAS BEEN COMPLETED

6.4.3 Setting Up a Geo-Redundant Site

6.4.3: Setting Up a Geo-Redundant Site

STEP #	This procedure will create "Sites" that will be used if Geo-Redundant Clusters will be added to the CMP Topology. A Geo-Redundant Cluster will be associated with these "Sites" in the next procedure. If Geo-Redundant Clusters will not be needed than this procedure can be skipped. **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.	
1. ☐	**CMP GUI:** Login to CMP Server GUIs (using VIP)	From Browser, enter CMP Server VIP in Navigation string. **Note:** Only the following Web Browsers are supported in OCMP 12.2 • Mozilla Firefox® release 31.0 or later • Google Chrome version 40.0 or later *Internet Explorer in not supported for this procedure  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 activities.  View of Alarms from CMP GUI upper right banner

6.4.3: Setting Up a Geo-Redundant Site

		 View of Alarms from System Wide Reports -> Active Alarms IMPORTANT: In Policy 12.2.x, there is On-line help provided for Alarm descriptions. In the Alarm views, click on the alarm Id to open the Alarm description help page. Alternatively, from the Menu select On-Line Help, and select Troubleshooting Guide. Search this for the Alarm Id.
3. ☐	**CMP:** View Topology Settings	**PLATFORM SETTINGS → Topology Settings** Confirm that "All Sites" appears in the Topology Settings Menu.  • **Note:** Sites may only be created when Manage Geo-Redundant mode is enabled.  **Note:** If Manage Geo-Redundant mode was not selected during initial configuration of the Site1 CMP Cluster, the CMP modes can be changed now if needed, but the method to access this mode selection is not documented. Contact Oracle Support if Mode selection is required to be changed after the initial configuration.

6.4.3: Setting Up a Geo-Redundant Site

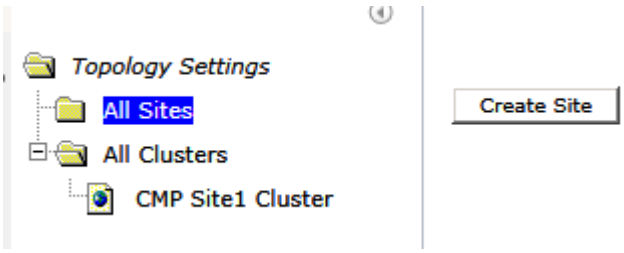
4. ☐

CMP GUI: Create Sites for Geo-Redundant Configuration

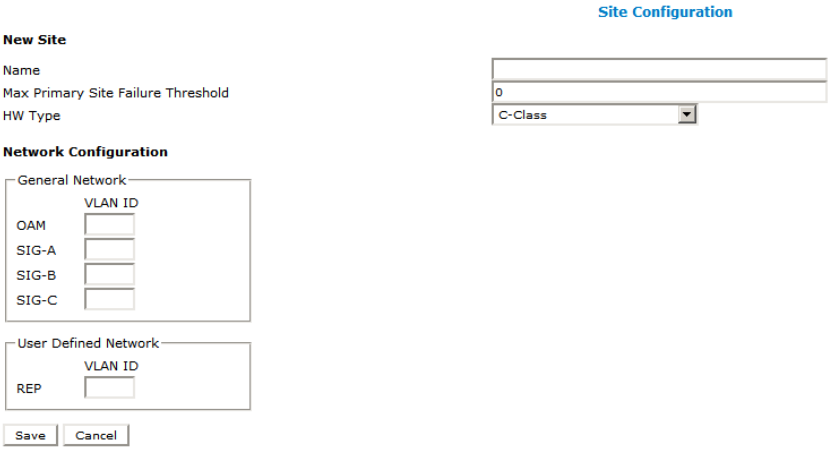
For a Geo-Redundant Configuration at least 2 Sites must be created before proceeding with this procedure. This step is preparation for adding Geo-Redundant MPE/MRA/Mediation clusters and is not needed to add a Geo-Redundant CMP Cluster. If Geo-Redundancy is not anticpated this step may be skipped.

PLATFORM SETTINGS →Topology Settings→All Sites

a. Select **Create Site**



The Site Configuration form opens.



b. 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)

If you selected C-Class, C-Class(Segregated Traffic), or NETRA, enter the General Network - VLAN IDs.

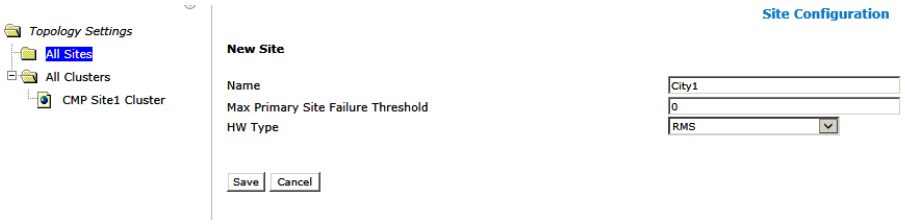
c. Enter the OAM, SIG-A, and (optionally) SIG-B virtual LAN (VLAN) IDs.

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

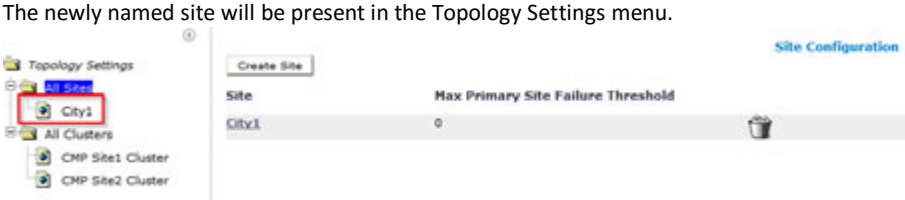
- OAM – 3
- SIG-A – 5
- SIG-B – 6

6.4.3: Setting Up a Geo-Redundant Site

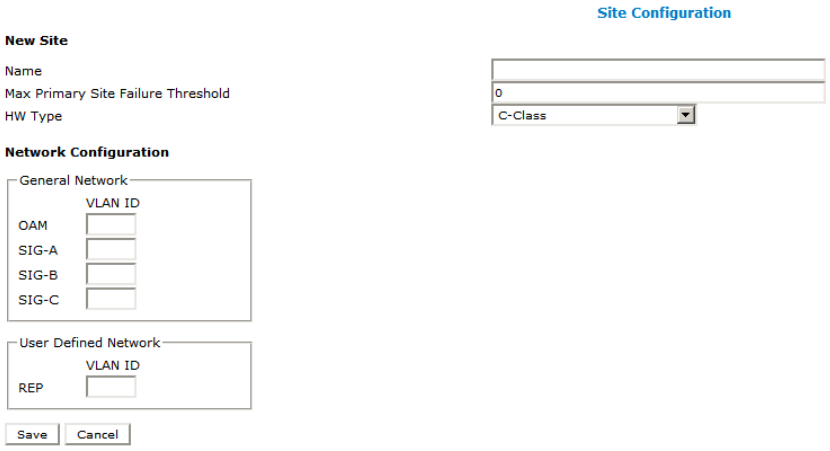
d. Name the new **Site** and **Save.**



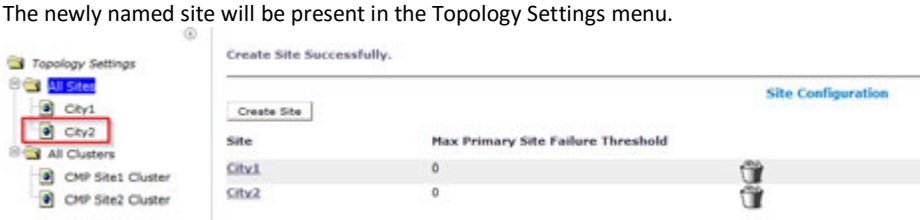
The newly named site will be present in the Topology Settings menu.



e. Create a 2nd Site and **Save.**



The newly named site will be present in the Topology Settings menu.



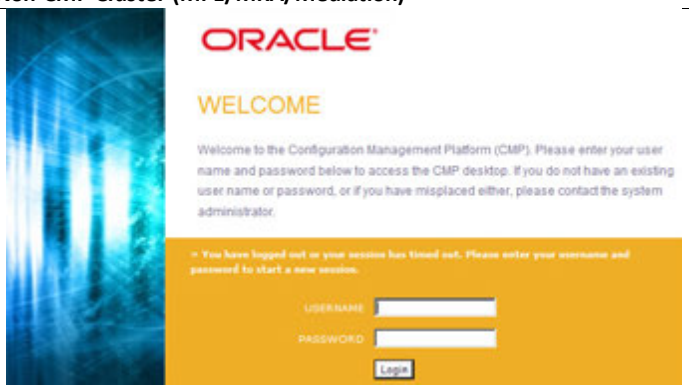
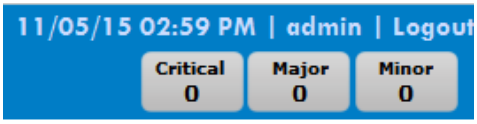
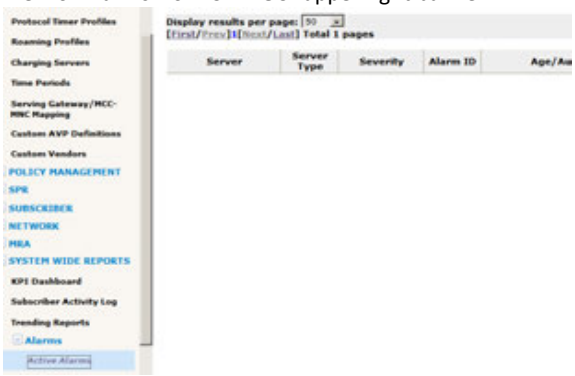
THIS PROCEDURE HAS BEEN COMPLETED

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

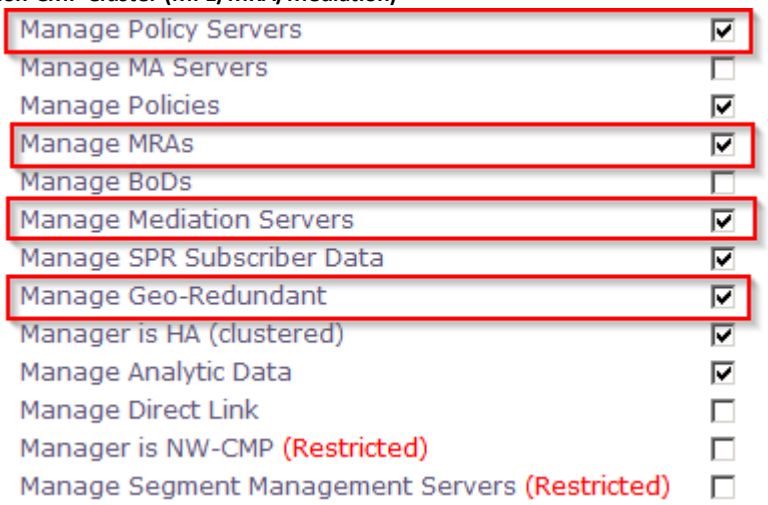
6.4.4: Setting Up a Geo-Redundant Non-CMP Cluster (MPE/MRA/Mediation)

STEP #	This procedure will configure the management relationships between the CMP and other Geo-Redundant Non-CMP in Wireless Mode. A non-CMP cluster includes one of the following server types: • MPE • MRA • 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.	
1. ☐	**CMP GUI:** Login to CMP Server GUIs (using VIP)	From Browser, enter CMP Server VIP in Navigation string. **Note:** Only the following Web Browsers are supported in OCMP 12.2 • Mozilla Firefox® release 31.0 or later • Google Chrome version 40.0 or later *Internet Explorer in not supported for this procedure

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

		 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 activities.  View of Alarms from CMP GUI upper right banner  View of Alarms from System Wide Reports -> Active Alarms IMPORTANT: In Policy 12.2.x, there is On-line help provided for Alarm descriptions. In the Alarm views, click on the alarm Id to open the Alarm description help page. Alternatively, from the Menu select On-Line Help, and select Troubleshooting Guide. Search this for the Alarm Id.
3. ☐	**Mode Configuration Considerations**	The 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 Geo-Redundant

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



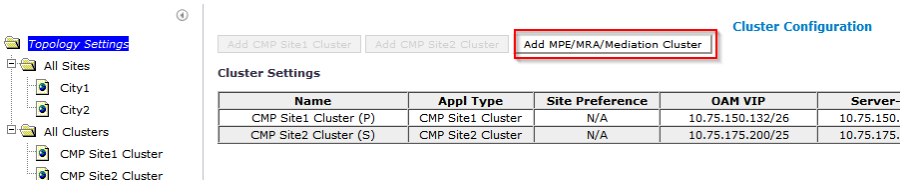
Notes:

- 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 this mode selection is not documented. Contact Oracle Support if Mode selection is required to be changed after the initial configuration.

4. ☐ **CMP GUI:** Add MPE/MRA/Mediation Clusters

PLATFORM SETTINGS → Topology Settings

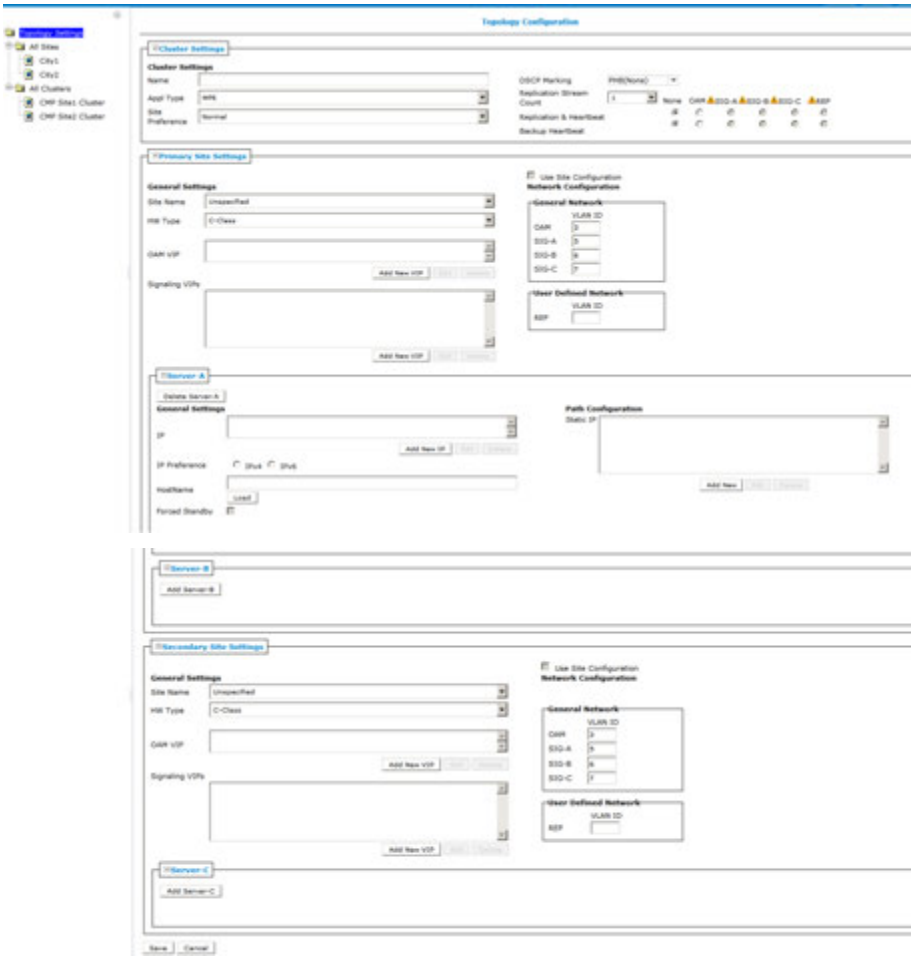


On the cluster Configuration page select "**Add MPE/MRA/Mediation**".

Note: "Mediation Cluster" will only be present if "Manage Mediation Servers" was selected in mode options.

- 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.

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

		The Topology Configuration page presents:  **Notes:** • "All Sites" will be present in the Topology Settings menu. • "Primary Site Settings" and "Secondary Site Settings" will be present on the Topology Configuration page. • Server-C will be present Under "Secondary Site Settings".
5. ☐	**CMP GUI:** Add MPE/MRA/Mediation Clusters	Complete the form according to the system design. It is allowed to add both Server-A, Server-B and Server-C at the same time. To add Server-C expand the Server-C option by clicking on the "+" sign for Server-C. **Notes:** • It is possible to come back at a later time and modify any settings made at this time. • The procedure for adding an MPE/MRA or Mediation Cluster is the same except for selecting "Appl Type" which will be MPE/MRA or Mediation respectively.

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

Define the "Cluster Settings"

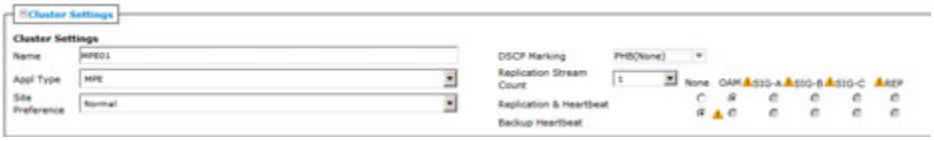
Name (required) — Name of the cluster. Enter up to 250 characters, excluding quotation marks(") and commas (,).

Appl Type — Select the type of server: **MPE** (default) **MRA** or **Mediation**

Site Preference – NORMAL (default)

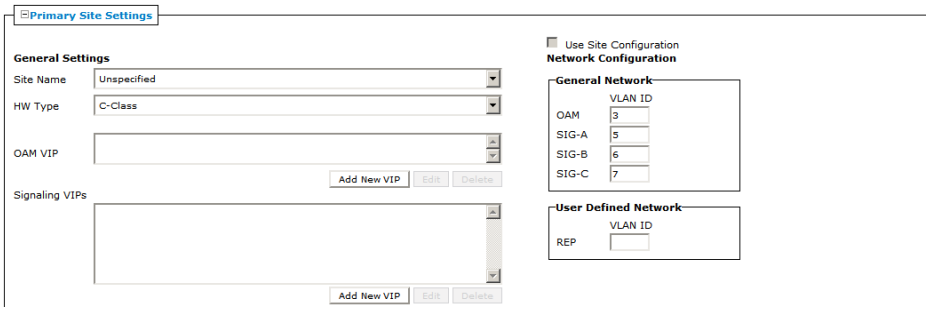
DSCP Marking = PHB(None)is the default
Replication Stream Count = 1 through 8. 1 is the default.
Replication and Heartbeat = None is the default. OAM is typically preferred.
Backup Heartbeat = None (default) or OAM

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 Geo-Redundant topology

HW Type — Select the type of hardware:

- C-Class (default) – HP ProLiant BL460 Gen6/Gen8 server
- C-Class (Segregated Traffic) (a configuration where Signaling and other networks are separated onto physically separate equipment) – HP ProLiant BL460 Gen6/Gen8
- Oracle RMS – Oracle Server X5-2 or Oracle Netra Server X5-2
- RMS (rack-mounted server) – HP ProLiant DL360 Gen6 or HP ProLiant DL380 Gen8/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.

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

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 1–4095.

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.

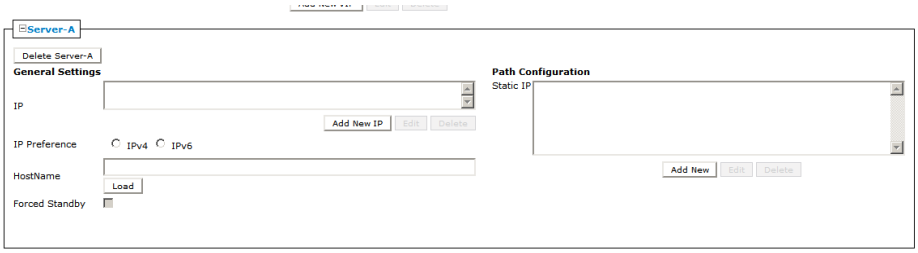
Signaling VIPs (required) — The signaling VIP is the IP address a PCEF (or Gateway) device uses to communicate with a cluster. Click **Add New VIP** to add a VIP to the system. A cluster supports the following redundant communication channels for carriers that use redundant signaling channels.

- SIG-A
- SIG-B
- SIG-C

At least one signaling VIP is required.

<u>Define the settings for **Server-A** in the "Primary Site Settings" section of the page</u>

Note: The "IP" address and "Host Name" of Server-A will be 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 to use the "load" button once the IP address and IP Preference have been defined. The CMP will attempt to load the hostname from the IP reachable server. This will not only confirm network connectivity but will also minimize the possibility of incorrectly defining the Host Name.



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

a) (Required) To enter the IP address, click Add New IP.

The Add New IP dialog box appears.

1. 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.

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

2. Select the IP Preference: IPv4 or IPV6.

The server will preferentially use 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.

b) 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 a sign that the IP address configured is not accessible across the network. Alternately, you may enter the host name manually but it is recommended to do any network troubleshooting that may be required.

c) In the **Path Configuration section**, to add a **Static IP**, click **Add New**.

The **New Path** dialog box appears.

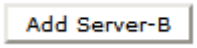
Note: If an alternate replication path and secondary HA heartbeat path is used, a server **Static IP** address must be entered in this field.

1. Enter a **Static IP** address and **Mask**.
2. Select the **Interface**:

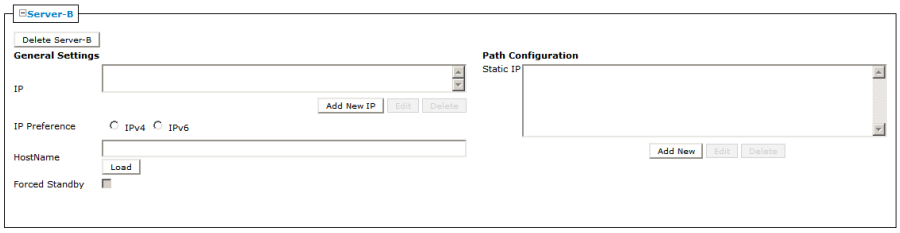
- SIG-A
- SIG-B
- SIG-C
- REP
- BKUP

<u>Define the settings for **Server-B** in the Server-B section of the page</u>

Select “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:

a) (Required) To enter the IP address, click Add New IP.

The Add New IP dialog box appears.

1. 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.

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

2. Select the IP Preference: IPv4 or IPV6.

The server will preferentially use 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.

b) 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 a sign that the IP address configured is not accessible across the network. Alternately, you may enter the host name manually but it is recommended to do any network troubleshooting that may be required.

c) In the **Path Configuration section**, to add a **Static IP**, click **Add New**.

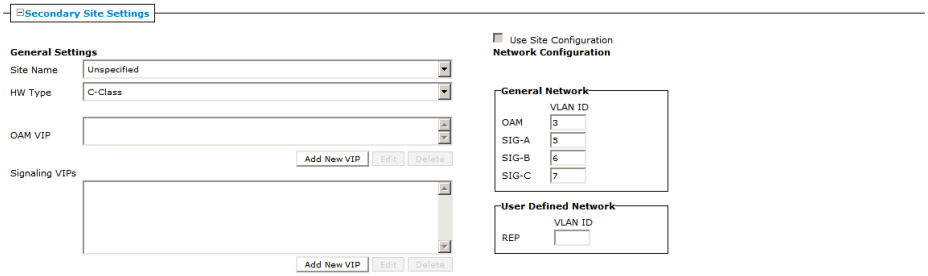
The **New Path** dialog box appears.

Note: If an alternate replication path and secondary HA heartbeat path is used, a server **Static IP** address must be entered in this field.

1. Enter a **Static IP** address and **Mask**.
2. 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 Geo-Redundant topology

HW Type — Select the type of hardware:

- C-Class (default) – HP ProLiant BL460 Gen6/Gen8 server
- C-Class (Segregated Traffic) (a configuration where Signaling and other networks are separated onto physically separate equipment) – HP ProLiant BL460 Gen6/Gen8
- Oracle RMS – Oracle Server X5-2 or Oracle Netra Server X5-2
- RMS (rack-mounted server) – HP ProLiant DL360 Gen6 or HP ProLiant DL380 Gen8/Gen9 server
- VM (virtual machine)
- VM(Automated) (VM managed by NF Agent)

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

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 1–4095.

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.

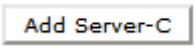
Signaling VIPs (required) — The signaling VIP is the IP address a PCEF (or Gateway) device uses to communicate with a cluster. Click **Add New VIP** to add a VIP to the system. A cluster supports the following redundant communication channels for carriers that use redundant signaling channels.

- SIG-A
- SIG-B
- SIG-C

At least one signaling VIP is required.

<u>Define the settings for **Server-C** in the "Secondary Site Settings" section of the page</u>

Select "Add Server-C" on the Topology Configuration page



The "Server-C" configuration form opens

a) (Required) To enter the IP address, click Add New IP.

The Add New IP dialog box appears.

1. 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.

2. Select the IP Preference: IPv4 or IPV6.

The server will preferentially use 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.

b) Enter the HostName of the server.

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

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 a sign that the IP address configured is not accessible across the network. Alternately, you may enter the host name manually but it is recommended to do any network troubleshooting that may be required.

For example:

In the **Path Configuration section**, to add a **Static IP**, click **Add New**.
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.

1. Enter a **Static IP** address and **Mask**.
2. Select the **Interface**:

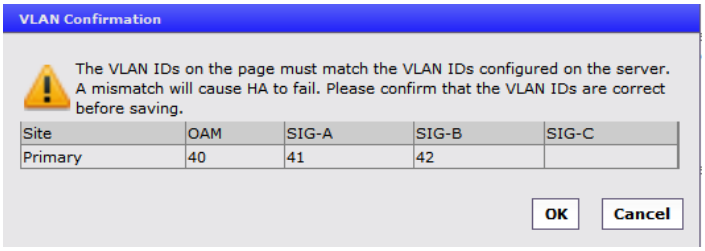
- SIG-A
- SIG-B
- SIG-C
- REP
- BKUP

Note: These settings are only an example of a likely configuration. An actual deployment will be specific to customer requirements.

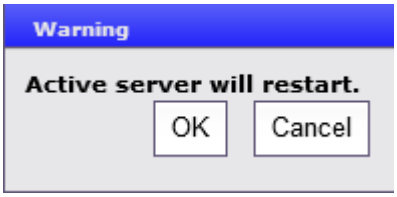
10. ☐ **CMP GUI:** Add MPE/MRA/Mediation Clusters

"**Save**" the Topology Configuration from the bottom of the Topology Configuration page.

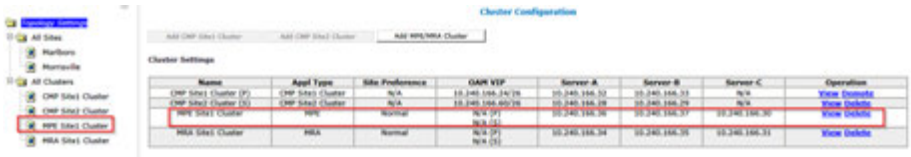
Confirm the VLAN configuration if the hardware type requires VLANs



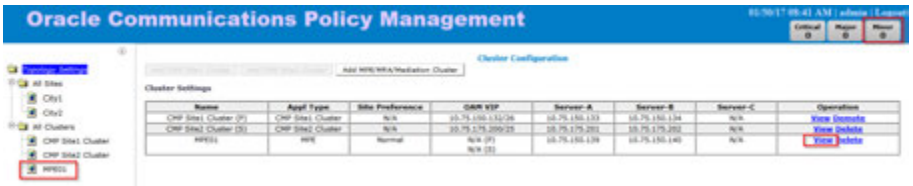
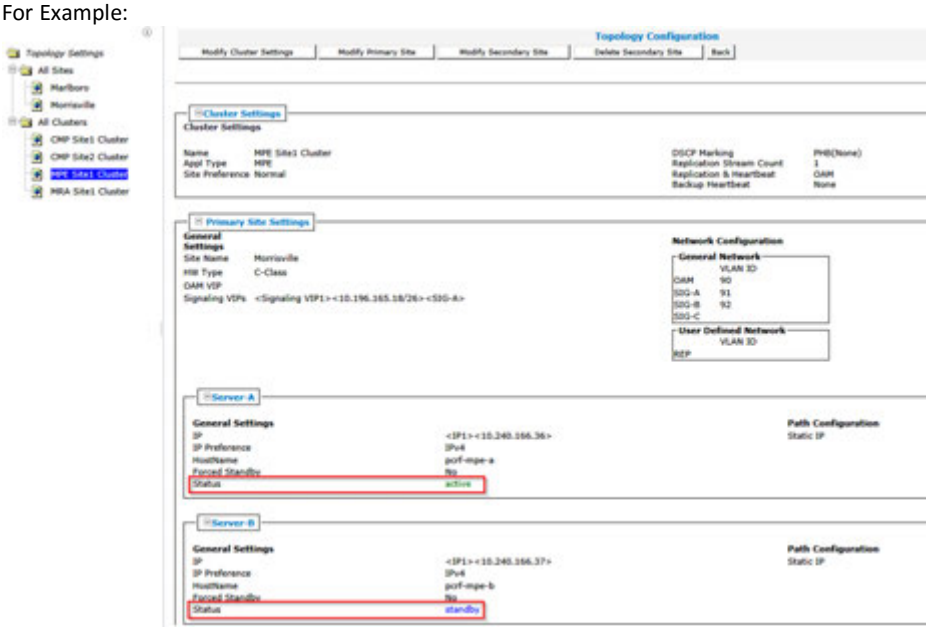
Click <**OK**> to confirm



If the cluster has been added successfully it will now be visible on the Cluster Configuration page. The Cluster Configuration page presents:



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

11. ☐	**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 on "View" for the Cluster that has just been added  "Server-A" and "Server-B" should be an "active" and "standby". It does not matter which server is active. Server-C should show a staus of "Spare". If this is the case, and there are no alarms, then the Geo-Redundant cluster has been added successfully. For Example: 

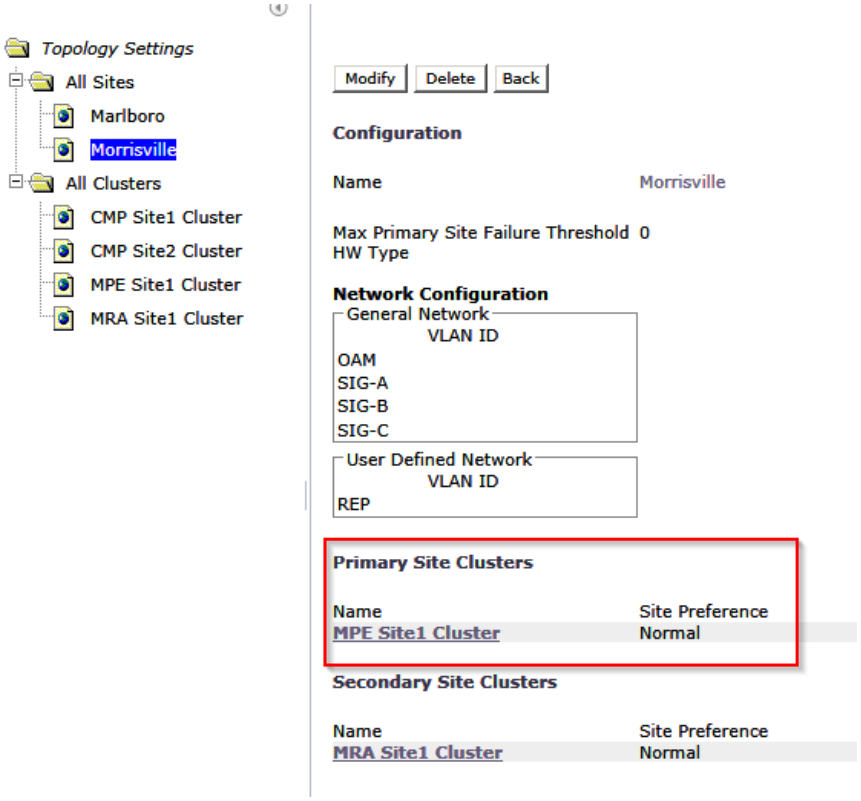
6.4.4: Setting Up a Geo-Redundant Non-CMP Cluster (MPE/MRA/Mediation)

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 newly added servers will show as "offline" and alarms will be generated due the offline state. These alarms will persist until such time as the servers become reachable from the CMP. The CMP will continually retry connecting to the servers that have been newly added in the topology. In this case no further configuration can be performed until the network connectivty between the CMP and the target servers is available. Do not proceed further but rather return to this step at such time the network connectivty from the CMP to the target servers is available. If the servers are reachable then proceed to the next step.

Confirm the newly added Non-CMP clusters have been associated with the correct "Site".

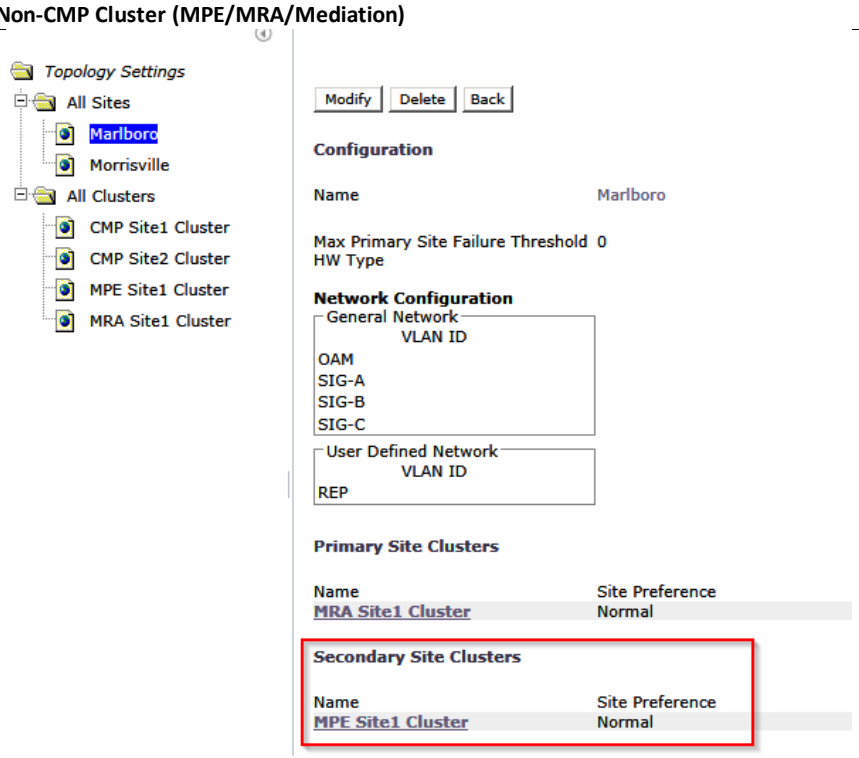
Topology Settings→All Sites→<Site Name>

For example: Here "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".

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

		 The new cluster has now been successfully added.
12. ☐	**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.
13. ☐	**If the CMP will Manage Remote sites, and these are not yet available.**	If the CMP will Manage Remote sites, and these are not yet available. a) Configure these clusters, but Return to the Verify Steps above after the connectivity has been established. -- OR —- b) Configure these clusters at a later time when the connectivity is established.
THIS PROCEDURE HAS BEEN COMPLETED		

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 execute 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, reexecute this procedure. The SSH provisioning utility will recheck the existing SSH key exchanges in the entire topology and provision any key exchanges not yet executed. You can execute the command multiple times, even if keys were previously exchanged.

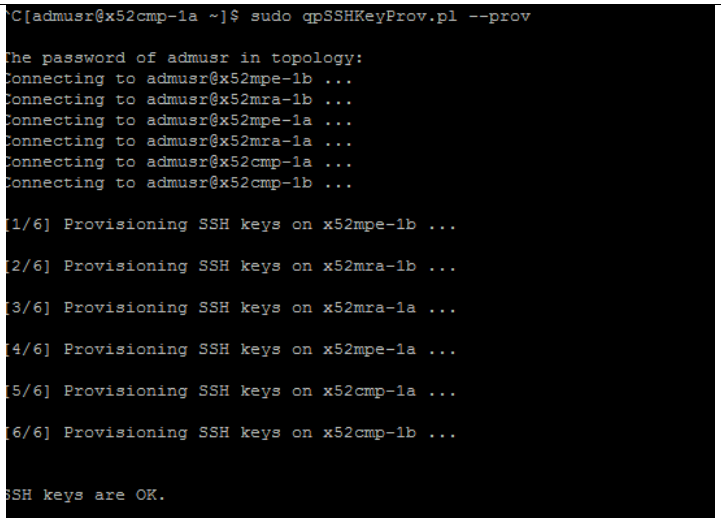
6.5 Performing SSH Key Exchanges

STEP #	**Prerequisite:** - CMP Site 1 cluster is configured and GUI available - Before beginning this procedure, the systems that are exchanging keys must be configured and reachable. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	

1. ☐	**Ssh to CMP Site 1 active server:** Execute Key Exchanges to 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 ~]$`

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

6.5 Performing SSH Key Exchanges

		
3. ☐	**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:

6.5 Performing SSH Key Exchanges

```
[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 ~]$
```

THIS PROCEDURE HAS BEEN COMPLETED

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 server ILOM or iLO remote console is always 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

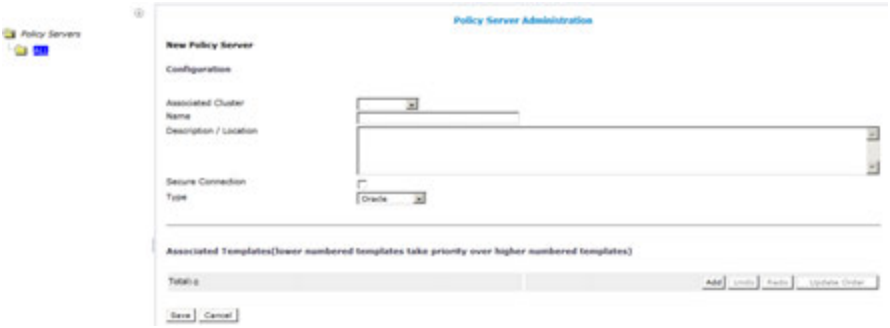
This section will cover procedures to configure the Policy Servers to a minimum level to execute a test call. Additional details can be found in the Configuration Management Platform Wireless User's Guide

6.7.1 Adding MPE and MRA to CMP Menu

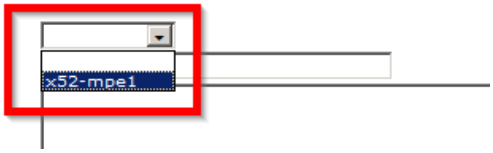
This procedure will configure the Policy Server (MPE) and MRA applications.

