Oracle® Communications Policy Management

Bare Metal Installation Guide 12.1.x

E70153-01
December 2015

Copyright © 2015 Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

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

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

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. INTRODUCTION 6
1.1 Purpose and Scope 6
1.2 References 7
1.3 Acronyms 8
1.4 Terminology 9

2. GENERAL DESCRIPTION 10
2.1 Starting Points for Installation 10
2.2 Networking (c-Class) 11
2.3 Networking Options (RMS) 11
2.4 Installation Time Estimates 11

3. INSTALL PLANNING 13
3.1 IP Network Survey 13
3.2 Network Configuration files 13
3.3 Required Materials 13
3.4 Acquiring Software 14
3.5 Acquiring Firmware 17
3.6 Preparations before going to Site 18
3.7 Cautions for on-site activities 19
3.8 FAQ for c-Class Installations 19
3.9 Logins/Passwords 20
3.10 Optional Features Planning 20

4. INSTALLATION (AND NETWORKING) IN A C-CLASS ENVIRONMENT 20
4.1 PM&C Installation 20
Procedure 1: Install TVOE 3.0.0 on Management Server (DL380) 21
Procedure 2: Upgrade DL380 Server Firmware 28
Note: Access to the HP 2.2.8 Firmware Upgrade Guide may require enablement form Oracle Support 28
Procedure 3: TVOE/Management Server Network Configuration 29
Procedure 4: Install PM&C Application 37
4.2 Complete the PM&C Installation 42
Procedure 5: Configure the PM&C Application 42
4.3 HP C-7000 Enclosure Configuration 47
Procedure 6: Configure the OA IP Addresses (Front Panel Display) 47
Procedure 7: Configure the OA IP Addresses (Configuration Wizard) 48
Procedure 8: Adding the Cabinet and the Enclosure to the PM&C 48
Procedure 9: Configuring 6120XG/6125XLG Enclosure Switches 51
4.4 Configuring the Application Blades 52
Procedure 10: Update Application Blade Firmware 52
Procedure 11: Confirm/Update Application Blade's BIOS Settings 53
Procedure 12: Loading Software Images onto the PM&C 55
Procedure 13: IPM Blades via PM&C 58
4.5 Install Policy Application Software 62
Procedure 14: Install the Application Software on Blades using PM&C 62
4.6 Establish Networking to Customer Network 65
4.6.1 Connect PM&C iLO to Customer Network 65
4.6.2 Connect c-Class system to Customer Network 66

5. INSTALLING AN HP RMS ENVIRONMENT 67
5.1 Preparation Procedures 67
Procedure 15: Configure DL380 iLO Port 67
Procedure 16: Update Server Firmware 70

Note: Access to the HP 2.2.8 Firmware Upgrade Guide may require enablement form Oracle Support 70
Procedure 17: Configure BIOS 70
5.2 Software Installation (RMS) 73
Procedure 18: IPM of HP RMS Server 73
Procedure 19: RMS Application Software Installation 79

6. INSTALLING AN ORACLE X5-2 RMS ENVIRONMENT 84
6.1 Preparation Procedures 84
Procedure 20: Configure Initial ILOM IP address and BIOS Settings 84
Procedure 21: Update Server Firmware 89
Procedure 22: Configure Oracle X5-2 iLOM from GUI 90
6.2 Software Installation (RMS) 92
Procedure 23: IPM of Oracle X5-2 RMS Server 92
Procedure 24: RMS Application Software Installation 102

7. CONFIGURE POLICY APPLICATION SERVERS 107
7.1 Configure Network Topology 107
Procedure 25: Perform Initial Configuration of Policy Servers Platcfg 107
Procedure 26: Perform Initial Configuration of the Policy Servers CMP GUI 113
Procedure 27: CMP Site1 Cluster Topology Configuration 116
Procedure 28: Topology Configuration of Additional Clusters 125
Procedure 29: SSH Key Exchanges to all Servers in the Topology 135
Procedure 30: Configure IP Routing on the MPE and MRA 137
7.2 Post Topology Configuration Tasks 142
7.3 Configure Policy Servers (and MRAs) 144
Procedure 31: Adding MPE and MRA to CMP Menu 144
Procedure 32: Configure MPE Pool on MRA (Policy Front End) 149
Procedure 33: Define and Add Network Elements 153
7.3.1 Load Policies and related Policy Data 157
7.3.2 Add a Data Source 157
7.3.3 Perform Test Call 158
7.4 Pre-Production Configurations 159
7.5 Tiered CMP SYSTEM 160
Procedure 34: Building a Tiered CMP System 162

8. SUPPORTING PROCEDURES AND INFORMATION 171
8.1 iLO (ILOM) Procedures 171
Procedure 35: Change iLO IP address from Console HP DL380 171
Procedure 36: Connect Laptop to iLO Port 172
Procedure 37: Access the HP iLO GUI 174
Procedure 38: Changing the HP iLO address from the iLO GUI 176
Procedure 39: Launching the Remote Console from the HP iLO GUI 178
Procedure 40: Virtual Mount an ISO image file from the HP iLO GUI 180
Procedure 41: Access the Oracle X5-2 iLO GUI 182
Procedure 42: Changing the Oracle X5-2 iLO address from the iLO GUI 184
Procedure 43: Launching the Remote Console from the Oracle X5-2 iLO GUI 186
Procedure 44: Virtually Mount an ISO image file from the Oracle X5-2 iLO GUI 189
Procedure 45: Launching the Remote Console using the OA (c-Class) 193
Procedure 46: SSH to the HP iLO and access the OS CLI 197
Procedure 47: SSH to the Oracle X5-2 iLOM and access the OS CLI 198
8.2 Additional Procedures 199
Procedure 48: Create a Bootable USB with TPD or TVOE ISO image 199
Procedure 49: Perform a Cluster File Sync 202
8.3 c-Class: Manufacturing IP Networking Configuration 204

8.3.1 Management VLAN 204
8.3.2 HP RMS Management Addresses 205
8.3.3 Application Default IP Addresses 207
8.3.4 External Default IP Addresses 207

APPENDIX A. DISCREPANCY LIST 208

APPENDIX B. ACCESSING ORACLE'S CUSTOMER SUPPORT SITE 209

1. INTRODUCTION

1.1 *PURPOSE AND SCOPE*

This document describes the procedures to install and configure Oracle Communications Policy Management Release 12.1.x on HP c-Class systems, HP Rack Mount Servers and Oracle X5-2 Rack Mount Servers. The audience for this document includes Oracle customers as well as these groups: Software System, Product Verification, Documentation, and Customer Service including Software Operations and First Office Application.

At the completion of this procedure, and assuming that the customer networking has been correctly configured, it should be possible to:

- Access the Management interfaces for the system from a customer lab
- Access the Management interfaces for the system from a remote access (Oracle office)
- Have a clear Alarms condition for the system
- Make a test call through the system

Work instructions provided may require further customization with respect to the target customer's network.

Release 12.1.x introduces support for the X5-2 Oracle Rack Mount Server (RMS) and compatibility with HP Gen-9 Rack Mount Servers and HP c-Class System Servers. The existing support for the HP Gen-6 and Gen-8 servers is continued.

1.2 *REFERENCES*

1.2.1

[1] E59722 - HP Solutions Firmware Upgrade Pack_Release 2.2.8_Release Notes*

[2] E59721 - HP Solutions Firmware Upgrade Pack, Upgrade Guide 2.2.8*

[3] E59723 - HP Solutions Firmware Upgrade Pack, Software Centric Release Notes 2.2.8

[4] E65467 - Oracle Firmware Upgrade Pack 3.1.5, Release Notes

[5] E65466 - Oracle Firmware Upgrade Pack Release 3.1.5 Upgrade Guide

[6] E53017 - TPD Initial Product Manufacture

[7] E53486 - Tekelec Platform 7.0.x Configuration Guide

[8] E53018 - TVOE 3.0.0.0.0 Software Upgrade Procedure

[9] E61655 - Policy and Charging Rules Function Installation Guide Release 11.5

[10]E62450 - Configuration Management Platform Wireless User's Guide Release 12.1.x

[11]E62447 - Platform Configuration User's Guide Release 12.1.x

[12]E62458 -SNMP User's Guide

These documents can be accessed at the following link

http://docs.oracle.com/en/industries/communications/

* The HP Solutions Firmware Upgrade Pack (HP FUP) is provided **for customers who bought their HP hardware through Oracle**. HP FUP firmware and documentation for Release 2.2.8 can be accessed on the internal Oracle HP FUP website. Contact Oracle Support for assistance if needed.

Locate Product Documentation on the Oracle Technology Network Site

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

1. Log into the Oracle Technology Network site at *http://docs.oracle.com*.

2. Under *Cloud,* click the link for *Industries* (on the left hand menu). Under *Industries* click the link for Oracle Communications documentation . The *Oracle Communications Documentation* window opens with *Tekelec* shown under *Platforms*. *Policy Management* will be shown under *Network Session Delivery and Control Infrastructure.*

3. Click **Oracle Communications Documentation->Platforms->Tekelec** for Platform related Documentation or **Oracle Communications Documentation-> Network Session Delivery and Control Infrastructure-> Policy Management** for Application related Documentation.

4. Navigate to your Product and then the Release Number, and click the *View* link (the *Download* link will retrieve the entire documentation set).

5. To download a file to your location, right-click the PDF link and select *Save Target As*.

1.3 *ACRONYMS*

An alphabetized list of acronyms used in the document:

Table 1. Acronyms

Acronym	Definition
BIOS	Basic Input Output System
BOM	Bill Of Materials
CD	Compact Disk
CMP	Configuration Management Platform
DVD	Digital Versatile Disc
EBIPA	Enclosure Bay IP Addressing
ECO	Engineering Change Order
FRU	Field Replaceable Unit
FUP	Firmware Upgrade Pack
GUI	Graphical User Interface
Gx	3GPP reference point between PCEF and PCRF
HP c-Class	HP blade server system
IE	Internet Explorer
iLO (ILOM)	Integrated Lights Out (Manager)
PFE	Policy Front End (also referred to as Multiprotocol Routing Agent
IPM	Initial Product Manufacture – the process of installing TPD on a hardware platform
IPv4	Internet Protocol version 4
Pv6	Internet Protocol version 6
MPE	Multimedia Policy Engine
MRA	Multiprotocol Routing Agent (also referred to as the Policy Front End (PFE)
NIC	Network Interface Card
NW-CMP	Network-Level CMP in a Multi-Level OAM Policy Deployment
OA	HP Onboard Administrator
OAM	Operations, Administration and Management
OCUDR	Oracel Communications User database Repsi
OS	Operating System (e.g. TPD or TVOE)
OTN	Oracle Technology Network
OVA	Open Virtualization Appliance
PCRF	Policy Charging andb Rules Function
PM&C	Platform Management & Configuration
PFE	Policy Front End (also referred to as the Multiprotocol Routing Agent (MRA)
S-CMP	Site-Level CMP in a Multi-Level OAM Policy Deployment
SFTP	Secure File Transfer Protocol
Sh	3GPP reference between the PCRF and Subscriber Profile Repository (SPR)
SNMP	Simple Network Management Protocol
SPP	Service Pack ProLiant
SPR	Subscriber Profile Repository
TPD	Tekelec Platform Distribution
TVOE	Tekelec Virtualization Operating Environment
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VSP	Virtual Serial Port

1.4 *TERMINOLOGY*

Multiple server types may be involved with the procedures in this manual. Therefore, most steps in the written procedures begin with the name or type of server to which the step applies. For example:

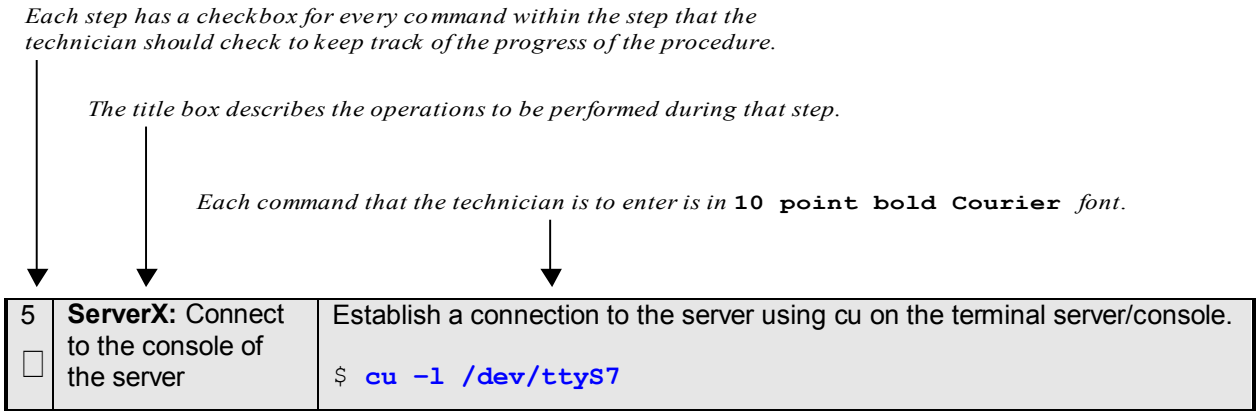


Figure 1. Example of an instruction that indicates the server to which it applies

Management Server	HP Proliant DL 380 G9 server (RMS) deployed with HP c-Class used to host PM&C application
PM&C Application	PM&C is an application that provides platform-level management functionality for HP system , such as the capability to manage and provision platform components of the system so it can host applications.
Configuration Management Platform (CMP)	(CMP) A centralized management interface to create policies, maintain policy libraries, configure, provision, and manage multiple distributed MPE policy server devices, and deploy policy rules to MPE devices. The CMP has a web-based interface.
Multimedia Policy Engine (MPE)	A high-performance,high-availability platform for operators to deliver and manage differentiated services over high-speed data networks. The MPE includes a protocol-independent policy rules engine that provides authorization for services based on policy conditions such as subscriber information, application information, time of day, and edge resource utilization
Multi-Protocol Routing Agent (MRA) **Now known as the Policy Front End (PFE)**	Scales the Policy Management infrastructure by distributing the PCRF load across multiple Policy Server (MPE) devices

2. GENERAL DESCRIPTION

This document defines the steps to execute the initial installation of the Policy 12.1.x application on supported Policy Hardware platforms. Supported platforms include:

[1] HP C-class Blade Server
[2] HP DL380 Rack Mount Server
[3] Oracle X5-2 Rack Mount Server

Policy 12.1.x installation paths are shown in the figures below. The general timeline for all processes to perform a software installation/configuration is also included below.