6.7.1: Adding MPE and MRA to the CMP Menu

6.7.1: Adding MPE and MRA to the CMP Menu

STEP #	This procedure will perform the configuration of MPE/Policy Server 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 12.2 • Mozilla Firefox® release 31.0 or later • Google Chrome version 40.0 or later *Internet Explorer in not supported for this procedure 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.	
1. ☐	**Create Policy Server in CMP GUI**	**Select: Policy Server→ Configuration→ Policy Servers**  Click "**Create Policy Server**" in the Policy Server Administration screen:  Enter values for the configuration attributes: a) **Associated Cluster** (required) — Select the cluster with which to associate this MPE device. MPE clusters already configured in Topology Settings will be listed. b) **Name** — Name of this MPE device. The default is the associated cluster name. c) **Description / Location** (optional) — Information that defines the function or location of this MPE device. d) **Secure Connection** — Designates whether or not to use the HTTPS protocol for communication (certifcates must be configured to use this option) between Policy

6.7.1: Adding MPE and MRA to the CMP Menu

		Management devices. If selected, devices communicate over port 8443. e) **Type** — Defines the policy server type: • **Oracle** (default) — The policy server is an MPE device and 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 drop down tab will only be populated with MPE clusters that have been configured in the CMP Topology from previous steps. **New Policy Server** **Configuration** Associated Cluster Name Description / Location  After completing the form, Click "**Save**" and confirm Configured Policy Server status is "On-line": 
2. ☐	**Check MPE cluster in Reports tab**	**Select: Policy Server→Configuration -> <MPE>→ Reports tab**

6.7.1: Adding MPE and MRA to the CMP Menu

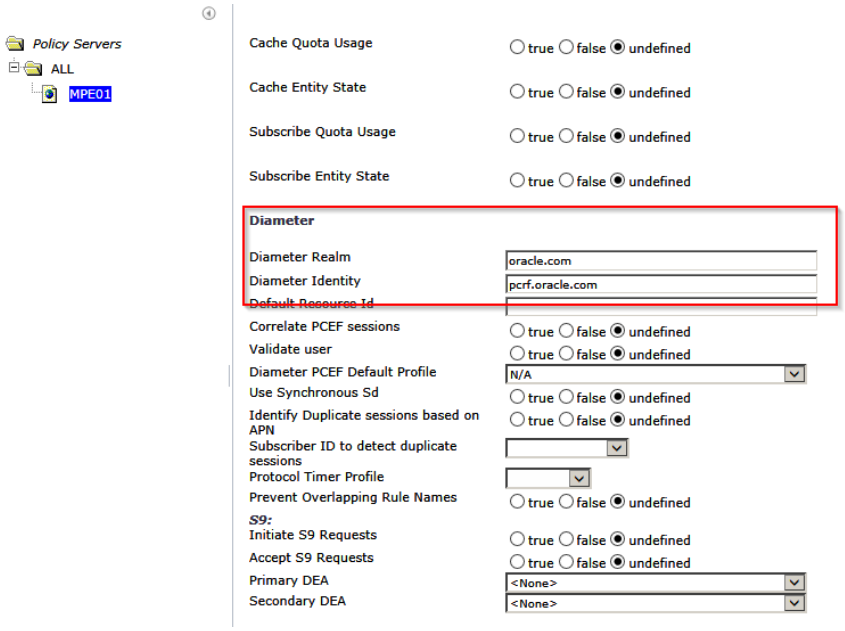
Validate that MPE cluster status is "On-line" and that both Active and Standby servers displayed correctly.

3. ☐

Diameter configuration of MPE

Select: Policy Server→ Configuration→MPE→Policy Server tab

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 the "Modify" button on top of page then fill in the Diameter Realm and Identity that your network will be using and click "Save":

6.7.1: Adding MPE and MRA to the CMP Menu

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:

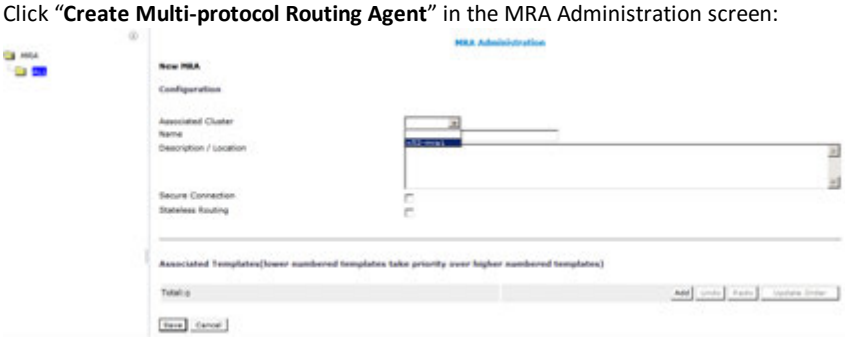
Diameter

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

4. ☐ **Create MRA in CMP GUI**

Select: MRA →Configuration→ ALL

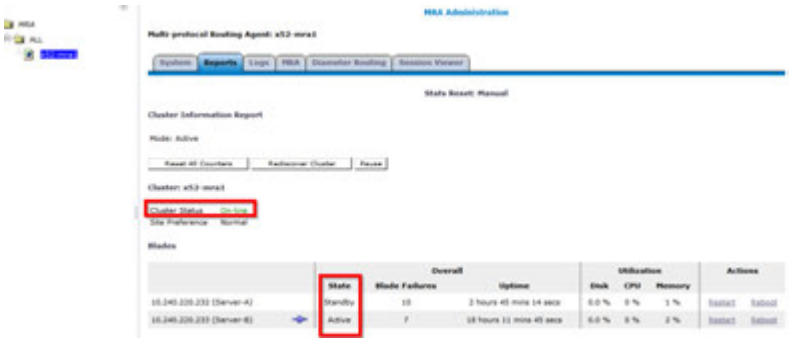
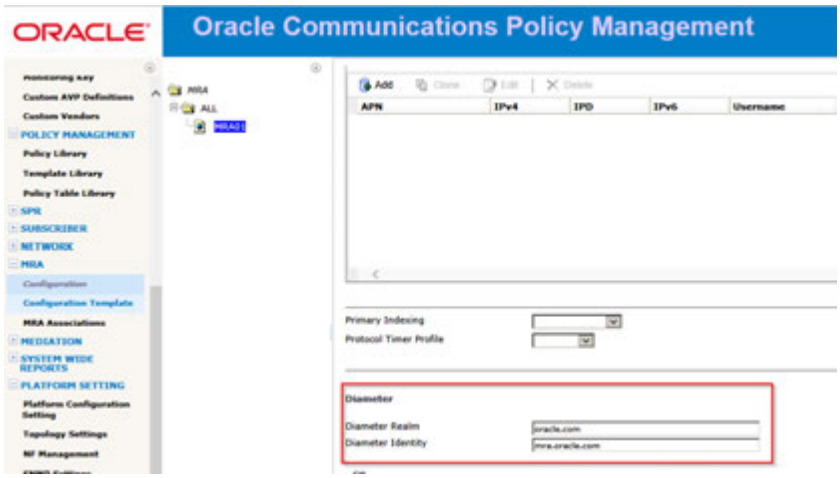
Click "**Create Multi-protocol Routing Agent**" in the MRA Administration screen:



Enter information as appropriate for the MRA cluster:
a) **Associated Cluster** (required) — Select the MRA cluster from the list.
b) **Name** (required) — Enter a name for the MRA cluster.
c) **Description/Location** (optional) — Free-form text. Enter up to 250 characters.
d) **Secure Connection** — Select to enable a secure HTTP connection (HTTPS) instead of a normal connection (HTTP). The default is a non-secure (HTTP) connection.
e) **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.

Then Click "**Save"** and confirm Configured MRA status is "On-line":

6.7.1: Adding MPE and MRA to the CMP Menu

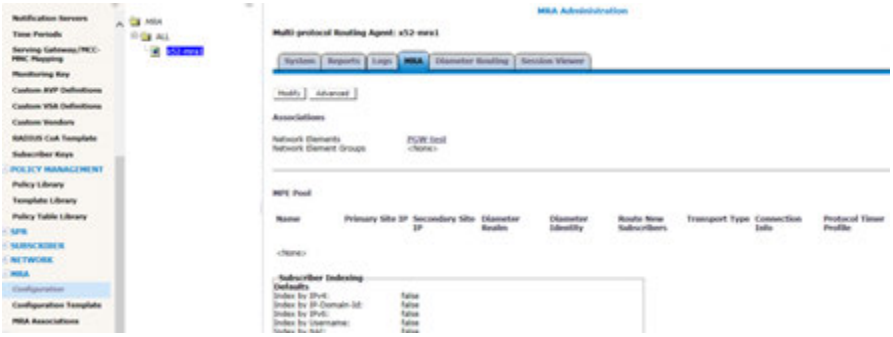
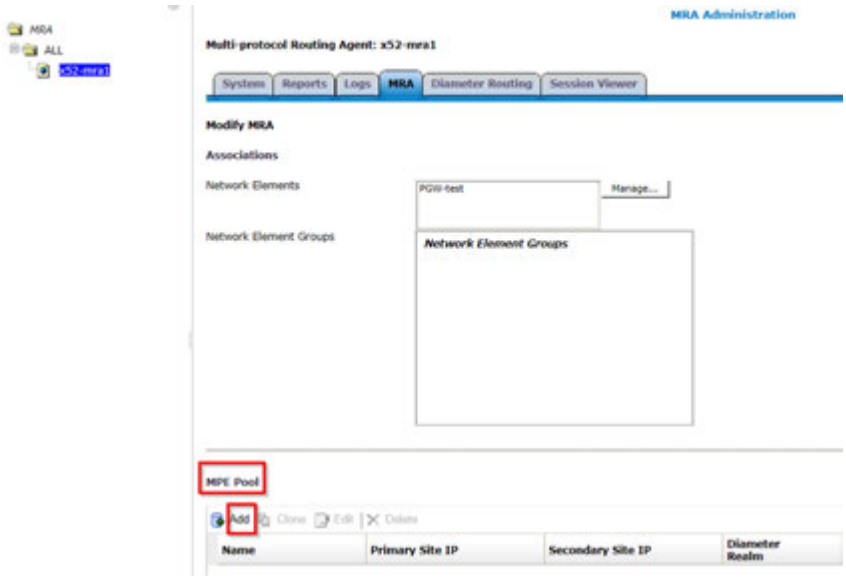
		
5. ☐	**Check MRA cluster in Reports tab**	**Select: MRA -> Configuration -> MRA -> Reports tab**  Validate that MPE cluster status is **"**On-line" and that both Active and Standby servers displayed correctly.
6. ☐	**Diameter configuration for MRA**	**Select: MRA -> Configuration -> MRA -> MRA tab** It is important to define Diameter Realm and identity to enable Diameter messaging to function correctly:  To define these Diameter parameters, click the "Modify" button on top of page then fill in the Diameter Realm and Identity that your network will be using and click "Save": **Diameter** Diameter Realm oracle.com Diameter Identity mra.oracle.com

THIS PROCEDURE HAS BEEN COMPLETED

6.7.2 Configure MPE Pool on MRA (Policy Front End)

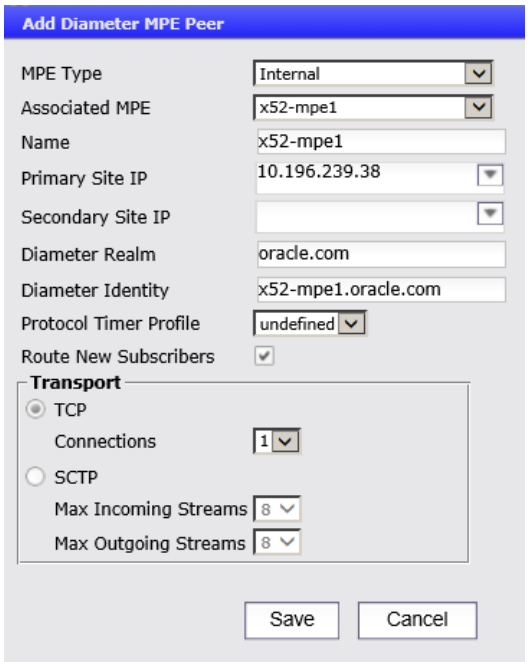
If MRAs (Policy Front End) are used in the Policy Management System, the MPEs for which the MRA will act as the Policy Front End, must be added to the MPE Pool on the MRA. If MPEs are not used in the Policy Solution this procedure can be skipped.

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

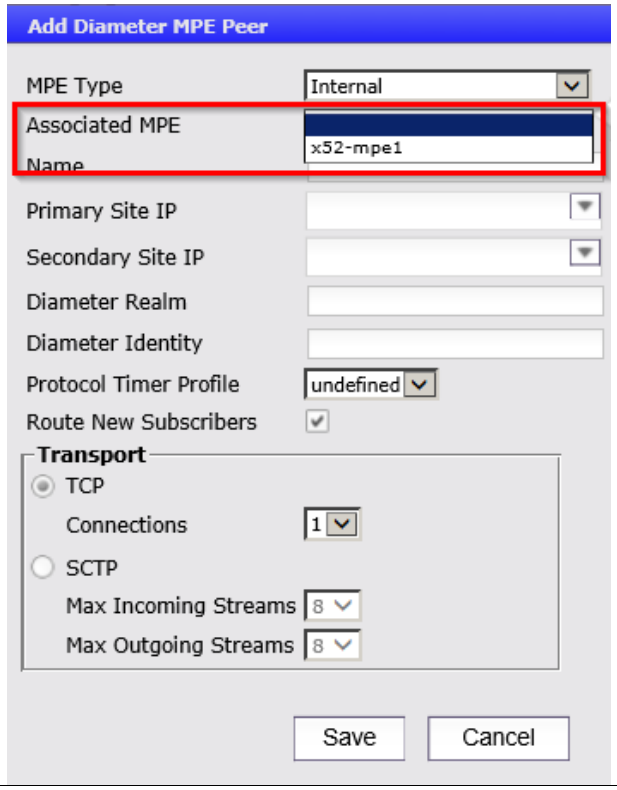
STEP #	This procedure will add the MPE clusters to the MPE Pool of the MRA (Policy Front End) **Prerequisite:** - Network access to the CMP OAM IP address, to bring up a web Browser GUI (http) - MRA and MPE clusters have been added to the CMP Menu Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1. ☐	**Create Network Element in CMP GUI**	**Select: MRA →Configuration→ <MRA>→MRA tab**  Click "**Modify**" in the MRA Administration screen: The "MPE Pool" configuration form is presented. 

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

Click "**Add**" under "MPE Pool": The "Add Diameter MPE Peer" form opens.

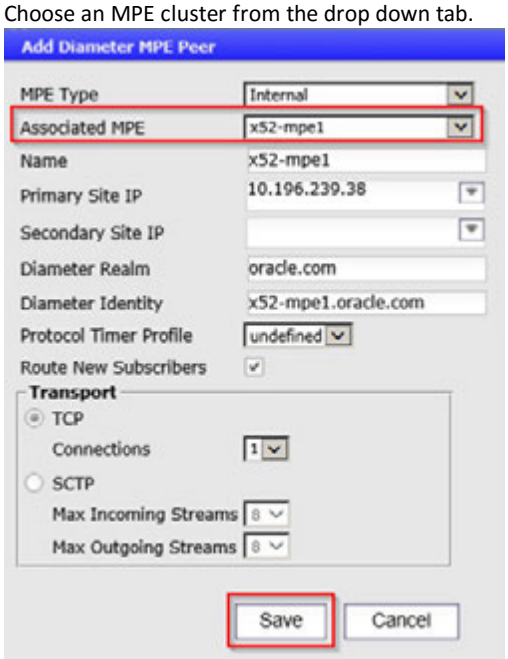


Click the "**Associated MPE**" drop down on the "Add Diameter MPE Peer" form. MPE clusters previously configured in the CMP topology and added to the CMP menu will be listed here.



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

Choose an MPE cluster from the drop down tab.

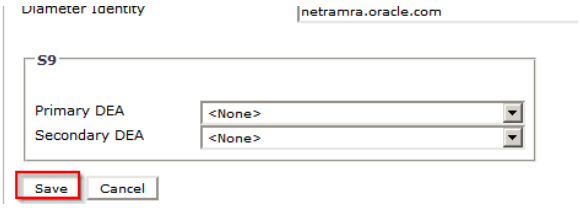


The required fields will auto-populate. Click "**Save**"

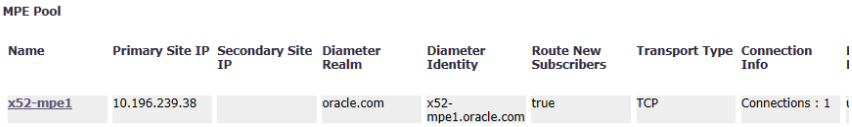
Note: The Diameter Realm and Diameter Identity must have already been data-filled on the MPE.

The added MPE cluster now appears in the MPE Pool.

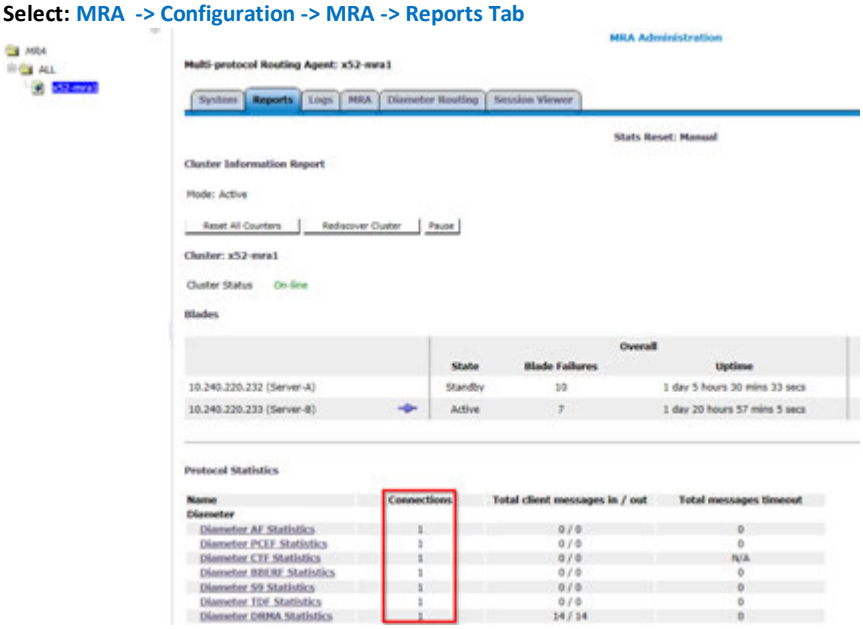
Navigate to the bottom of the form and click "**Save**" again.



The added MPE cluster can now be seen in the "MPE Pool".



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

		Confirm the Diameter connection to the MPE from the MRA on the MRA Reports tab **Select: MRA -> Configuration -> MRA -> Reports Tab**  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

THIS PROCEDURE HAS BEEN COMPLETED

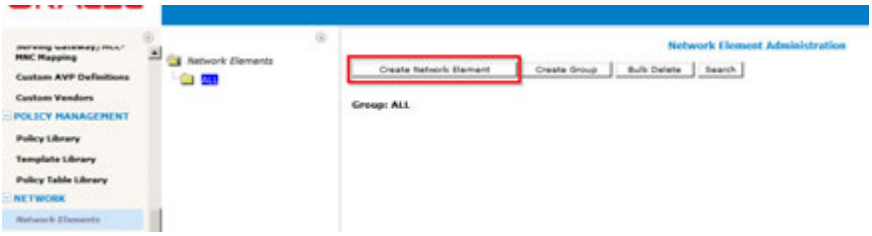
6.7.3 Define and Add Network Elements

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

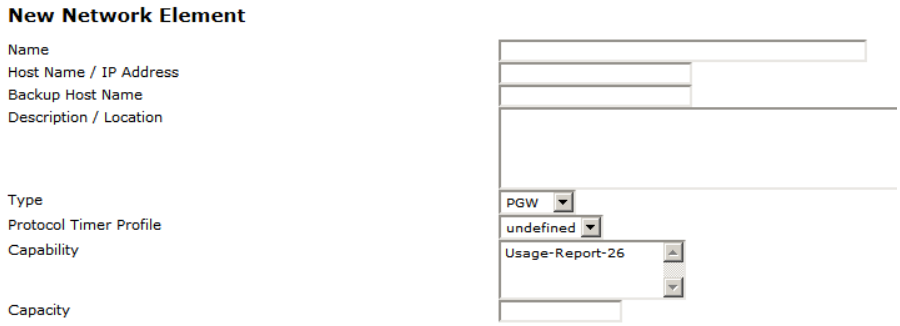
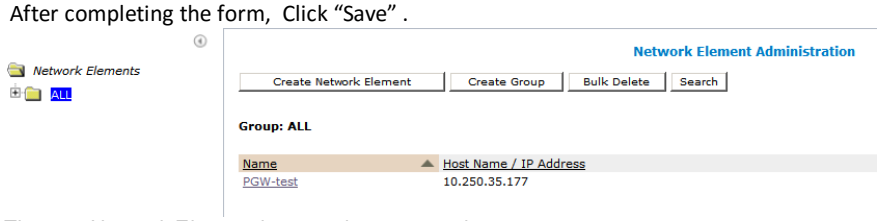
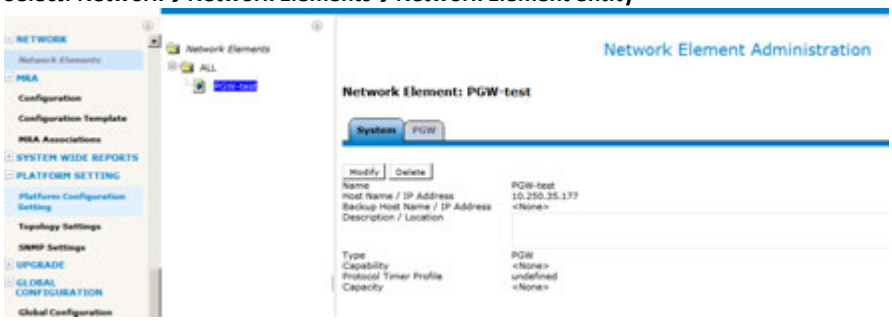
6.7.3: Define and Add Network Elements

STEP #	This procedure will add 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.	
1.	**Create Network Element**	**Select: Network→Network Elements→All**

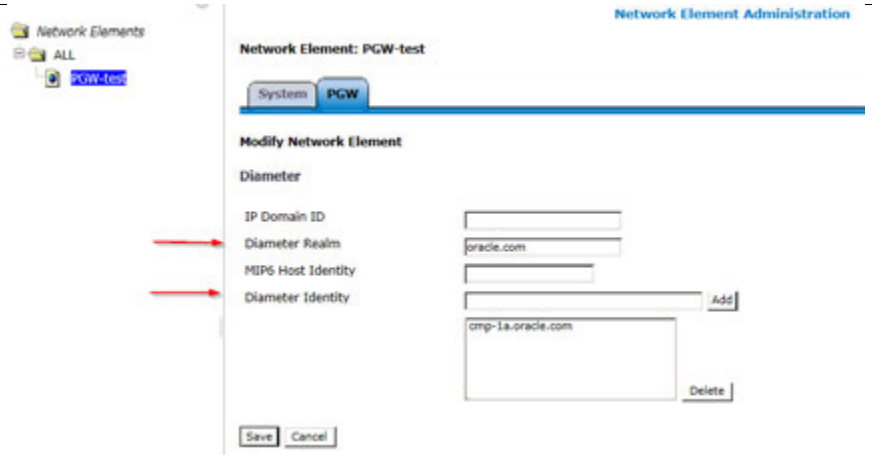
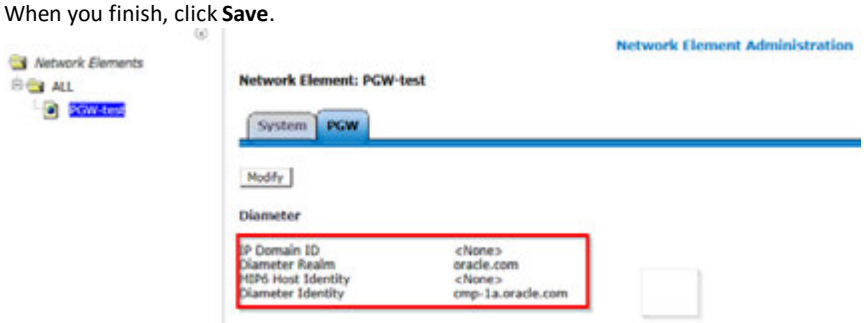
6.7.3: Define and Add Network Elements

☐	**in CMP GUI**	 Click "**Create Network Element**" in the "Network Element Administration" screen:  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 network element's primary address 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 • **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. When you finish, click **Save**.

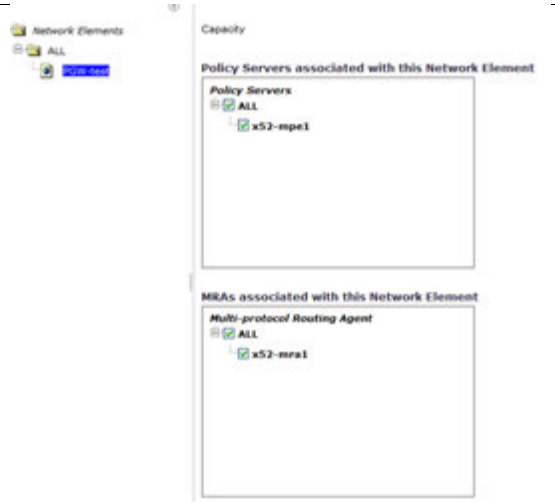
6.7.3: Define and Add Network Elements

		For this example a "**PGW**" Network Element has been defined.  After completing the form, Click "Save" .  The new Network Element has now been created.
2.	**Configure Network Element in CMP GUI**	**Select: Network→Network Elements→Network Element entity**  The newly created Network Element will display on the "System" tab, showing the configuration from the previous step. For an initial call to the Policy Management System, the Network Element will need connectivity to the Policy Management System. In addition the Network Element will need a Diameter Identity assigned that will be used to authenticate the Diameter connection from the Network Element. Click on the "**PGW**" tab of the Network Element to assign the Diameter Identity that will be used to authenticate to the Policy Management System. Click "**Modify**".

6.7.3: Define and Add Network Elements

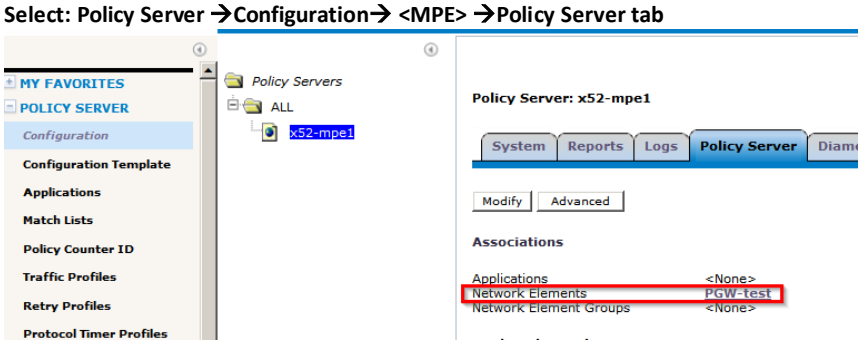
		 **Note:** This tab is dependent on the Network Element "**Type**" that was configured during the previous step. In this example the Network Element "**Type**" used is a "**PGW**" (Packet Gateway) which will be used to establish a Diameter connection to the Policy Management System. When you finish, click **Save**. 
3. ☐	**Deploy Network Element in CMP GUI**	**Select: Network→Network Elements →<Network Element entity>**  Click "**Modify**" in the Network Element Administration screen and check the boxes as appropriate to deploy the network element to the MPE and MRA if present.

6.7.3: Define and Add Network Elements



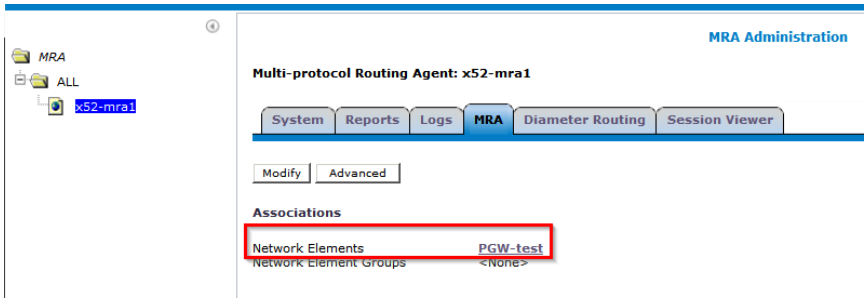
When you finish, click "**Save**".

Select: Policy Server →Configuration→ <MPE> →Policy Server tab



Confirm the deployed Network Element has now been associated with the MPE.

Select: MRA →Configuration→<MRA> →MRA tab



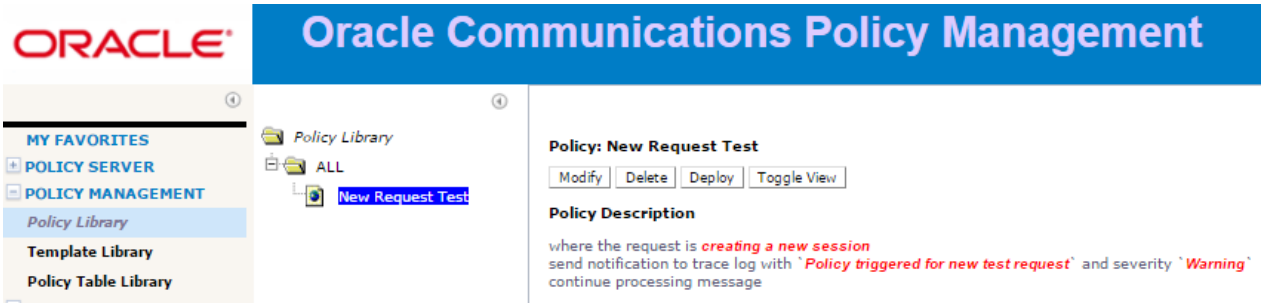
Confirm the deployed Network Element has now been associated with the MRA.

THIS PROCEDURE HAS BEEN COMPLETED

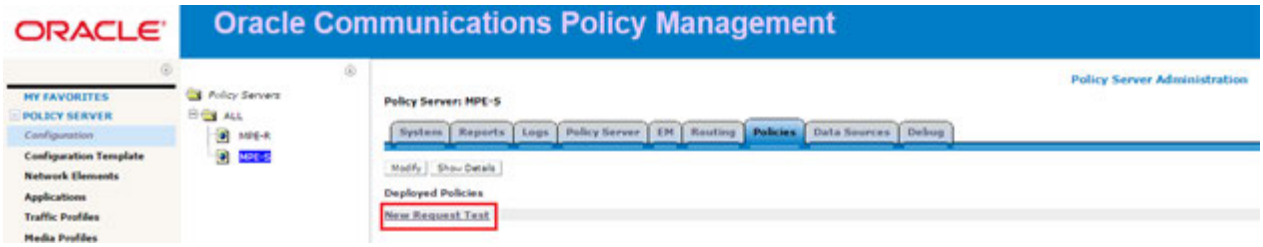
6.8 LOAD POLICIES AND RELATED POLICY DATA

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 will process 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.

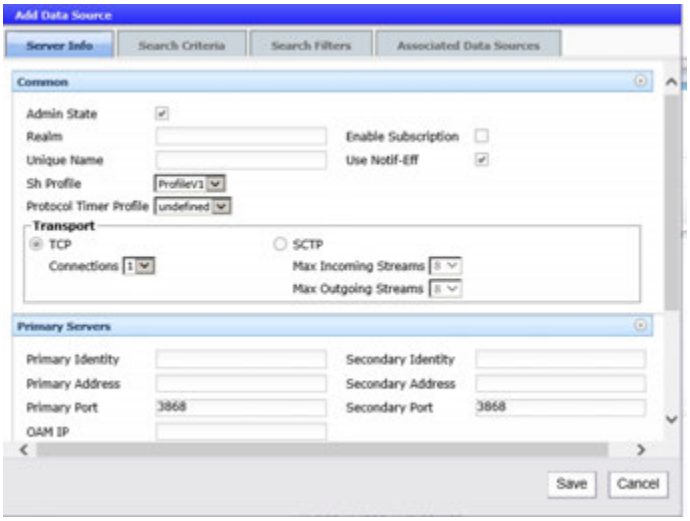


Note that this policy needs to be deployed to the relevant MPE that will process Diameter session requests. Deployed Policies can be verified from the "Policies" tab of the MPE that will process the test request:

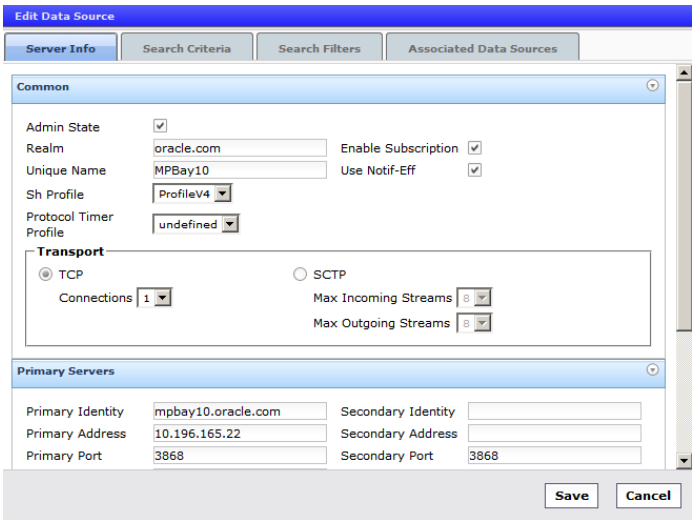


6.9 ADD A DATA SOURCE

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. Refer to [CMP Wireless User's Guide] for more information.



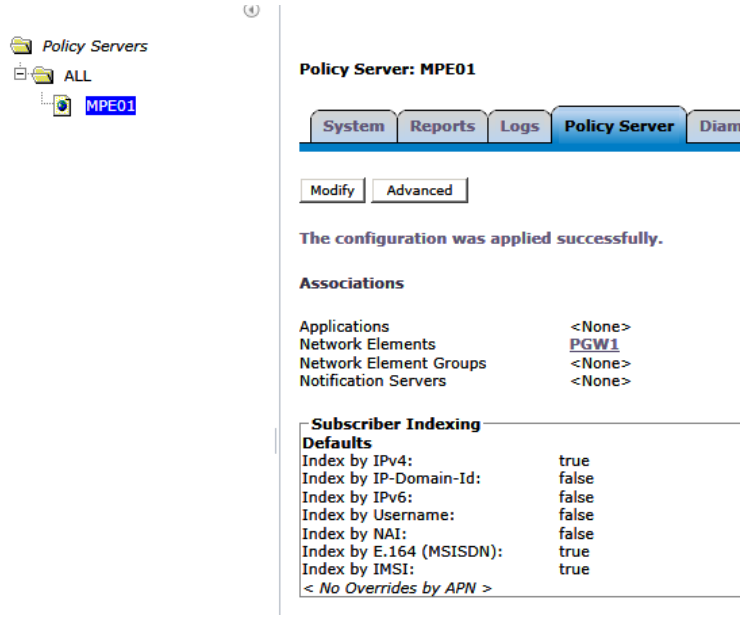
Here is a sample configuration. This form will be specific to the customer site.



6.10 PERFORM TEST CALL

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

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



6.11 PRE-PRODUCTION CONFIGURATIONS

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

Please reference the following document for information on configuring SNMP:

SNMP User's Guide 12.2

Additional Procedures can be referenced from the following documents:

Platform Configuration User's Guide Release 12.2

CMP Wireless User's Guide 12.2

Changes in the behavior of Release 12.2 are documented in the Oracle® Communications Policy Management Release Notes Release 12.2

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

7. CONFIGURE POLICY APPLICATION SERVERS IN CABLE MODE

The following procedures configure the Policy Management Application in Cable Mode and establish the network relationships, to a level that would allow a basic test call though the system.

The following procedures are common to HP and Oracle RMS environments, except for small differences noted within the procedures.

For the greater detail please refer the following documents as found in the reference section of this document.