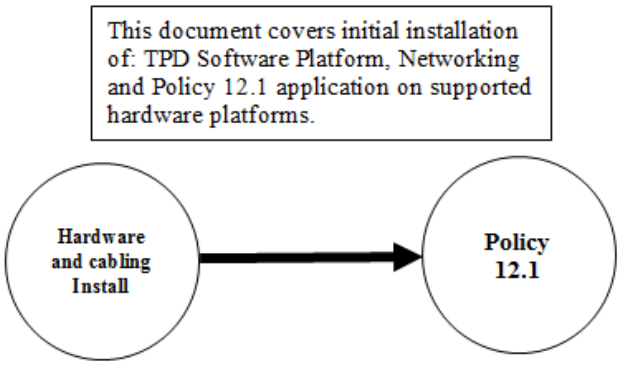


Figure 2: Policy 12.1.x Application Installation Path

2.1 STARTING POINTS FOR INSTALLATION

There are two starting points for the Installation activity:

1. Equipment ordered from Oracle, and pre-configured from Oracle, and installed by Oracle or Oracle contractor
2. Equipment ordered by the customer, and installed by another party

In the first case, there will be a known pre-configuration of the equipment that can reduce the installation time. See “Manufacturing IP Networking Configuration” section for information. Also, the internal cabinet cabling will be verified.

In the second case, more time will be required to verify the hardware install and cabling before starting. Also, additional steps will be required to make initial configuration of the system. In this case, it is possible that Firmware revisions may be newer than what is approved, and the equipment will need to be back-rev’ed to Oracle standards. This document may not be enough to deal will all issues for this installation. At a minimum, the hardware configuration and cabling Technical References for the installation will be needed.

This document assumes that all the internal cabinet cabling is correct and verified, and all hardware meets Oracle supported versions.

2.2 NETWORKING (C-CLASS)

IP networking for a C-class system.

- Uplinks to customer network, direct from c-Class Enclosure switches (HP Proliant 6120XG or HP6125XLG) with 10G uplinks.

The decision of what interconnect method will be used is typically made even before equipment order is placed.

2.3 NETWORKING OPTIONS (RMS)

Rack Mount Server installations are typically networked directly to customer provided IP networking switches. This includes NIC1, NIC2, and iLo.

2.4 INSTALLATION TIME ESTIMATES

The following table illustrates the progression of the installation process by procedure with estimated times. The estimated times and the phases that must be completed may vary depending on experience and preparation, and un-expected site issues. The phases outlined are to be executed in the order they are listed.

- Estimate is based on a single Cabinet with a single Enclosure.
- Installation time increases significantly if the equipment was not prepared/verified by the Oracle manufacturing process.

Table 2: Installation times (c-Class)

Procedure	Phase	Elapsed Time (Hours)	
		This Step	Cumulative
Procedure 1	Install TVOE 3.0.0 on Management Server (DL380)	1.0	
Procedure 2	Upgrade DL380 Server Firmware	1.0	
Procedure 3	TVOE/Management Server Network Configuration	.5	
Procedure 4	Install PM&C Application	1.0	
Procedure 5	Configure the PM&C Application (Web GUI)	.5	
Procedure 6	Configure initial OA IP (Front Panel)	.25	
Procedure 7	Configure the OA IP (OA Configuration Wizard)	.75	**5.0**
Procedure 8	Add Cabinet and Enclosure to the PM&C	.5	
Procedure 9	Configuring HP6125XLG Enclosure Switches	1.0	**6.75**
Procedure 10	Update Application Blade Firmware	2.0	
Procedure 11	Confirm/Update Application Blade BIOS Settings	.5	
Procedure 12	Load Appliction TPD ISO onto PM&C Server	.5	**9.5**
Procedure 13	IPM Server Blades via PM&C	1.0	
Procedure 14	Install Policy Application Software via PM&C	1.5	**12.0**

Table 3: Installation times per server (HP-RMS)*

Procedure	Phase	Elapsed Time (Hours)	
		This Step	Cumulative
Procedure 15	Configure iLO on HP RMS Server	.5	
Procedure 16	Update HP RMS Server Firmware	1.0	
Procedure 17	Configure HP RMS Server BIOS	.5	
Procedure 18	IPM of HP RMS Servers	1.0	
Procedure 19	Install Policy Application RMS	1.0	**4.0**

Table 4: Installation times per server (Oracle X5-2)

Procedure	Phase	Elapsed Time (Hours)	
		This Step	Cumulative
Procedure 20	Configure Initial ILOM IP address and BIOS Settings	.5	
Procedure 21	Update X5-2 RMS Server Firmware	1.0	
Procedure 22	Configure X5-2 iLOM from GUI	.5	
Procedure 23	IPM of Oracle X5-2 RMS Server	1.0	
Procedure 24	Application Software Installation X5-2 RMS	1.0	**4.0**

Table 5: Configure Policy Application Servers

Procedure	Phase	Elapsed Time (Hours)	
		This Step	Cumulative
Procedure 25	Perform Initial Config of Policy Servers (Platcfg)	.5	
Procedure 26	Perform Initial Config of the Policy Servers (CMP GUI)	.5	
Procedure 27	CMP Site1 Cluster Topology Configuration	1	
Procedure 28	Topology Configuration of Additional Clusters	1	
Procedure 29	SSH Key Exchanges to all Servers in the Topology	.25	
Procedure 30	Configure IP Routing on the MPE and MRA	.25	
Procedure 31	Adding MPE and MRA to CMP Menu	.25	
Procedure 32	Configure MPE Pool on MRA (Policy Front End)	.25	
Procedure 33	Define and Add Network Elements	.5	**4.5**

3. INSTALL PLANNING

This section provides a planning overview of the Installation activities.

3.1 IP NETWORK SURVEY

The Network Architecture Planning Document (NAPD) must be completed (with the customer input), before Installation.

This will provide the IP addresses that the installer will need to configure at the equipment while on-site. It also allows the customer to properly prepare for switch ports, cable drops, and IP network address assignments for their network.

3.2 NETWORK CONFIGURATION FILES

For c-Class Enclosure installations it is VERY IMPORTANT that the Network configuration files, used to configure the Enclosure switches and Aggregation switches, are prepared and verified before going to site.

For procedures to prepare the network configuration files please refer to Platform Configuration Guide- Section 3.1 Networking

[7] E53486 - Tekelec Platform 7.0.x Configuration Guide

The preparation has these steps:

- Use Template files are provided on the Policy Application ISO image file, and may change from one release to another. These template files are then edited to make them specific for the customer install, and placed on the PM&C server (after it is installed). The files are used to by the PM&C NetConfig tool to push the configuration to the switches.
- Once the files are prepared, have them reviewed and verified to minimize the time required on site to fix errors.

Note: It is important to keep the installation as close to the Oracle standards as possible, to minimize support issues.

3.3 REQUIRED MATERIALS

Oracle Communications Policy Management Application Software:

1. **ISO** or **USB** image of Tekelec Platfrom Distubution **(TPD)**
   - *TPD.install-7.0.2.0.0_86.28.0-OracleLinux6.6-x86_64.iso* or
   - *TPD.install-7.0.2.0.0_86.28.0-OracleLinux6.6-x86_64.usb*
2. **ISO** image of Comunnication Management Platform **(CMP)**
   - *12.1.x.0.0.0_35.1.0-cmp-x86_64.iso*
3. **ISO** image of Multimedia Policy Engine **(MPE)** :

- *12.1.x.0.0.0_35.1.0-mpe-x86_64.iso* **or**
- *12.1.x.0.0.0_35.1.0-mpe-li-x86_*64.iso (for Lawful Intercept)

4. **ISO** image of Multiprotocol Routing Agent **(MRA)…**also referred to as the Policy Front End **(PFE)**
   - *12.1.x.0.0.0_35.1.0-mra-x86_64.iso*

Note: Later versions may be posted as per latest Oracle ECO

Oracle Communications Policy Management and Configuration Platform **(PM&C)**:

1. **ISO** or **USB** image of Tekelec Virtual Operating Environment **(TVOE)**
   - *TVOE-3.0.2.0.0_86.28.0-x86_64.iso* or
   - *TVOE-3.0.2.0.0_86.28.0-x86_64.usb*
2. **ISO** image of Policy Configuration Management Platform **(PM&C)**:
   - *PMAC-6.0.1.0.0_60.21.0-x86_64.iso*

Note: Later versions may be posted as per latest Oracle ECO

Other:

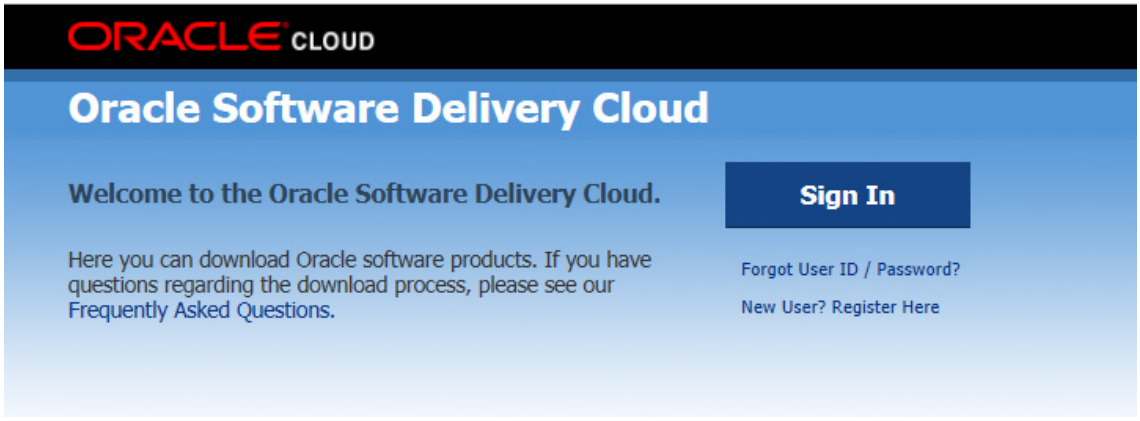
1. HP or Oracle Solution firmware (.usb or .iso image files) , as described in the next section
2. USB Flash Drives (for creating bootable USB media if using .usb files)
3. Standard Login information for components of system
4. Laptop and Cat 5 Ethernet cable (for direct connection to iLO from laptop)

3.4 ACQUIRING SOFTWARE

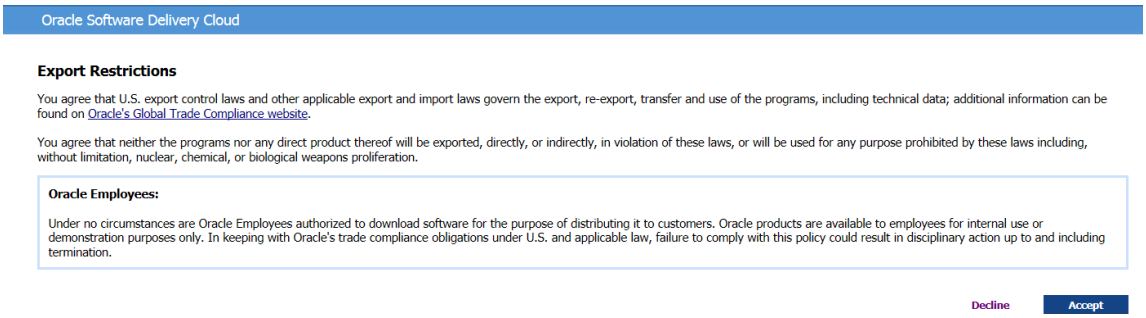
Customers:

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.

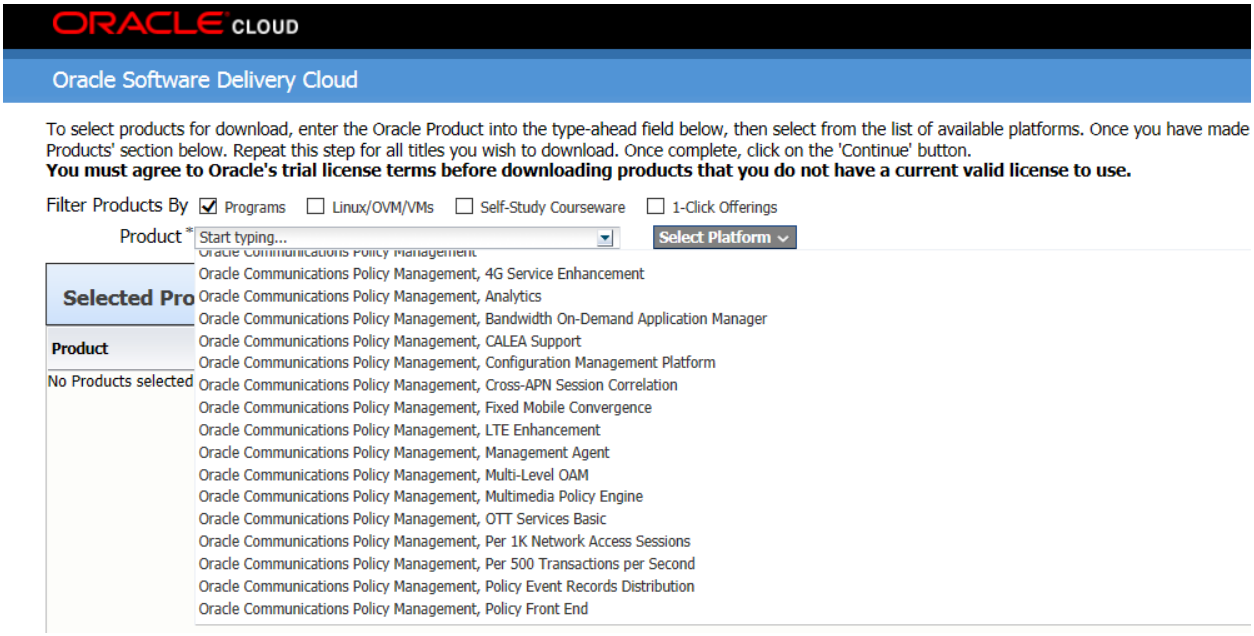
For patches, see My Oracle Support.



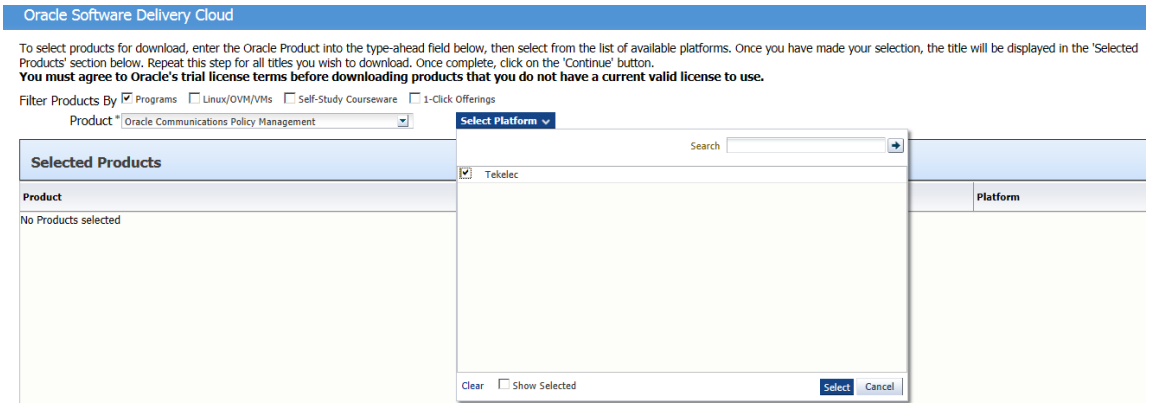
Sign in and Accept the Export restrictions:



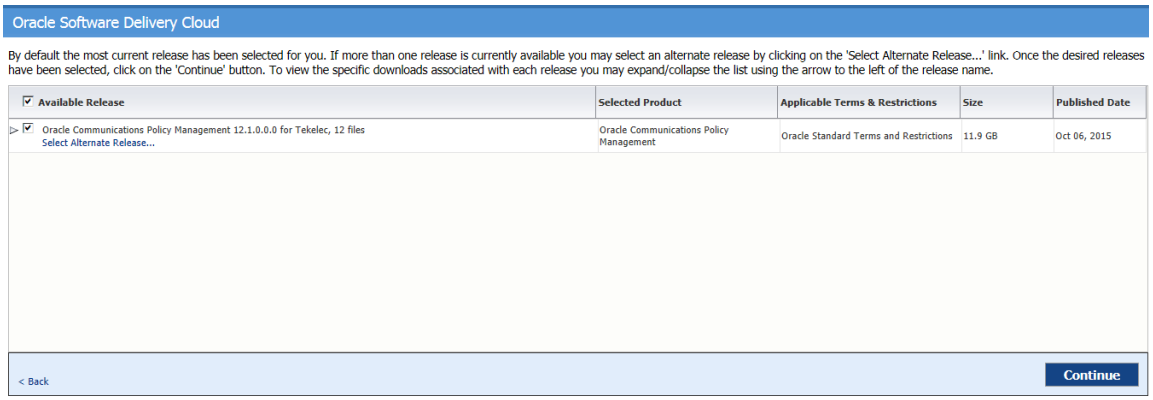
Choose Oracle Communications Policy Management Option



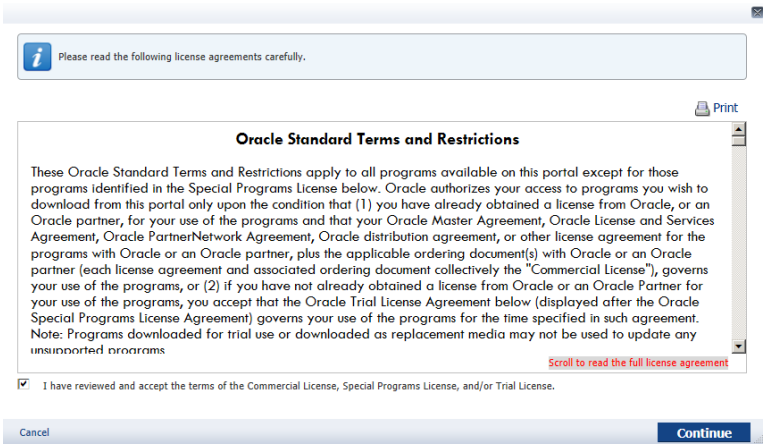
Choose Select Platform and check the Tekelec box and then Continue



Confirm Oracle Communications Policy Management 12.1.x.0.0.0 for Tekelec and Continue



Confirm the License Agreement



Choose the required Software Versionsin their .zip compressed format

Note: OVA (Open Virtualization Appliance) files are specific to Virtual Installation and not covered in this document. For information regarding the use and deployment of 12.1.x Policy OVA image files please refer to the Policy Management 12.1.x Virtual Installation Guide.

Note: The following table maps the image files referenced in the beginning of this section to the corresponding zip files posted on the Oracle Software Delivery Cloud.

Oracle Software Delivery Cloud		
Zip File	Description	Image File
V77937-01.zip	OC Policy Configuration Management Platform	cmp-12.1.0.0.0_35.1.0-x86_64.iso
V77938-01.zip	OC Policy Front End	mra-12.1.0.0.0_35.1.0-x86_64.iso
V77967-01.zip	OC Policy Multimedia Policy Engine	mpe-12.1.0.0.0_35.1.0-x86_64.iso
V77390-01_1of2.zip	OC Tekelec Virtual Operating Environment	TVOE-3.0.2.0.0_86.28.0-x86_64.iso
V77390-01_2of2.zip	OC Tekelec Virtual Operating Environment	TVOE-3.0.2.0.0_86.28.0-x86_64.usb
V77391-01_1of2.zip	OC Tekelec Platform Distribution	TPD.install-7.0.2.0.0_86.28.0-OracleLinux6.6-x86_64.iso
V77391-01_2of2.zip	OC Tekelec Platform Distribution	TPD.install-7.0.2.0.0_86.28.0-OracleLinux6.6-x86_64.usb
V77937-01.zip	OC Tekelec Configuration Management Platform	PMAC-6.0.1.0.0_60.21.0-x86_64.iso

Note: Later versions may be posted as per latest Oracle ECO

3.5 ACQUIRING FIRMWARE

Several procedures in this document pertain to the upgrading of firmware on various servers and hardware devices.

The HP Solutions Firmware Upgrade Pack (HP FUP) is provided **for customers who bought their HP hardware through Oracle**. It describes new functionalities, fixed Bugs, known Bugs, and any additional installation and configuration instructions required, relative to this release. For Policy Manager Release 12.1.x, the minimum supported firmware is 2.2.8.

Please refer to the HP FUP Release Notes as per the reference section of this document for more information

[1] E59722 - HP Solutions Firmware Upgrade Pack_Release 2.2.8_Release Notes

[2] E59721 - HP Solutions Firmware Upgrade Pack, Upgrade Guide 2.2.8

HP FUP firmware and documention for Release 2.2.8 can be accessed on the internal Oracle HP FUP website. Contact Oracle Support for assistance if needed.

- HP Smart Update Firmware ISO - FW2_SPP-2.2.8.0.0_10.43.0.iso
  or -FW2_SPP-2.2.8.0.0_10.43.0.usb
- HP Misc Firmware ISO - FW2_MISC-2.2.8.0.0_10.43.0.iso

Note: Later versions may be posted as per latest Oracle ECO

For customers who have purchased their own HP hardware please refer to the HP FUP *Software Centric* Release Notes as per the reference section of this document. For these customers, Firmware Upgrade media is not directly provided by Oracle.

[3] E59723 - HP Solutions Firmware Upgrade Pack, Software Centric Release Notes 2.2.8

Note: HP Gen9 servers are supported in a software centric model only. Please refer to the HP FUP *Software Centric* Release Notes.

For customers who purchase Oracle Rack Mount Server X5-2 hardware directly from Oracle please refer to

[4] E65467 - Oracle Firmware Upgrade Pack 3.1.5, Release Notes

[5] E65466 - Oracle Firmware Upgrade Pack Release 3.1.5 Upgrade Guide

Note: Firmware Upgrade media for the Oracle X5-2 RMS can be obtained from Oracle OTN. Specific downloading instructions can be found in the section 3.1 "Downloading Oracle Software Release Patches" of the Upgrade Pack Release Notes.

Policy 12.1.x Servers and devices that may require firmware updates are:

- HP c7000 Blade System Enclosure Components:
  - Onboard Administrator
  - HP 6120XG/6125XLG Network Switches
  - HP BL460c G6/G8 Blade Servers
- HP Rack Mount Servers (DL380/DL360)
- Oracle X5-2 Rack Mount Server

3.6 PREPARATIONS BEFORE GOING TO SITE

It is important to have all the resources and as much planning as possible before going to the site to begin installation.

Below is a checklist of items to have prepared.

Table 4: Checklist of preparations before going to site

Checkbox	Item Description	Comments
	Site Access Authorization from Customer	
	IP Address Assignments	
	Enclosure Layout diagram	
	Login/Passwords	
	netConfig prepared xml files	For c-Class installation
	TPD for Applications Servers	ISO or USB images
	TVOE and TPD for PM&C	ISO or USB images*
	PM&C Application software	ISO image
	Policy Application software (CMP,MPE) required	ISO image
	Policy Application software (MRA, MPE-li*) optional	ISO image
	Firmware	ISO or USB images
	Cisco Console Cable (for laptop connections to switches)	For c-Class Installation
	9ft Cross-over CAT-5 cable	To connect Laptop to local 4948 switch, serial over LAN console

		connections and to access system GUIs
	Access to Monitor/Keyboard cart at site	Optional: Preferred for direct serial console connections***
	HP Blade Monitor/Keyboard/usb front handle cable	Optional: Allows Console and USB access direct to the blade for C-Class installation
	Customer provided Network drop cable - ready at site	Optional: allows the user to establish and verify remote connectivity to site

* The “MPE-li” ISO image file is used in place of the MPE ISO image file to provide Lawful Intercept on the functionality on the MPE if required

3.7 CAUTIONS FOR ON-SITE ACTIVITIES

Below is a list of points to remember while on customer site:

- Be certain of the equipment location, and system identification method.
- If there are any differences in the installation from what was expected, follow up with installation team to confirm.
- Do not connect or move cables that are external to the site equipment cabinets for an HP c_Class installation or external to the Rack Mount Servers for a RMS installtion. Look but don’t touch.
- Think twice before shutting down or booting a server – is it safe?
- ***Follow the procedure.*** Skipped steps can lead to problems.

3.8 FAQ FOR C-CLASS INSTALLATIONS

- How do I verify the Firmware levels of the Installation, before going to site?

  If the equipment went through Oracle Mfg process, it will have the latest rev available at the time it was shipped. If the installation is c-Class then the OA (Online Administrator) GUI will have a summary of the firmware revisions of all the equipment in the C-class enclosure, if it is possible to access this (it will generally not be possible to access this until the install of the enclosure is complete).

- Can Firmware Updates be done later?

  Yes, in general – but it will take more time to do this remotely because of file download speeds. Important - these updates must be done before the system goes in-service.

- Can the Cisco and HP switches be configured without using the PM&C NetConfig tool?

  Not recommended. It is certainly possible to login to the switches from PM&C and make config 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. Also, it is important to backup the final switch configuration to PM&C so that it can be restored in a repair operation. Also, it must be clearly documented if the netConfig files are not to be used for restore operation (because the installer has made switch configs outside of this tool).

- How do I get NetConfig Template files?

  Please refer to

  [7] E53486 - Tekelec Platform 7.0.x Configuration Guide

3.9 LOGINS/PASSWORDS

The standard configuration steps will configure standard passwords for root, admin and some other standard logins referenced in this procedure. These passwords are not included in this document. Contact Oracle support for this information.

Initial login to a HP server/module is configured by HP at the factory and provided on a plastic pull-out tag on the front of the server/module. However, if the equipment went through Oracle Manufacturing, then the HP passwords will have been replaced with the standard passwords.

3.10 OPTIONAL FEATURES PLANNING

When Policy installation is complete, further configuration and/or installation steps will need to be taken for optional features that may be present in this deployment. Please check with Oracle Support for the corresponding documentation relevant to any customer specific features for the post-Policy install configuration steps needed.

Feature	Document

4. INSTALLATION (AND NETWORKING) IN A C-CLASS ENVIRONMENT

The c-Class Hardware and software environment provides a platform for management and growth of blade applications servers. The procedures in this section will configure this environment.

As mentioned earlier, the hardware installation and verification should be completed before executing the procedures in this document. Also, the IP networking plan and IP assignments need to be completed before executing this procedure.

IP addresses throughout this document show examples using IPv4, but IPv6 can be used if that is preferred. Please note that mixed IP addresses (some systems IPv4 others IPv6) are not supported.

4.1 PM&C INSTALLATION

This section provides the procedures to install the TVOE (Tekelec Virtual Operating Environment) platform and PM&C server application.

The TVOE and PM&C server is a rack mount server (DL380) with an Oracle Application that provides tools to manage multiple c-Class enclosures and blade software, as well as networking equipment (Enclosure switches) for the c-Class environment.

IMPORTANT: The correct time setting in the PM&C server CMOS BIOS (step 4 below) must be performed to ensure later procedure steps will be successful. **DO NOT CONTINUE** to the next steps unless the time has been correctly set. [This time setting will be pushed to the blades during IPM of the blade servers, and will cause various issues during installation if not set correctly.]

Even if PM&C was previously installed, it is necessary to re-install the PM&C server, in order to assure a correct installation for this customer site.

PM&C 6.0.1 is deployed on a Virtual OS (TVOE) environment. The TVOE OS must be installed first, and then the PM&C application ISO is installed. PM&C install is not service affecting for the Policy system.