Configuration Management Platform Cable User's Guide Release 12.2

Platform Configuration User's Guide Release 12.2

7.1 PERFORM INITIAL CONFIGURATION OF POLICY SERVERS - PLATCFG

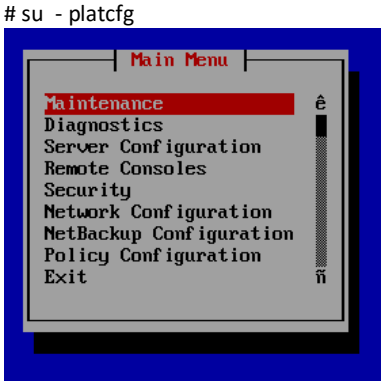
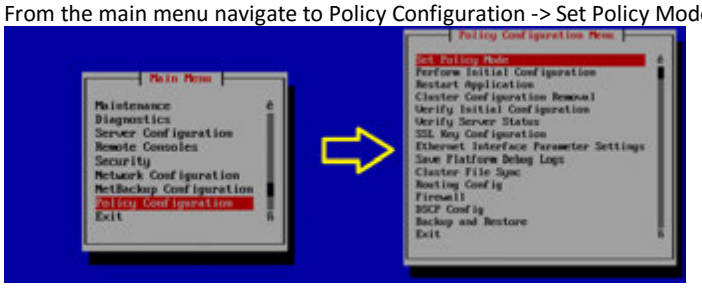
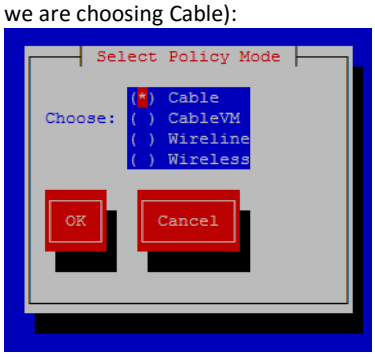
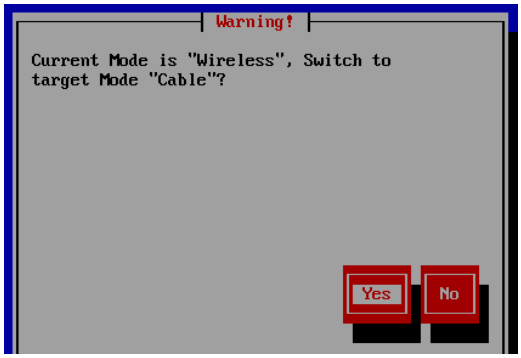
7.1: Perform Initial Configuration of the Policy Servers- Platcfg

STEP #	You must configure the operation, administration, and management (OAM) network address of the server, as well as related networking. Execute the referenced procedure on every server in the Policy Management network. **Prerequisites:** To complete this procedure, you need the following information: • This procedure assumes that you are using Policy Management in a cable network. • You need to know whether or not the server has an optional Ethernet Mezzanine card installed. • Hostname — the unique hostname for the device being configured. • OAM Real IP IPv4 Address — the IP address that is permanently assigned to this device. • OAM Default IPv4 Route — the default route of the OAM network. The MPE, BOD and MA system will move the default route to the SIG-A interface once 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,BOD and MA system will move the default route to the SIG-A interface once 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 for Oracle X5-2 RMS. • SIG A VLAN Id — the Signaling-A network VLAN ID for Oracle X5-2 RMS. • SIG B VLAN Id (optional) — the Signaling-B network VLAN ID for Oracle X5-2 RMS. • SIG C VLAN Id — **SIG-C is not supported in Cable mode** IF THIS PROCEDURE FAILS, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ASSISTANCE. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

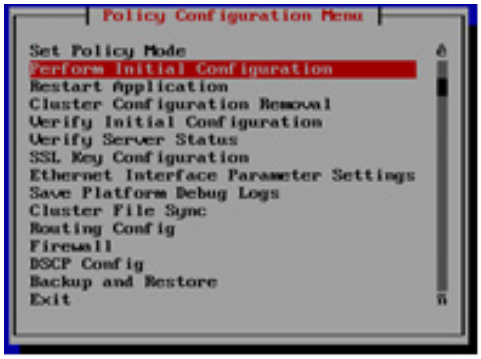
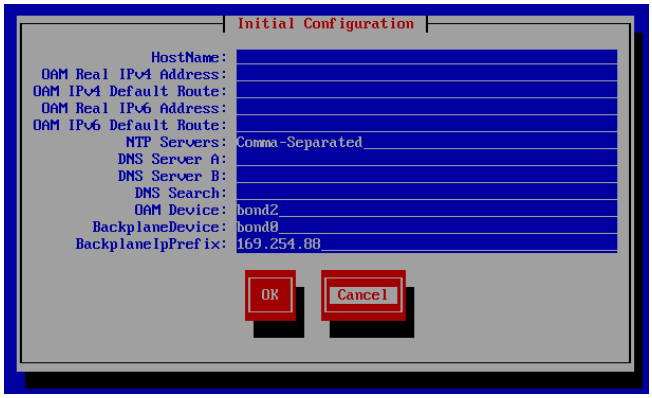
7.1: Perform Initial Configuration of the Policy Servers- Platcfg

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 8: Accessing the iLO VGA Redirection Window 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. hostnamef153e93d6590 login:
2. ☐	Verify the type of server logged in to	Login as root, via Console. # getPolicyRev –p Output will be either bod, cmp, ma, or mpe as in the following example for cmp policy server: [root@hostnamef153e93d6590 ~]# getPolicyRev -p cmp [root@hostnamef153e93d6590 ~]# _

7.1: Perform Initial Configuration of the Policy Servers- Platcfg

3. ☐	Verify Policy Mode in platcfg	Run platcfg tool: # su - platcfg  From the main menu navigate to Policy Configuration -> Set Policy Mode  Choose the relevant Policy mode from the deployment as shown below (in this procedure we are choosing Cable):  Confirm switching the policy mode from the default “Wireless” to “Cable”: 

7.1: Perform Initial Configuration of the Policy Servers- Platcfg

4. ☐	Perform Initial Configuration	After mode is set, system will return back to the Policy Configuration menu. Scroll to "Perform Initial Configuration" to start performing the initial configuration of the server:  Fill in the initial configuration values for the server: 

7.1: Perform Initial Configuration of the Policy Servers- Platcfg

5. ☐

Enter the configuration values and then select **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**--A directive to a DNS resolver (client) to append the specified domain name (suffix) before sending out 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.
- **BackPlane Device [*Only available in Cable mode*]** -- the bond interface of the backplane device Note that the default value should be used, as changing this value is not supported.
- **BackPlane IP Prefix [*Only available in Cable mode*]** -- The Ip address prefix assigned for the Backplane direct link.

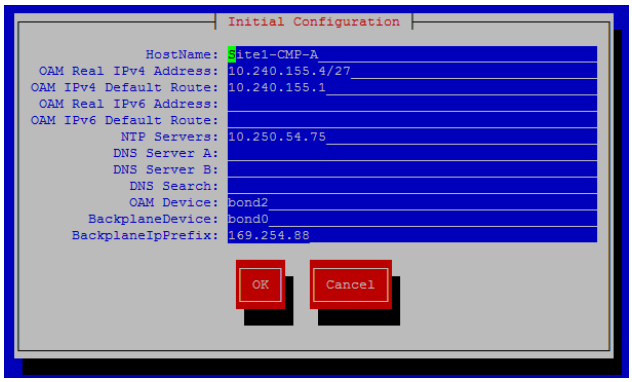
In case the H/W used is Oracle X5-2 or NETRA RMS, VLANs can be used and the following prameters will be available for configuration in this menu:

- **OAMVLAN**--The OAM network VLAN Id
- **SIG A VLAN** --The Signaling-A network VLAN Id
- **SIG B VLAN** --The Signaling-B network VLAN Id
- **SIG C VLAN** --**Not supported in Cable mode**

Note:

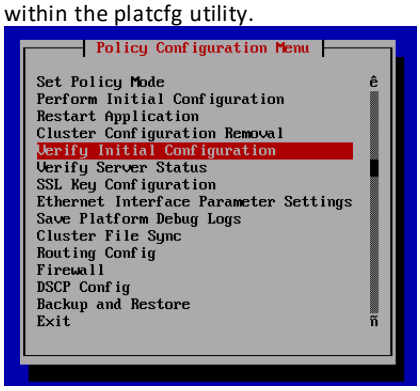
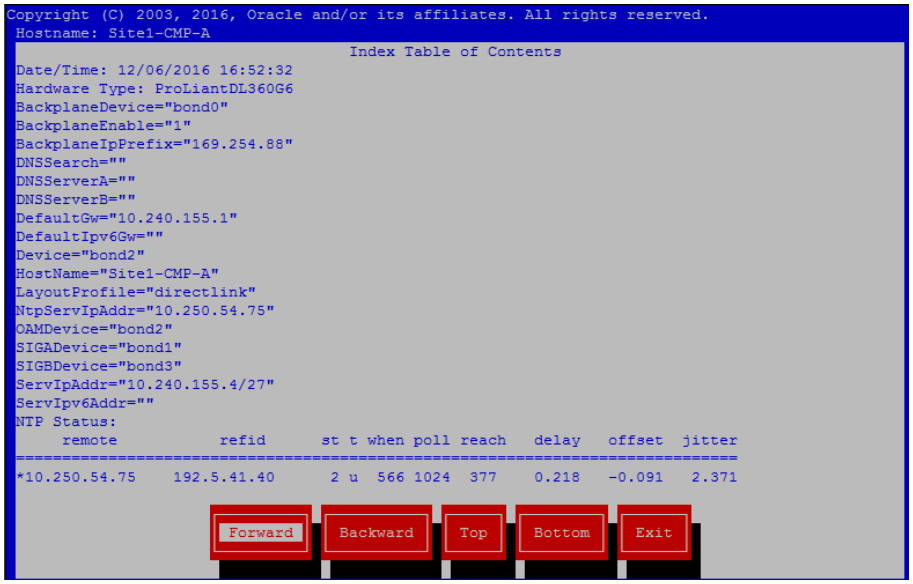
1. All of the fields listed above are required, except for fields *DNS Server* and *DNS Search*, which are optional but recommended
2. Every network service and IP flow that is supported by IPv4 is now supported by IPv6. Either interface or a combination of the two can be configured.

When finished completing the form , select **OK** to save and apply the configuration.
The configuration in the following snapshot is only an example for HP RMS H//W. Actual configuration should be in accordance with network design requirements

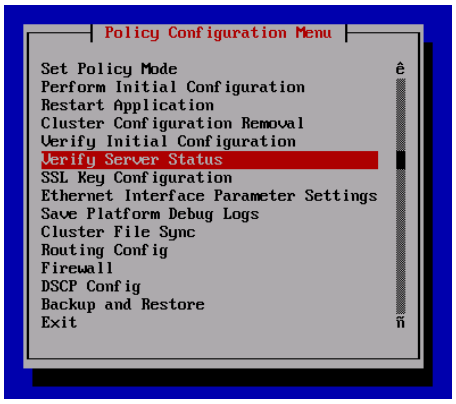
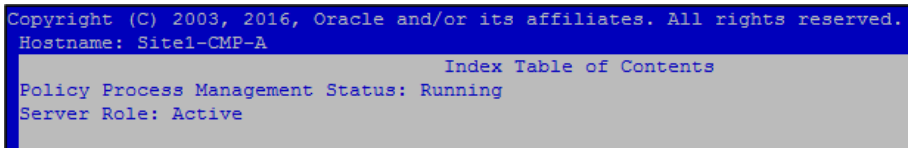
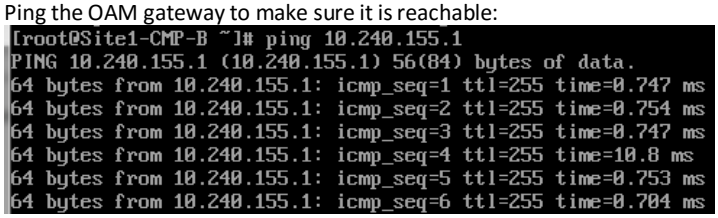


The platcfg form will process the configuration of the server, and then it will return to the platcfg menu.

7.1: Perform Initial Configuration of the Policy Servers- Platcfg

6. ☐	**Verify Config**	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 may need to press the Forward button to view the NTP status.

7.1: Perform Initial Configuration of the Policy Servers- Platcfg

7. ☐	**Verify Server Status**	Exit from this screen and select Verify Server Status:  The server should be in a running state. For example:  Press "Exit" repeatedly until completely exiting the platcfg utility. You will be returned back to Linux prompt screen.
8. ☐	**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:  **If the gateway is reachable it should be possible to SSH to the server IP and login as admusr** In case 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. Execute ip -4 addr (IPv4) or ip -6 addr (IPv6) to confirm the IP addresses configured during the intialization are present.

7.1: Perform Initial Configuration of the Policy Servers- Platcfg

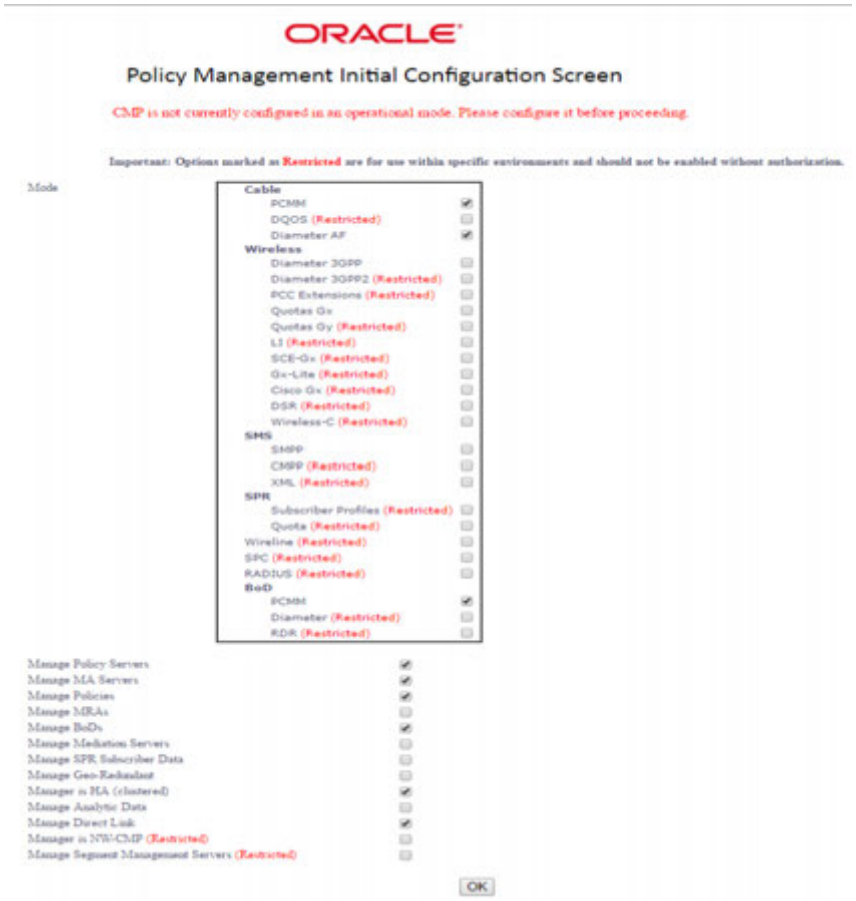
9. ☐	**Verify NTP connectivity**	**NOTE**: Server sync to Network Time Protocol (NTP) is very important to the later steps in this install. To sync and verify NTP server connectivity, perform these steps: # **ntpq -pn** [root@Site1-CMP-A ~]# ntpq -pn remote refid st t when poll reach delay offset jitter ========== *10.250.54.75 192.5.41.40 2 u 766 1024 377 0.218 -0.091 2.371 [root@Site1-CMP-A ~]# The "*" sign besides the NTP server Ip indicates the NTP server is in sync. In case the sign is not there, you may try manually to sync with NTP server through the following steps: # **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 ntpdate has a bad response, follow up to get the needed networking, firewalls and permissions to solve this connectivity issue with the NTP server. **NOTE**: '*ntpdate*' is an emergency utility; use only when you see significant time difference between system and the actual time.
10. ☐	**Repeat on remaining servers**	Repeat this procedure on all Policy components' servers that are planned for service. If solution is geo-redundant, this procedure need to be performed on site1 and site2 Policy servers
THIS PROCEDURE HAS BEEN COMPLETED		

7.2 PERFORM INITIAL CONFIGURATION OF THE POLICY SERVERS - CMP GUI

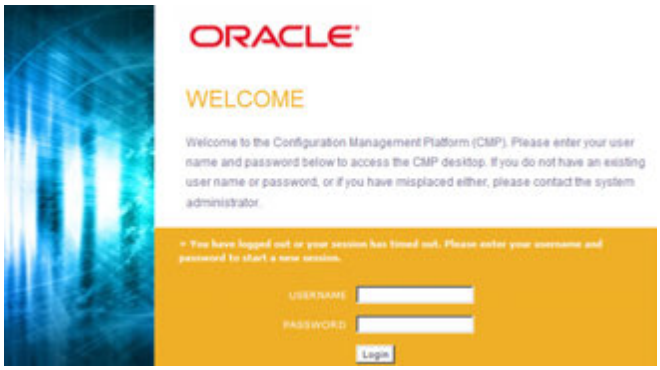
This procedure will perform initial configuration of the CMP GUI on a newly installed environment.

IMPORTANT:
In a deployment that will have Geo-Site CMP servers (requires a secondary Site2-CMP cluster) , the Geo-site CMP servers do not get configured with this procedure. Instead, the Active (Site1) CMPs are configured with this procedure, and are designated as "CMP Site 1". The other pair of CMPs will be added to the network Topology from the CMP Site 1 GUI . The CMP Site 1 cluster will push the configuration to the Geo-Site (site2 cluster) CMPs at a later step in these procedures.

7.2: Perform Initial Configuration of the Policy Servers - CMP GUI

STEP #	This procedure will configure the CMP at the Active site (CMP Site 1). **Prerequisite:** - Network access to the CMP OAM REAL 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.	
1. ☐	Open CMP GUI	Open CMP GUI for the first time by navigating 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 will be located at Site1. If this is not geo-redundant solution there will be no Site 2 location.
2. ☐	Set CMP Mode in 1st selected CMP	Once connected to the CMP GUI for the 1st time, user will be prompted to select the "modes" for the system, which define what functionality will be configurable from the CMP GUI. The mode selection depends on the customer deployment. Select the check boxes as needed, and click OK. The following page provides a sample selection for Cable common related options.  [Note: modes can be changed at a later time if needed, but the method to access to this

7.2: Perform Initial Configuration of the Policy Servers - CMP GUI

		mode selection is not documented.] Contact Oracle Support if Mode selection is required to be changed after the initial configuration. **For the greater detail please refer to "The Mode Settings Page" in the following document (as found in the reference section of this document).** Configuration Management Platform Cable User's Guide Release 12.2
3. ☐	Login to CMP GUI	After finishing the policy mode selection and pressing "OK", login screen below will be displayed: 
4. ☐	Set admin password	Initial, default login is admin/policies After login, the system will prompt the user to change the admin password.  Enter the default old password then the new password twice and press "Change Password" button.
5. ☐	Verify that the CMP GUI is displayed, with expected menus.	

THIS PROCEDURE HAS BEEN COMPLETED

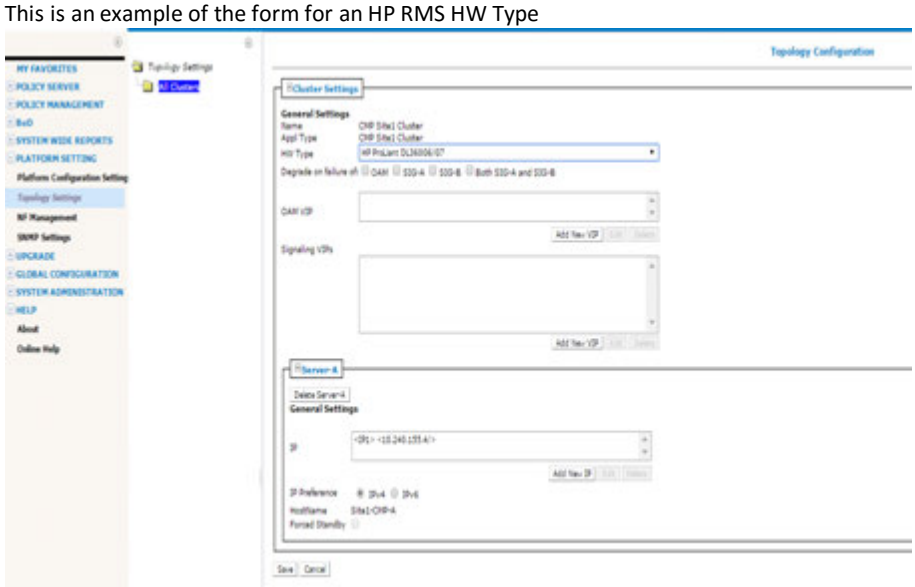
7.3 CMP SITE1 CLUSTER CONFIGURATION

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

7.3: CMP Site1 Cluster Configuration

STEP #	
	This procedure will perform configure the CMP at the Active site (CMP Site 1) For additional detail please refer to the following (as per the reference section in this document). Configuration Management Platform Cable User's Guide Release 12.2 Note: The recommended sequence of creating the Policy Management topology is as follows: **1.** Configure the primary CMP cluster — You start to build a topology by logging in to the active CMP server at the primary site. Configure the CMP cluster settings. The settings are replicated (pushed) to the standby CMP server. Together, the two servers form a primary, or Site 1, CMP cluster. This will be the primary CMP site for the whole topology network. The primary site cannot be deleted from the topology. **2.** Configure the secondary CMP cluster (optional) — Use the primary CMP cluster to configure a secondary, or Site 2, CMP cluster. A secondary CMP cluster can provide geo-redundancy. **3.** Configure MPE, MA and BOD clusters — Enter MPE, MA and BOD clusters settings on the active CMP server on the primary site. **4.** For geo-redundancy (optional), configure additional sites for MPE-S and BOD clusters. **IMPORTANT:** In a deployment that has Geo-Site CMP servers, these Geo-site CMP servers DO NOT get configured with this procedure. Instead, the Active site CMPs are configured with this procedure, and are designated as "CMP Site 1". The other pair of CMPs will be added to the network Topology from the CMP Site 1 GUI. The CMP Site 1 cluster will push the configuration to the Geo-Site CMPs at a later step in these procedures. **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 to indicate whether the cluster will use an external signaling network. If you specify either SIG-A, SIG-B, 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 Oracle X5-2, or Netra hardware, VLANs are required. For HP 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.

7.3: CMP Site1 Cluster Configuration

1. ☐	**View Topology Settings**	**Select: Menu -> Platform Settings -> Topology Settings ->all clusters** The initial form will open, and display a message that initial configuration detected and CMP Site 1 Cluster should be added. 
2. ☐	**Add CMP Site 1 Cluster – Server A**	Select the button to **Add CMP Site 1 Cluster**. The Topology Configuration form is displayed. In this form, the CMP cluster can be given a name, and certain characteristics of the cluster are defined. This form will define a VIP address to be assigned to the active server in the cluster. Note: The HW-Type will determine whether VLANs are required. For Oracle X5-2 and Netra options VLANs are used. The VLANs will have been designated during the Initial Configuration done with placfg. They should be used here as well. • HP RMS Hardware (HP DL360 G6/G7 and HP G8/G9 RMS)-Types do not require VLANs. • Oracle RMS-Type do require VLANs. This is an example of the form for an HP RMS HW Type 

7.3: CMP Site1 Cluster Configuration

Complete the form for Cluster Settings and Server-A. The information below should be reviewed to determine the appropriate selections

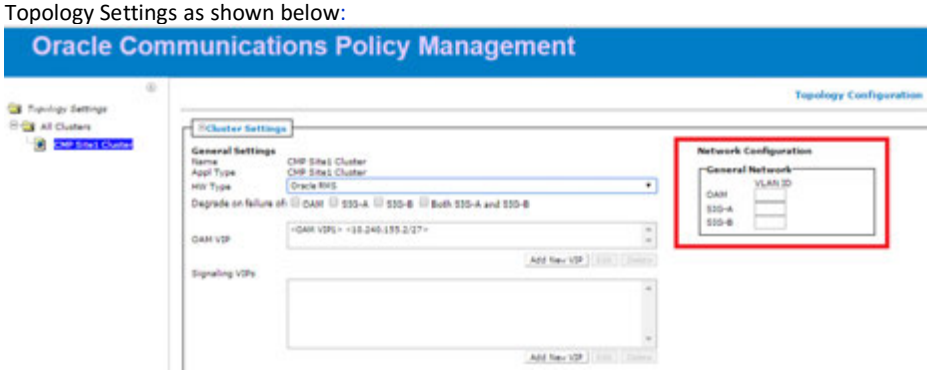
— Select the right type hardware

HW Type — Select the type of hardware:

- **HP ProLiant DL360G6/G7** (for a HP DL360 Gen 6 and Gen7 servers)
- **HP ProLiant G8/G9 RMS** (for HP Gen 8 and Gen 8 servers)
- **Oracle RMS** (for a Oracle X5-2 and NETRA servers)
- **VM** (for a virtual machine) Not covered in this guide – refer to Install guide for virtual environment

— Complete Network Configuration VLAN IDs per network design if applicable.

In case hardware used is Oracle RMS you will have the option to configure VLAN IDs in Topology Settings as shown below:



— Complete the OAM VIP

OAM VIP (required) — The OAM VIP is the IP address the CMP uses to communicate with a Policy Management cluster. Enter up to two OAM VIP addresses (one IPv4 and one IPv6) and their masks. Enter the address in the standard dot format and the subnet mask in CIDR notation from 0–32 (IPv4), or standard 8-part colon-separated hexadecimal string format and the subnet mask in CIDR notation from 0–128 (IPv6).

— Complete Signaling VIP if applicable

Signaling VIP 1 through **Signaling VIP 4** (optional) — Enter up to four IPv4 or IPv6 addresses and masks of the signaling virtual IP (VIP) addresses; for each, select **None**, **SIG-A**, or **SIG-B** to indicate whether the cluster will use an external signaling network. You must enter a Signaling VIP value if you specify either SIG-A or SIG-B. If you enter an IPv4 address, use the standard dot format, and enter the subnet mask in CIDR notation from 0–32. If you enter an IPv6 address, use the standard 8-part colon-separated hexadecimal string format, and enter the subnet mask in CIDR notation from 0–128.

Note: predefined for the first Site 1 CMP Cluster configuration, no input necessary.

—Complete Server-A IP

The IP address of the server. Up to two IP addresses can be entered (one IPv4 and one IPv6). Use the standard dot-formatted IP address string for an IPv4 address, and the standard 8-part colon-separated hexadecimal string format for an IPv6 address.
Server-A Hostname — hostname for the first server (predefined, no input).

—Checkbox for IP Preference

Specify the preferred IP version, either **IPv4** or **IPV6**. If IPv6 is selected, the server will prefer to use the IPv6 address for communication. If neither an IPv6 OAM IP nor a static IP address is defined, the IPv6 radio button cannot be selected here. Similarly, If neither an IPv4 OAM IP nor a static IP address is defined, the IPv4 radio button isn't accessible.

—Complete HostName

The name of the server. This must exactly match the host name provisioned for this server (that is, the output of the Linux command **uname –n**)

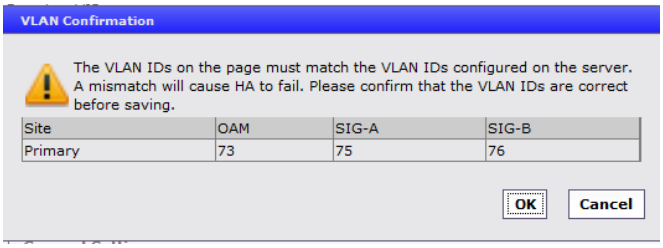
Note: If the server has a configured server IP address, highlight or select the ip address and

7.3: CMP Site1 Cluster Configuration

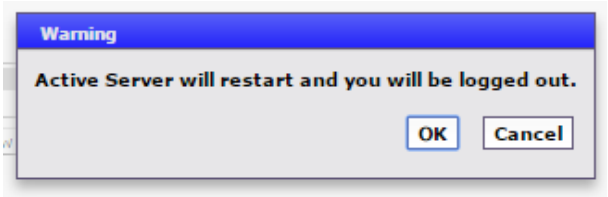
then you can click **Load** to retrieve the remote server host name. If retrieval fails, you must enter the host name. This is the preferred method of datafilling the hostname to avoid errors. If the target server IP address is unreachable the host name will not be fetched and network connectivity should be checked.

When done, save the form and select **OK.**

If the configuration is for Oracle RMS and contains VLAN IDs you will be prompted to confirm the VLAN IDs.



Then the following confirmation prompt appears. Click <OK>



At this point, you will be logged out of CMP GUI as OAM VIP should be used from this step and on.

3. ☐ **Login using the CMP cluster VIP.**

After the Topology Configuration is saved, the CMP VIP address will be taken by the Active CMP server of the cluster. This may take a minute.

Login to the CMP GUI using the VIP address, then navigate to **Platform Settings -> Topology Settings -> all clusters -> CMP Site1 Cluster**

Verify the configured CMP server is now in "Active" state

4. ☐ **IF the CMP VIP is not available…**

SSH to the CMP Real IP address of the CMP server as admusr then switch to root user to confirm the server role is "active" as shown below

ha.mystate

7.3: CMP Site1 Cluster Configuration

```
login as: admusr
Using keyboard-interactive authentication.
Password:
Last login: Fri Dec  9 11:51:22 2016 from 10.154.153.169
[admusr@Site1-CMP-A ~]$ sudo su - root
[root@Site1-CMP-A ~]# ha.mystate
          resourceId   role         node       subResources      lastUpdate
       DbReplication Active    A2020.228                  0 1209:111746.422
                 VIP Active    A2020.228                  0 1209:111746.423
                  QP Active    A2020.228                  0 1209:111749.532
   DbReplication_old    OOS    A2020.228                  0 1209:111733.886
[root@Site1-CMP-A ~]#
```

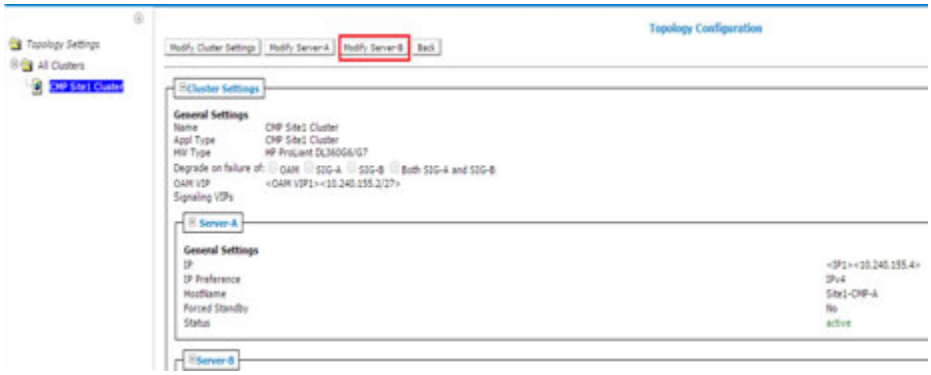
NOTE: “DbReplication_old” with role “OOS” is not an indication of a problem and can be ignored.

It is still possible to login to the CMP server with its Real IP address, if needed, to verify that the Topology Configuration was done correctly.

5. ☐ **Modify CMP Site 1 Cluster – add Server B**

If second CMP server (for redundancy in an HA cluster) will be used, then Server-B needs to be added to the CMP Site 1 Cluster. The next three steps do this.

Select: **Menu -> Platform Settings -> Topology Settings**
Select View for **CMP Site 1 Cluster**
Select **Modify Server B**



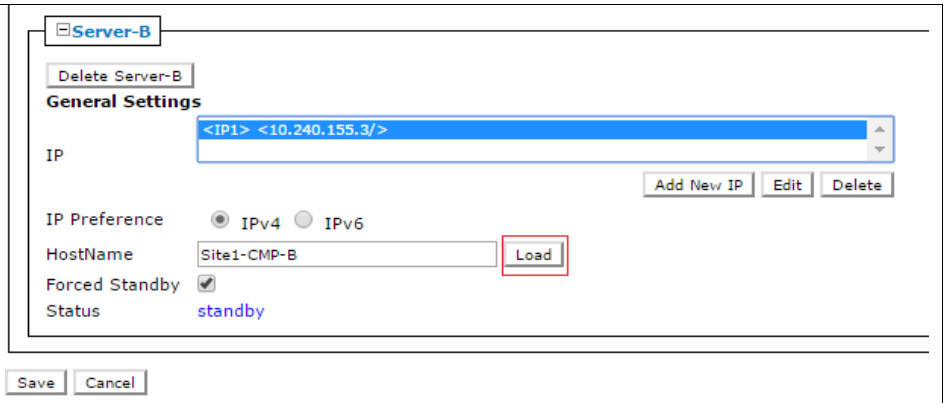
Enter:

- Server-B IP — OAM Real IP address for the second server.
- Server-B Hostname — hostname for the second server. This hostname must exactly match the hostname configured in platcfg (same as uname -n). Alternatively, you may highlight the server IP then press the “Load” button for the system to automatically look up the server name from initial configuration

Note: The “load” option should be used to correctly populate the Hostname. If the server B IP address is reachable “load” will automatically pick up the correct hostname from the target server.

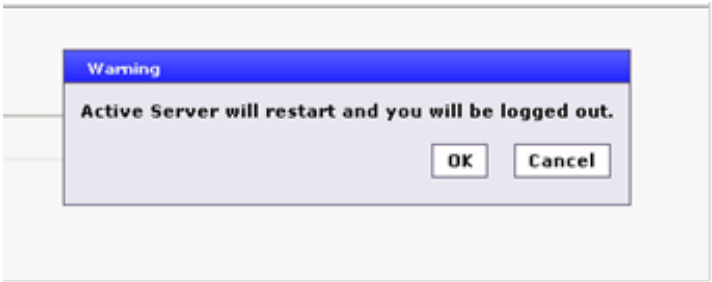
Example of Site1 CMP Cluster Server B Topology Configuration

7.3: CMP Site1 Cluster Configuration

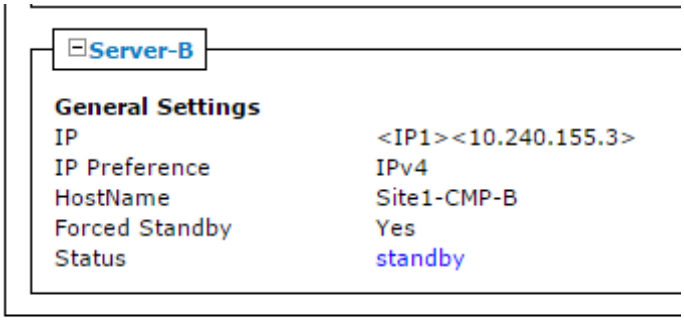


Note: the Forced Standby checkbox is checked by default

Select "save" then "OK" on the following confirmation message.



The server status will be "out-of-service" for few minutes and that is expected until the cluster forms then it will get to "**standby**" state:



Note: Wait for any Alarms, such as the following, to clear.

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

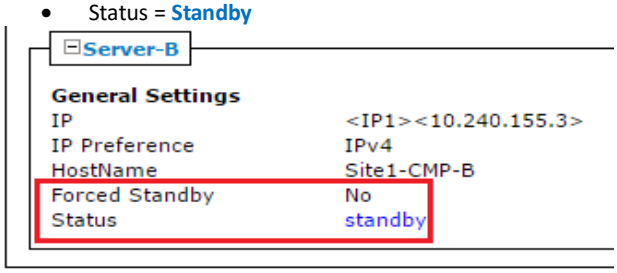
6. ☐	**CMP GUI: Remove Force Standby on Server B**	Click **Modify Server-B** button and uncheck **Force Standby**, then click **Save** when finished and "OK" to the following confirmation message:

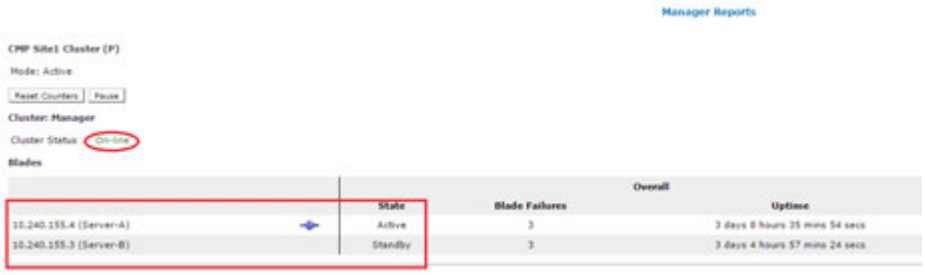
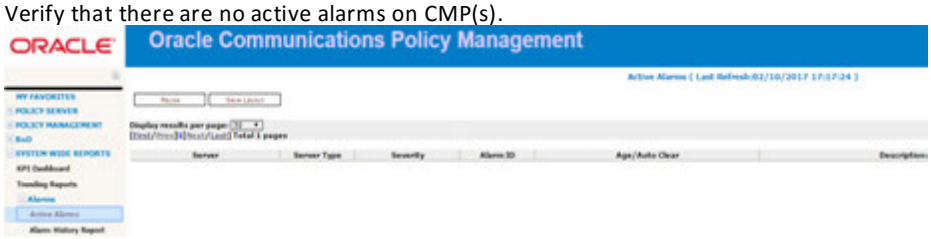
7.3: CMP Site1 Cluster Configuration

Save Cancel

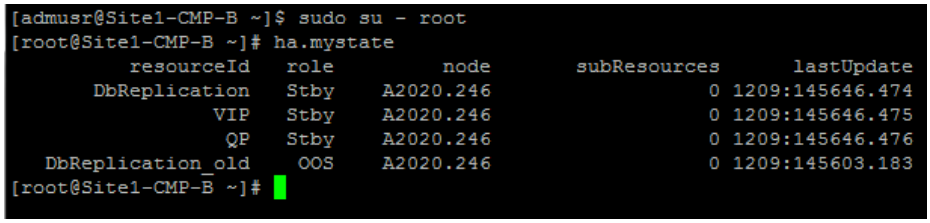
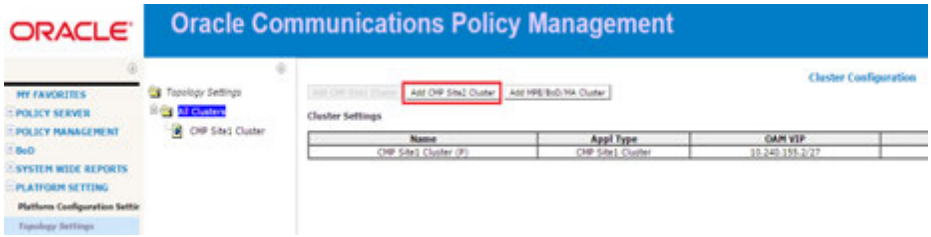
Verify status becomes:

- Forced Standby = no
- Status = **Standby**



7. ☐	**CMP GUI: Verify CMP cluster**	SYSTEM ADMINISTRATION → Reports Verify both CMP servers are present , with one "Active" and the other in "standby" status and also the status of the cluster is "On-line": 
8. ☐	**GUI: Verify CMP cluster**	SYSTEM WIDE REPORTS → Active Alarms Verify that there are no active alarms on CMP(s). 