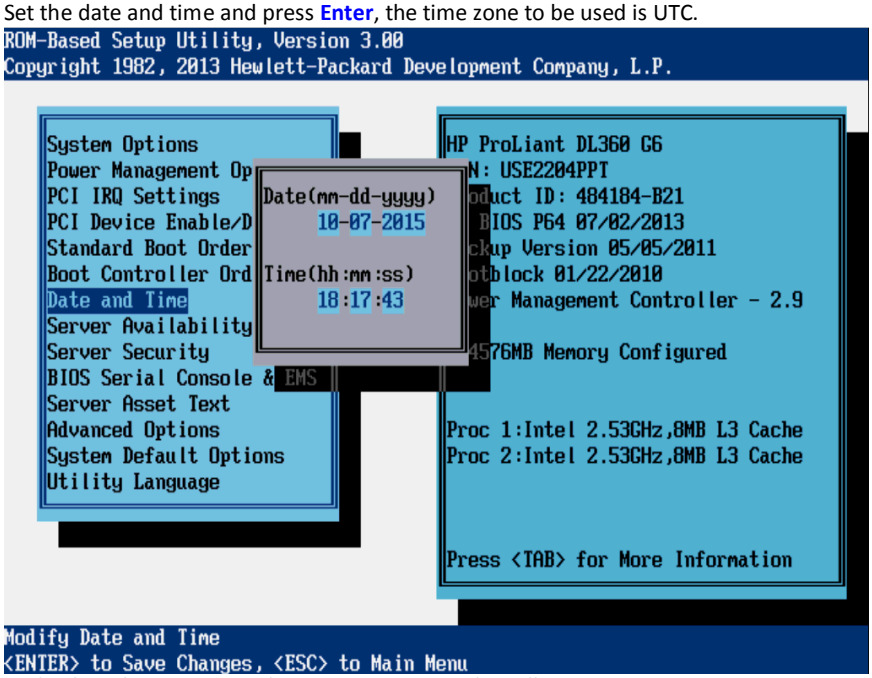
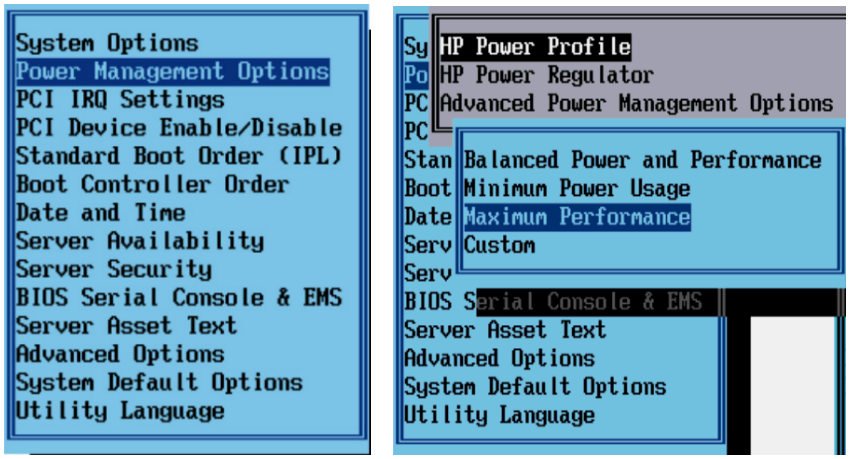
Note that in Policy Rel 12.1.x, PM&C Server is used for Installation activities, growth of new servers and Field repair activities. It is also used for deploying Firmware upgrades.

Procedure 1: Install TVOE 3.0.0 on Management Server (DL380)

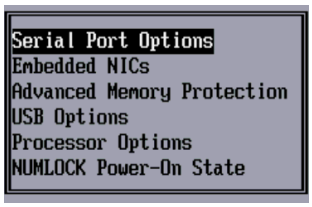
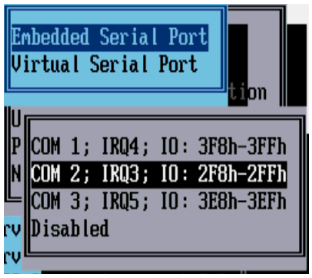
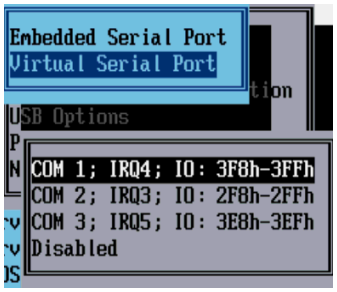
Procedure 1: Install TVOE 3.0.0 on Management Server (DL380)

STEP #	This procedure will install TVOE 3.0.0 on the Management Server. **Needed material:** - TVOE 3.0.0 Media 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 ☐	**Connect to the Server Console**	Connect to the Server Console using a VGA Display and USB Keyboard, or access the iLO interface and Remote Console application. See Supporting Procedures and Information in Section 8 of this document for further detail how to access the iLO remote console.
2 ☐	**Prepare to boot the server to the TVOE install ISO**	The TVOE 3.0.0 software is provided as an .iso or a .usb image file. To boot the server from the .usb or .iso image file, two methods are possible: - The TVOE .usb image file is used to provide a bootable USB device Note: To prepare a bootable USB device follow the instructions in this document as found in the references section. [2] E59721 - HP Solutions Firmware Upgrade Pack, Upgrade Guide 2.2.8 **Section3.3.1 Preparing USB Media** This information is also contained in the readme file co-located with the TVOE .usb image file on the Oracle Softare Delivery Cloud. - The TVOE ISO image file is available on the user's laptop, and the virtual DVD mount capability of the server iLO interface is used to mount the ISO file from the laptop to the server. Note: see supporting procedures at the end of this document for further detail on how to use the iLO remote console to mount an ISO image file Use one of these two methods to prepare the server to boot from the image file.
3 ☐	**Access the Server BIOS**	Reboot the server and after the server is powered on, as soon as you see <F9=Setup> in the lower left corner of the screen, press **F9** to access the BIOS setup screen.

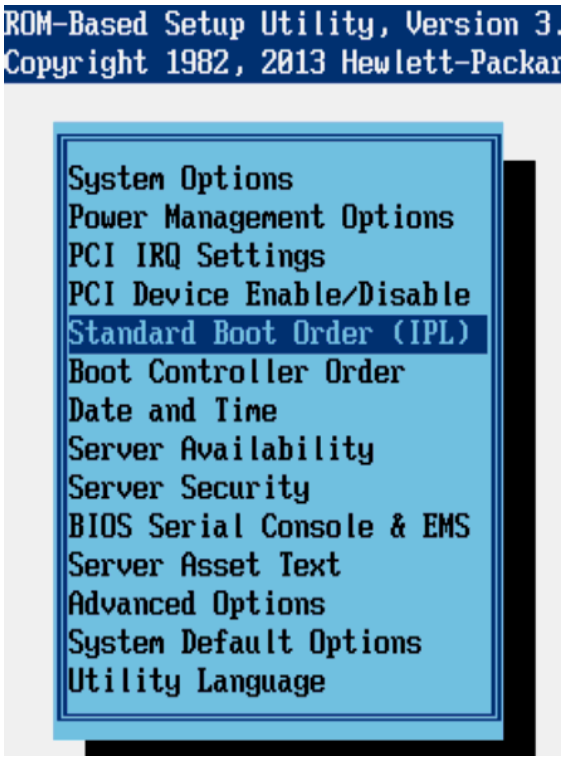
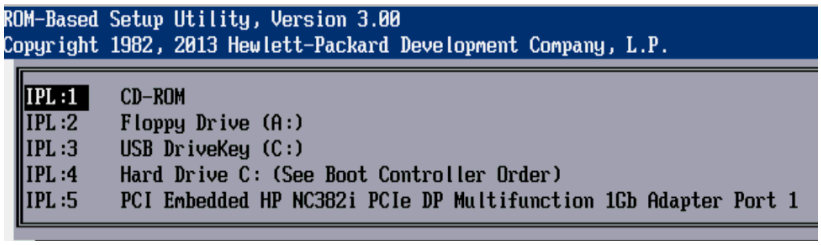
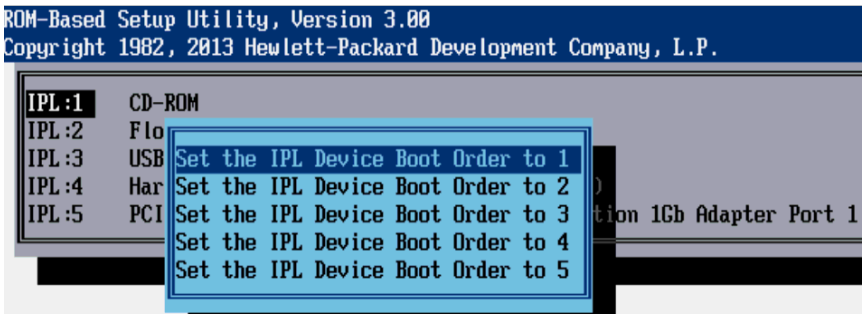
Procedure 1: Install TVOE 3.0.0 on Management Server (DL380)

4 ☐	**Set CMOS Clock**	Scroll to *Date and Time* and press **Enter** Set the date and time and press **Enter**, the time zone to be used is UTC.  Go back to the main menu by pressing **<Esc>** and scroll up to *Power Management Options* and press **Enter** Select *HP Power Profile* and press **Enter** Scroll down to *Maximum Performance* and press **Enter**  Press **<Esc>** to return to the main menu

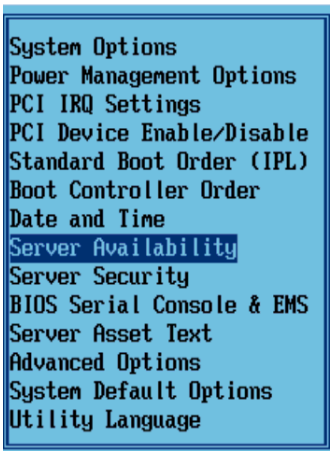
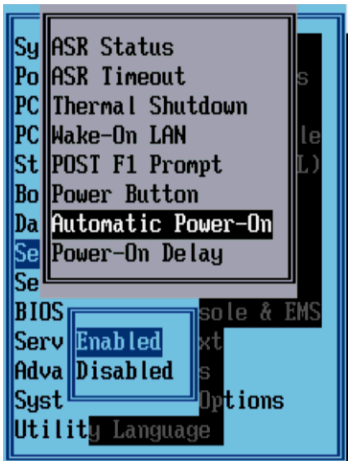
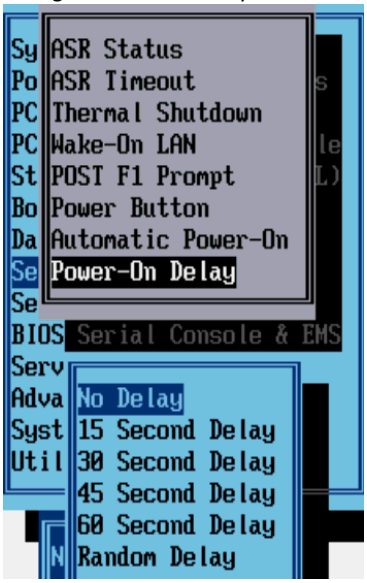
Procedure 1: Install TVOE 3.0.0 on Management Server (DL380)

5 ☐	**Configure iLO Serial Port**	Scroll to ***System Options*** and press **Enter** **Change power profile (same as blades)** Select *Serial Port Options* and press **Enter**  Press **Enter** to select ***Embedded Serial Por***t and change it to *COM2* and press **Enter**  Press **Enter** to select ***Virtual Serial Port*** and change it to *COM1* and press **Enter**  Press **<ESC>** 2 times to return to the main menu

Procedure 1: Install TVOE 3.0.0 on Management Server (DL380)

6 ☐	**Double Check boot Order.**	Scroll to *Standard Boot Order* and press **Enter**  Review the settings as follows. Note: Floppy Drive A may be moved to the last position in the boot order if desired but this is not required.  (Make changes if needed) for example:  Press **<ESC>** to return to the main menu.

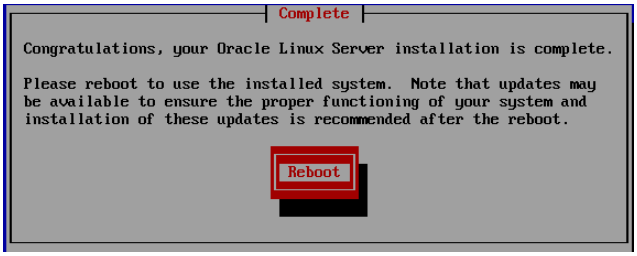
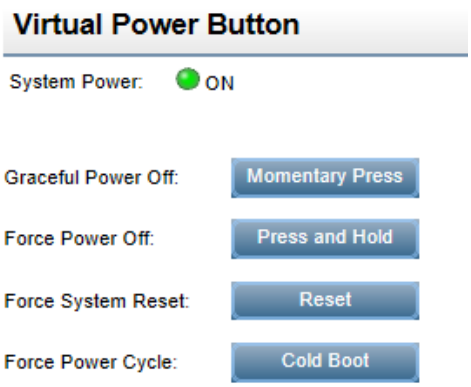
Procedure 1: Install TVOE 3.0.0 on Management Server (DL380)

7 ☐	**Configure Server Availability**	Select "**Server Availability**"  Change "Automatic Power-On" to "Enabled"  Change "Power-On Delay" to "No Delay" 

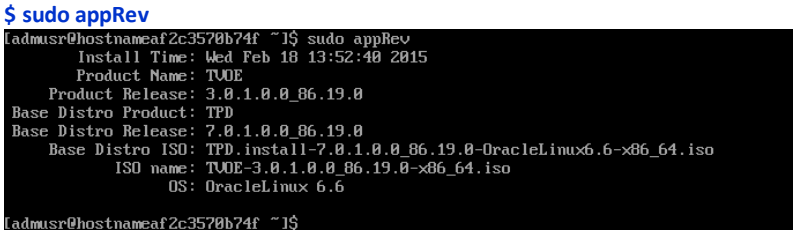
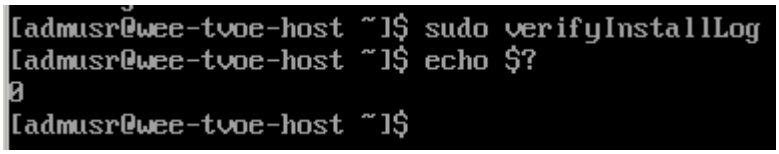
Procedure 1: Install TVOE 3.0.0 on Management Server (DL380)

8 ☐	**Save Configuration and Exit**	Press **<ESC>** until back to the main menu and then press **F10** to save the configuration and exit. The server will reboot.
9 ☐	**Begin IPM Process**	If the ISO is properly prepared, the server will boot from the ISO and will display the boot selection screen as follows: At the boot prompt as in the snapshot above type the following and then execute a carriage return boot: **`TPDnoraid console=tty0 diskconfig=HWRAID,force`** **Note:** If you are using a direct serial console connection for installation, do not use the console=tty0 option **Note:** The actual version of the TVOE release to be installed will be the latest released version per Oracle ECO (Engineering Change Order)

Procedure 1: Install TVOE 3.0.0 on Management Server (DL380)

10 ☐	**IPM Complete**	The IPM process takes about 45 minutes, you will see several messages and screens in the process. Once the IPM is complete, you will be prompted to press Enter as shown below. **Remove the USB drive or unmount the TVOE image from the iLO** and press **Enter** to reboot the server..  **Note:** If you do not remove the drive or unmount the TPD image before the system reboots you will simply be presented with the boot prompt again as in the rpevious screen. In this is the case, confirm that **the USB drive has been removed or the image ISO has been unmounted from the iLO** and manually reboot again. For example, you can use the power setting in the iLO to force a soft shutdown and reboot. 
11 ☐	**Server Reboot**	Once the Server Reboots, you should see a login prompt. Note that during the first system boot, swap files may be initialized and activated. Each swap file will take about 2 minutes. If no login prompt is displayed after waiting 15 minutes, contact Oracle Customer Support for Assistance.