7.3: CMP Site1 Cluster Configuration

9. ☐	**Server: Verify the server role**	Use the following Server-B real IP address and SSH to the just configured Server-B. Use the ha.mystate command to verify that the server role is **Stby** as shown below: # ha.mystate  NOTE: "DbReplication_old" with role "OOS" is not an indication of a problem and can be ignored.
10.	**CMP GUI: Configure a secondary site CMP cluster**	Follow the same steps in this procedure to add secondary site CMP cluster if it is part of the Cable Policy deployment: 

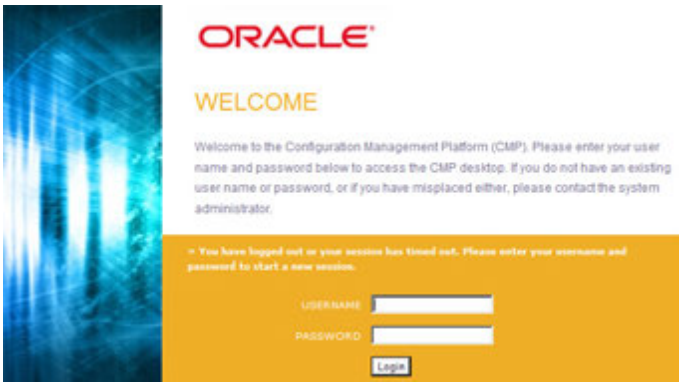
THIS PROCEDURE HAS BEEN COMPLETED

7.4 CONFIGURING ADDITIONAL CLUSTERS

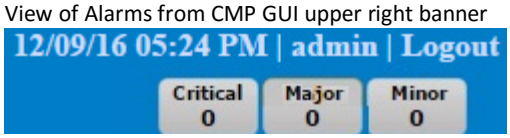
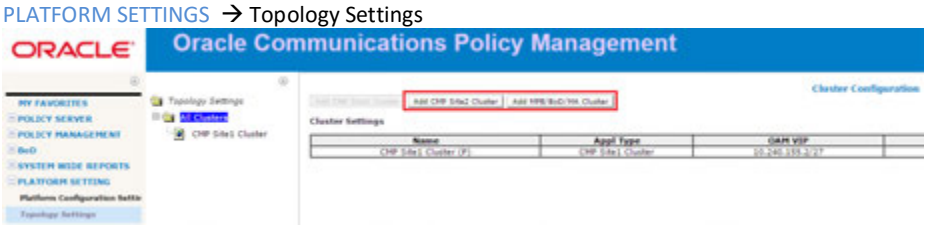
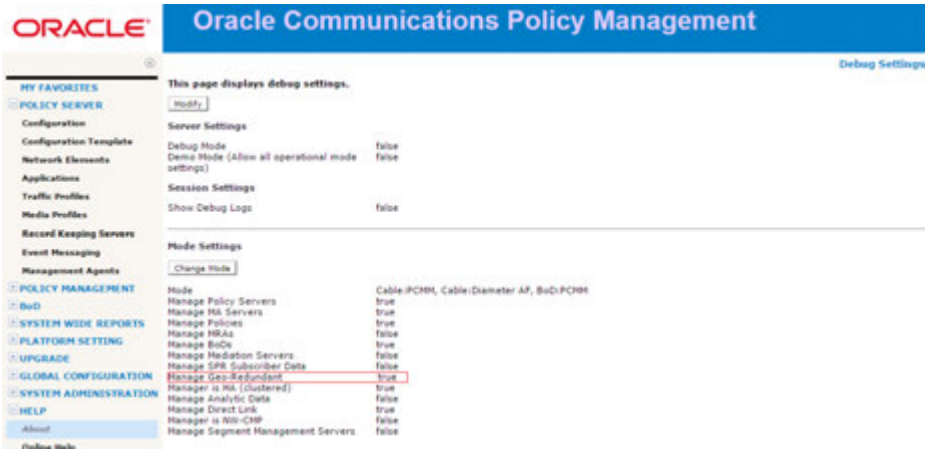
This procedure will configure the management relationships between the Active site CMP cluster and the remaining policy components of the Cable Policy deployment like MPE-Rs, MPE-Ses, MAs and BODs. After this, the status of the servers will be available from the CMP GUI.

It is allowed to perform a Topology Configuration for clusters at remote sites, even if those sites are not fully networked or configured. The CMP will report Alarms in this case, and will continue to try to establish the management services to the clusters until it is able to reach them. When the clusters become available, the CMP will update status and the Alarms will clear.

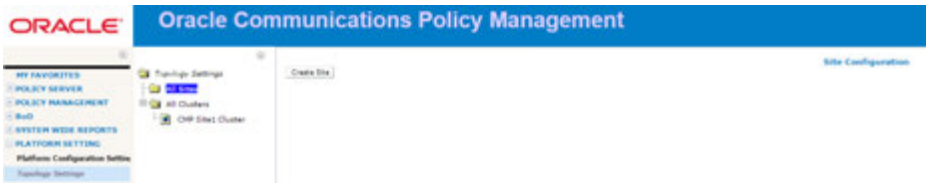
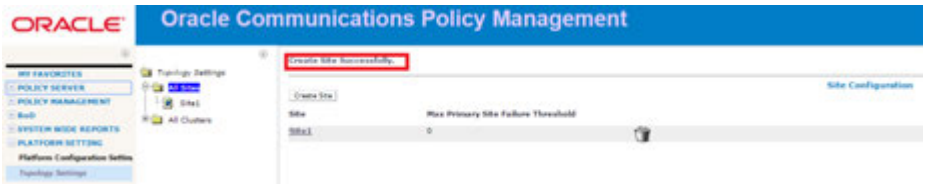
7.4: Configuring Additional Clusters

STEP #	This procedure will configure the management relationships between the CMPs and the other servers (MPEs/MAs/BODs), and the cluster assignments. After this, the status of the servers will be available from the CMP GUI. **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. **Prerequisite:** - Network access to the CMP OAM IP address, to bring up a web Browser GUI (http) - The server software is installed on all servers in the target cluster - The servers have been configured with network time protocol (NTP), domain name server (DNS), IP Routing, and OAM IP addresses To complete this procedure, you need the following primary site settings: • Site Name • HW Type — Determines whether VLANs are required. If you select Oracle X5-2 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 MA or BOD 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. • Network VLAN IDs — The values designated during the Initial Configuration done with placfg. • If you are configuring a Geo-Redundant (Site 2) CMP cluster, the information that you previously configured for the CMP Site 1 cluster (the default cluster name is CMP Site 2 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	
1. ☐	**Login to CMP Server GUIs (using VIP)**	From Browser, enter CMP Server VIP in Navigation string.  Login as admin (or a user with admin privileges)
2. ☐	**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.

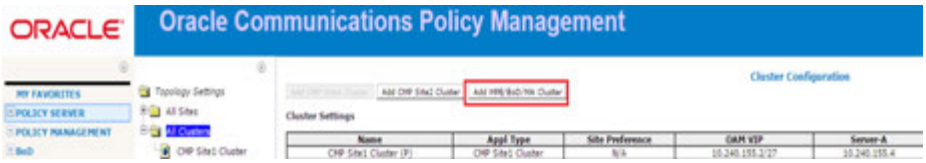
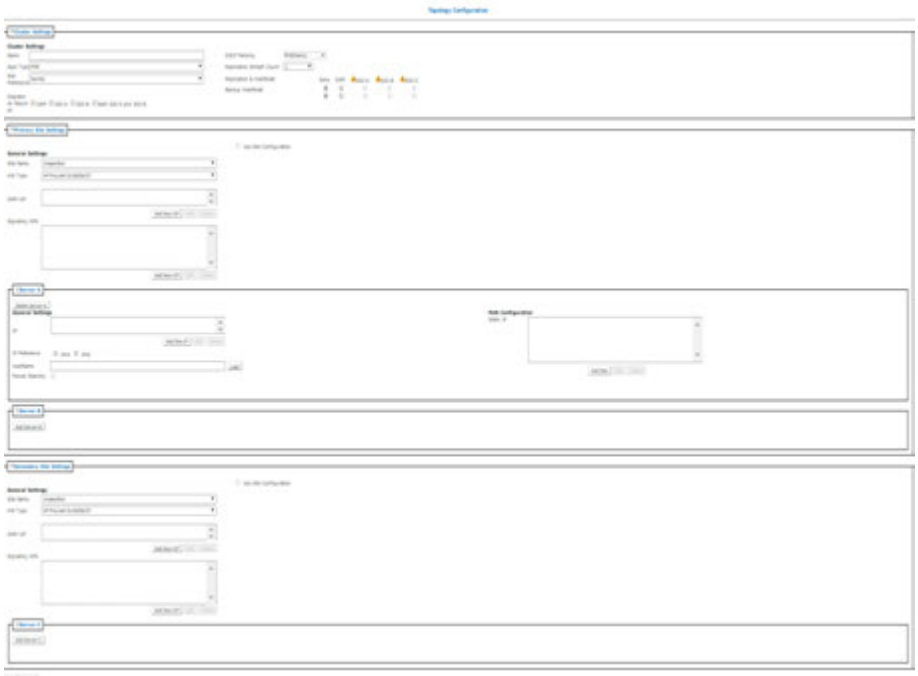
7.4: Configuring Additional Clusters

		View of Alarms from CMP GUI upper right banner  View of Alarms from System Wide Reports -> Active Alarms  IMPORTANT: In Policy 12.2, there is Online help provided for Alarm descriptions. In the Alarm views, click on the alarm Id to open the Alarm description help page. Alternatively, from the Menu select On-Line Help, and select Troubleshooting Guide. Search this for the Alarm Id.
3. ☐	**View Topology Settings**	PLATFORM SETTINGS → Topology Settings  The Topology Settings screen allows for the selection of adding a CMP Site2 or adding an MPE/BoD/MA Cluster. For a Secondary site CMP Cluster select : • Add CMP Site 2 Cluster For a MPE or BoD or MA cluster select: • Add MPE/BoD/MA Cluster **Note:** For a Geo-Redundant BoD/MPE cluster the option "**Manage Geo-Redundant**" will need to have been selected in the Initial CMP mode Configuration. 
4. ☐	**Add SITE 2 CMP Cluster-Server-A**	**Adding a CMP Site2 CMP cluster is optional.** If the Policy Management Solution design calls for "Geo-Redundant" CMP clusters, the "Site 2 CMP Cluster" must be configured from CMP Site1 Cluster GUI.

7.4: Configuring Additional Clusters

		Select "Add CMP site2 cluster" and datafill the CMP Site2 Cluster form. **Note:** The fields that need to be datafilled in this form are the same as the CMP Site1 Cluster.
5. ☐	**Create and name Site-1 and Site-2** **NOTE:** This step is to be done once only.	**MPE-S and BOD clusters** can be dispersed between a primary site and a secondary site. This provides Geo-Redundancy for the MPE-S/BOD clusters where Server-A and Server-B form an HA Cluster at the Primary Site and Server-C provides a backup server at a secondary site. **Note:** For a Geo-Redundant MPE/BOD cluster the option "**Manage Geo-Redundant**" will need to have been selected in the Initial Mode Configuration of CMP GUI as shown in step 2 of Procedure 26 above This step will create two separate sites into which MPE and MRA clusters can be added. PLATFORM SETTINGS → Topology Settings • Ensure that "All Sites" configuration option is available **Note:** "**Manage Geo-Redundant**" should be selected in the CMP GUI Initial Configuration form. If Sites is not visible go back and make this change now.  • Click on 'Create Site' to create a new site name i.e. < Site-1> • Click on 'Create Site' to create a new second site i.e.< Site2> • Name each additional site accordingly and save the configuration. **Note:** If the hardware being used required VLANs you will need to configure VLANs in the Add SITE form as well  CMP will display message that site is successfully created and you can now see the newly created site displayed under site configurations:  After configuring all sites in CMP , they would now be viewed in the Topology. MPE-S and BoD clusters will be added to these sites at the time the topology for these servers are created.

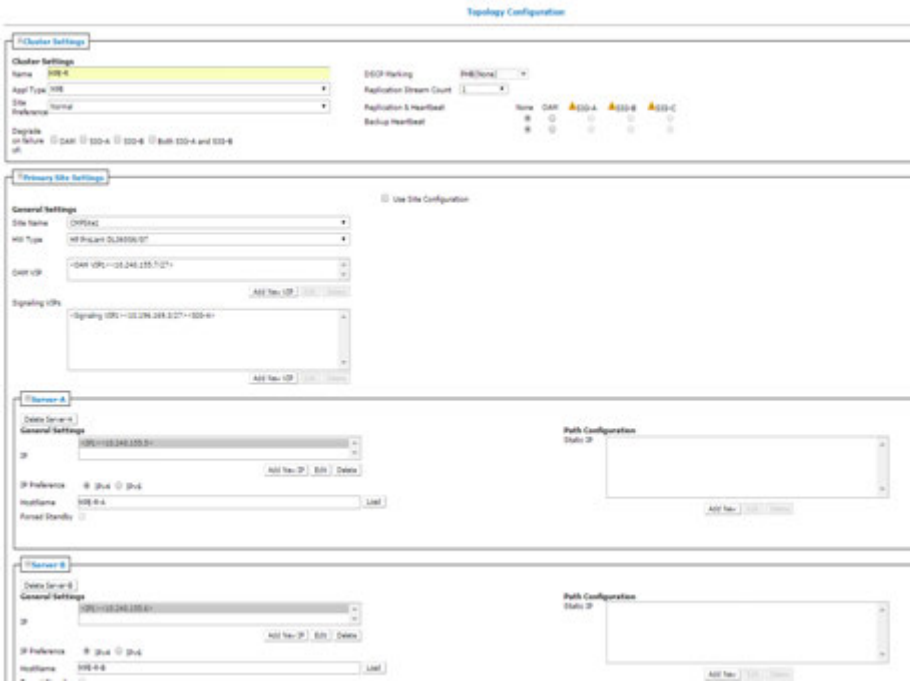
7.4: Configuring Additional Clusters

		 **Note:** "CMPSite1" and "CMPSite2" are reserved site names for CMP Clusters so they can not be used as valid names when configuring sites in the topology. CMP GUI also prohibit users of using these names in configuring new sites.
6. ☐	**Add MPE/BoD/MA Cluster**	PLATFORM SETTINGS → Topology Settings  Click on <Add MPE/BoD/MA Cluster>. In the Topology Configuration form, enter the information for this cluster.  It is allowed to add both Server-A, Server-B and Server-C in this form at the same time **Note:** These settings are only an example of a likely configuration. An actual deployment will be specific to customer requirements. <u>Define the Cluster Settings</u>

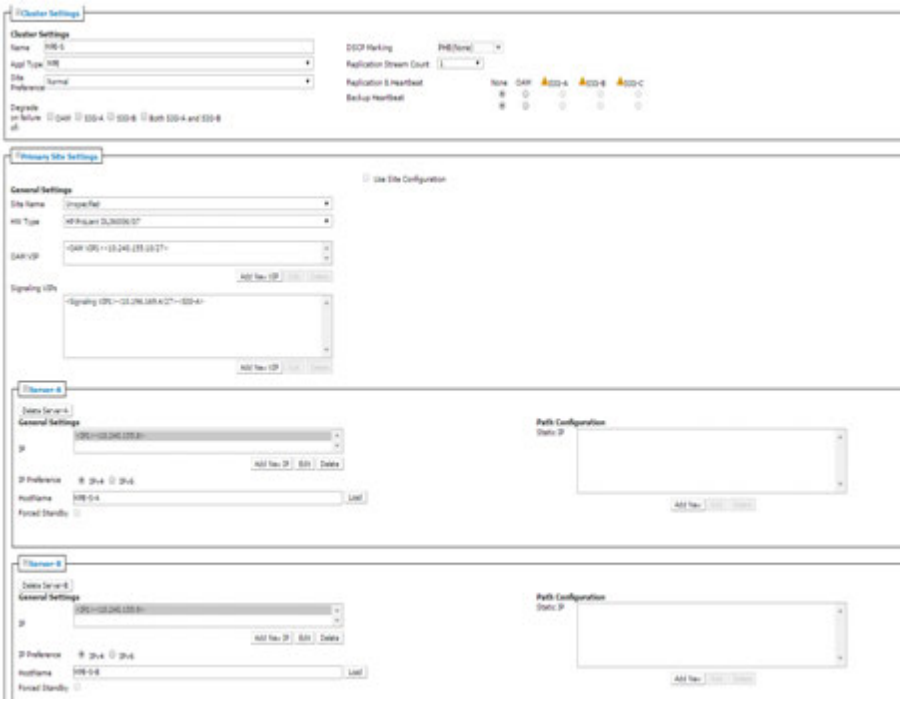
7.4: Configuring Additional Clusters

		a) **Name** (required) — Name of the cluster. Enter up to 250 characters, excluding quotation marks(") and commas (,). b) **Appl Type** — Select the type of server: **MPE** (default) or **BOD** or **MA** c) **Site Preference** – NORMAL DSCP Marking = NONE Replication Stream Count = 1 through 8 Replication and Heartbeat = REP Backup Heartbeat = OAM <u>Define the Primary Site Settings</u> **Site Name –**Here the added server can be associated with a previously configured site in the drop down tab if this will be Geo-Redundant topology **HW Type** — Select the type of hardware: • **HP ProLiant DL360G6/G7** (default) • **Oracle RMS** (for a Oracle X5-2 and Netra server) • **HP ProLiant G8/G9 RMS** • **VM** (for a virtual machine) Not covered in this guide • **VM Automated** Not covered in this guide **OAM VIP** — The OAM VIP is not typically used for the MRAs or the MPEs. The Real IP address is used by the CMP to communicate with the MPE or MRA cluster. **Signaling VIPs** (required) — The signaling VIP is the IP address a PCEF 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 – NOT supported in Cable mode At least one signaling VIP is required. Define the general network configuration for Netra servers in the Network Configuration section of the page. This section is not available for RMS. a) Enter the VLAN IDs, in the range 1–4095 for the following: 1. Define the settings for **Server-A** in the Server-A section of the page. 2. Define the settings for **Server-B** in the Server-B section of the page. 3. Define the settings for **Server-C** in the Server-C section of the page. **Note:** If the cluster is not a Geo-Redundant topology Server-C is not required Example of an MPE-R Cluster configuration on HP RMS HW

7.4: Configuring Additional Clusters

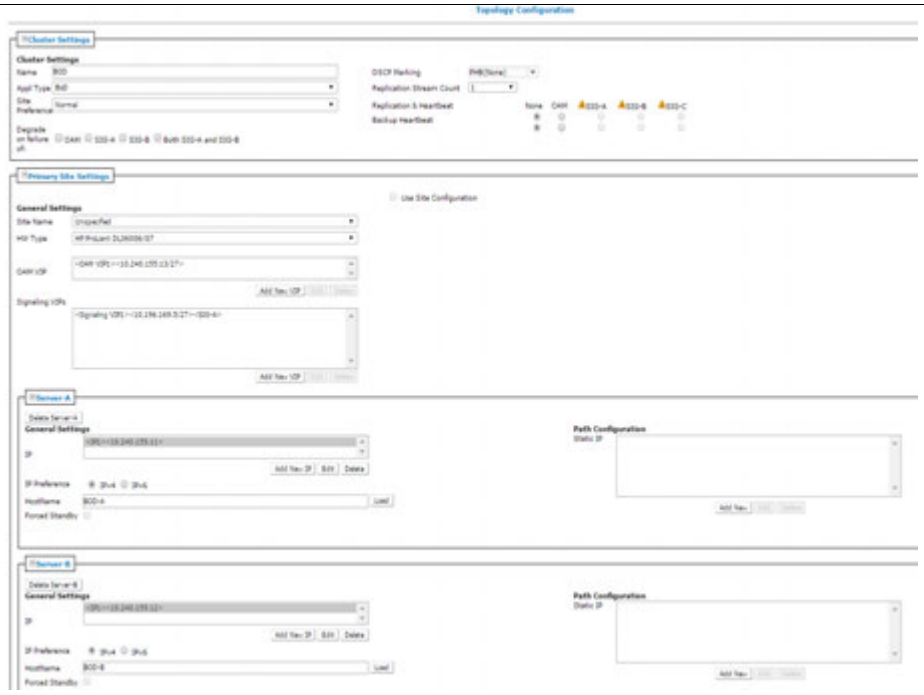


Example of an MPE-S cluster configuration on HP RMS H/W

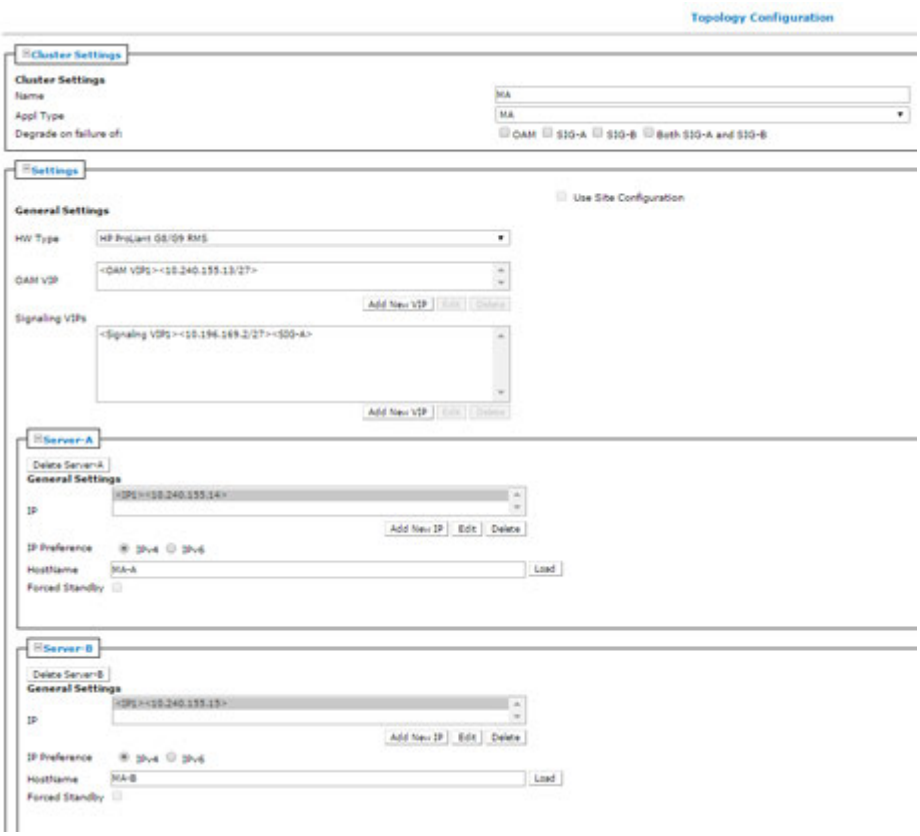


Example of an BOD cluster configuration on HP RMS H/W

7.4: Configuring Additional Clusters



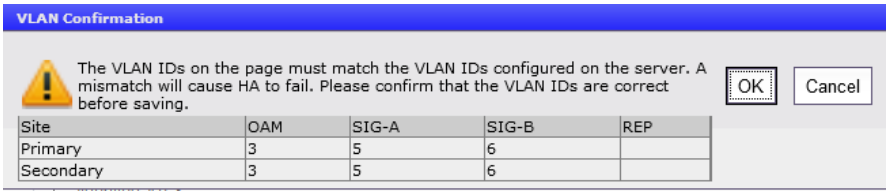
Example of an MA cluster configuration on HP RMS H/W



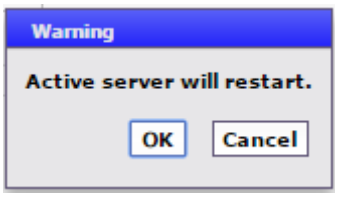
<**Save**> the topology configuration

7.4: Configuring Additional Clusters

Confirm the VLAN configuration if the hardware type and network architecture uses VLANs:



Click <**OK**> to confirm



If clusters has been added succesfully it will now be visible on the Cluster Configuration page.

Note: Initally several alarms will be generated. Wait for all the alarms to clear - then refresh the view of the topology screen to confirm that the newly added BOD/MA/MPE-R/MPE-S now shows an "active" and a "standby" status for Server-A and Server-B. If there was a Server-C added to the MPE-S and/or BOD clusters topology check that server-C status shows "spare".

Note: CMP clusters are associated with <CMP Site 1 cluster > and <CMP Site 2 Cluster> upon creation. Only the MPE-S and BOD are associated directly to the configured sites populated under "All Sites".

Note: If the topology configuration is performed at a time when there is no network connectivity between the CMP and the other policy components servers (MPE/BOD/MA) being added to the topology, the status of these newly added servers will show as "offline" and alarms will be generated due the offline state. These alarms will persist until such time as the servers become reachable from the CMP. The CMP will continually retry connecting to the servers that have been newly added in the topology. When the new servers are reachable, the topology configuration will complete and any alarms present due to the topology configuration will resolve/clear. In this scenario, return to the CMP topology settings when connectivity is established between the CMP and the newly added servers and confirm there are no alarms and the status of the added servers are correct.

7.4: Configuring Additional Clusters

7. ☐	**Repeat the previous step for additional clusters**	**A list of Clusters to be configured can be added to this step as a reminder.**
8. ☐	**Verify Topology**	**Select: Menu -> Topology Settings → View Cluster** The status of each cluster can be viewed from this form. Normal condition will be Active/Standby (and not Forced Standby) and Spare.
9. ☐	**Verify Alarms**	If there are problems with the Management relationships between the CMP and the servers, there will be alarms reported. Verify that Alarms do not indicate problems.
10. ☐	**If the CMP will manage Remote sites, and these are not yet available.**	***If the CMP will Manage Remote sites, and these are not yet available.*** ***a) Configure these clusters, but Return to the Verify Steps above after the connectivity has been established.*** ***-- OR –-*** ***b) Configure these clusters at a later time when the connectivity is established.***
THIS PROCEDURE HAS BEEN COMPLETED		

7.5 PERFORMING SSH KEY EXCHANGES

You must exchange SSH keys between the CMP, MPE-R, MPE-S, BoD, MA servers. Perform this procedure whenever you add additional servers to the Policy Management topology. You can execute 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, reexecute this procedure. The SSH provisioning utility will recheck the existing SSH key exchanges in the entire topology and provision any key exchanges not yet executed. You can execute the command multiple times, even if keys were previously exchanged.

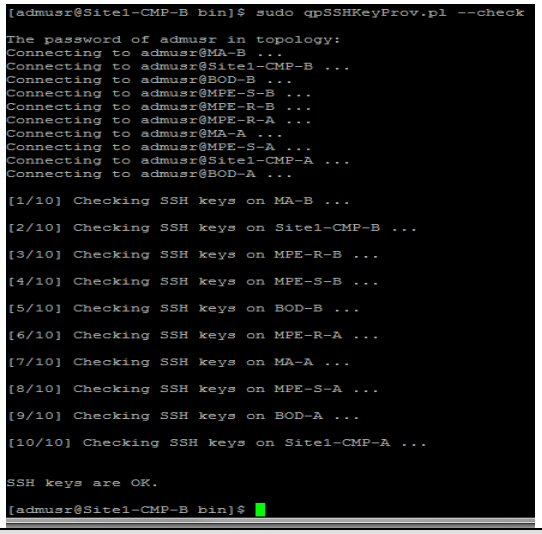
7.5: SSH Performing SSH Key Exchanges

STEP #	**Prerequisite:** - CMP Site 1 cluster is configured and GUI available - Before beginning this procedure, the systems that are exchanging keys must be configured and reachable. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1. ☐	**Ssh to CMP Site 1 active server:** Execute Key Exchanges to 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:

7.5: SSH Performing SSH Key Exchanges

		[admusr@CMP-A ~]$ sudo ha.mystate resourceId role node subResources lastUpdate DbReplication Active A0120.120 0 0109:192637.717 VIP Active A0120.120 0 0109:192637.719 QP Active A0120.120 0 0109:192640.143 DbReplication_old OOS A0120.120 0 0109:191834.248 [admusr@CMP-A ~]$
2. ☐	**Ssh to CMP Site 1 active server:** Execute Key Exchanges to all servers	Enter the following command: $ **sudo qpSSHKeyProv.pl --prov** You are prompted: *The password of admusr in topology:* **3.** Enter the admusr password (admusr_password). The procedure exchanges keys with the rest of the servers in the Policy Management topology. If the key exchange is successful, the procedure displays the message SSH keys are OK. The following example shows a successful key exchange: Enter the Password of admusr [admusr@Site1-CMP-B ~]$ cd /opt/camiant/bin [admusr@Site1-CMP-B bin]$ sudo qpSSHKeyProv.pl --prov The password of admusr in topology: Connecting to admusr@MA-B ... Connecting to admusr@Site1-CMP-B ... Connecting to admusr@BOD-B ... Connecting to admusr@MPE-S-B ... Connecting to admusr@MPE-R-B ... Connecting to admusr@MPE-R-A ... Connecting to admusr@MA-A ... Connecting to admusr@MPE-S-A ... Connecting to admusr@Site1-CMP-A ... Connecting to admusr@BOD-A ... [1/10] Provisioning SSH keys on MA-B ... [2/10] Provisioning SSH keys on Site1-CMP-B ... [3/10] Provisioning SSH keys on MPE-R-B ... [4/10] Provisioning SSH keys on MPE-S-B ... [5/10] Provisioning SSH keys on BOD-B ... [6/10] Provisioning SSH keys on MPE-R-A ... [7/10] Provisioning SSH keys on MA-A ... [8/10] Provisioning SSH keys on MPE-S-A ... [9/10] Provisioning SSH keys on BOD-A ... [10/10] Provisioning SSH keys on Site1-CMP-A ... SSH keys are OK. [admusr@Site1-CMP-B bin]$
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** 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

7.5: SSH Performing SSH Key Exchanges

		have been checked and have been exchanged successfully:  [admusr@Site1-CMP-B bin]$ sudo qpSSHKeyProv.pl --check The password of admusr in topology: Connecting to admusr@MA-B ... Connecting to admusr@Site1-CMP-B ... Connecting to admusr@BOD-B ... Connecting to admusr@MPE-S-B ... Connecting to admusr@MPE-R-B ... Connecting to admusr@MPE-R-A ... Connecting to admusr@MA-A ... Connecting to admusr@MPE-S-A ... Connecting to admusr@Site1-CMP-A ... Connecting to admusr@BOD-A ... [1/10] Checking SSH keys on MA-B ... [2/10] Checking SSH keys on Site1-CMP-B ... [3/10] Checking SSH keys on MPE-R-B ... [4/10] Checking SSH keys on MPE-S-B ... [5/10] Checking SSH keys on BOD-B ... [6/10] Checking SSH keys on MPE-R-A ... [7/10] Checking SSH keys on MA-A ... [8/10] Checking SSH keys on MPE-S-A ... [9/10] Checking SSH keys on BOD-A ... [10/10] Checking SSH keys on Site1-CMP-A ... SSH keys are OK. [admusr@Site1-CMP-B bin]$
THIS PROCEDURE HAS BEEN COMPLETED		

7.6 CONFIGURE POLICY COMPONENTS

This section will cover procedures to configure the 2 tier MPE to a minimum level to execute a test call. Additional details can be found in the CMP Cable User's Guide.

Configuration Management Platform Cable User's Guide Release 12.2

7.6.1 Configuring MPE-R and MPE-S in Policy Servers

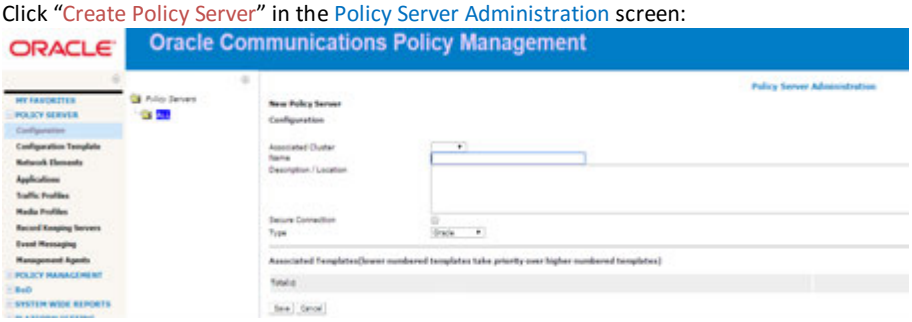
This procedure will configure MPE-R and MPE-S applications.

7.6.1: Configuring MPE-R and MPE-S in Policy Servers

STEP #	This procedure will perform the configuration of MPE-R and MPE-S applications **Prerequisite:** - Network access to the CMP OAM IP address, to bring up a web Browser GUI (http) - MPE-R and MPE-S clusters have been added to Topology Settings 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.	
1. ☐	**Create MPE-R and MPE-S Policy Servers in CMP GUI**	**Select:** **Policy Server -> Configuration -> Policy Servers** 

7.6.1: Configuring MPE-R and MPE-S in Policy Servers

Click "Create Policy Server" in the Policy Server Administration screen:



Enter values for the configuration attributes:
a) **Associated Cluster** (required) — Select the cluster with which to associate this MPE device.

b) **Name** — Name of this MPE device. The default is the associated cluster name.

c) **Description / Location** (optional) — Information that defines the function or location of this MPE device.

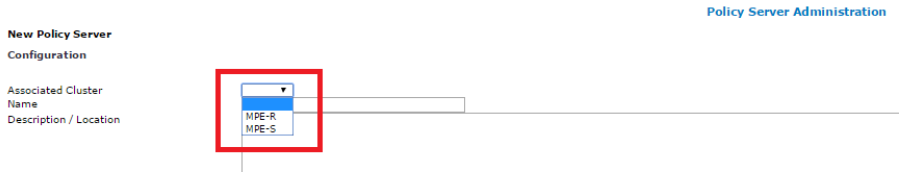
d) **Secure Connection** — Designates whether or not to use the HTTPS protocol for communication (certifcates must be configured to use this option) between Policy Management devices. If selected, devices communicate over port 8443.

e) **Type** — Defines the policy server type:

• **Oracle** (default) — The policy server is an MPE device and can be fully managed by the CMP.

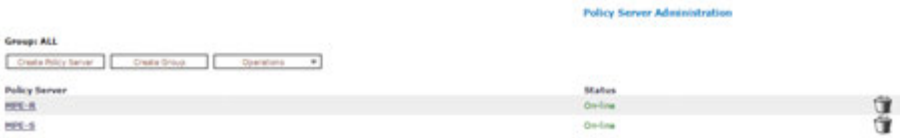
• **Unmanaged** — The policy server is not an MPE device and therefore cannot be actively managed by the CMP. This selection is useful when an MPE device is routing traffic to a non-Oracle policy server.

Note: When configuring an "Associated Cluster", the drop down tab will only be populated with MPE clusters that have been configured in the CMP Topology from previous steps.

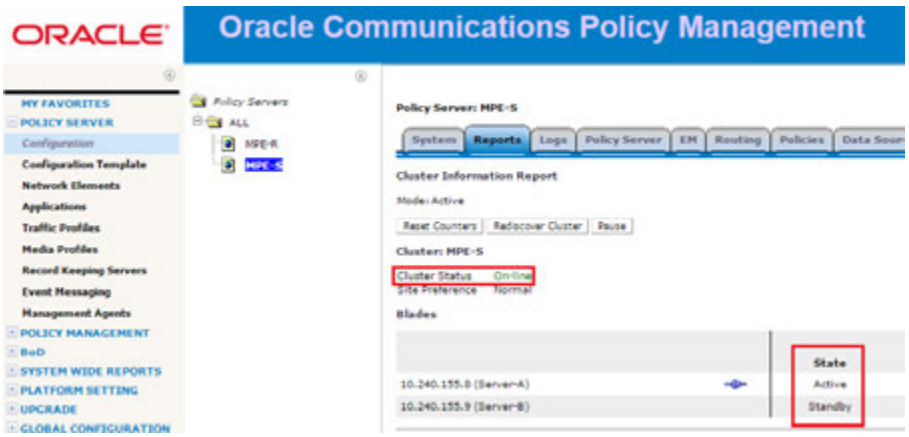
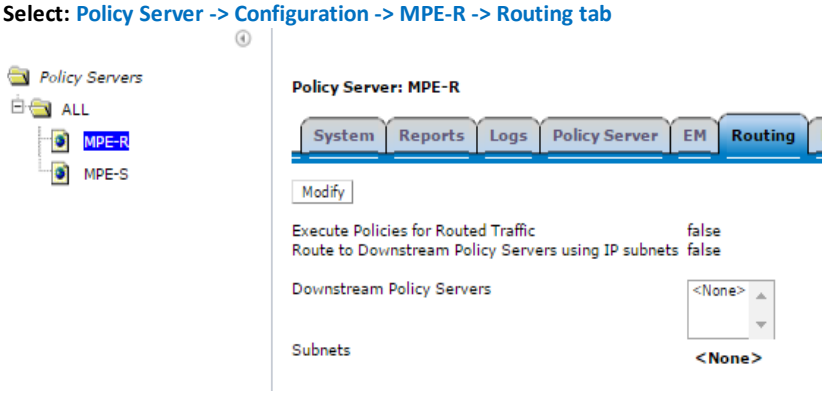


Complete the form to configure MPE-R Policy Server then click "Save" and confirm Configured Policy Server status is "On-line":

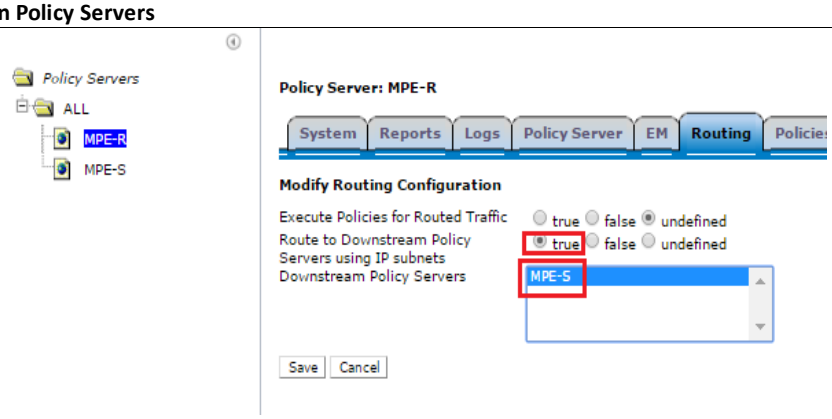
In the same fashion, complete the form to configure MPE-S Policy Server then "Save" and confirm Configured Policy Server status is "On-line":



7.6.1: Configuring MPE-R and MPE-S in Policy Servers

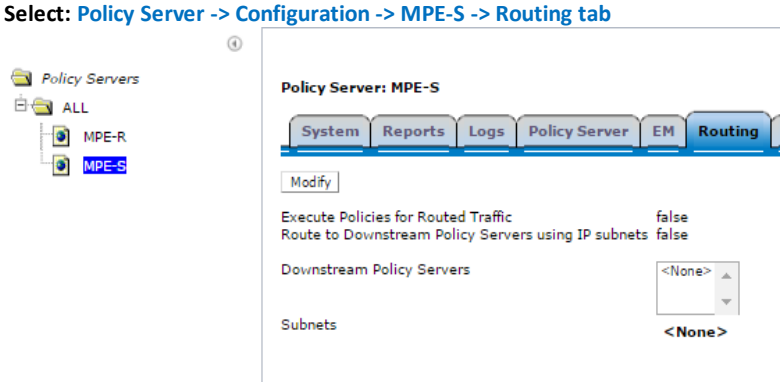
2. ☐	**Check added MPE-R/S clusters in Reports tab**	**Select:** Policy Server -> Configuration -> *Configured MPE-R/S* -> Reports tab **MPE-R:**  **MPE-S:**  Validate that cluster status is On-line and that Servers assume the Active and Standby roles.
3. ☐	**Routing configurations for the 2 tier MPE Policy Servers**	**Select:** Policy Server -> Configuration -> MPE-R -> Routing tab  Click "Modify" then set "Route to Downstream Policy" to "True" and choose the MPE-S configured Policy Server that will MPE-R will route messages to:

7.6.1: Configuring MPE-R and MPE-S in Policy Servers



Click "Save":

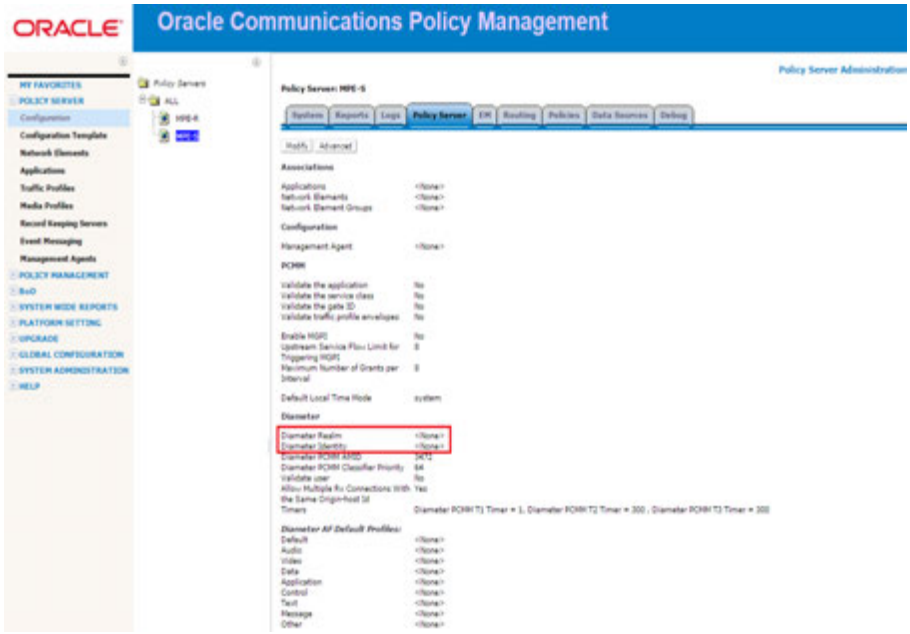
Select: **Policy Server -> Configuration -> MPE-S -> Routing tab**



Click "Modify" then set "Execute Policies for Routed Traffic" to "True":

7.6.1: Configuring MPE-R and MPE-S in Policy Servers

Click "Save":

4. ☐	**Diameter configurations for MPE-S**	**Select:** **Policy Server -> Configuration -> MPE -> Policy Server tab** 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. 

7.6.1: Configuring MPE-R and MPE-S in Policy Servers

To define these diameter parameters, click the "Modify" button on top of page then fill in the diameter Realm and Identity that your network will be using 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:

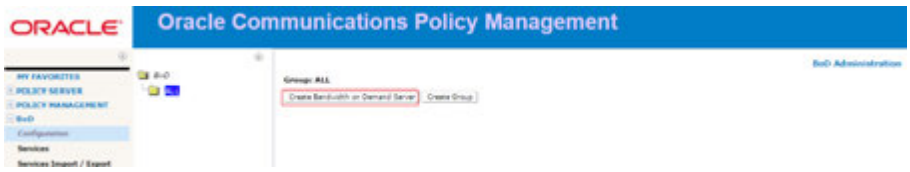
Diameter	
Diameter Realm	oracle.com
Diameter Identity	pcrf.oracle.com
Diameter PCMM AMID	3472
Diameter PCMM Classifier Priority	64
Validate user	No
Allow Multiple Rx Connections With the Same Origin-host Id	Yes
Timers	Diameter PCMM T1 Timer = 1, Diameter PCMM T2 Timer = 300 , Diameter PCMM T3 Timer = 300

THIS PROCEDURE HAS BEEN COMPLETED

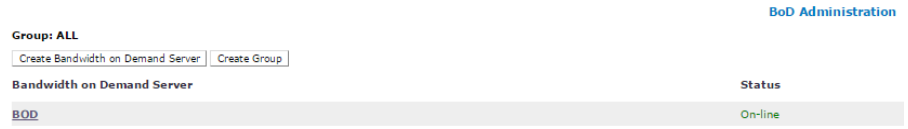
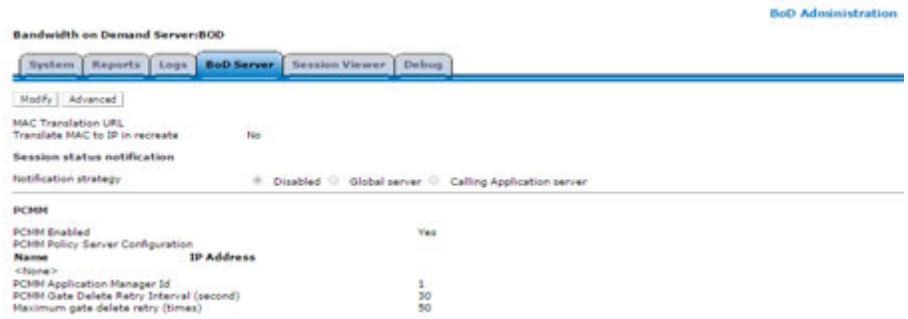
7.6.2 Configure BoD and MA

If customer is using BoD and MA components in Policy Deployment, this section will walk through configuring these components. If these components are not used, this procedure can be skipped.

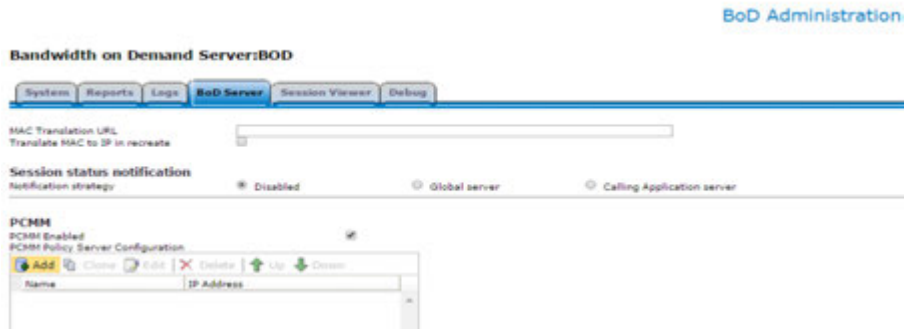
7.6.2: Configure BoD and MA components

STEP #	This procedure will add the BoD and MA components in CMP GUI **Prerequisite:** - Network access to the CMP OAM IP address, to bring up a web Browser GUI (http) - BoD and MA clusters have been added to the CMP Topology Settings - Manage BODs and Manage MA servers need to be enabled in CMP initial mode settings 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.	
1. ☐	**Create BoD Application**	**Select: BOD -> Configuration -> ALL**  Click "**Create Bandwidth On Demand Server**" in the BOD Administration screen:

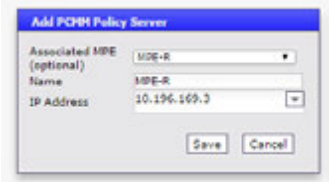
7.6.2: Configure BoD and MA components

		 Note that configured BOD cluster in Topology would be available in Associated Cluster drop down. Complete the form to configure BOD then click "Save" and confirm BoD status is "On-line": 
2. ☐	**Check added BOD cluster in Reports tab**	**Select: BOD -> Configuration -> All -> *Configured BOD* -> Reports tab**  Validate that cluster status is "On-line" and that Servers assume the Active and Standby roles.
3. ☐	**Associate Policy Server with BOD**	**Select: BOD -> Configuration -> All -> *Configured BOD* -> BoD Server tab**  Click "Modify" then "Add" under PCMM Policy Server Configuration:

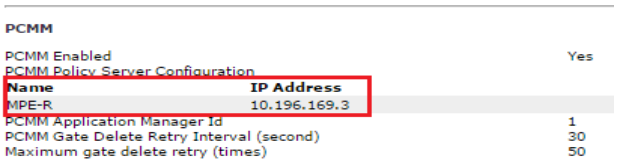
7.6.2: Configure BoD and MA components



Select the MPE-R configured Policy server from the associated MPE drop down. The name and IP address would be populated automatically, click "Save":

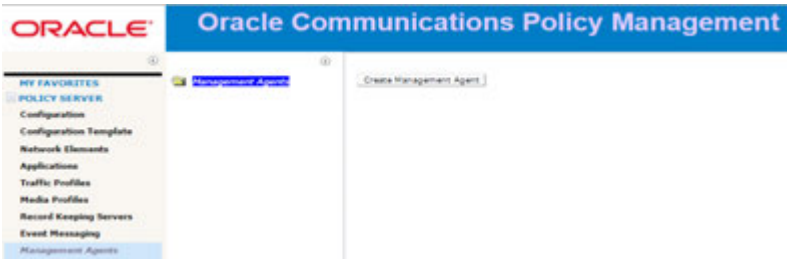


Click "save" in BoD Administration page:



4. ☐ **Create MA Application**

Select: Policy Server -> Management Agents -> Management Agents

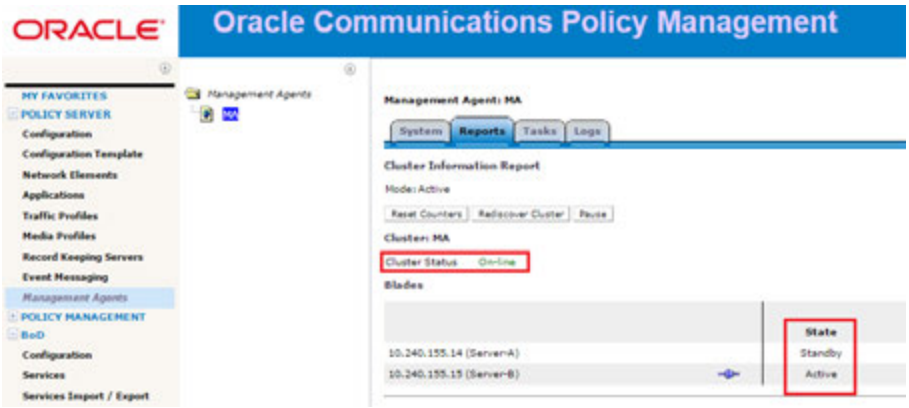


Click "**Create Management Agent**" in the Management Agent Administration screen:

Note that configured MA cluster in Topology would be available in Associated Cluster drop down.

Complete the form to configure MA then click "Save" and confirm Configured MA status is

7.6.2: Configure BoD and MA components

		"On-line": 
5. ☐	**Check added BOD cluster in Reports tab**	**Select:** **Policy Server -> Management Agents -> *Configured MA* -> Reports tab**  Validate that cluster status is "On-line" and that Servers assume the Active and Standby roles.
THIS PROCEDURE HAS BEEN COMPLETED		

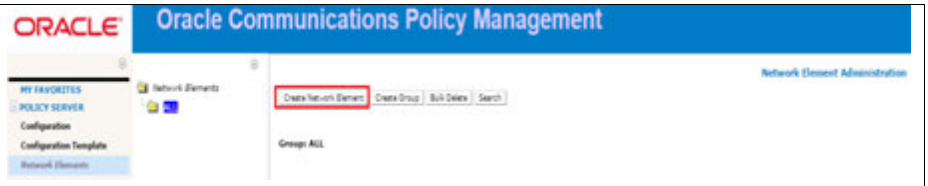
7.6.3 Define and Add Network Elements

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

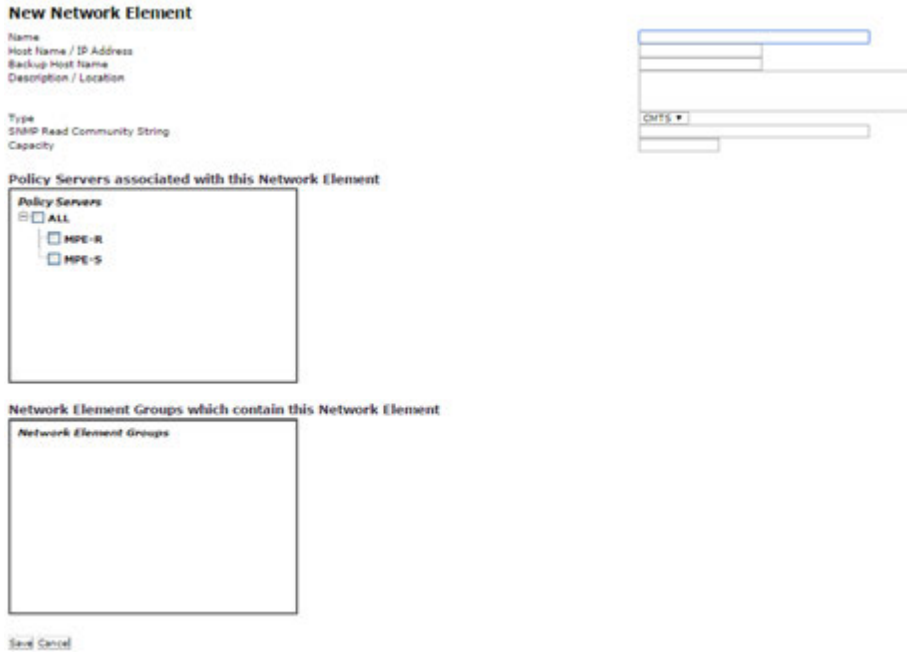
7.6.3: Define and Add Network Elements

STEP #	This procedure will add 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) - MPE-R and MPE-S 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.	
1. ☐	**Create Network Element in CMP GUI**	**Select:** **Policy Server -> Network Elements -> All**

7.6.3: Define and Add Network Elements



Click "Create Network Element" in the Network Element Administration screen:



Enter information for the network element:

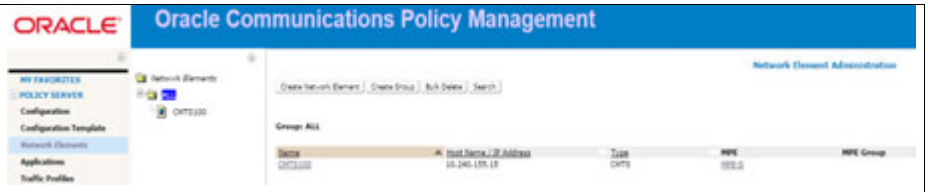
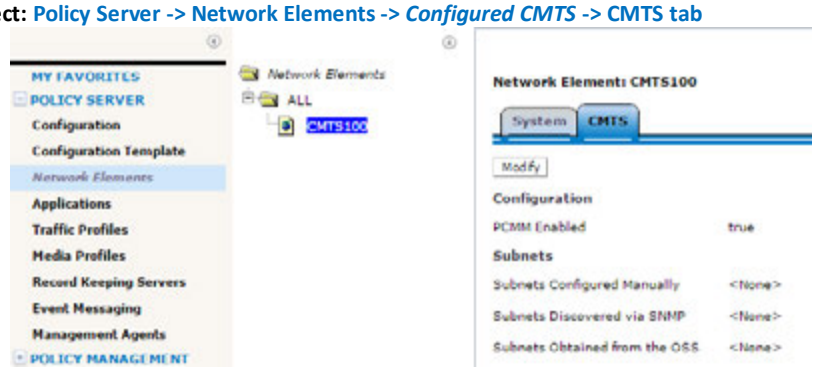
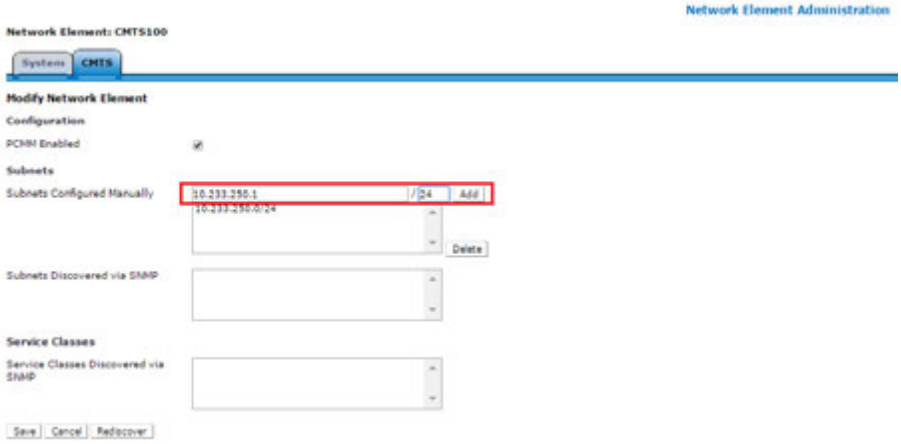
a) **Name** (required) — The name you assign to the network element.
b) **Host Name/IP Address** (required) — Registered domain name, or IP address in IPv4 or IPv6 format, assigned to the network element.
c) **Backup Host Name** — Alternate address that is used if communication between the MPE device and the network element's primary address fails.
d) **Description/Location** — Free-form text. Enter up to 250 characters.
e) **Type** (required) — Select the type of network element.
The only supported Network Element type in Cable mode is "**CMTS**"
f) **SNMP Read Community String**— A password-like field that allows read-only access to the MIBs for the network element that are used for SNMP polling. If a value is not entered, SNMP data is not collected from this network element.
g) **Capacity** — The bandwidth allocated to this network element.
h) **Policy Servers associated with this Network Element** — select one or more policy servers (MPE devices) to associate with this network element.

i) **Network Element Groups which contain this Network Element** — select one or more groups.

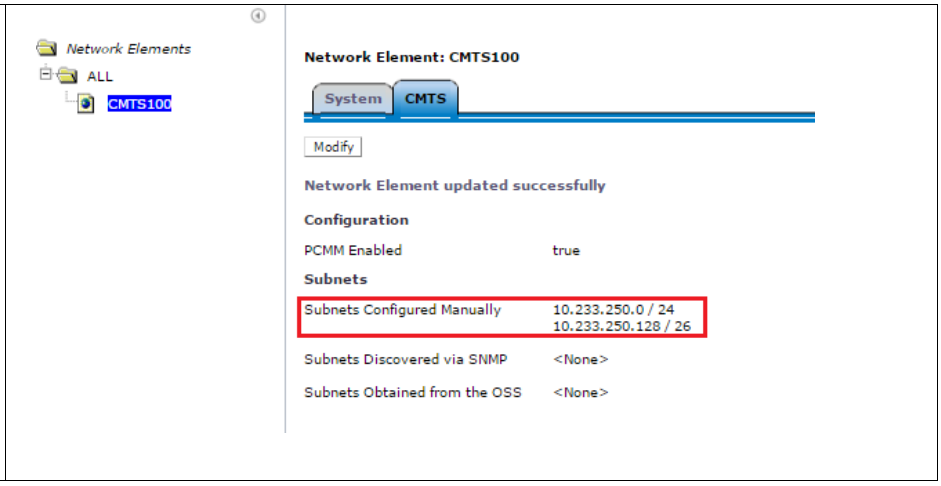
When you finish, click **Save**.

Following an example of a configured Network Element.

7.6.3: Define and Add Network Elements

		 The new Network Element has now been created.
2. ☐	**Manually add subnets to newly created CMTS**	In case the customer needs to add subnets to the newly created subnets manually: **Select:** **Policy Server -> Network Elements -> *Configured CMTS* -> CMTS tab**  Click Modify then fill in the subnets IP address and subnet mask and click add for each:  When finished click “Save”:

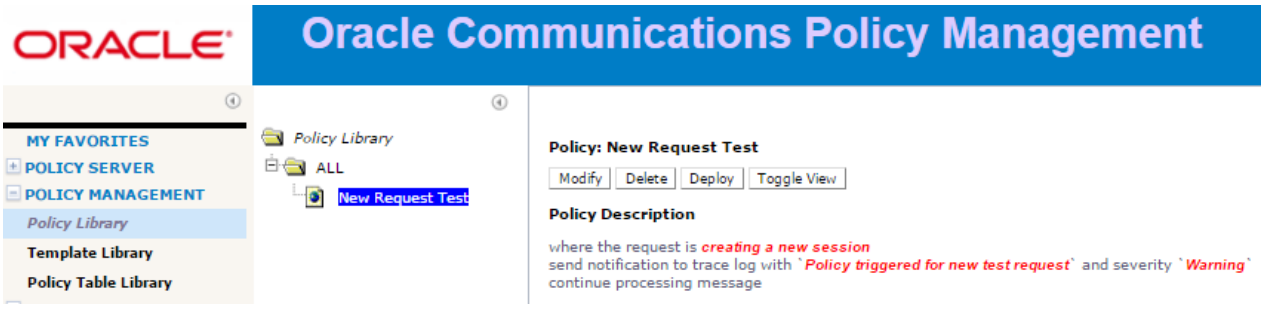
7.6.3: Define and Add Network Elements



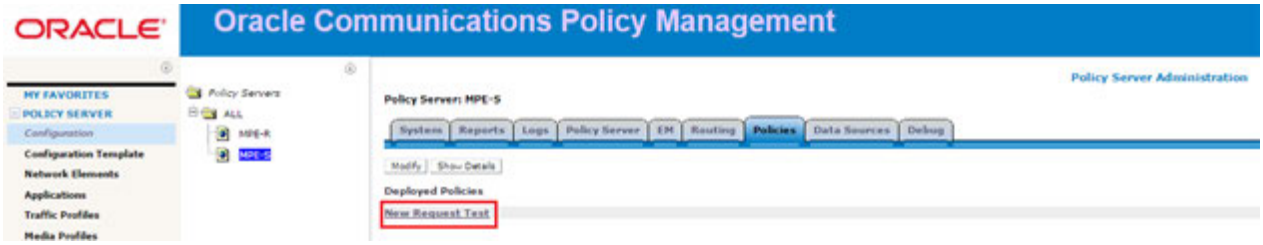
7.7 LOAD POLICIES AND RELATED POLICY DATA

This step is optional. Policies are not required to process a test call but for the purpose of verification, a basic Policy can be created manually, or using an import action and an xml file if applicable. The policy must be deployed to the MPE-S which will process the test request in order to be triggered.

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



Note that this policy needs to be deployed to the relevant MPE-S that will process diameter session requests. Deployed Policies can be verified from the “Policies” tab of the MPE-S that will process the test request:



7.8 PERFORM TEST CALL

A basic test call will confirm that the system is ready for testing of call scenarios defined by the customer. For example, AF/P-CSCF will first establish a Diameter connection with the PCRF and then initiate the test call by sending an Rx Diameter AAR message.

Alternatively, Customer's system can send a new session request via HTTP or SOAP to BOD component which will result in a new PCMM message sent by MPE-S to CMTS network Element.

CMTS network element must be configured and associated to the subscriber's relevant test session as shown in the following sample :

7.9 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 need to be planned and executed.

Please reference the following document for information on configuring SNMP:

SNMP User's Guide

Additional Procedures can be referenced from the following documents:

Platform Configuration User's Guide Release 12.2

Configuration Management Platform Cable User's Guide Release 12.2

Changes in the behavior of Release 12.2 are documented in the Oracle® Communications Policy Management Release Notes Release 12.2

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

8. SUPPORTING PROCEDURES

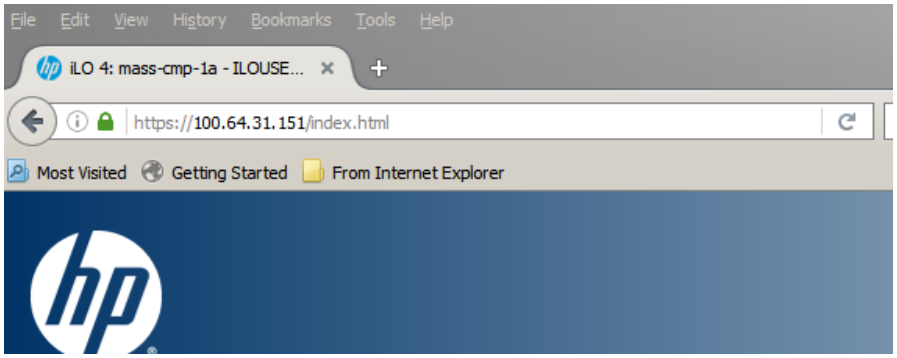
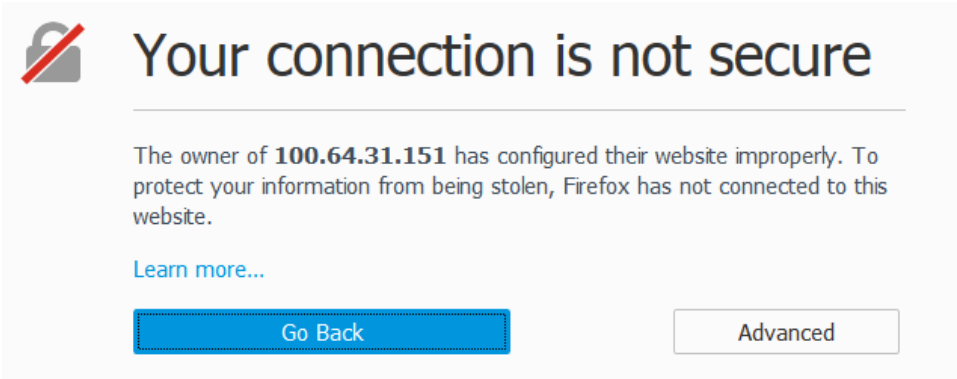
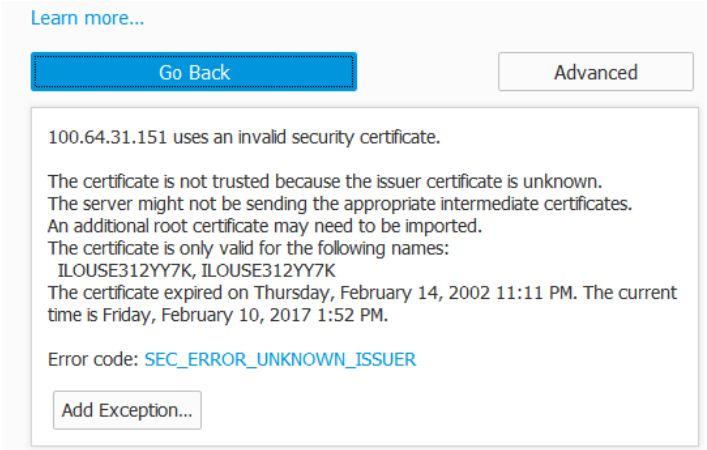
The following procedures may be referenced during installation.

8.1 ACCESSING THE ILO VGA REDIRECTION WINDOW

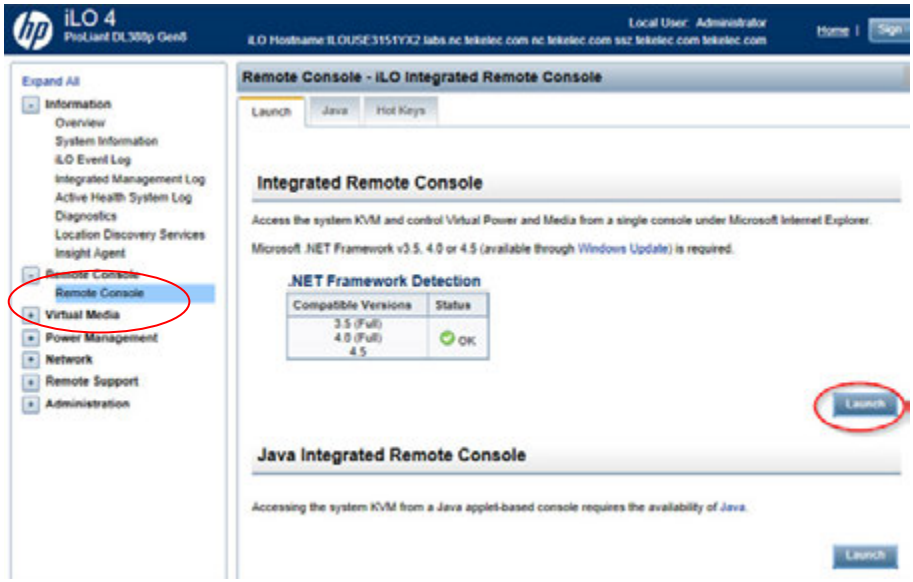
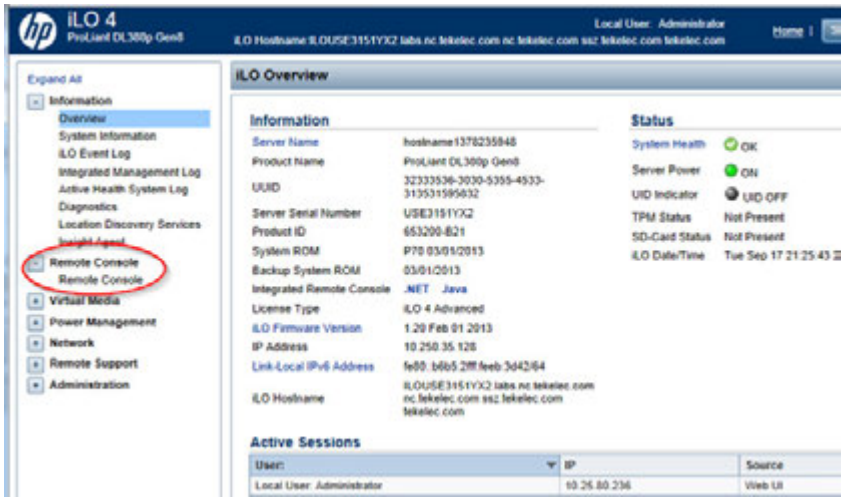
8.1.1 Accessing the iLO VGA Redirection Window for HP Servers

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

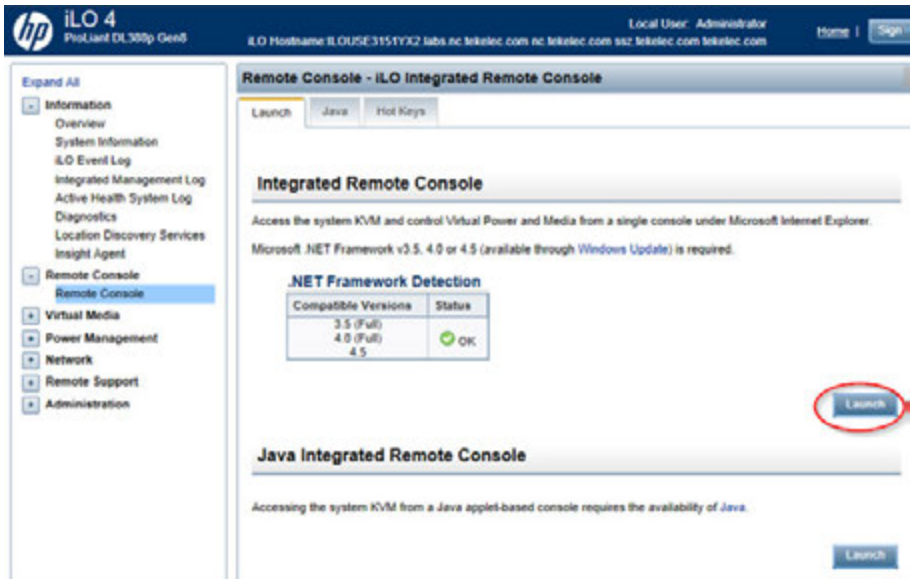
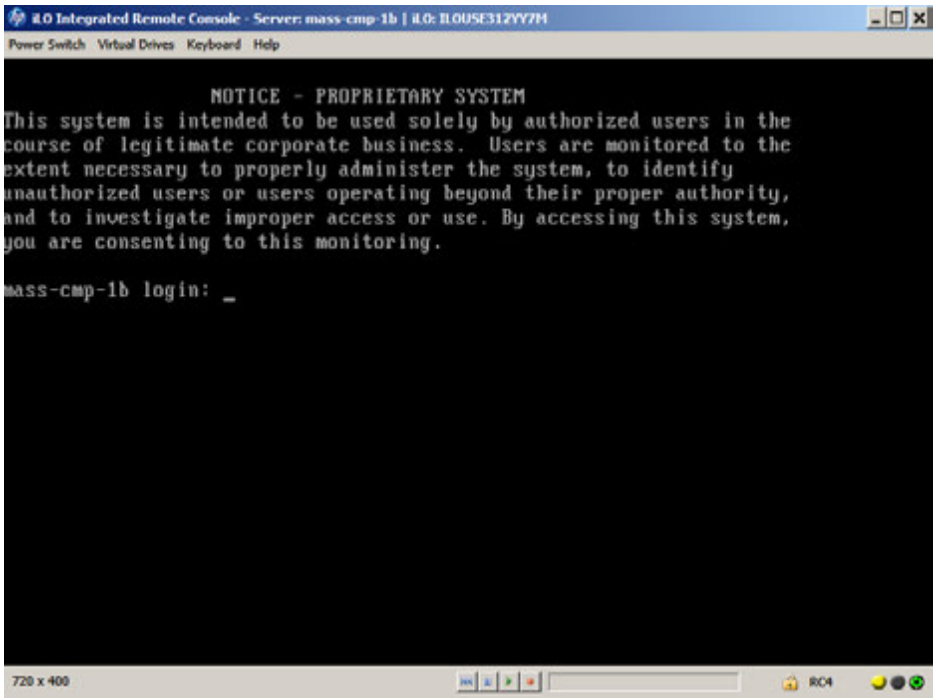
8.1.1 Accessing the iLO VGA Redirection Window for HP

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.	
3. ☐	Select "Advanced" and the "Add Exception" and then "Confirm Security Exception" in the resulting window.	