Procedure 1: Install TVOE 3.0.0 on Management Server (DL380)

12 ☐	**Verify release**	Login as admusr Example output below – Product Release may be different. **$ sudo appRev** 
13 ☐	**Confirm no errors**	As admusr Example output below – Product Release may be different. **$ sudo verifyInstallLog** **$ sudo echo $?**  Expected result is “0” errors **You have now completed this procedure.**

Procedure 2: Upgrade DL380 Server Firmware

NOTE: Please refer to the FUP 2.2.8 upgrade documents to update the Firmware on the TVOE Server.

[2] E59721 - HP Solutions Firmware Upgrade Pack, Upgrade Guide 2.2.8

[3] E59723 - HP Solutions Firmware Upgrade Pack, Software Centric Release Notes 2.2.8

Note: Access to the HP 2.2.8 Firmware Upgrade Guide may require enablement form Oracle Support

Further detail is also provided in section 3.5 “Acquiring Firmware” of this document

Procedure 3: TVOE/Management Server Network Configuration

Procedure 3: TVOE/Management Server Network Configuration

<table>
<tr><td>STEP #</td><td colspan="2">This procedure will configure the Network on the TVOE/Management Server

Prerequisite: Procedure 1 - Install TVOE 3.0.0 on Management Server has been completed.

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.</td></tr>
<tr><td>1. ☐</td><td>Determine Bridge names and interfaces</td><td>Determine the bridge name to be used on the TVOE management server for the management network and fill in the <TVOE_Management_Bridge_Interface> values in the table below. The following table shows a typical example.
If NetBackup is to be used, determine the bridge name to be used for the NetBackup network and fill in the <TVOE_NetBackup_Bridge_Interface> values in the table below:
<table>
<tr><th>PM&C Interface Alias</th><th>TVOE Bridge Name</th><th>TVOE Bridge Interface</th></tr>
<tr><td>control</td><td>control</td><td>Fill in the appropriate value:
bond0 for untagged (default) or
bond0.<vlan#> for tagged

_____

<TVOE_Control_Bridge_Interface></td></tr>
<tr><td>management</td><td>management</td><td>Fill in the appropriate value:
bond0.<vlan#>, or bond1

_____

<TVOE_Management_Bridge_Interface></td></tr>
<tr><td>NetBackup (if applicable)</td><td>NetBackup</td><td>Fill in the appropriate value:
(bond0.<vlan#>, or bond2

_____

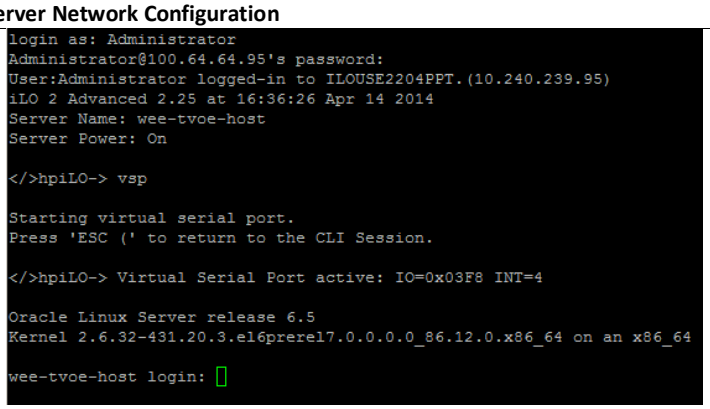
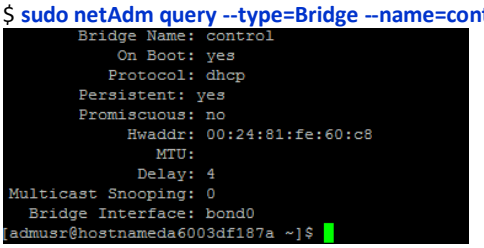
<TVOE_NetBackup_Bridge_Interface></td></tr>
</table></td></tr>
<tr><td>2. ☐</td><td>TVOE iLO: Login and launch the integrated remote console</td><td>Log in to iLO with Internet Explorer or Mozilla Firefox using the iLO password and launch the iLO remote console:
http://<management_server_iLO_ip>

Click in the Remote Console tab and launch the Integrated Remote Console on the server.

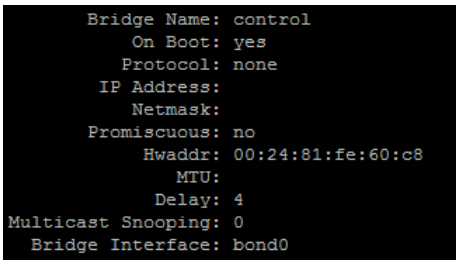
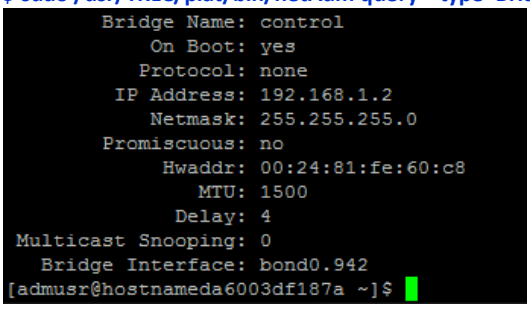
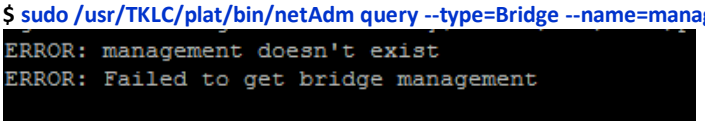
Click Yes if the Security Alert pops up.

Alternately, the iLO can be logged into with an “ssh” client using the <management_server_iLO_ip> . The login credentials will be the same as used for the web browser authentication to the iLO. When the </>hpiLO-> prompt is accessed use the virtual serial port command “vsp” and thenunthenticate to the TVOE platform same as with the iLO remote console.</td></tr>
</table>

Procedure 3: TVOE/Management Server Network Configuration

		 Section 8: See "Procedures for iLO" for information for using the iLO
3. ☐	**TVOE iLO:** Verify the Control Network	**Login as admusr** Verify the control network by running the following command **Note:** The output below is for illustrative purposes only. The example output below shows the control bridge configured. $ **sudo netAdm query --type=Bridge --name=control**  If the bridge has been configured, remove it by issuing the following commands**.** **$sudo netAdm delete --type=Bridge --name=control** **$sudo netAdm delete --device=bond0** **Note:** The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure. Add control bridge: **$sudo netAdm add --device=bond0** **--onboot=yes --type=Bonding --mode=active-backup --miimon=100** Device <bond0> added **$sudo netAdm set --device=eth01 --type=Ethernet --master=bond0 --slave=yes --onboot=yes** <eth01 _interface> added to bond0 **$ sudo netAdm set --device=eth02 --type=Ethernet --master=bond0 --slave=yes --onboot=yes** <eth02 _interface> added to bond0 **$ sudo netAdm add --type=Bridge --name=control --bootproto=none --onboot=yes --bridgeInterfaces=bond0 --delay=4** Bridge <control> added with bridgeInterface=bond0

Procedure 3: TVOE/Management Server Network Configuration

4 ☐	**TVOE iLO:** Set tagged control interface.	Confirm creation of control bridge **$ sudo netAdm query --type=Bridge --name=control**  Bridge Name: control On Boot: yes Protocol: none IP Address: Netmask: Promiscuous: no Hwaddr: 00:24:81:fe:60:c8 MTU: Delay: 4 Multicast Snooping: 0 Bridge Interface: bond0 **$ sudo netAdm add --device=bond0.<vlan#> --onboot=yes** This is the agreed upon vlan# configured per network design. In the snapshot below vlan#=942 was used. **$ sudo set --type=Bridge --name=control --bridgeInterfaces=bond0. .<vlan#> --address=192.168.1.2 --netmask=255.255.255.0** control bridge <vlan#), IP address and netmask set This is the typical IP address and netmask that will be used on the private network within the c-Class enclosure. Reference network design if needed. In the snapshot below ip address 192.168.1.2 net mask 255.255.255.0 is used <u>Confirm tagged configuration:</u> $ **sudo /usr/TKLC/plat/bin/netAdm query --type=Bridge --name=control**  Bridge Name: control On Boot: yes Protocol: none IP Address: 192.168.1.2 Netmask: 255.255.255.0 Promiscuous: no Hwaddr: 00:24:81:fe:60:c8 MTU: 1500 Delay: 4 Multicast Snooping: 0 Bridge Interface: bond0.942 [admusr@hostnameda6003df187a ~]$
5 ☐	**TVOE iLO:** Verify the Management Network	Verify if the management network has been configured, by running the following command **Note:** The output below is for illustrative purposes only. For a new install it is expected that the management bridge has not yet been created. **$ sudo /usr/TKLC/plat/bin/netAdm query --type=Bridge --name=management**  ERROR: management doesn't exist ERROR: Failed to get bridge management **<u>Create Management bridge using tagged interface on bond0</u>** **$sudo netAdm add --type=Bridge --name=management --bootproto=none --onboot=yes --bridgeInterfaces=bond0 --delay=4** Bridge <management> added with bridgeInterface=bond0 Confirm creation of management bridge **$ sudo netAdm query --type=Bridge --name=management**

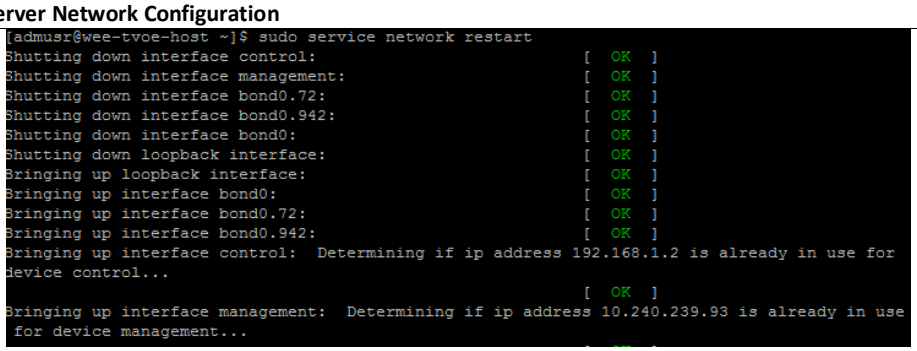
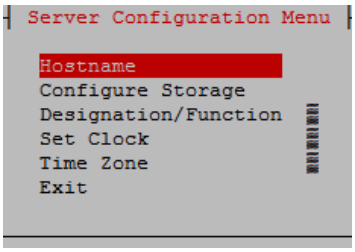
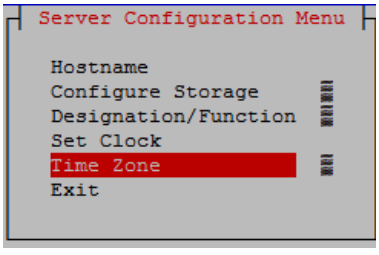
Procedure 3: TVOE/Management Server Network Configuration

		Create vlan **$ sudo netAdm add --device=bond0.<vlan#> --onboot=yes** This is the agreed upon vlan# configured per network design. In the snapshot below vlan#=72 was used. **$ sudo set --type=Bridge --name=management --bridgeInterfaces=bond0.<vlan#> --address=10.240.239.93 --netmask=255.255.255.192** management bridge <vlan#), IP address and netmask set This is the agreed upon IP address and netmask that will be accessible from the network per network design. In the snapshot below ip address 10.240.239.93 netmask 255.255.255.192 is used **$ sudo netAdm query --type=Bridge --name=management** Bridge Name: management On Boot: yes Protocol: none IP Address: 10.240.239.93 Netmask: 255.255.255.192 Promiscuous: no Hwaddr: 9c:8e:99:16:30:1c MTU: 1500 Delay: 4 ast Snooping: 0 ge Interface: bond0.72
6. ☐	**TVOE iLO:** Verify the NetBackup Network (Optional)	Verify the NetBackup network. If the NetBackup feature is not needed, skip to the next step. **Note:** The output below is for illustrative purposes only. The example output below shows the control bridge configured. # **netAdm query --type=Bridge --name=netbackup** Bridge Name: netbackup On Boot: yes Protocol: none IP Address: 10.240.6.2 Netmask: 255.255.255.0 Promiscuous: no Hwaddr: 00:24:81:fb:29:58 MTU: Bridge Interface: bond2 If the bridge has been configured as needed, skip to the next step. **Note:** The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, network devices, bonds, and bond enslaved devices, to configure. **Note:** The example below illustrates a TVOE Management Server configuration with the NetBackup feature enabled. The NetBackup network is configured with a non-default MTU size. **Note:** The MTU size must be consistent between a network bridge, device, or bond, and associated VLANs.

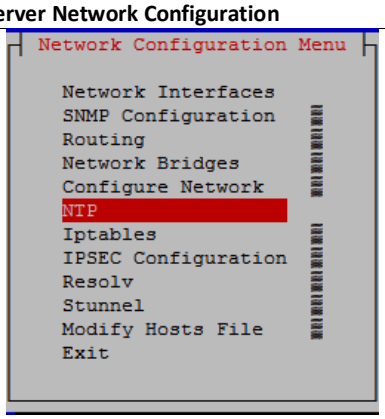
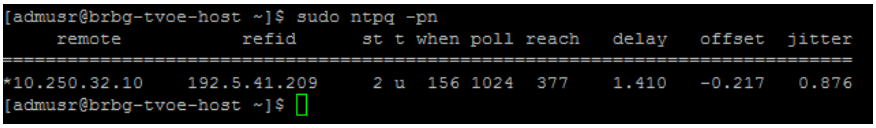
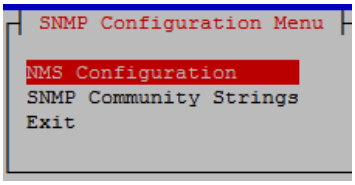
Procedure 3: TVOE/Management Server Network Configuration

		EXAMPLE 1: Create NetBackup bridge using tagged interface on bond0. # **netAdm add --device=bond0.<vlan#>** # **netAdm add --type=Bridge --name=netbackup** **--onboot=yes --MTU=<NetBackup_MTU_size>** **--bridgeInterfaces=bond0.<vlan#>** EXAMPLE 2: For this example, create NetBackup bridge using untagged interfaces (eth05 and eth06) and bonding. <bond2> # **netAdm add --device=bond2** **--onboot=yes --type=Bonding --mode=active-backup --miimon=100** **--MTU=<NetBackup_MTU_size>** Interface <TVOE_NetBackup_Bridge_Interface> added # **netAdm set --device=<ethernet_interface_5> --type=Ethernet** **--master=bond<2> --slave=yes** **--onboot=yes** Interface <ethernet_interface_5> updated # **netAdm set --device=<ethernet_interface_6> --type=Ethernet** **--master=bond<2> --slave=yes** **--onboot=yes** Interface <ethernet_interface_6> updated # **netAdm add --type=Bridge --name=netbackup** **--onboot=yes --MTU=<NetBackup_MTU_size>** **--bridgeInterfaces=bond2**
7. ☐	**TVOE iLO:** Verify the Default Route	Note: The output below is for illustrative purposes only. The example output below shows the management bridge configured. **$ sudo netAdm query --route=default --device=management** Routes for TABLE: main and DEVICE: management * NETWORK: default GATEWAY: 10.240.4.1 If the route has been configured, skip to the next step. **Note:** The default route must be configured per the network plan as per site information For this example add default route on management network. **$ sudo netAdm add --route=default --device=management** **--gateway=<mgmt_gateway_address>** Route to <TVOE_Management_Bridge> added
8. ☐	**TVOE iLO:** Restart the network interfaces	Restart the network interfaces **$ sudo service network restart**

Procedure 3: TVOE/Management Server Network Configuration

		 **Note:** A successful restart should return [OK] in each line. If there are any failures or errors there it is likely the configuration is not correct. The output of the command **ifconfig –a** may be helpful in troubleshooting.
9. ☐	**TVOE iLO:** Set Hostname	Set the server hostname by running the following: **$ sudo su - platcfg** **1.** Navigate to **Server Configuration ➢ Hostname ➢ Edit**. **2.** Set TVOE Management Server hostname **3.** Press OK. **4.** Navigate out of Hostname 
10. ☐	**TVOE iLO:** Set the time zone and/or hardware clock	**1.** Navigate to **Server Configuration ➢ Time Zone.** **2.** Select Edit. **3.** Set the time zone and/or hardware clock. **4.** Press OK. **5.** Navigate out of Server Configuration [Accept H/W clock for GMT] 
11. ☐	**TVOE iLO:** Set NTP	**1.** Navigate to **Network Configuration ➢ NTP**. **2.** Set NTP server IP address to point to the customer provided NTP server. **3.** Press OK. **4.** exit platcfg.

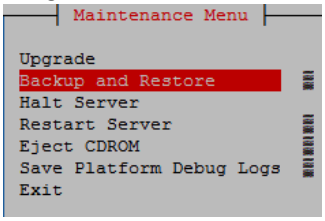
Procedure 3: TVOE/Management Server Network Configuration

		 Ensure that the time is set correctly by executing the following commands: **$ sudo service ntpd stop** **$ sudo ntpdate ntpserver1** **$ sudo service ntpd start** **Note:** The above steps sync the management server NTP with the remote NTP server. After executing this step allow some time and confirm that NTP is active with the "ntpq –pn" command. There should be a star next to the configured NTP server IP address.  For troubleshooting purposes make sure the designated NTP server is reachable with the ping command
12. ☐	**TVOE iLO:** Set SNMP	Set SNMP by running the following: **$sudo su - platcfg** 1. Navigate to **Network Configuration ➢ SNMP Configuration ➢ NMS Configuration**. 2. Select **Edit** and then choose Add a New NMS Server. The 'Add an NMS Server' page will be displayed. 3. Complete the form by entering in all information about the SNMP trap destination. Select **OK** to finalize the configuration. The 'NMS Server Action Menu' will now be displayed. Select **Exit**. The following dialogue will then be presented. 4. Select **Yes** and then wait a few seconds while the Alarm Routing Service is restarted. At that time the SNMP Configuration Menu will be presented. 5. exit platcfg. 

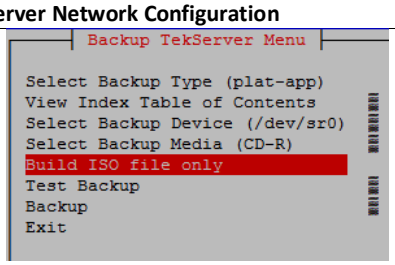
Procedure 3: TVOE/Management Server Network Configuration

13. ☐	**Management server iLO:** Setup syscheck	syscheck must be configured to monitor bonded interfaces. Replace "bondedInterfaces" with "bond0" or "bond0,bond1" if segregated networks are used:
		
		$ sudo syscheckAdm net ipbond --set --var=DEVICES --val=<bondedInterfaces>
		For example: bond0
		
		$ sudo syscheckAdm net ipbond --enable
		
		Confirm the bonded interfaces have been added to syscheck
		
		$ sudo syscheckAdm net ipbond --get
		`[admusr@wee-tvoe-host ~]$ sudo syscheckAdm net ipbond --get`
		`DEVICES=bond0`
		
		`[root@MPE-1a-Wireline ~]# syscheckAdm net ipbond -get`
		`DEVICES=bond0,bond3,bond1,bond2`

14. ☐	**TVOE iLO:** Verify Server Health	Execute the following:
		
		$ sudo **alarmMgr –alarmStatus**
		`[admusr@ocpm-12r1-brbg-g6-cmp-a ~]$ sudo alarmMgr --alarmStatus`
		`[admusr@ocpm-12r1-brbg-g6-cmp-a ~]$`
		
		This command should return no output on a healthy system. If any alarms are reported, contact Customer Care Center.

15. ☐	**TVOE iLO:** Perform a TVOE backup using TPD platcfg utility	Execute the following: $sudo **su - platcfg** Navigate to **Maintenance ➢ Backup and Restore**  Select "**Backup Platform (CD/DVD)**" **Note:** You will be presented with a list of backup options. Select an applicable backup option, and press enter to continue. For example choosing *Build ISO only* will place a backup image ISO file in the directory /var/TKLC/bkp

Procedure 3: TVOE/Management Server Network Configuration

		
		I
		Exit from TPD platcfg utility and Confirm the backup has been successfully created
		
		The TVOE backup can be found in the "/var/TKLC/bkp/" directory, and is prefixed by the server hostname
		
		`[admusr@wee-tvoe-host bkp]$ pwd`
		`/var/TKLC/bkp`
		`[admusr@wee-tvoe-host bkp]$ ls -l`
		`total 56160`
		`-rw-rw----. 1 root sys 28753920 Sep 22 14:24 wee-tvoe-host-plat-app-201509221424.iso`
		`-rw-rw----. 1 root sys 28753920 Oct 8 12:03 wee-tvoe-host-plat-app-201510081203.iso`
		`[admusr@wee-tvoe-host bkp]$`
		
		Move the TVOE backup to a customer provided backup server for safe keeping.
		
		You have now completed this procedure.

Procedure 4: Install PM&C Application

Procedure 4: Install PM&C Application

STEP #	This procedure will deploy PM&C application on the TVOE Host **Prerequisites:.** TVOE Installed TVOE/Management Server Network Configured Note: Use the following command to delete a TVOE guest (in the example below, the guest name is “PM&C”):: **# guestMgr --remove PM&C** 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. ☐	**TVOE iLO:** Login and launch the integrated remote console	Log in to iLO by Internet Explorer or Mozilla Firefox using the password provided by the application: **http://<management_server_iLO_ip>** Click in the **Remote Console** tab and launch the **Integrated Remote Console** on the server. Click **Yes** if the Security Alert pops up. Note: As an alternative to the using the remote console it may be possible to use network access to start a "vsp" session to the iLO IP address of TVOE Management Server or ssh to the Management network address that was configured in prerequisite procedures.
2.	**TVOE iLO:** Copy the PM&C ISO to the TVOE	The PM&C Application ISO image file must be copied to the TVOE environment. This can be done by either:

Procedure 4: Install PM&C Application

☐	Management server	• inserting a non-bootable USB key into the server, and copying the ISO image file from the USB key to the server • As the server has had a network address configured in the prerequisite procedures, by using an ftp application such as SCP, it may be possible to transfer the PM&C ISO image file from a laptop directly to the TVOE Management Server. The PM&C ISO image file should be copied to /var/TKLC/upgrade. The user *admusr* can be utilized for this purpose. Confirm the image file has completed its transfer by listing the files in /var/TKLC/upgrade. Now run the following to mount the ISO image file. **$ sudo mount -o loop /var/TKLC/upgrade/6.0._x.x.x-x86_64.iso /mnt/upgrade**
3. ☐	**TVOE iLO:** Validate ISO	**$ cd /mnt/upgrade/upgrade** **$ sudo .validate/validate_cd** If the media validation fails, the media is not valid and should not be used. **Note:** The actual ISO image file name should be as per the latest Oracle ECO
4 ☐	**TVOE iLO:** deploy PM&C ONE Command→	Using the PM&C-deploy script, deploy the PM&C instance using the configuration captured during the site survey. **$ cd /mnt/upgrade/upgrade** If deploying PM&C without netbackup feature, run the following command: **$ sudo ./PM&C-deploy --guest=PM&C** **--hostname=<PM&C_HostName>** **--controlBridge=control** **--controlIP=192.168.1.1** **--controlNM=255.255.255.0** **--managementBridge=management** **--managementIP=<PM&C_Management_ip_address>** **--managementNM=<PM&C_Management_netmask>** **--routeGW=<PM&C_Management_gateway_address>** **--ntpserver=<TVOE_Management_server_ip_address>** If deploying PM&C with netbackup feature, run the following command: # **./pmac-deploy --guest=pmac** **--hostname=<PMAC_HostName>** **--controlBridge=control** **--controlIP=192.168.1.1** **--controlNM=255.255.255.0** **--managementBridge=management** **--managementIP=<PMAC_Management_ip_address>**

Procedure 4: Install PM&C Application

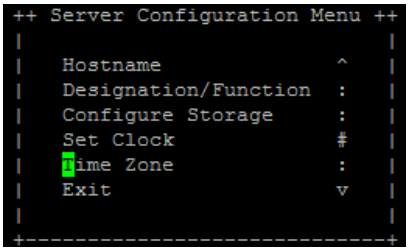
		--managementNM=<PMAC_Management_netmask> **--routeGW=<PMAC_Management_gateway_address>** **--ntpserver=<TVOE_Management_server_ip_address>** **--bridge=<TVOE_NetBackup_Bridge>** **--nic=netbackup** The PM&C will deploy and boot. The management and control network will come up based on the settings that were provided to the PM&C-deploy script. **Note:** All IP addresses and netmasks used here should be as per the deployment network design. The controlBridge configuration used here is typical for the c-Class enclosure private IP network. **Note:** If any issue is encountered with adding the routeGW or NTP server remove these lines from the deploy command and try again. The default gateway can added with platcfg on the Guest PM&C at a later point if necessary. **IF it is necessary to remove the guest and try again….** **$ sudo guestMgr --remove PM&C**
5 ☐	**TVOE iLO:** Unmount the media	The media should auto-unmount, if it does not, unmount the media using the following command: **$ cd /** **$ sudo umount /mnt/upgrade** **Note:** A reboot of the server should also result in unmounting the ISO image **file** If using USB media, remove it from the server.

6. ☐	**TVOE:** Access PM&C Console from TVOE	Access TVOE Console, using either iLO Remote Console or SSH client such as putty. Login using TVOE host admusr credentials.
		