8.1.1 Accessing the iLO VGA Redirection Window for HP

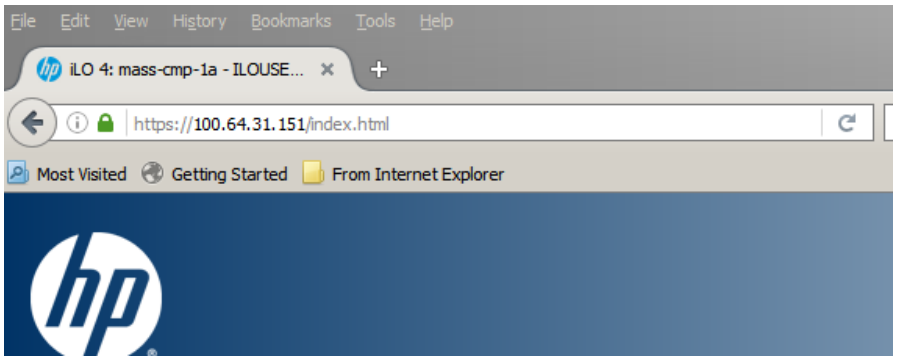
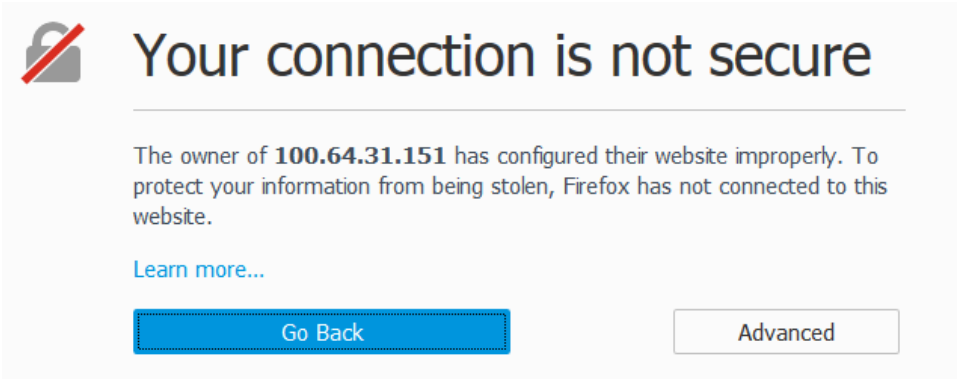
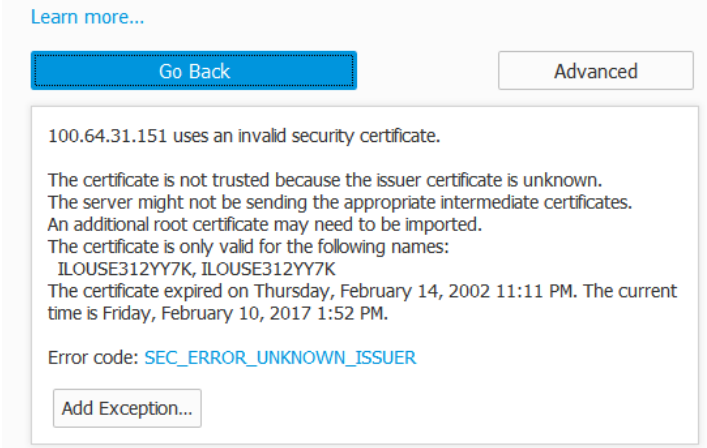
4. ☐	Login to the iLO console as "Administrator"	
5. ☐	The admin GUI is displayed. Expand the "**Remote Console**" tab in the left panel of the GUI.	
6. ☐	The Remote Console tab is expanded Click on the "**Remote Console**" option	

8.1.1 Accessing the iLO VGA Redirection Window for HP

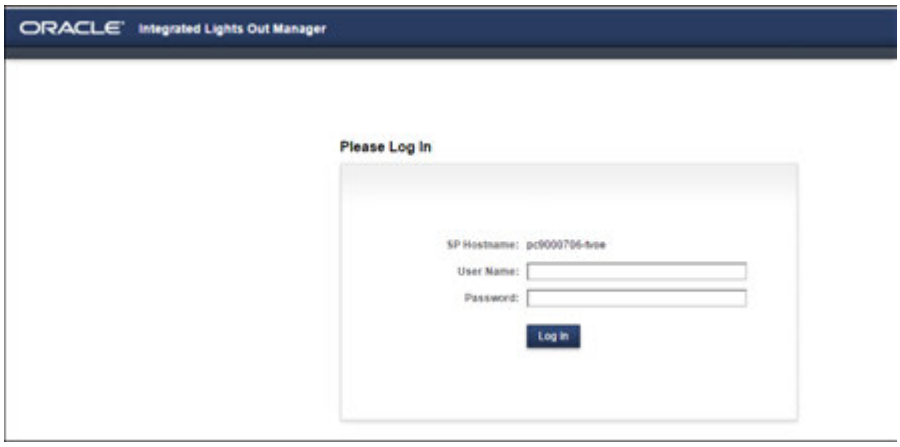
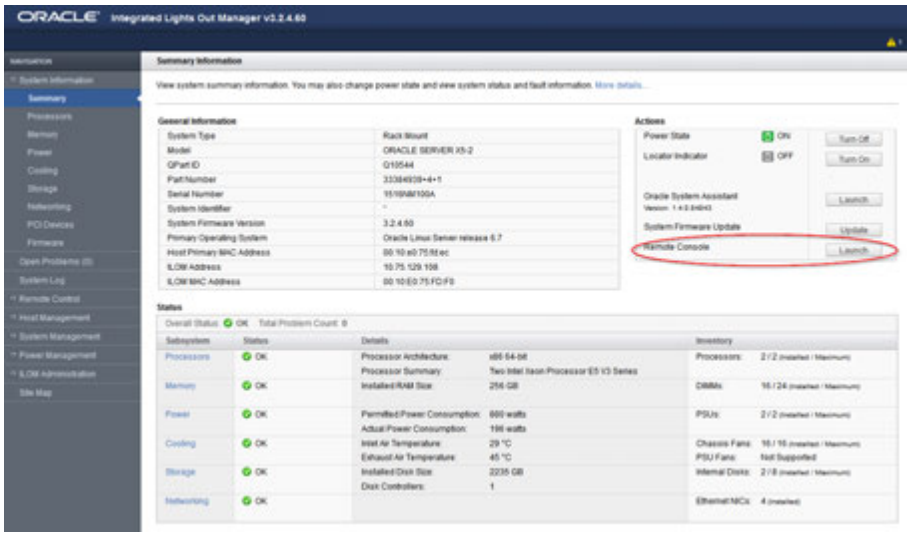
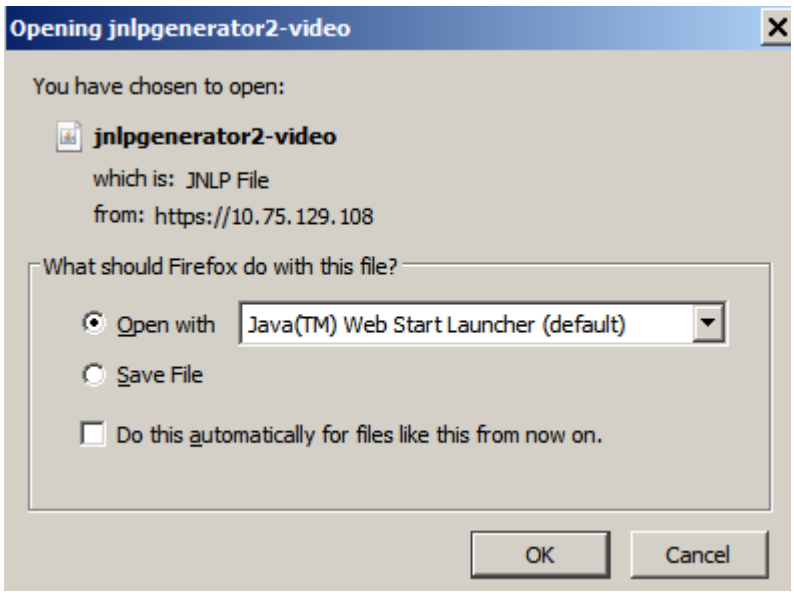
7. ☐	The Remote Console GUI is displayed Click on the "**Launch**" button under "**Integrated Remote Console**"	
8. ☐	The iLO Console window is displayed. .	
THIS PROCEDURE HAS BEEN COMPLETED		

8.1.2 Accessing the iLOM VGA Redirection Window for Oracle RMS Servers

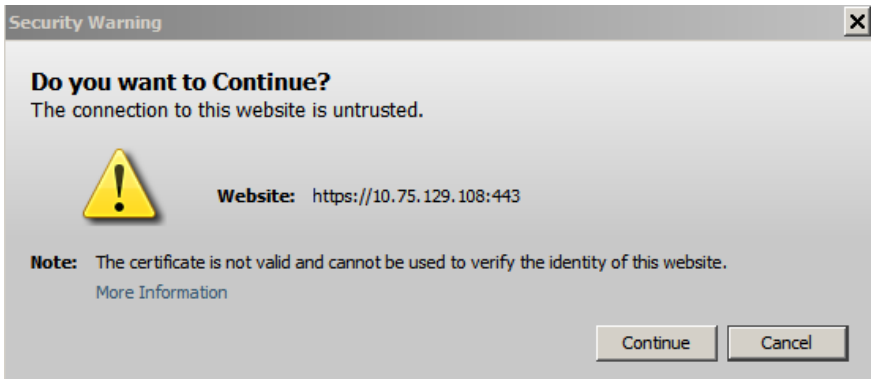
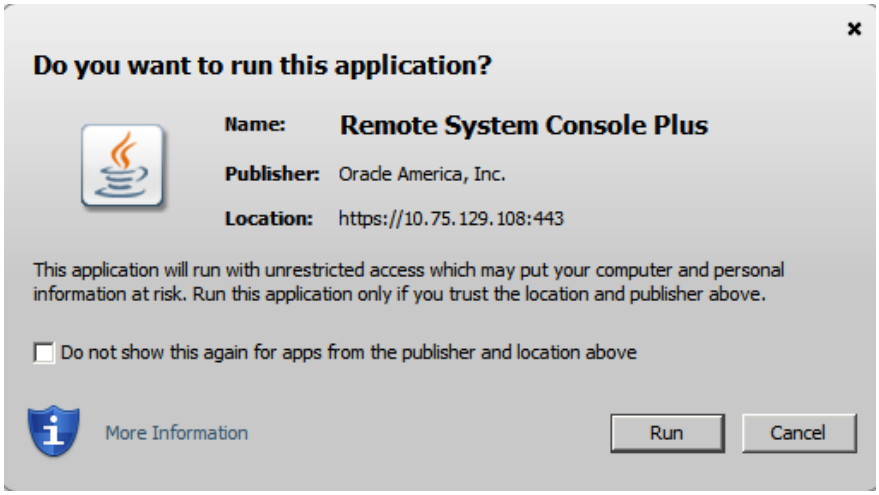
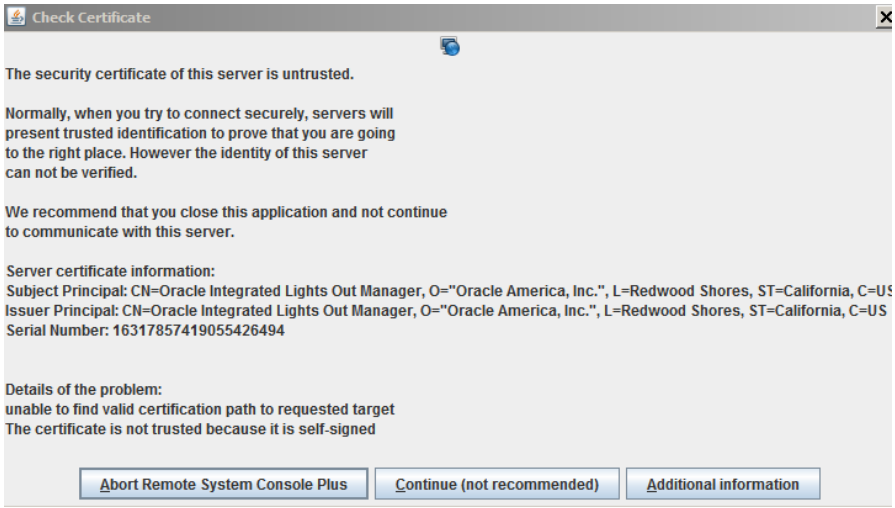
8.1.2: Accessing the iLOM VGA Redirection Window for Oracle RMS Servers

Step	Procedure	Result
1. ☐	Launch an approved web browser and connect to the iLO interface **NOTE:** *Always use https:// for iLO GUI access.*	
2. ☐	The first time the web browser connects to the iLO a warning message will be displayed regarding the Security Certificate.	
3. ☐	Select "Advanced" and the "Add Exception" and then "Confirm Security Exception" in the resulting window.	

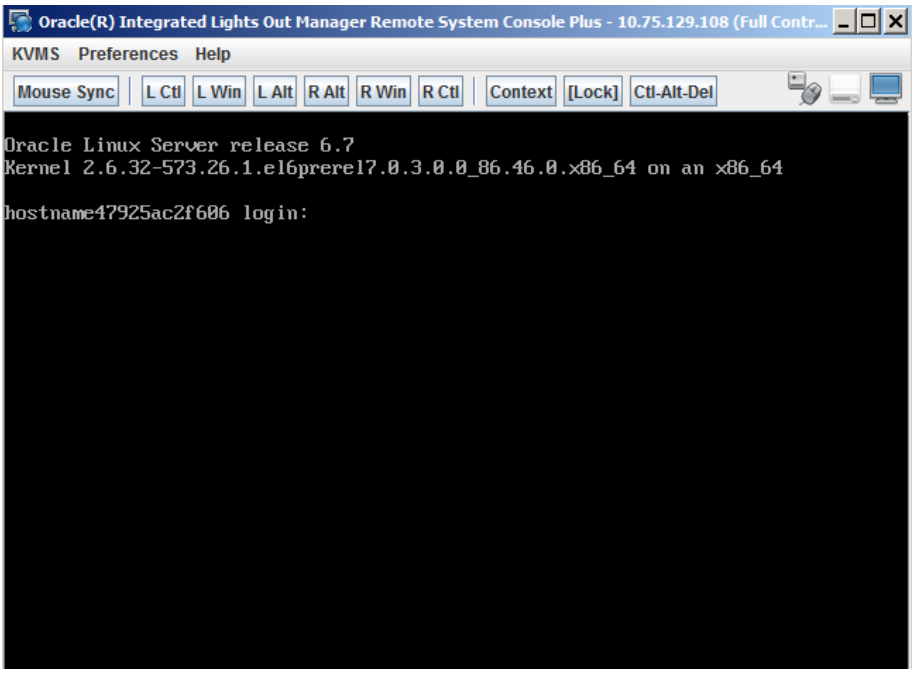
8.1.2: Accessing the iLOM VGA Redirection Window for Oracle RMS Servers

4. ☐	Login to the iLO console as "Administrator"	
5. ☐	The admin GUI is displayed. "Launch" the "**Remote Control**" from the right side of the screen.	
6. ☐	Open "Java Web Start" when prompted.	

8.1.2: Accessing the iLOM VGA Redirection Window for Oracle RMS Servers

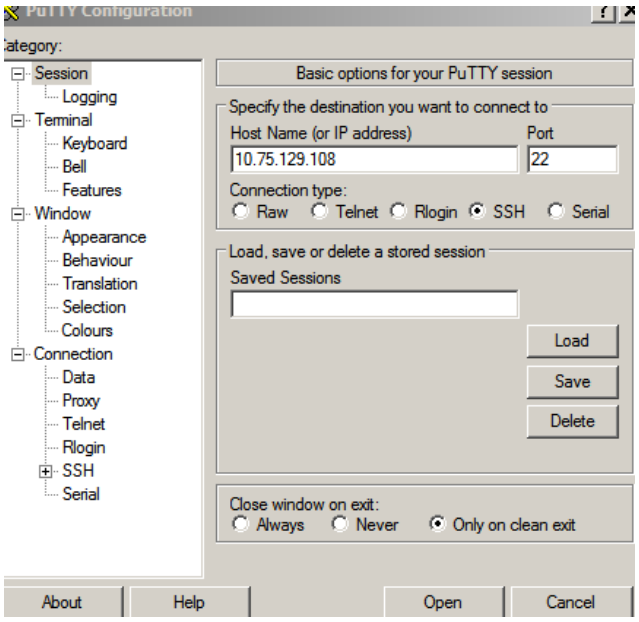
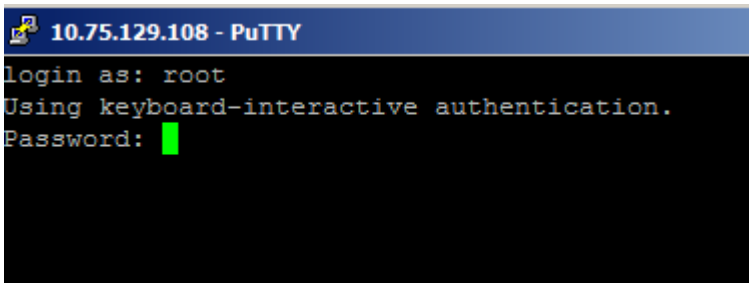
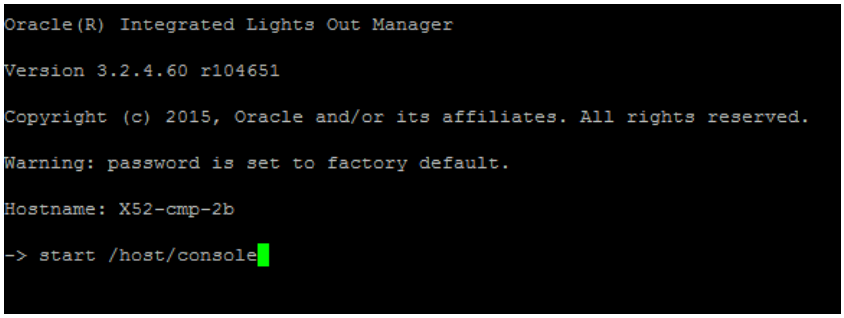
7. ☐	"Continue" if prompted. .	
8. ☐	And "Run" if prompted. .	
9. ☐	"Continue" if prompted. .	

8.1.2: Accessing the iLOM VGA Redirection Window for Oracle RMS Servers

10. ☐	The iLO Console window is displayed. .	
THIS PROCEDURE HAS BEEN COMPLETED		

8.1.3 Accessing the iLOM Console for Oracle RMS Servers using SSH

8.1.3: Accessing the iLO Console for Oracle RMS Servers

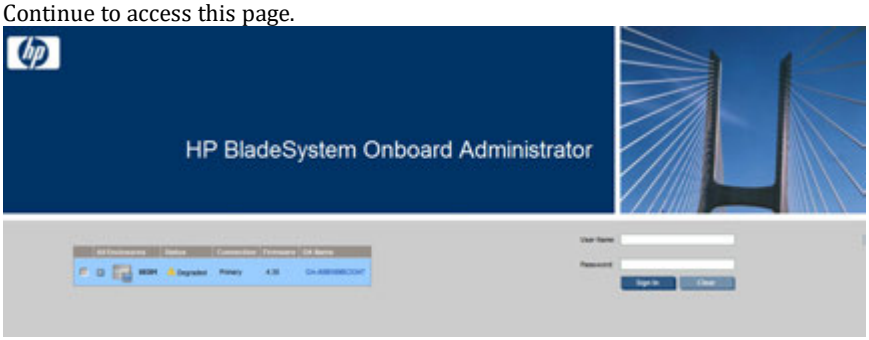
Step	Procedure	Result
1. ☐	Login to the Server ILOM console with "ssh".	Using putty or something similar-open an ssh session to iLOM of the target server using the iLOM IP address:  **login as: root** **Password:<root_password)**  ->
2. ☐	From the iLOM prompt:	Type "start /host/console" from the "→" prompt to login into the server console. 

8.1.3: Accessing the iLO Console for Oracle RMS Servers

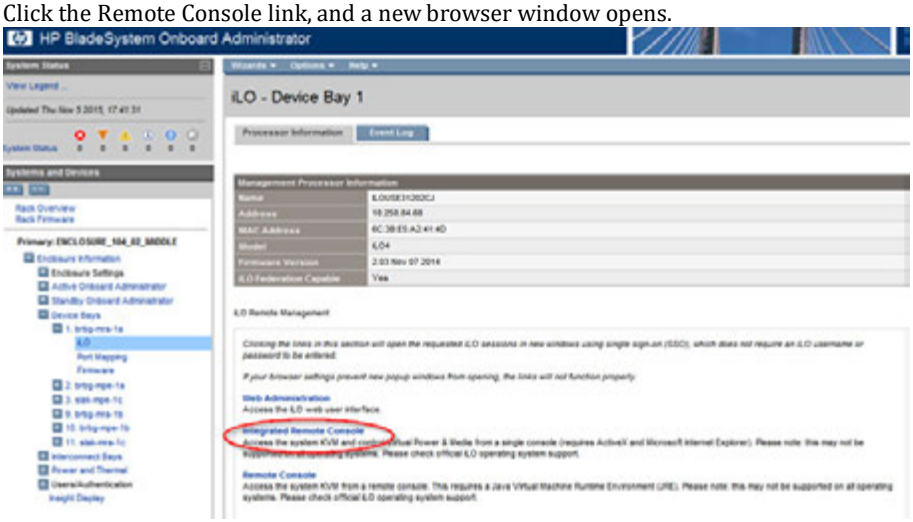
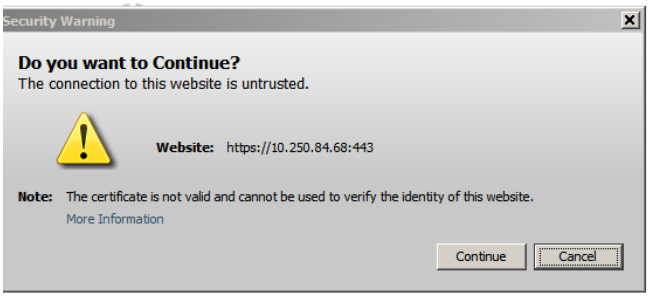
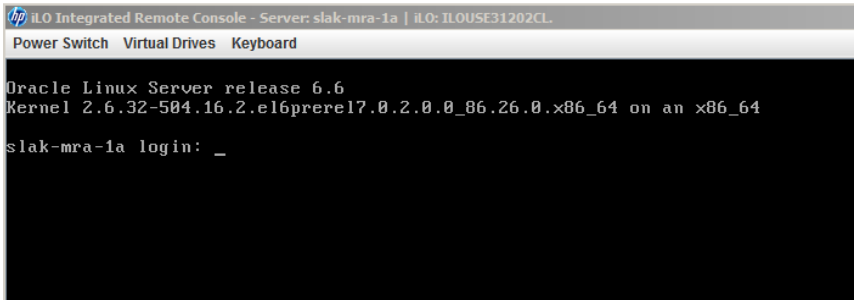
3. ☐	From the iLOM prompt:	Answer "**y**" to confirm login to the console. `-> start /host/console` `Are you sure you want to start /HOST/console (y/n)? y` The prompt will respond with "Serial Console Started". `Serial console started.  To stop, type ESC (` Hit the carriage return to get the server prompt 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:`  You can then login to the server with admusr/<admusr_password> 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 type "ESC ("  `Serial console started. To stop, type ESC (`
THIS PROCEDURE HAS BEEN COMPLETED		

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

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

Step	Procedure	Result
1. ☐	**Web Browser:** Access Onboard Administrator Login (must be Active OA)	Open a web browser and navigate to the OA IP address. Note that you be prompted with a warning for security certificates, because the certificate is self-signed. You must select Continue to access this page. 
2. ☐	**Web Browser:** Login as Administrator, and view available server blades	Log in to HP OA as a user with Administrative privilege. 
3. ☐	**Web Browser:** Open the iLO form for the server blade you wish to connect to	From the navigation pane, select **Device Bays**, select the expand button on the desired device, and click on the iLO link. 

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

4. ☐	**Web Browser:** Click the remote Console link	Click the Remote Console link, and a new 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 select Continue or Yes to proceed.
5. ☐	**Web Browser**:	After a few moments, the Console window will open. 
THIS PROCEDURE HAS BEEN COMPLETED		

8.2 MOUNTING MEDIA (IMAGE FILES)

8.2.1 Mounting Physical Media (RMS only)

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

8.2.1: Mounting Physical Media on HP Rack Mount Servers

Step	In this procedure you will mount media on HP rack mount servers, for ISO access or other file transfer.	
1. ☐	Access the server's console.	Connect to the server's console using one of the access methods described in ***Section 8.1.1***

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 the **<ENTER>** key 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 ~]#`

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

8.2.1: Mounting Physical Media on HP Rack Mount Servers

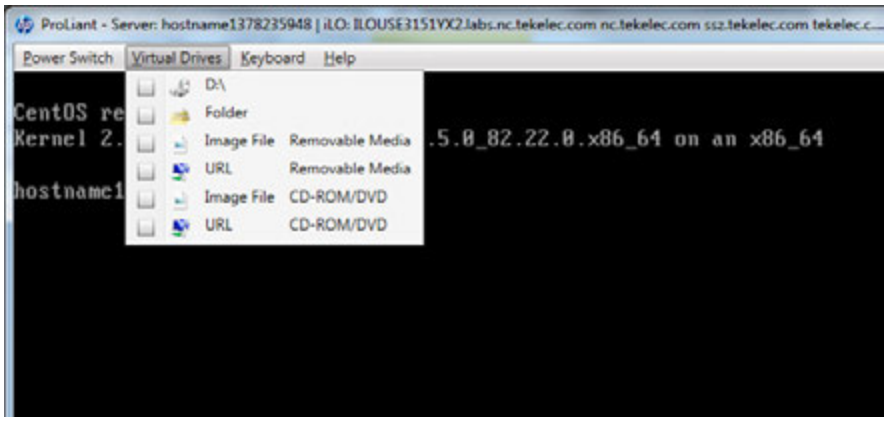
6. ☐	**HP Server:**
	USB media may be accessed via the path shown
		`[root@hostname1260476099 ~]# cd /media/sdb1`
		
		`[root@hostname1260476099 ~]#`

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***
THIS PROCEDURE HAS BEEN COMPLETED		

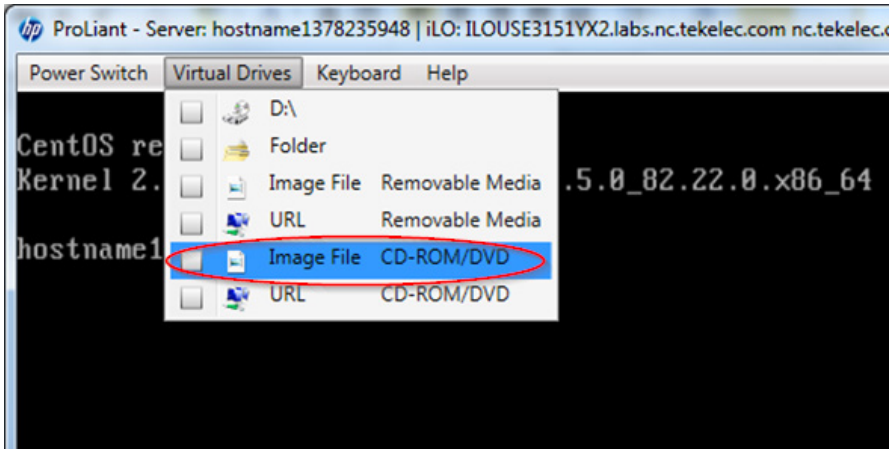
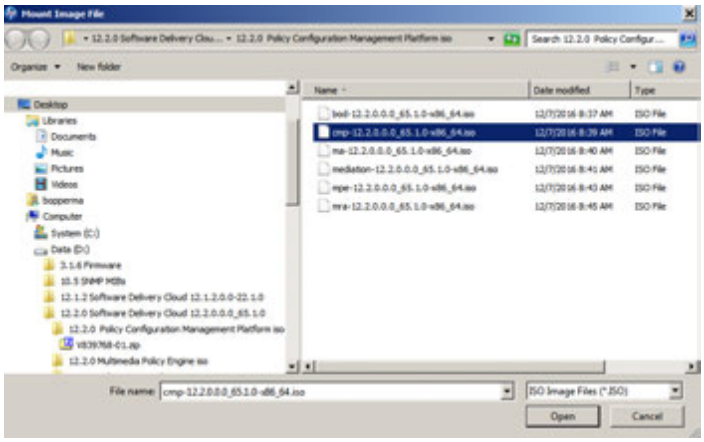
8.2.2 Mounting Virtual Media on HP Servers

This procedure contains steps to mount virtual media on HP rack mount servers via ILO.

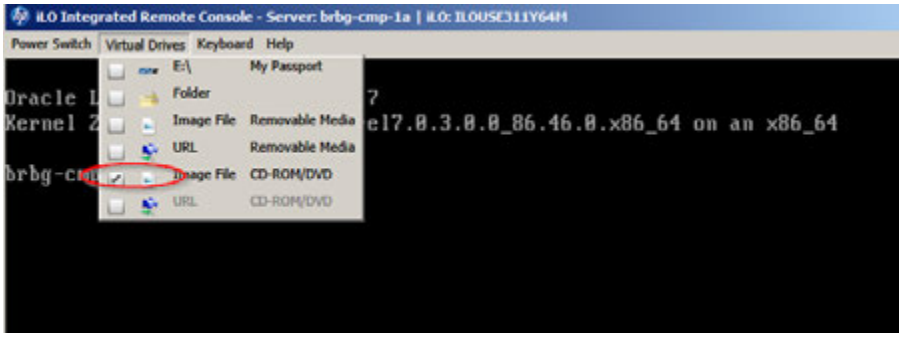
8.2.2: Mounting Virtual Media on HP Rack Mount Servers

Step	In this procedure you will mount media on HP rack mount servers via ILO, for ISO access or other file transfer.	
1. ☐	Access the server's ILO VGA.	Connect to the server's ILO VGA using the access method described ***Section 8.1.1***
2. ☐	**ILO Remote Console:** Select "**Virtual Drives**" from the top menu bar.	

8.2.2: Mounting Virtual Media on HP Rack Mount Servers

3. ☐	**HP Server:** Select from the menu options presented: **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**" 
4. ☐	**HP Server:** Select an image file to mount	A window will popup to browse the client browser workstation or laptop.  Choose the desired image file.

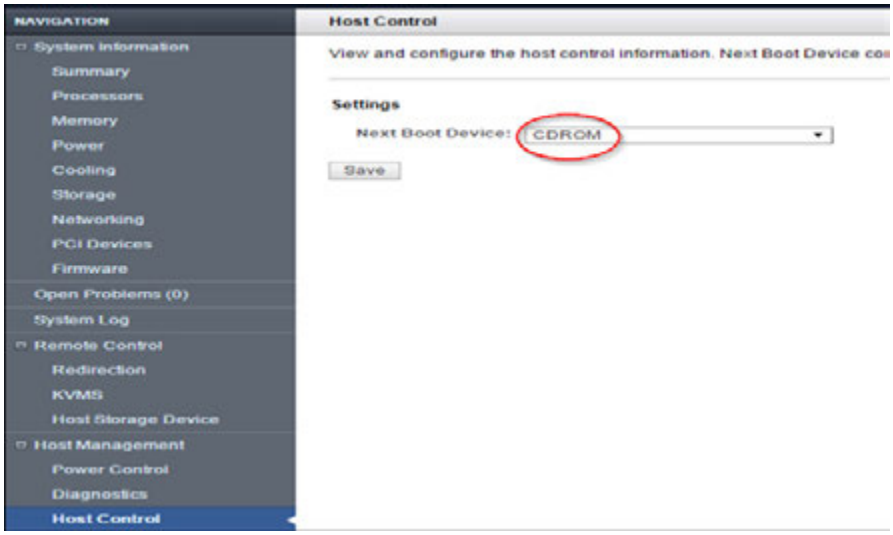
8.2.2: Mounting Virtual Media on HP Rack Mount Servers

5. ☐	**HP Server:** Confirm the target image file has been mounted	Return to the "Virtual Drives" drop down tab and the **"Image File / CD-ROM/DVD"** will now be checked indicating that the image file has been mounted. 
THIS PROCEDURE HAS BEEN COMPLETED		

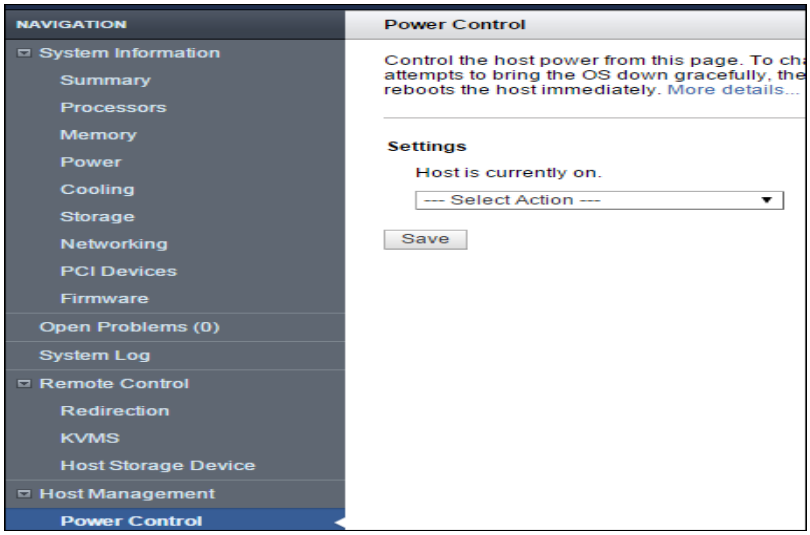
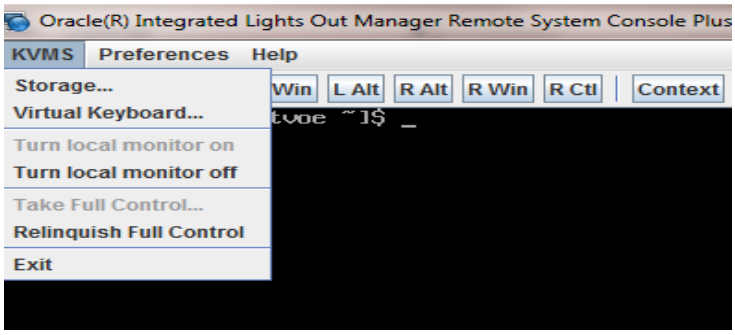
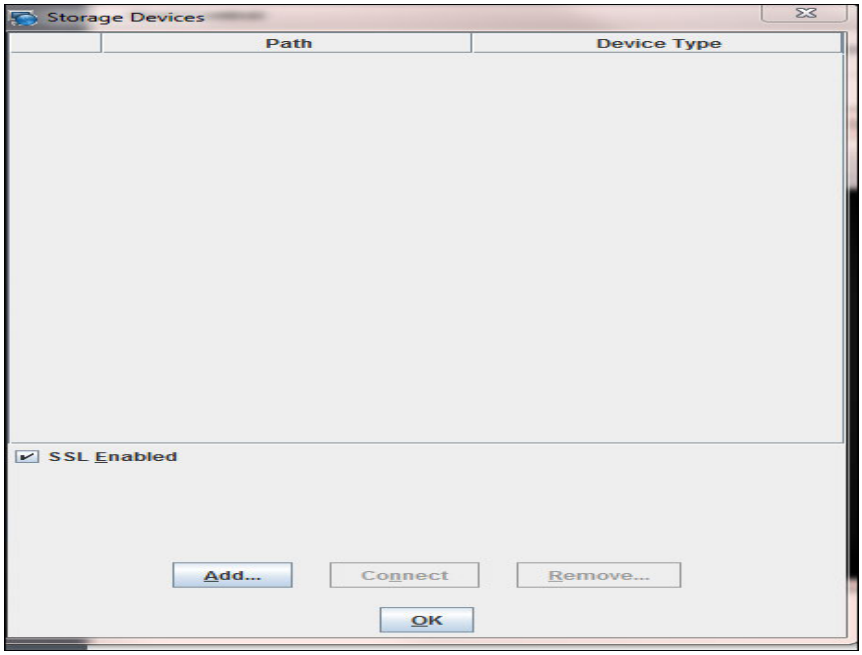
8.2.3 Mounting Virtual Media on Oracle RMS Servers

This procedure contains steps to mount virtual media on Oracle RMS servers via ILO.