		Access PM&C Console using **virsh**, and wait until you see the login prompt:
		
		$ sudo virsh list
		`[admusr@wee-tvoe-host ~]$ sudo virsh list`
		` Id Name State`
		`----------------------------------------------------`
		` 1 pmac running`
		
		$ sudo virsh console <PM&C name>
		`[admusr@wee-tvoe-host ~]$ sudo virsh console pmac`
		`Connected to domain pmac`
		`Escape character is ^]`
		
		`Oracle Linux Server release 6.6`
		`Kernel 2.6.32-504.3.3.el6prerel7.0.1.0.0_86.18.0.x86_64 on an x86_64`
		
		`wee-pmac login:`
		PM&C login: **admusr**
		
		password: **<admusr_password>**

Procedure 4: Install PM&C Application

		wee-pmac login: admusr Password: Last login: Thu Oct 8 14:25:56 from 10.154.129.169 [admusr@wee-pmac ~]$
7. ☐	**PM&C Console:** Verify the PM&C is configured correctly on first boot	Run the following command (there should be no output): $sudo **ls /usr/TKLC/plat/etc/deployment.d** [admusr@wee-pmac deployment.d]$ sudo ls /usr/TKLC/plat/etc/deployment.d/ [admusr@wee-pmac deployment.d]$
8. ☐	**Network Access:** Verify network connectivity to the PM&C application	Confirm the PM&C network configuration and ping the default gateway **$ ip -4 addr** {or ip -6 addr for IPv6 addresses} **Note:** These are examples only [admusr@wee-pmac /]$ ip -4 addr 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN inet 127.0.0.1/8 scope host lo 2: control: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000 inet 192.168.1.1/24 brd 192.168.1.255 scope global control 3: management: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000 inet 10.240.239.94/26 brd 10.239.240.127 scope global management **Note:** Here the loopback, controlBridge and managementBridge addresses are seen **$ netstat -r** [admusr@wee-pmac /]$ netstat -r Kernel IP routing table Destination Gateway Genmask Flags MSS Window irtt Iface 10.240.239.64 * 255.255.255.192 U 0 0 0 management 192.168.1.0 * 255.255.255.0 U 0 0 0 control link-local * 255.255.0.0 U 0 0 0 control link-local * 255.255.0.0 U 0 0 0 management default 10.240.239.65 0.0.0.0 UG 0 0 0 management **Note:** Here the default gateway, controlBridge and managementBridge networks are seen **Note**: If the default gateway is not present because it was not entered when the deploy script was executed it can be added with the following command **sudo netAdm add --route=default --device=management --gateway=<IP address>** **$ ping <default gateway>** [admusr@wee-pmac /]$ ping 10.240.239.65 PING 10.240.239.65 (10.240.239.65) 56(84) bytes of data. 64 bytes from 10.240.239.65: icmp_seq=1 ttl=255 time=0.928 ms 64 bytes from 10.240.239.65: icmp_seq=2 ttl=255 time=0.741 ms
9. ☐	**PM&C CLI:** Set the PM&C timezone	Determine the TimeZone to be used for the PM&C **Note:** Valid time zones can be found on the server in the directory "/usr/share/zoneinfo". Only the time zones within the sub-directories (i.e. America, Africa, Pacific, Mexico, etc…..) are valid with platcfg. $sudo **set_PM&C_tz.pl <timezone>**

Procedure 4: Install PM&C Application

		For example: $sudo **set_PM&C_tz.pl America/New_York** Verify that the timezone has been updated: $sudo **date** Alternateley the time zone may be selected using platcfg on the PM&C **$ sudo su – platcfg** Navigate to Server Configuration  Choose edit and select appropriate time zone
10. ☐	**PM&C Console:** Set SNMP for PM&C	Set SNMP by running the following: $sudo **su - platcfg** 1. Navigate to **Network Configuration ➢ SNMP Configuration ➢ NMS Configuration**. 2. Select **Edit** and then choose Add a New NMS Server. The 'Add an NMS Server' page will be displayed. 3. Complete the form by entering in all information about the SNMP trap destination. Select **OK** to finalize the configuration. The 'NMS Server Action Menu' will now be displayed. Select **Exit**. A dialogue will then be presented. 4. Select **Yes** and then wait a few seconds while the Alarm Routing Service is restarted. At that time the SNMP Configuration Menu will be presented. 5. exit platcfg.
11. ☐	**PM&C Console:** Reboot the PM&C	Reboot the PM&C server by running: $sudo **shutdown –r now** **You have now completed this procedure.**

4.2 COMPLETE THE PM&C INSTALLATION

Procedure 5: Configure the PM&C Application

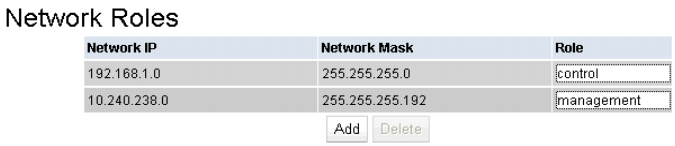
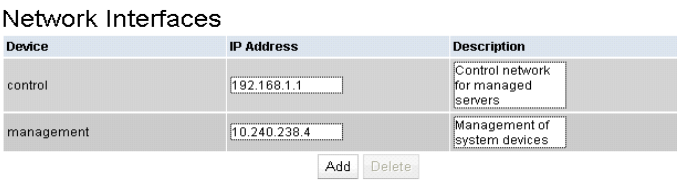
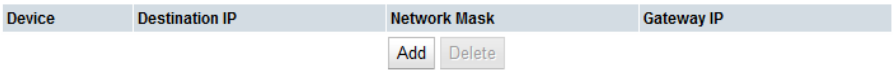
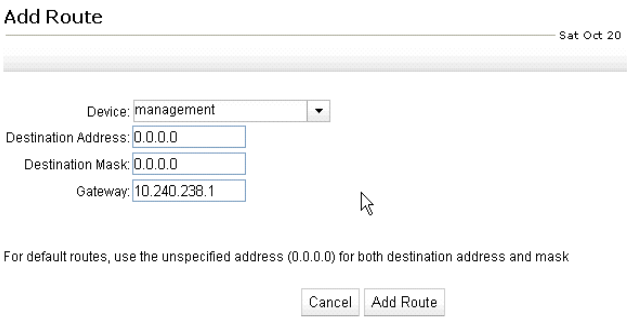
Procedure 5: Configure the PM&C Application

STEP #		
	This procedure will provide PM&C configuration using the web interface. **Prerequisite:** *Procedure 4. PM&C Deployment Procedure* has been completed. **Note:** The installer must be knowledgeable of the network. If you make a mistake, click Cancel and try again. The finish step may take longer time because it reconfigures the network and attempts to connect may fail. **Note:** After you have completed an initialization, the network parameters can no longer be changed through the GUI. If you need to reset any of the network information, you must run the **PM&Cadm resetProfileConfig** command in the PM&C shell. This will delete the existing configuration and allow you to run through the initialization wizard again. Keep in mind that the reset will not run until all provisioned enclosures and cabinets are deleted 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:** Load GUI initialization wizard	Open web browser and enter: **http://<management_network_ip>/gui** Login as PM&Cadmin user.

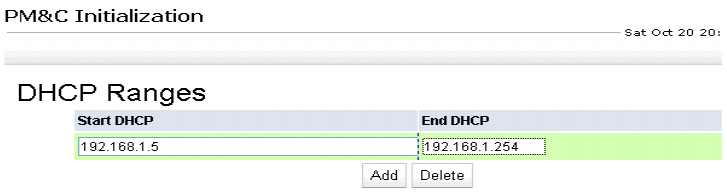
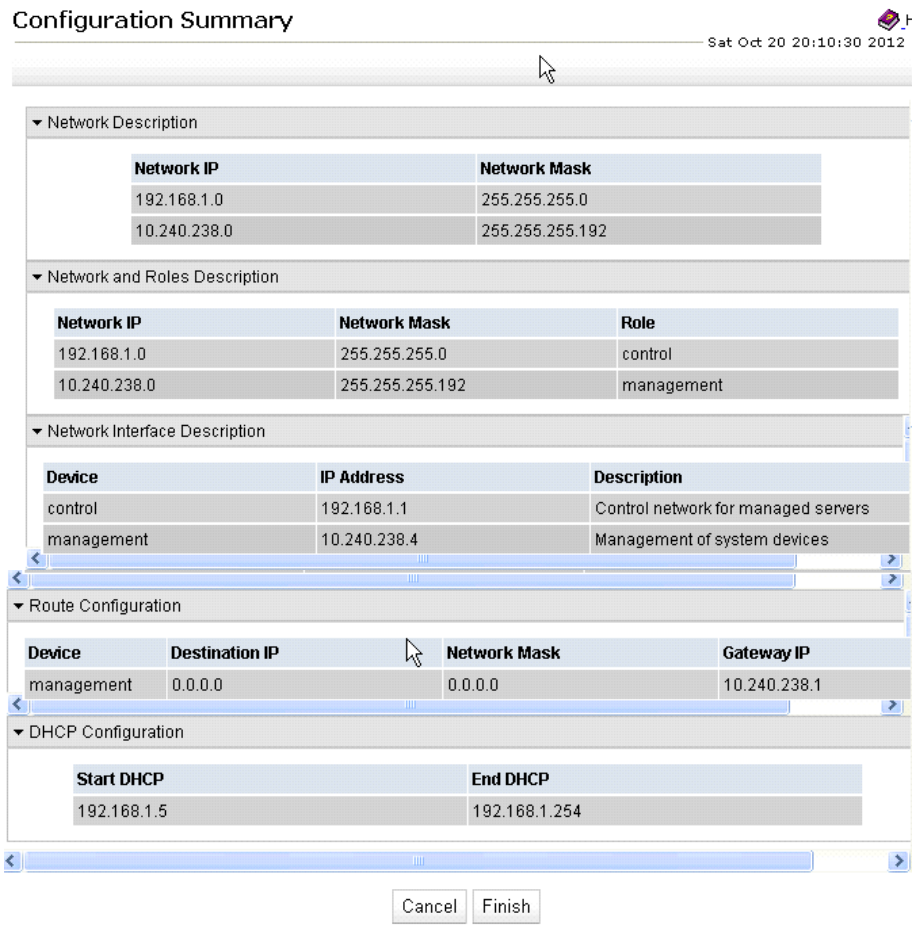
Procedure 5: Configure the PM&C Application

2 ☐	**PM&C GUI:** Select a profile	The first screen will be similar to image below Profiles File Name: TVOE | Name: PM&C TVOE Guest | Comment: Manage systems from a TVOE hosted PM&C | Version: 6.0.0 Select the **TVOE** profile and click on **Initialize**, the following features screen will display Feature / description / Role / Enabled: DEVICE.NETWORK.NETBOOT — Network device PXE initialization — management — ☑ DEVICE.NTP — PM&C as a time server — management — ☑ PMAC.MANAGED — Remote management of PM&C server — management — ☐ PMAC.REMOTE.BACKUP — Remote server for backup — management — ☑ PMAC.NETBACKUP — NetBackup client — management — ☐ For more information on Feature Configuration please consult the *Feature Configuration* page from Online help available from PM&C GUI menu. The snapshot above is an example of a typical feature configuration but requirements may be particular to a specific deployment. Features can be enabled and disabled at a later time if needed. In this example the role for all features should be set to **Management.** The following features are enabled by selecting the checkbox: DEVICE .NETWORK .NETBOOT DEVICE.NTP PMAC.REMOTE.BACKUP PMAC.NETBACK (only if NetBackup is used) For more information on Feature Configuration please consult the *Feature Configuration* page from Online help available from PM&C GUI menu. And click on **Next.**
3 ☐	**PM&C GUI:** Network Description	You will see this default screen similar to: Networks Network IP: 192.168.1.0 | Network Mask: 255.255.255.0 10.240.238.0 | 255.255.255.192 Add Delete Enter the Network IPs and Netmasks for the control and Management Networks. Click **Next**.

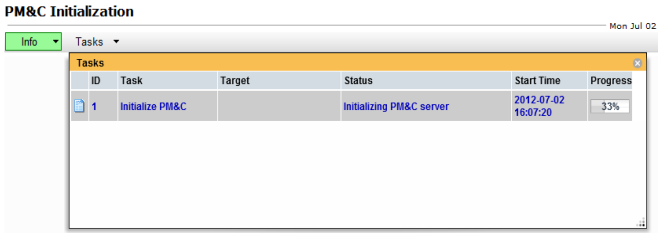
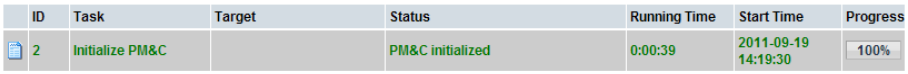
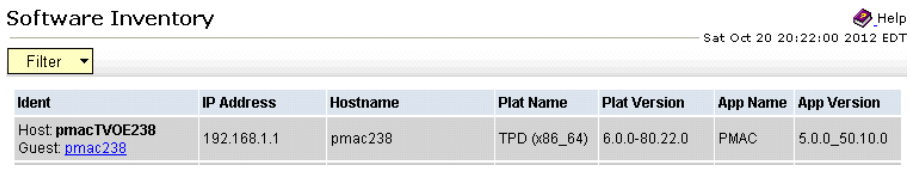
Procedure 5: Configure the PM&C Application

4 ☐	**PM&C GUI:** Network Roles	You will see this default screen similar to:  Verify the Roles and update if necessary. Click **Next**.
5 ☐	**PM&C GUI:** Network Interface	You will see this default screen similar to:  Verify the IP addresses for each Device and update if necessary. Click **Next**.
6 ☐	**PM&C GUI:** Network Route	You will see this default screen similar to:  Click **Add** to create new routes. At a minimum a default route should be defined. The following screen will be displayed. **Note:** In Procedure 4 the default route was already defined for the Guest PMAC. If this is the case and the default route is again defined here the system will respond that a default route already exists. If this is encountered simply proceed to the next step. For the default route, select the “management” Device, enter “0.0.0.0” for both Destination Address and Destination Mask, and enter the gateway IP under Gateway as shown below  Click **Add Route.** Repeat to define more routes. Click **Next** when done.

Procedure 5: Configure the PM&C Application

7 ☐	**PM&C GUI:** DHCP Ranges	You will see this default screen similar to below. Set the starting DHCP address for the control network to 192.168.1.5. [Note: 192.168.1.1 is allocated to the PM&C application, 192.168.1.2 is allocated to the TVOE, and 192.168.1.3/4 are reserved for redundant PM&C. Addresses in the allowed range will be allocated to the Enclosure blades for use by PM&C.]  If you need to define additional DHCP ranges, press "Add" (most deployments DO NOT require additional DHCP Ranges). Otherwise, click **Next**.
8 ☐	**PM&C GUI:** Settings summary	The following summary screen will be displayed.  Verify the values and click **Finish**.

Procedure 5: Configure the PM&C Application

9 ☐	**PM&C GUI:** Complete the configuration	The following summary screen will be displayed, click on Tasks to view the Initialization Progress.  Click **Task Monitoring** for status of this task.  Wait till the Progress bar turns green, which signifies that the PM&C Initialization was successful.
10 ☐	**PM&C GUI:** Verify Control Network	Software → Software Inventory The Software Inventory shows a summary of the servers discovered by DHCP on the control network. At a minimum, the PM&C application will be shown. If there are blade servers in the Enclosures that have TPD installed, then a list of these may also appear. However, the information in this form will not be fully complete until: a) the Enclosure OA(s) are configured (next Procedure), b) the blades all have TPD installed, and c) the PM&C Hardware → Add Cabinet, Add Enclosure are completed.  If some blade servers are also shown, it is an indication that the control network is properly configured and networked. However, if there are no blades servers with TPD installed, then this view may still be empty except for the PM&C. It is OK to proceed in either case. **You have now completed this procedure.**

4.3 HP C-7000 ENCLOSURE CONFIGURATION

Configuring the Onboard Administrator (OA) IP addresses is required prior to proceeding with the configuration of the c-Class enclosure using the PM&C Management Server GUI in Procedure 8.