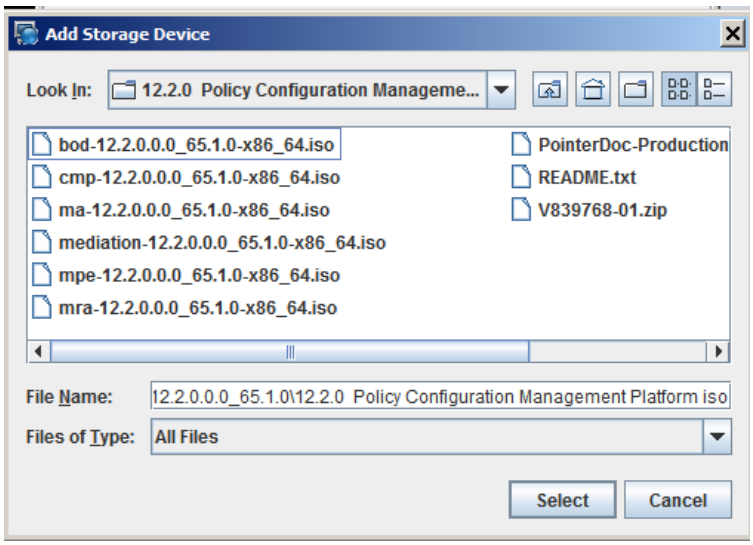
8.2.3: Mounting Virtual Media on Oracle RMS Servers

Step	In this procedure you will mount media on Oracle RMS servers via the iLOM, for ISO access or other file transfer.	
1. ☐	Access the server's ILO VGA.	Connect to the server's ILO VGA using the access method described in ***Section 8.1.2***
2.	**ILO Admin GUI:** Change the Next Boot Device Select "**Host Management/Host Control**" Select "**CDROM**" from "**Next Boot Device**" drop down box. Click "**Save**"	

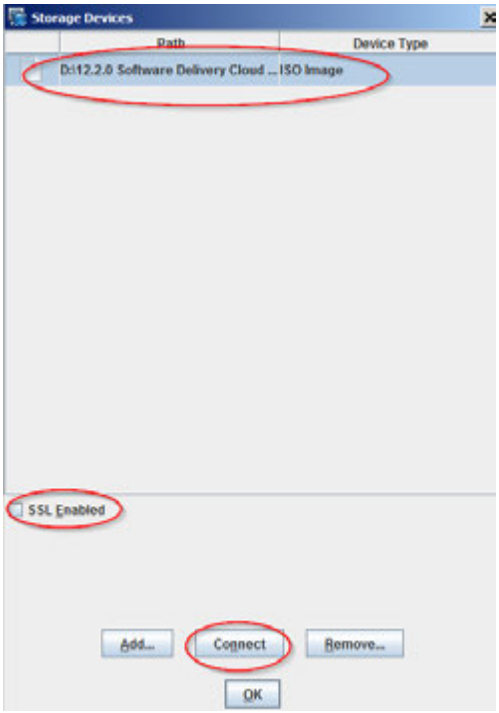
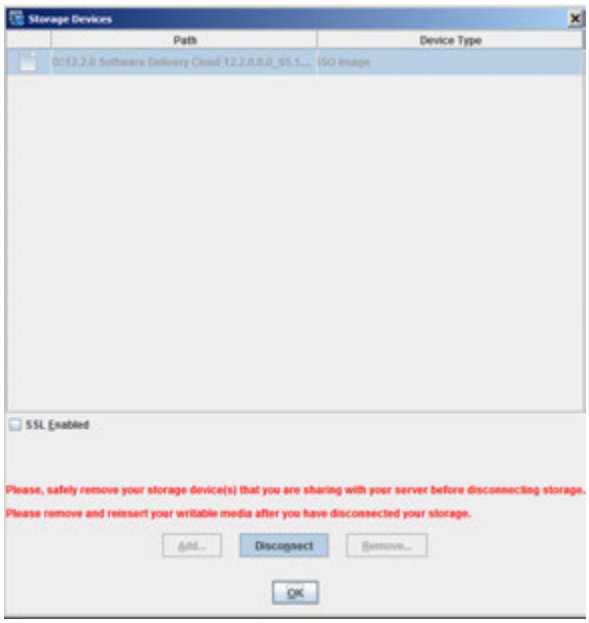
8.2.3: Mounting Virtual Media on Oracle RMS Servers

3.	**ILO Admin GUI:** Go to "**Host Management/Power Control**" Verify "**Host is currently on**" Note: If it's turned off, turn it back on.	
4. ☐	**ILO Remote Console:** Select "**KMVS/Storage**" from the top menu bar. Select "Add" button on next screen near bottom of the screen.	 

8.2.3: Mounting Virtual Media on Oracle RMS Servers

5. ☐	**ILO Remote Console:** Select desired **Image File** from files on your laptop/desktop client machine.	

8.2.3: Mounting Virtual Media on Oracle RMS Servers

6.	**ILO Remote Console:** 1. Select/highlight the ISO file 2. **Uncheck SSL Enabled** checkbox before connecting to the TVOE iso. 3. Click **Connect** 4. Click **OK**	 
THIS PROCEDURE HAS BEEN COMPLETED		

8.3 HARDWARE SETUP (BIOS CONFIGURATION)

Reference material:

TPD Initial Product Manufacture, Release 6.7.2+

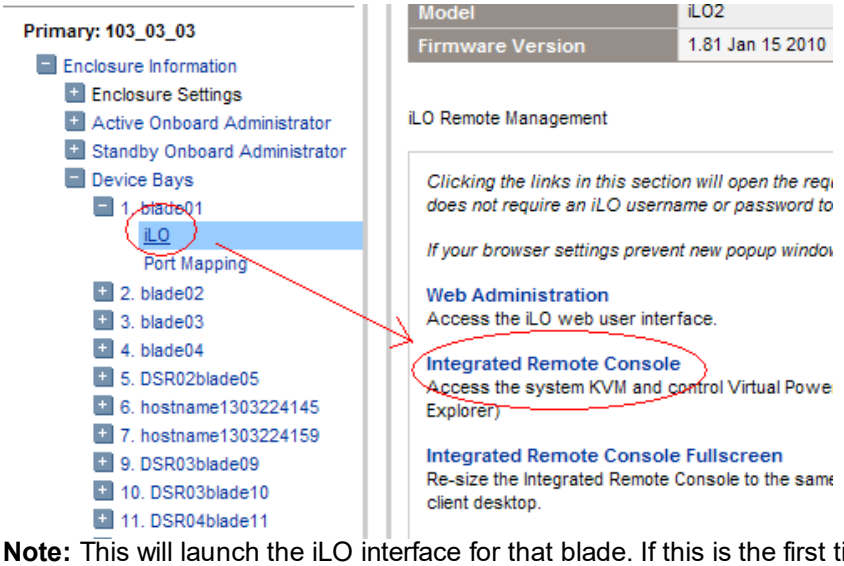
Tekelec Platform 7.0.x Configuration Guide

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

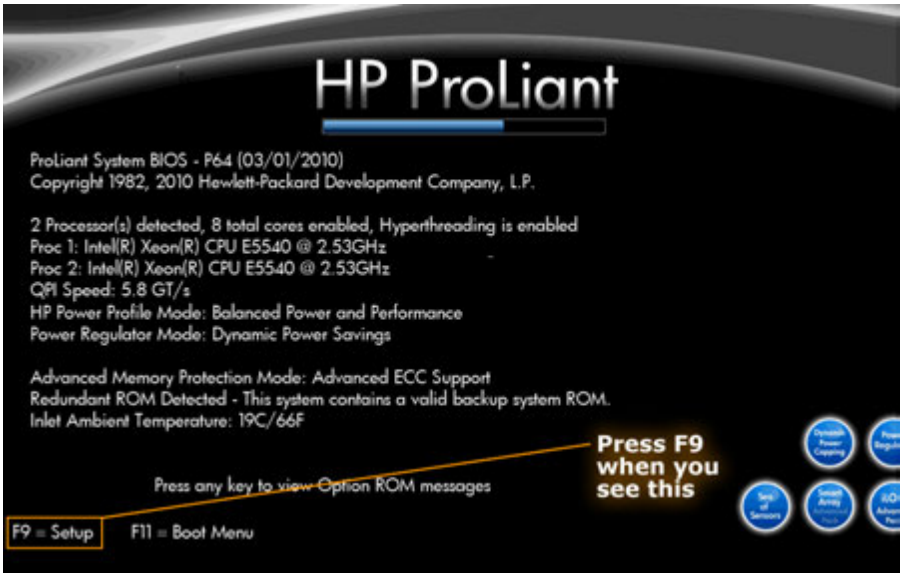
This procedure will configure HP BIOS settings for Gen 8 Blade and RMS.

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

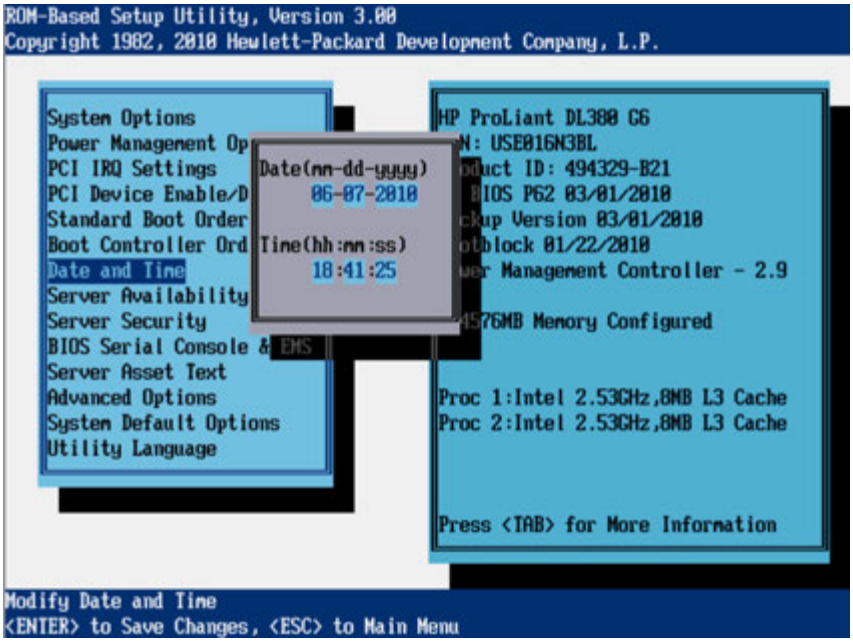
8.3.1:BIOS Settings for HP Gen 8 Blade and Rack Mount Servers

Step	In this procedure you will configure BIOS settings for HP hardware.	
1. ☐	Access the HP server's console.	Connect to the server's console using one of the access methods described in ***Section 8.1.1***
2. ☐	Access the HP server's console according to its hardware type	For Rack Mount Servers (RMS), connect to the server's console using one of the access methods described in ***Section 10.1*** For Blade servers: a. Navigate to the IP address of the active OA. Login as an administrative user. b. Navigate to **Enclosure Information > Device Bays ><Blade 1>> iLO** c. Click on **Integrated Remote Console**  **Note:** This will launch the iLO interface for that blade. If this is the first time the iLO is being accessed, you will be prompted to install an add-on to your web browser, follow the on screen instructions to do so.

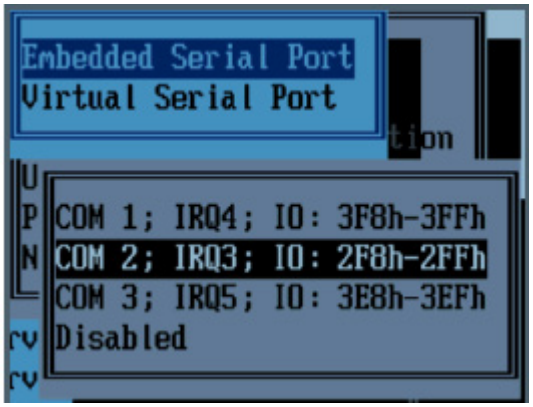
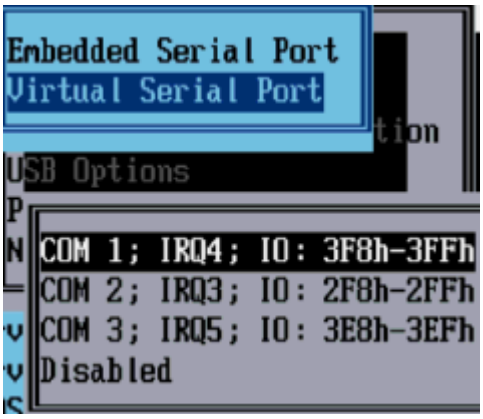
8.3.1:BIOS Settings for HP Gen 8 Blade and Rack Mount Servers

3. ☐	Access the Server BIOS	Reboot the server. **For Blade and RMS**, this can be achieved by selecting **Cold Boot** from under the Integrated Console's **Power Management→Server Power** menu. **For RMS**, this can also be achieved by pressing and holding the power button until the server turns off, then after approximately 5-10 seconds press the power button to enable power. As soon as you see **F9=Setup** in the lower left corner of the screen, press **[F9]** to access the BIOS setup screen. You may be required to press [F9] 2-3 times. The F9=Setup will change to F9 Pressed once it is accepted. See example below.  **Expected Result:** ROM-Based Setup Utility is accessed and the ROM-Based Setup Utility menu will be displayed.

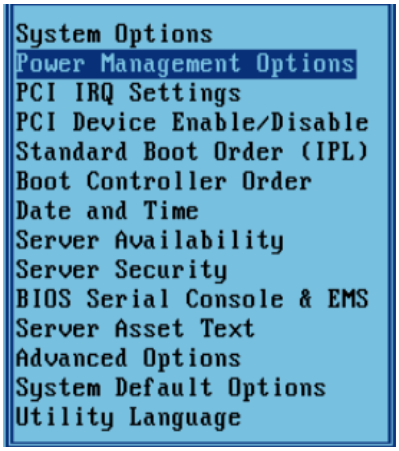
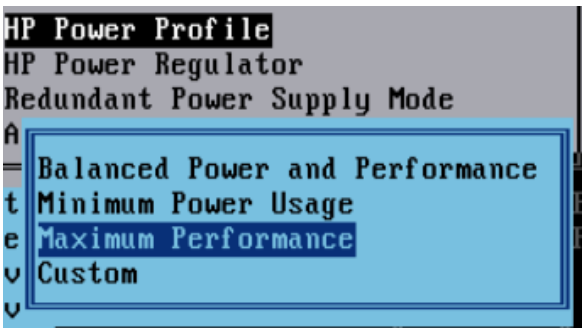
8.3.1:BIOS Settings for HP Gen 8 Blade and Rack Mount Servers

4. ☐	Set Server CMOS Clock	Scroll to *Date and Time* and press **[ENTER]** Set the date and time and press **[ENTER]**.  Correct Time & Date is set.

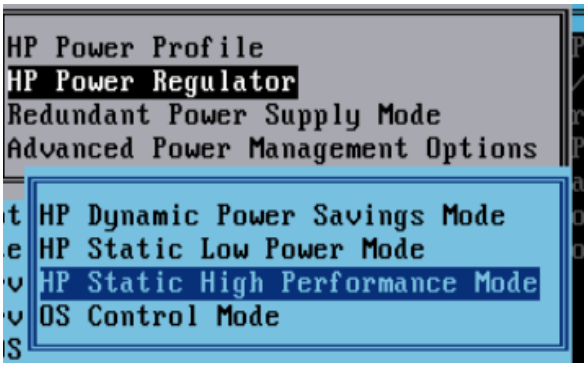
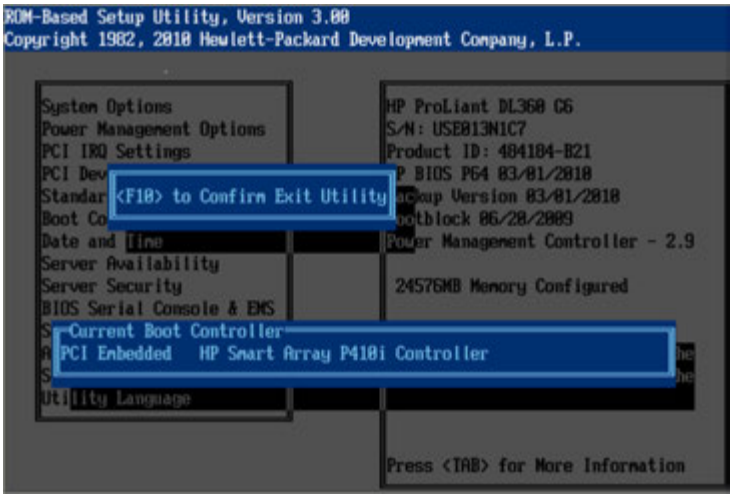
8.3.1:BIOS Settings for HP Gen 8 Blade and Rack Mount Servers

5. ☐	Configure iLO serial port settings ***(RMS Only)***	For RMS only, the serial ports on HP DL360 G8 rack mount servers need to be configured so the serial port used by the BIOS and TPD are connected to the "VSP" on the iLO. This will allow 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 "syscheck -v hardware serial" test will fail. Select **System Options** option and press **[ENTER]**. Select **Serial Port Options** option and press **[ENTER]**. Change **Embedded Serial Port** to **COM2** and press **[ENTER]**.  Change **Virtual Serial Port** to **COM1** and press **[ENTER]**.  Press <ESC> two times

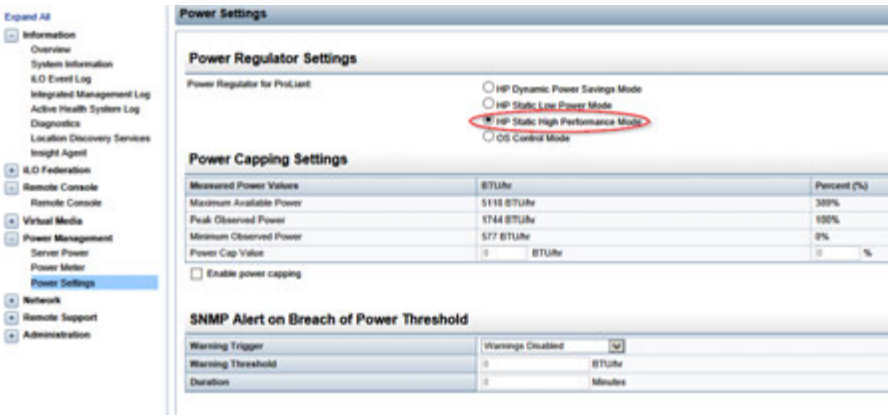
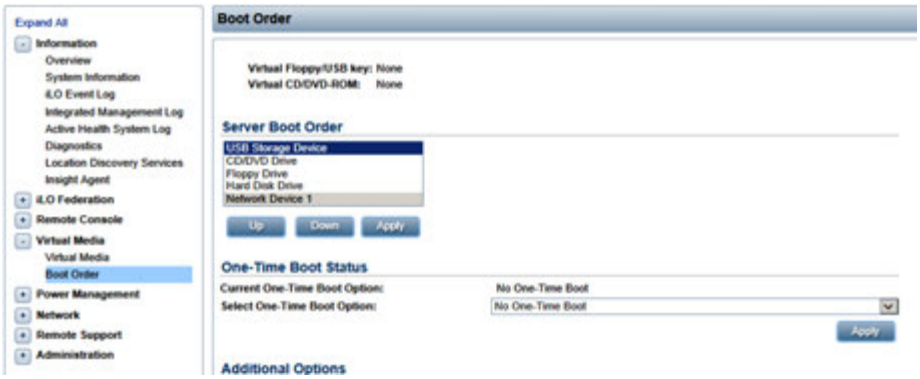
8.3.1:BIOS Settings for HP Gen 8 Blade and Rack Mount Servers

6. ☐	Configure Power Profile settings	The Power Profile on HP servers need to be configured for optimum software performance on both RMS and blade hardware. Select **Power Management Options** option and press **[ENTER]**.  Select **HP Power Profile** option and press **[ENTER]**.  Change it to **Maximum Performance** and press **[ENTER]**. 

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

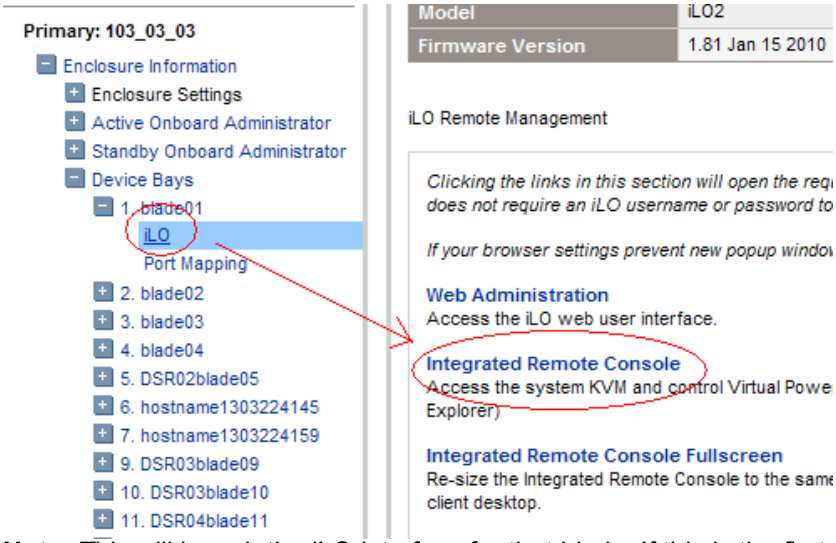
7. ☐	Configure Power Regulator settings	The Power Regulator on HP servers need to be configured for optimum performance on both RMS and blade hardware. Still under **Power Management Options**… Select **HP Power Regulator** option and press **[ENTER]**. *Note:* A note may appear to say certain processors 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	Press <ESC> two times Press **[F10]** to save the configuration and exit. The server will reboot.  **Expected Result:** Settings are saved and server reboots.

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

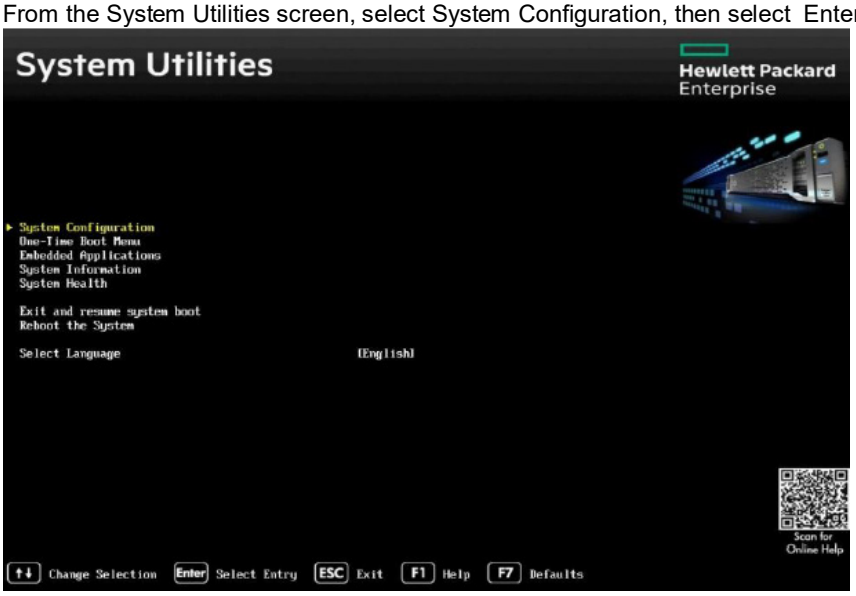
9. ☐	Confirm the HP server's Power Regulator setting.	If not already connected to the server's iLO, connect using 8.1.1 Accessing the iLO VGA Redirection Window for HP. On the HP Server's iLO: 1. Navigate to **Power Management→Power Settings** 2. Confirm **Power Regulator for ProLiant** is set to: **'HP Static High Performance Mode'** 
10. ☐	**Server ILO:** Verify the Boot Order	From left tree menu Click: **Virtual Media > Boot Order**  **Note 1:** The boot order should look like the above snapshot unless the customer has specified otherwise.
THIS PROCEDURE HAS BEEN COMPLETED		

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

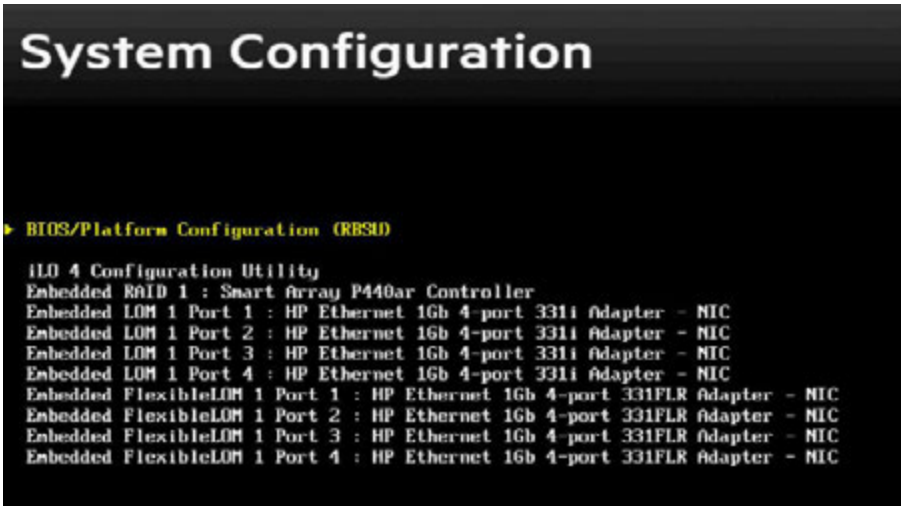
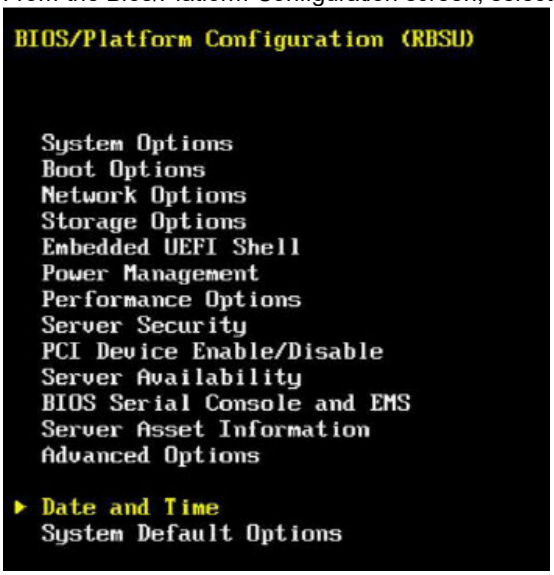
8.3.2:BIOS Settings for HP Gen 9 Blade and Rack Mount Servers

Step	In this procedure you will configure BIOS settings for HP hardware.	
1. ☐	Access the HP server's console.	Connect to the server's console using one of the access methods described in ***Section 8.1.1***
2. ☐	Access the HP server's console according to its hardware type	For Rack Mount Servers (RMS), connect to the server's console using one of the access methods described in ***Section*** For Blade servers: a. Navigate to the IP address of the active OA. Login as an administrative user. b. Navigate to **Enclosure Information > Device Bays ><Blade 1>> iLO** c. Click on **Integrated Remote Console**  **Note:** This will launch the iLO interface for that blade. If this is the first time the iLO is being accessed, you will be prompted to install an add-on to your web browser, follow the on screen instructions to do so.

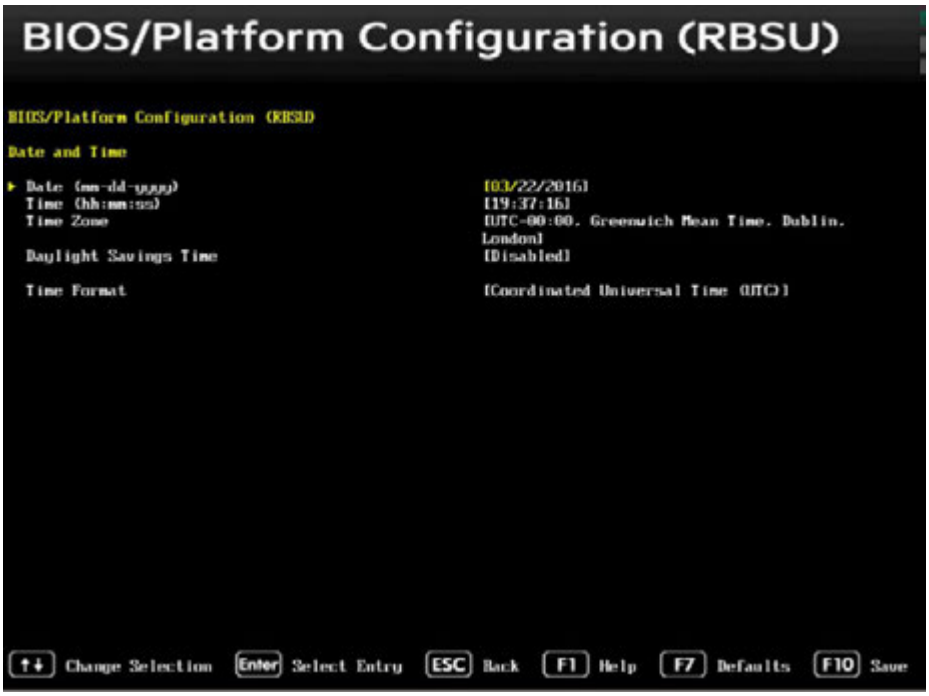
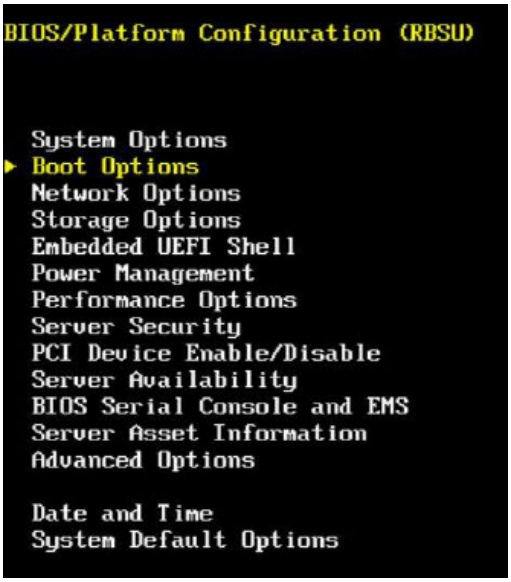
8.3.2:BIOS Settings for HP Gen 9 Blade and Rack Mount Servers

3. ☐	Access the Server BIOS	Reboot the server. **For Blade and RMS**, this can be achieved by selecting **Cold Boot** from under the Integrated Console's **Power Management→Server Power** menu. **For RMS**, this can also be achieved by pressing and holding the power button until the server turns off, then after approximately 5-10 seconds press the power button to enable power. As soon as you see `F9=Setup` in the lower left corner of the screen, press **[F9]** to access the BIOS setup screen. You may be required to press [F9] 2-3 times. The F9=Setup will change to F9 Pressed once it is accepted. See example below.  **Expected Result:** System Utilities screen will display
4. ☐	System Utilities Configuration	From the System Utilities screen, select System Configuration, then select Enter 

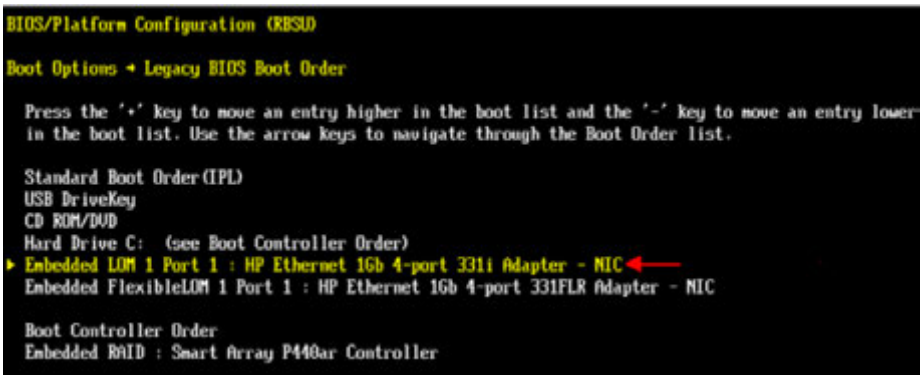
8.3.2:BIOS Settings for HP Gen 9 Blade and Rack Mount Servers

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

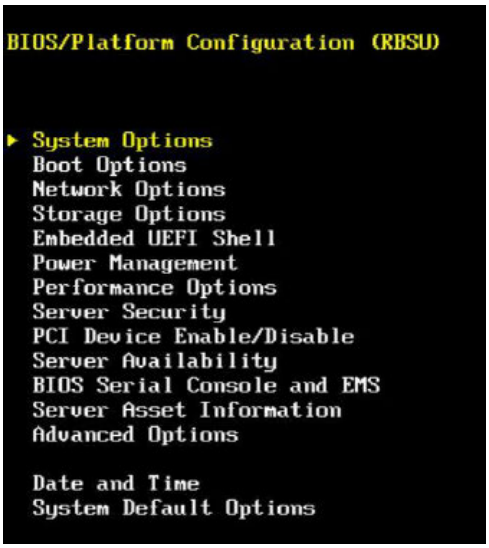
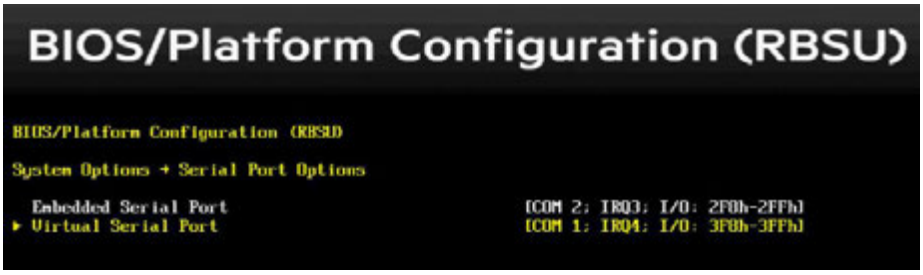
8.3.2:BIOS Settings for HP Gen 9 Blade and Rack Mount Servers

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

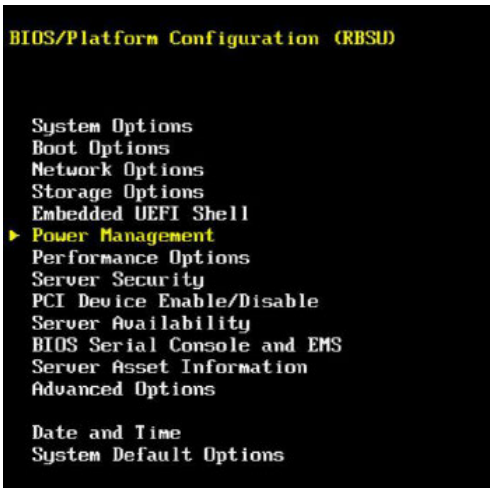
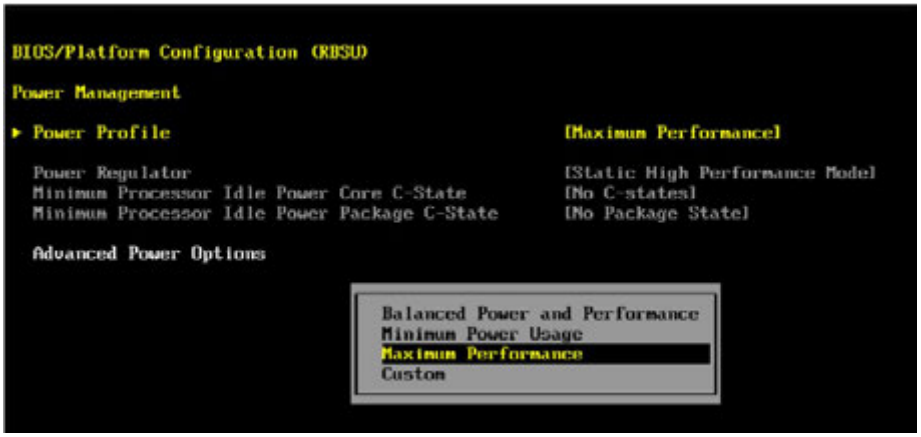
8.3.2:BIOS Settings for HP Gen 9 Blade and Rack Mount Servers

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

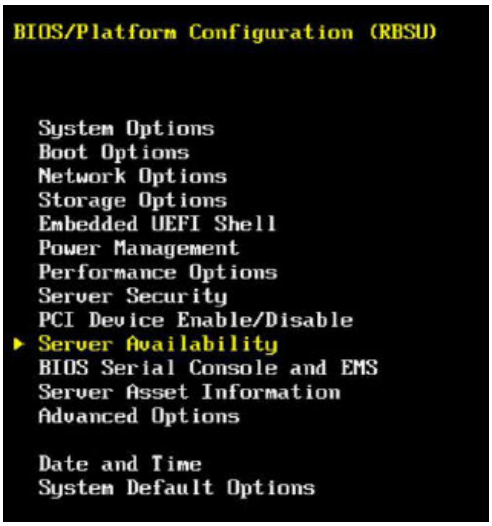
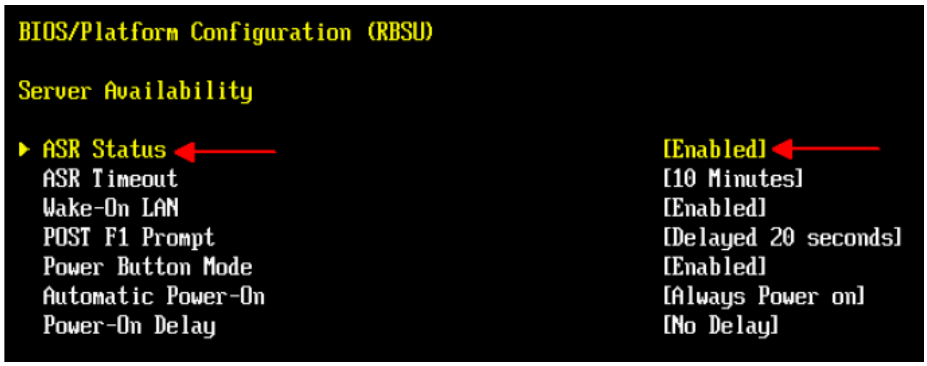
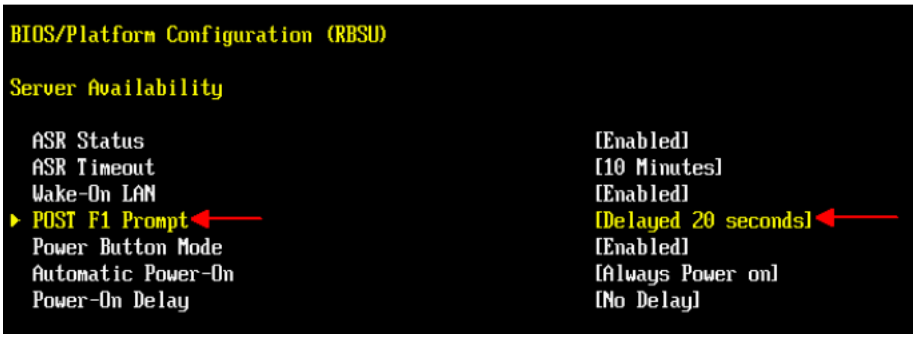
8.3.2:BIOS Settings for HP Gen 9 Blade and Rack Mount Servers

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

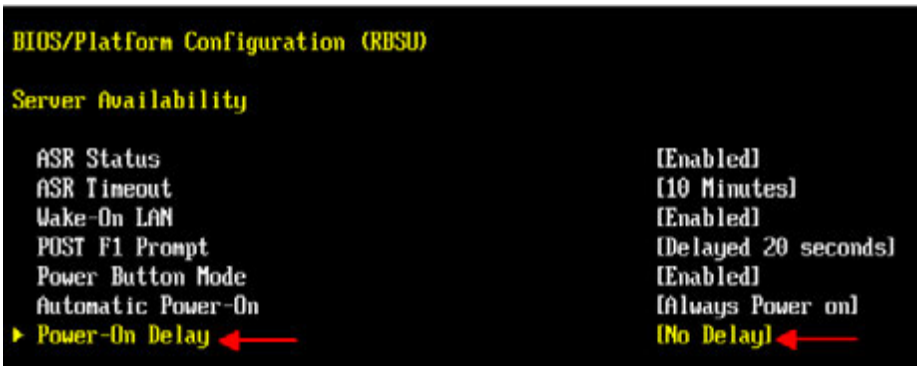
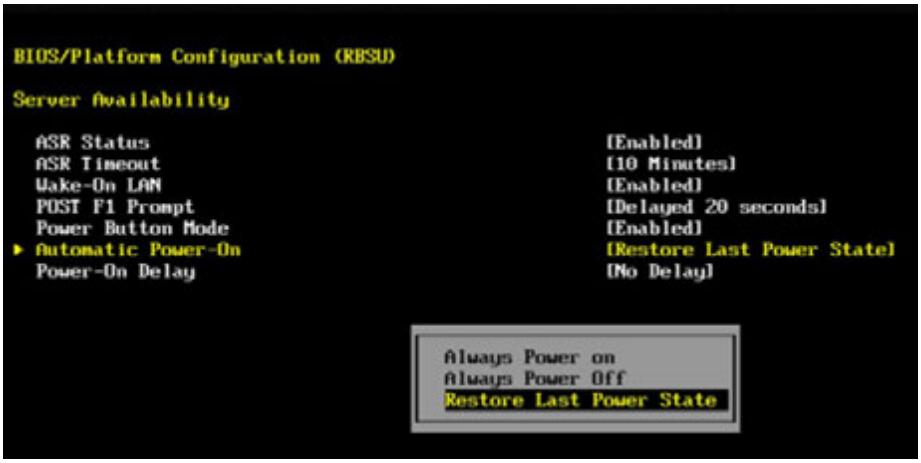
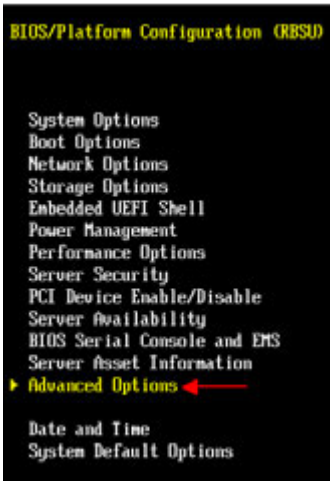
8.3.2:BIOS Settings for HP Gen 9 Blade and Rack Mount Servers

14. ☐	System Utilities Configuration	From the Bios/Platform Configuration screen, select Power Management Option and press enter. 
15. ☐	System Utilities Configuration	From the Power Management screen, set Power Profile to Maximum Performance, then select F10 to save your changes. Then select ESC to return to the Bios/Platform Configuration screen. 

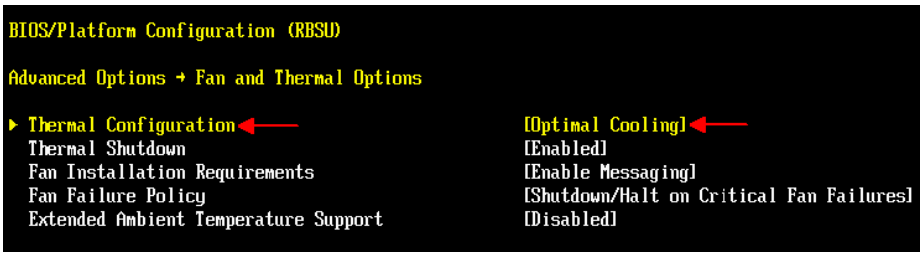
8.3.2:BIOS Settings for HP Gen 9 Blade and Rack Mount Servers

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

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

19. ☐	System Utilities Configuration	Set Power-On Delay to No Delay. 
20. ☐	System Utilities Configuration	Set Automatic Power-On to Restore Last Power State, then select F10 to save your changes. After saving, select ESC to return to the Bios/Platform Configuration screen. 
21. ☐	System Utilities Configuration	From the Bios/Platform Configuration screen, select Advanced Options and press Enter. 

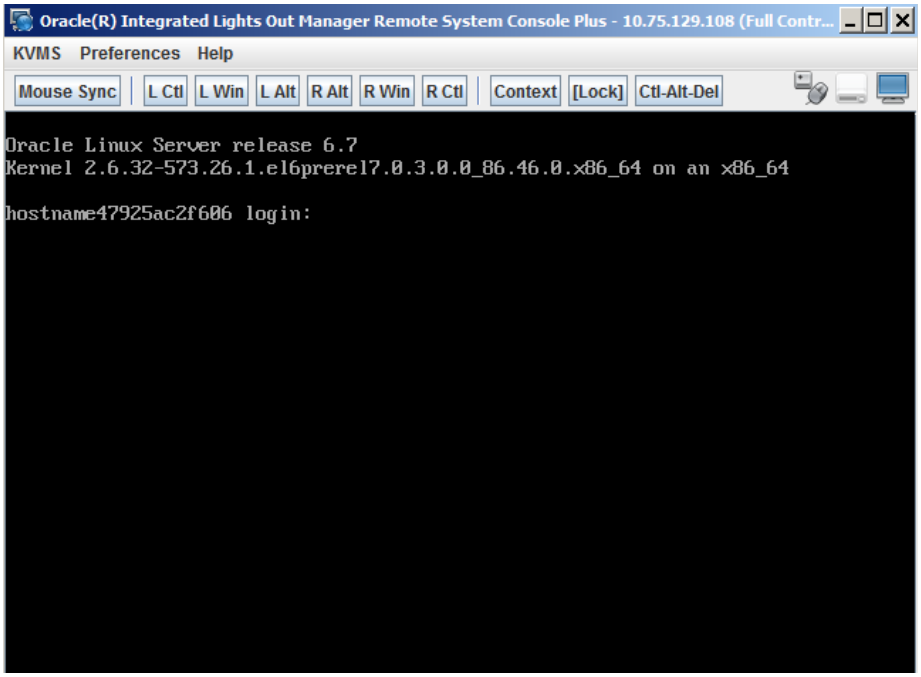
8.3.2:BIOS Settings for HP Gen 9 Blade and Rack Mount Servers

22. ☐	System Utilities Configuration	Set Thermal Configuration to Optimal Cooling, then select F10 to save your changes. After saving, select ESC to return to the Bios/Platform Configuration screen.  Select ESC to return to the System Utilities screen.
THIS PROCEDURE HAS BEEN COMPLETED		

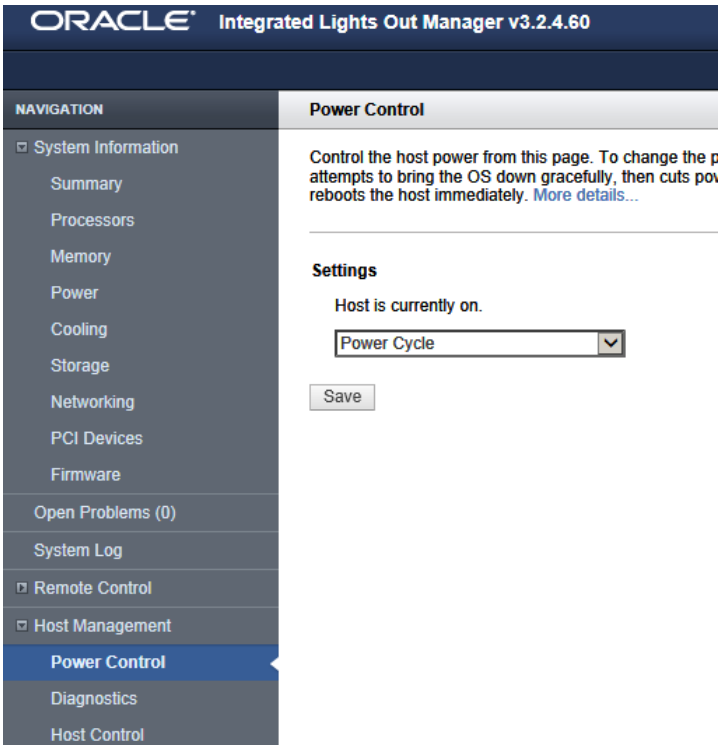
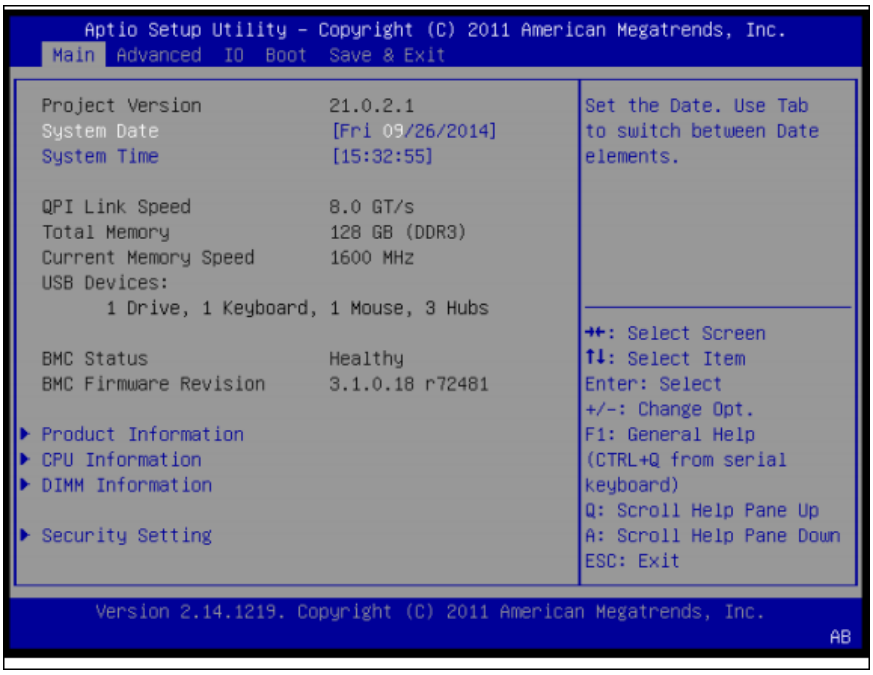
8.3.3 BIOS Settings for Oracle RMS Servers

This procedure will configure BIOS settings for Oracle Rack Mount Servers.

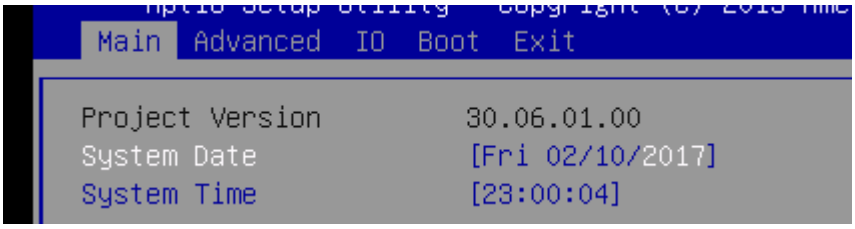
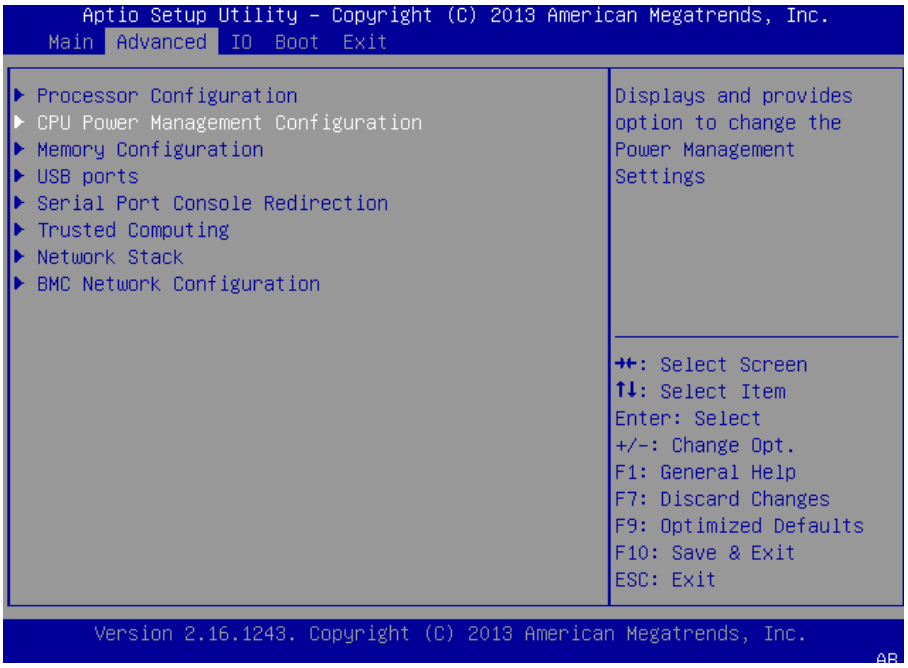
8.3.3:BIOS Settings for Oracle Rack Mount Servers

Step	In this procedure you will configure BIOS settings for Oracle RMS hardware.	
1. ☐	Access the Oracle server's console.	Connect to the server's console as per ***Section 8.1.2*** 

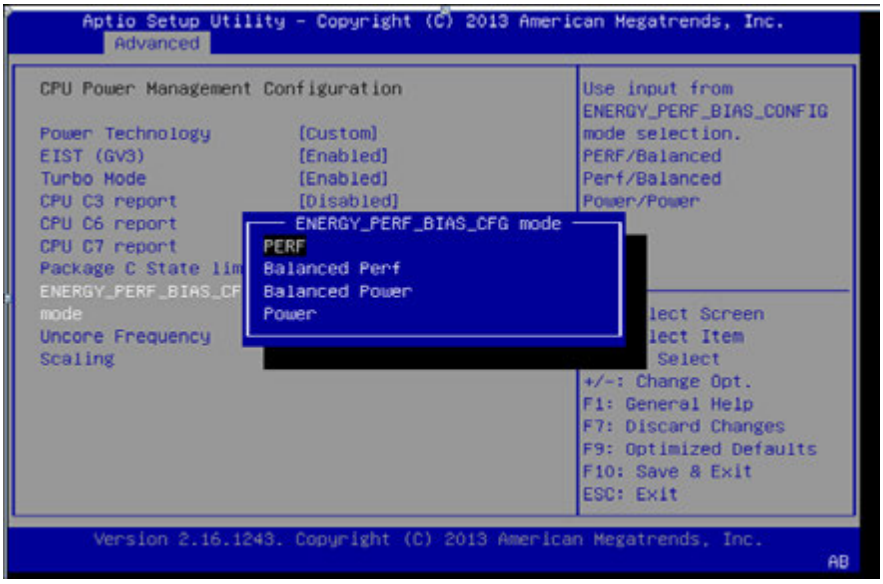
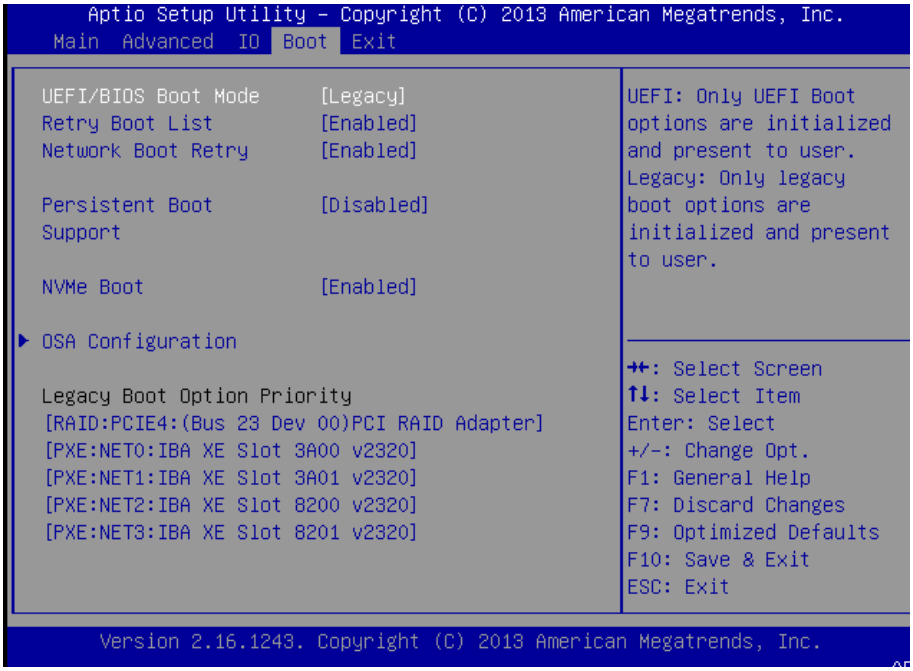
8.3.3:BIOS Settings for Oracle Rack Mount Servers

2. ☐	Reboot the server from the iLOM	Navigate to Host Management→Power Control and choose “power Cycle” in the settings and “Save” to reboot the server. 
3. ☐	Oracle server’s console Reboot the server and press F2 Key	After the server is powered on, press the F2 key when prompted to access the Setup Utility. 

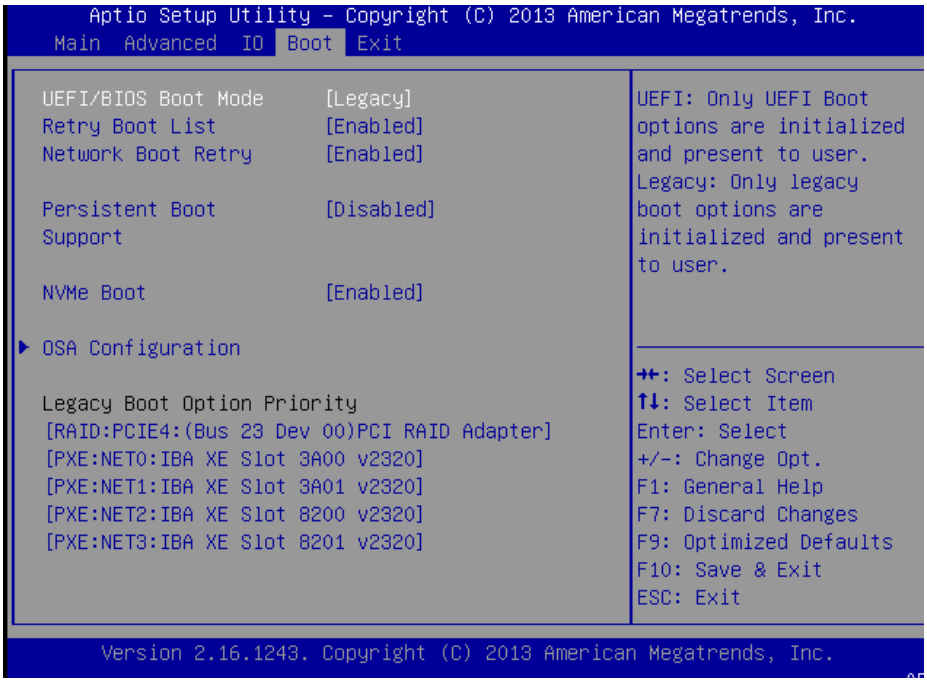
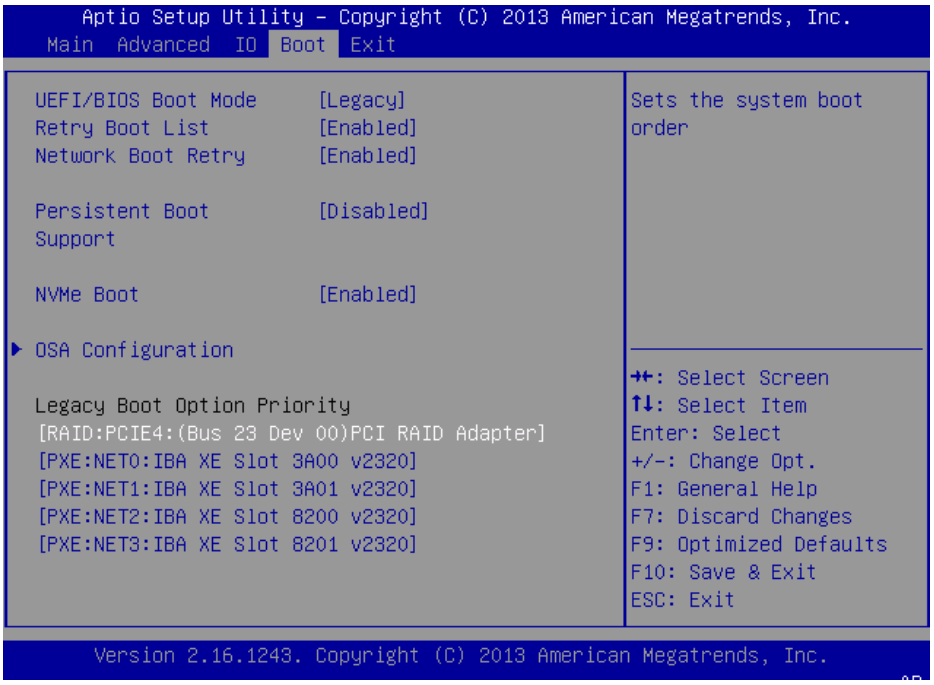
8.3.3:BIOS Settings for Oracle Rack Mount Servers

4. ☐	Oracle server's console	With "System Date" selected hit "enter" to move forward and set the server date and time to GMT (Greenwich Mean Time). 
5. ☐	Oracle server's console	Go to the Advanced Menu→CPU Power Management Configuration 

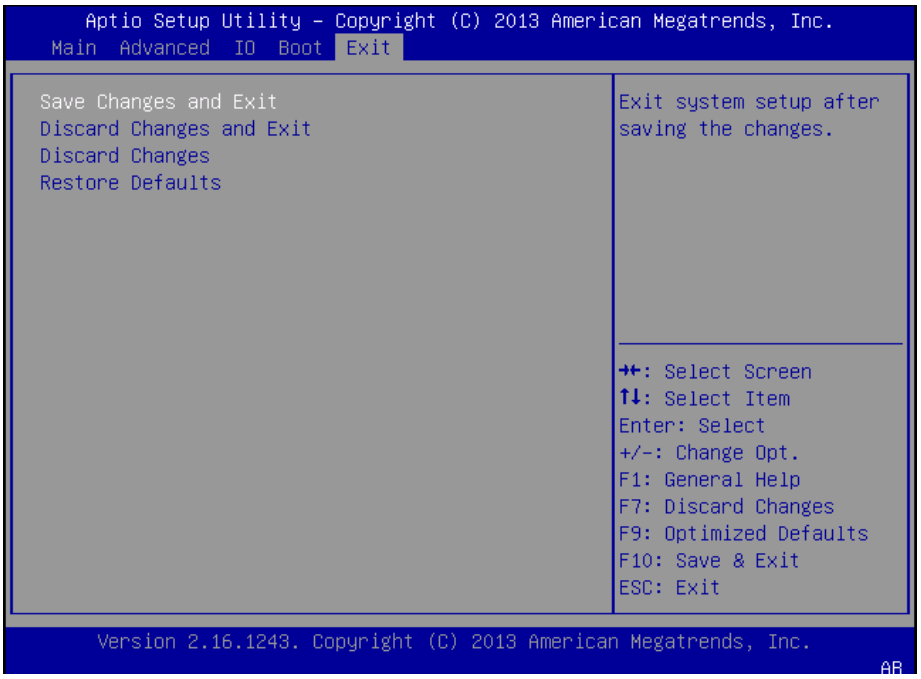
8.3.3:BIOS Settings for Oracle Rack Mount Servers

6. ☐	Oracle server's console	From CPU Power Management Configuration scroll to "ENERGY_PERF_BIAS_CFG". If Energy Performance is not set to [Perf], select "Perf" and press Enter. 
7. ☐	Oracle server's console	Go to the Boot Menu. 

8.3.3:BIOS Settings for Oracle Rack Mount Servers

8. ☐	Oracle server's console	Go to the Boot Menu. 
9. ☐	Oracle server's console	Under Legacy Boot Option Priority, verify the RAID Adapter is listed first. If not, highlight it and use + key to move it to the top of the list. 

8.3.3:BIOS Settings for Oracle Rack Mount Servers

10. ☐	Oracle server's console	Go to the **Exit** menu. Select "**Save Changes and Reset"** 
THIS PROCEDURE HAS BEEN COMPLETED		

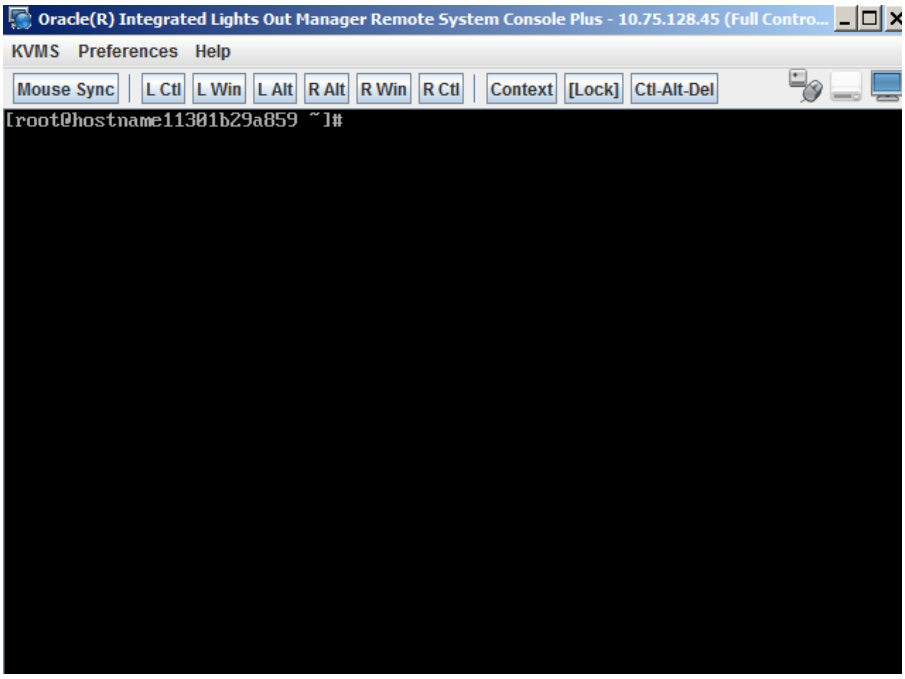
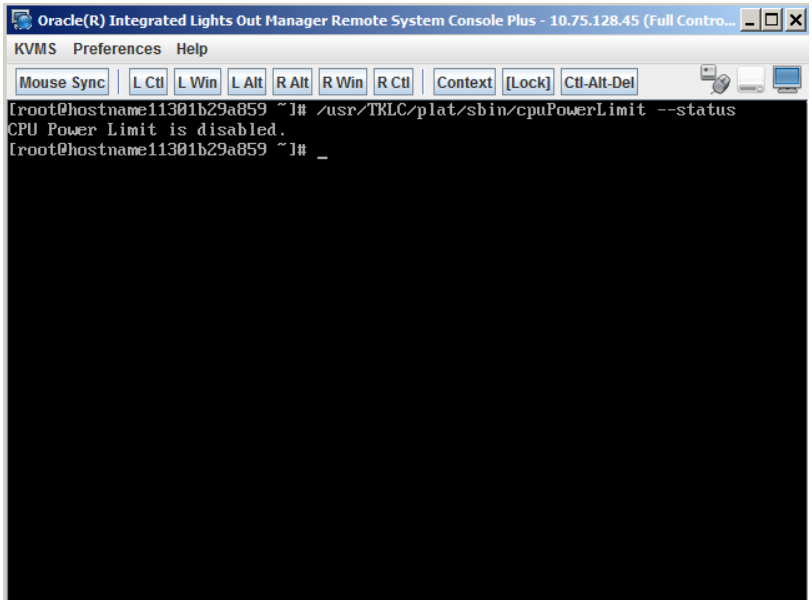
8.3.4 Configuring CPU Power Limit on Netra X5-2 Servers

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/or writing out to the current BIOS values and can take 10-30 seconds to complete each action.

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

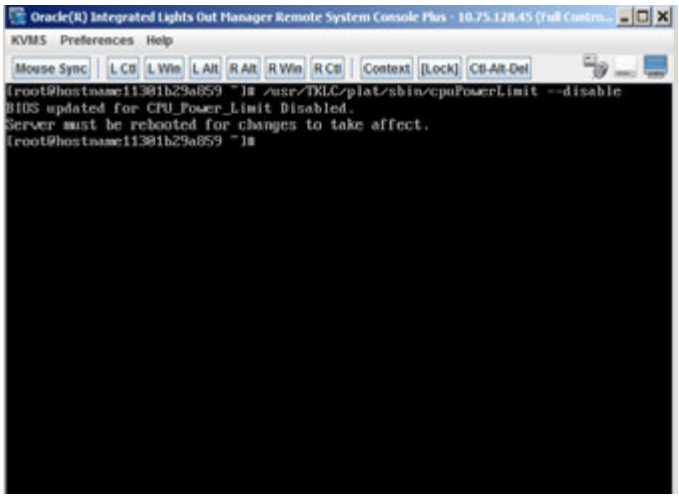
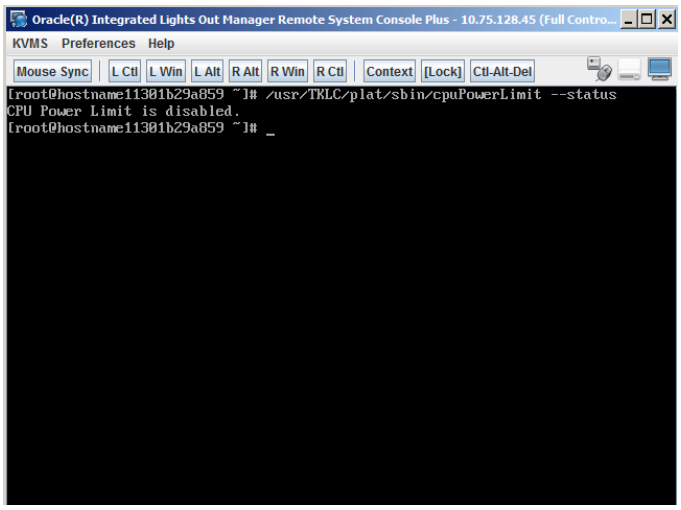
Step	In this procedure you will configure the CPU Power Limit for Netra X5-2 Servers Note: This procedure is performed after the Platform software has been installed.

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

1. ☐	Access the Oracle server's console.	Connect to the server's console as per section 8.1.2: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

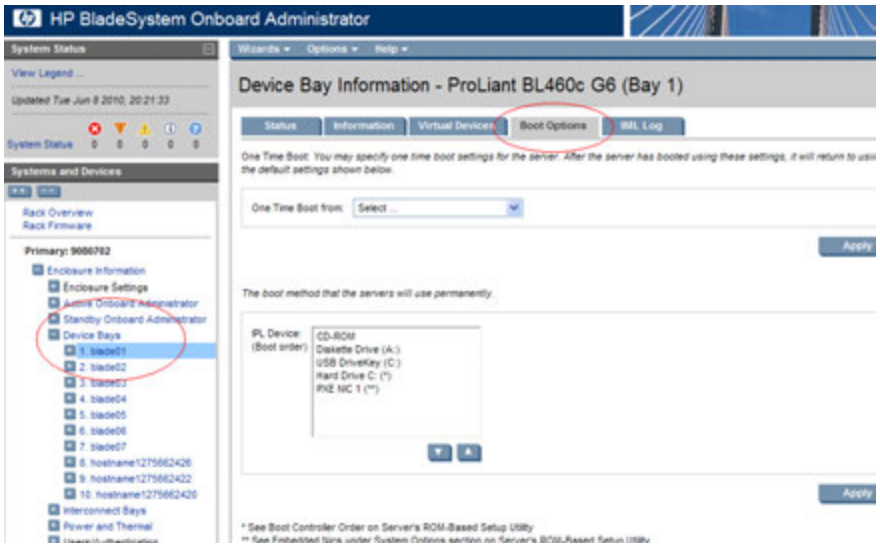
8.3.4: Configuring CPU Power Limit on Netra X5-2 Servers

3. ☐	Remote Console command line: enable settings	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 ~]#`
		Reboot the server for the new setting to take effect.
		`[root@X52-mpe-1a ~]# /usr/TKLC/plat/sbin/cpuPowerLimit -status`
		`CPU Power Limit is enabled.`
		`[root@X52-mpe-1a ~]#`
		CPU_PowerLimit Enabled

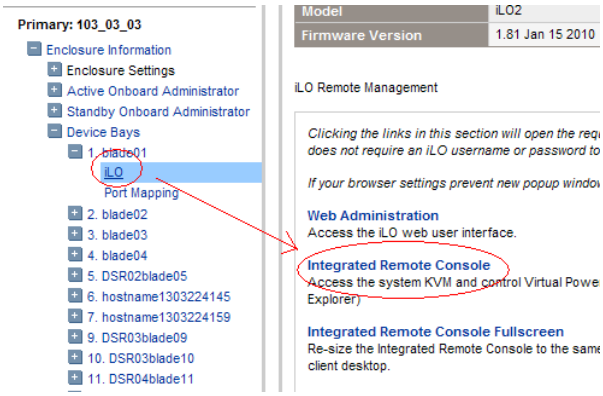
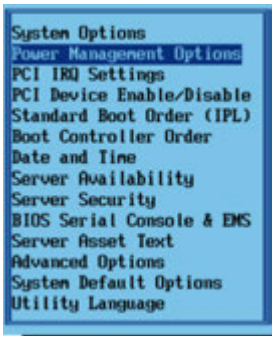
4. ☐	Remote Console command line: disable settings	To disable CPU Power Limit log into the server as root and run: **/usr/TKLC/plat/sbin/cpuPowerLimit –disable**  Reboot the server for the new setting to take effect.  CPU_PowerLimit Disabled
THIS PROCEDURE HAS BEEN COMPLETED		

8.3.5 Using c-Class Enclosure OA to Update Application Blade's BIOS Settings

8.3.5: Using c-Class Enclosure OA to Update Application Blade's BIOS Settings

STEP #	This procedure will provide the steps to confirm and update the BIOS configuration on Blade servers using the C-Class enclosure OA. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
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	Navigate to **Enclosure Information** -> **Device Bays** -> **<Blade 1>** Click on **Boot Options** Tab 
3. ☐	**OA:** Verify/update Boot device Order	Verify that the Boot order is as follows. If it is not, use the up and down arrows to adjust the order to match the picture below, then click on "**Apply**". IPL Device: (Boot order) CD-ROM Diskette Drive (A:) USB DriveKey (C:) Hard Drive C: (*) PXE NIC 1 (**)

8.3.5: Using c-Class Enclosure OA to Update Application Blade's BIOS Settings

4. ☐	**OA:** Access the Blade iLO	Navigate to **Enclosure Information** -> **Device Bays** -> **<Blade 1>** -> **iLO** Click on **Integrated Remote Console**  This will launch the iLO interface for that blade. If this is the first time the iLO is being accessed, you may be prompted to install an add-on to your web browser, follow the on screen instructions to do so.
5. ☐	**OA:** restart the blade and access the bios	You might be prompted with a certificate security warning, just press continue. Once a prompt is displayed, login onto the blade using the "root" username. Once logged in, Reboot the server (using the "reboot" command). After the server is powered on and is booting , press **F9** to access the BIOS setup screen (as soon as you see <F9=Setup> in the lower left corner of the screen).
6. ☐	**OA:** Update bios settings	Scroll down to *Power Management Options* and press **Enter** Select *HP Power Profile* and press **Enter** Scroll down to *Maximum Performance* and press **Enter**   Press **<Esc>** twice to return to exit the BIOS setup screen and press **F10** to confirm Exiting the utility. The blade will reboot afterwards
7. ☐	**OA:** Repeat for the remaining blades	Repeat Steps 2 through 6 for the remaining blades. Once done, exit out of the OA GUI.
THIS PROCEDURE HAS BEEN COMPLETED		

9. TROUBLESHOOTING THE INSTALLATION

This chapter describes how to troubleshoot the installation.

9.1 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 (On-line 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 to be used for restore operation (since 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. Once Policy Management software is installed on a server, you will find the files in the directory /usr/TKLC/plat/etc/netconfig/.

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.

9.2 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 will be 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.