The following procedures are applied for each enclosure. (PM&C may manage multiple enclosures.)

Note: Once the OA IP address and network configuration has been completed the OA should be accessed with a browser to determine if the OA Firmware is at the required level. For the procedure to determine the OA firmware version and update the OA firmware if needed, please refer to *Section 4.19: C7000 Onboard Administrator* of the *HP Solutions Firmware Upgrade Pack, Upgrade Guide 2.2.8* as found in the reference section of this document.

[1] E59722 - HP Solutions Firmware Upgrade Pack_Release 2.2.8_Release Notes

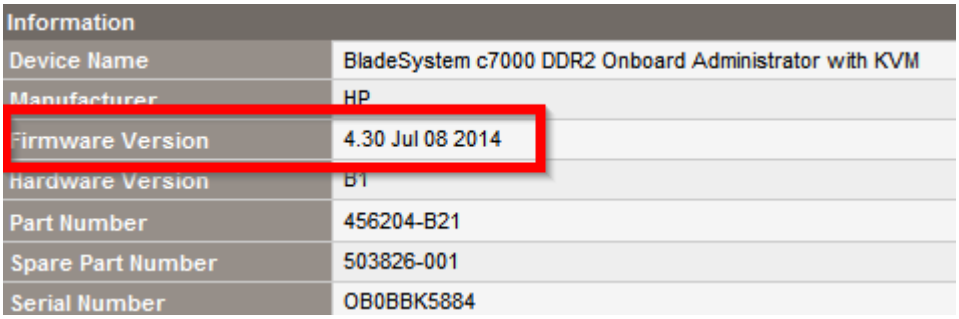
[2] E59721 - HP Solutions Firmware Upgrade Pack, Upgrade Guide 2.2.8

Firmware package to be used to execute an OA Firmware Upgrade

- HP Misc Firmware ISO - FW2_MISC-2.2.8.0.0_10.43.0.iso

For more details on acquiring the firmware for the OA refer to the HP FUP 2.2.8 Upgrade Guide

The following is an example of the OA firmware version



Information	
Device Name	BladeSystem c7000 DDR2 Onboard Administrator with KVM
Manufacturer	HP
Firmware Version	4.30 Jul 08 2014
Hardware Version	B1
Part Number	456204-B21
Spare Part Number	503826-001
Serial Number	OB0BBK5884

Procedure 6: Configure the OA IP Addresses (Front Panel Display)

NOTE: Please refer to Tekelec Platform 7.0.x Configuration Guide to Configure the Onboard Administrator (OA) IP addresses

Section ***3.5.1 Configure Initial OA IP*** of the above document will provide the details required to configure the Initial OA IP addresses using the front panel display.

Prerequisite: Onboard Administrator must be present in the OA Bay 1 location.

Note: The enclosure should be provisioned with two Onboard Administrators. This procedure needs to be executed only for OA Bay 1, regardless of the number of OA's installed in the enclosure.

Procedure 7: Configure the OA IP Addresses (Configuration Wizard)

NOTE: Please refer to the Tekelec Platform 7.0.x Configuration Guide as found in the reference section of this document to Configure the Onboard Administrstor (OA) IP addresses

Section ***3.5.2 Configure Initial OA Settings Using the Configuration Wizard*** of the above document will provide the details required to configure the Initial OA IP addresses using the Configuration Wizard.

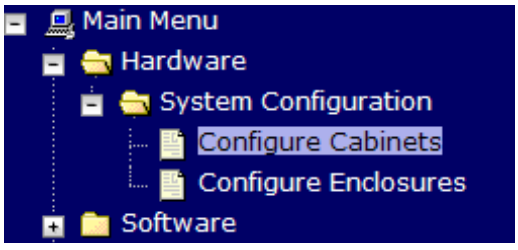
This procedure will configure initial OA settings using a configuration wizard. This procedure should be used for initial configuration only and should be executed when the Onboard Administrator in OA Bay 1 (left as viewed from rear) is installed and active.

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.
• In addition, section *3.5.1 Configure Initial OA IP* must be completed.

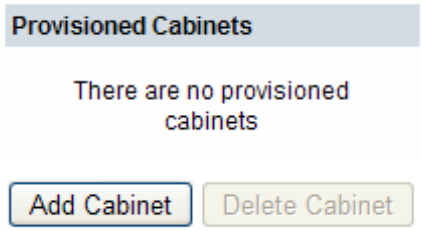
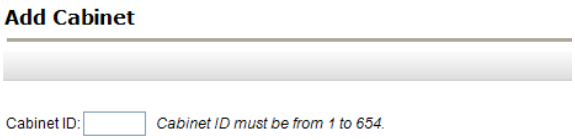
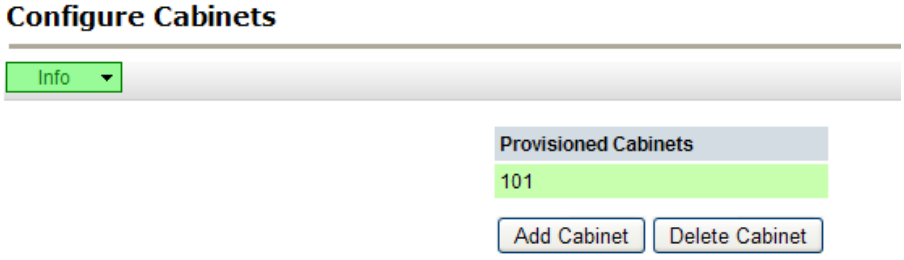
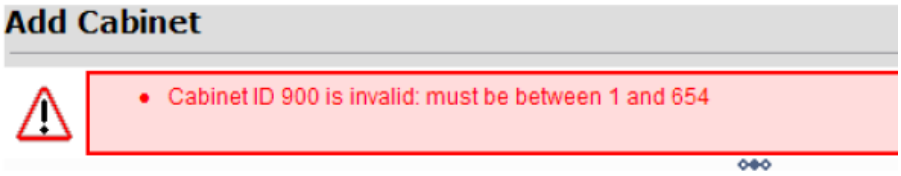
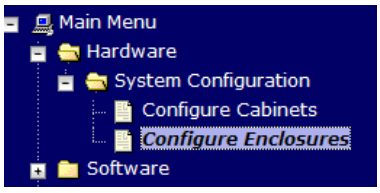
Note: The enclosure should be provisioned with two Onboard Administrators. Note that the OA in Bay 2 will automatically acquire its configuration from the OA in Bay 1 after the configuration is complete.

Procedure 8: Adding the Cabinet and the Enclosure to the PM&C

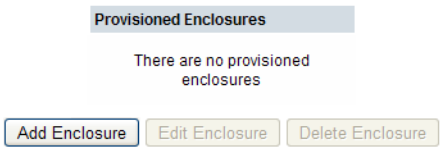
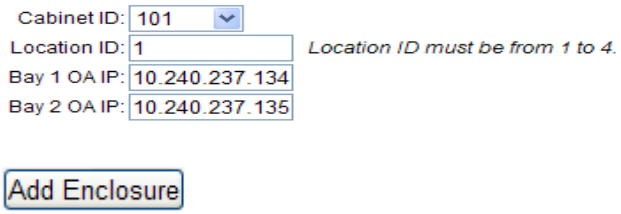
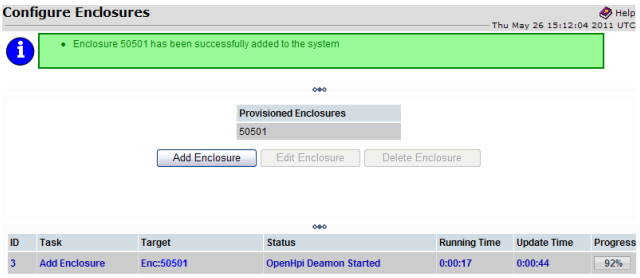
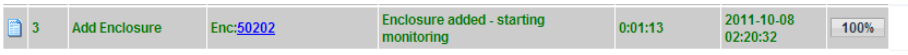
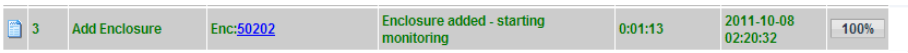
Procedure 8: Adding the Cabinet and Enclosure to PM&C

STEP #	This procedure provides instructions to add a cabinet and an enclosure to the PM&C system inventory. ***Prerequisite:*** *Prior procedure has been completed.* **Note:** The installer must be knowledgeable of the network. If you make mistake, hit cancel and try again. The finish step may take longer time because it reconfigures the network and attempts to connect may fail. 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: **http://<management_network_ip>/gui** Login into the PM&C as admin user.
2. ☐	**PM&C GUI:** Configure Cabinets	Navigate to **Main Menu** -> **Hardware** -> **System Configuration** -> **Configure Cabinets**. 

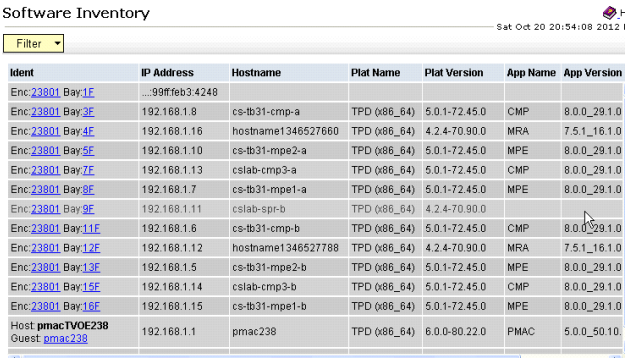
Procedure 8: Adding the Cabinet and Enclosure to PM&C

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**. 

Procedure 8: Adding the Cabinet and 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	In the Add Enclosure panel enter Cabinet ID, Location ID and Bay 1 OA IP and Bay 2 OA IP. 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.
11. ☐	**PM&C GUI:** Wait until the Add Enclosure task finishes	The color of the progress bar will change to green when complete:  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.

Procedure 8: Adding the Cabinet and Enclosure to PM&C

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:  NOTE: The procedure to configure the Enclosure switches, if they have not been previously configured, is yet to be performed. **You have now completed this procedure.**

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.

Procedure 9: Configuring 6120XG/6125XLG Enclosure Switches

NOTE: Please refer to section 3.1.3 “C-Class Enclosure Switch-netConfig Procedures” in the Platform 7.0 Configuration Guide to configure enclosure switches.

[7] E53486 - Tekelec Platform 7.0.x Configuration Guide

To configure the HP 6120XG/6125XLG Enclosure switch refer to following section of the Platform 7.0 Configuration Guide

3.1.3.3 Configure HP 6120XG/6125XLG Switch (netConfig)

This procedure will configure the 6120XG/6125XLG switches from the PM&C server and the command line interface using templates included with an application.

Prerequisites:

It is essential that PM&C is installed. In addition, complete these procedures from the Tekelec 7.0 Platform Configuration Guide:

- Configure Initial OA Settings Using the Configuration Wizard
- Configure netConfig Repository
- Configure Initial OA IP .

Needed materials:

- HP MISC firmware ISO image
- Release Notes of the *HP Solutions Firmware Upgrade Pack* [2]
- Application-specific documentation (documentation that referred to this procedure)
- Template xml files in an application ISO on an application media.

4.4 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.

Procedure 10: Update Application Blade Firmware

NOTE: Please refer to the HP FUP 2.2.8 upgrade documents to update the Firmware on the Application Blades.

Further detail is also provided in section 3.5 "Acquiring Firmware" of this document

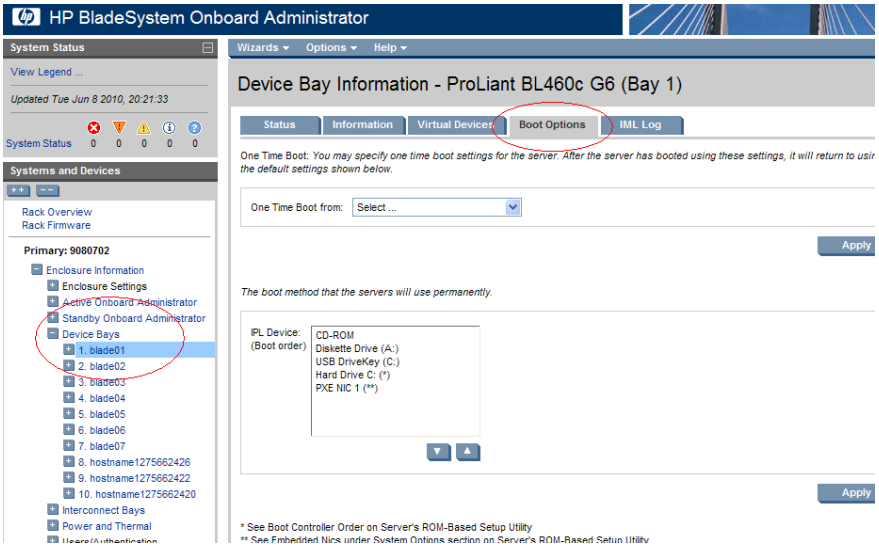
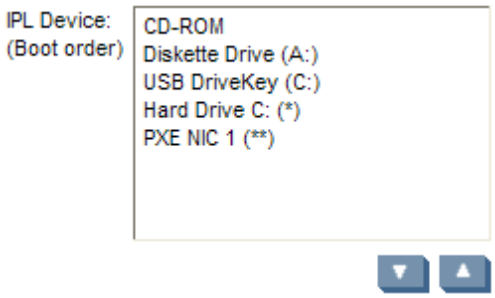
[2] E59721 - HP Solutions Firmware Upgrade Pack, Upgrade Guide 2.2.8

[3] E59723 - HP Solutions Firmware Upgrade Pack, Software Centric Release Notes 2.2.8

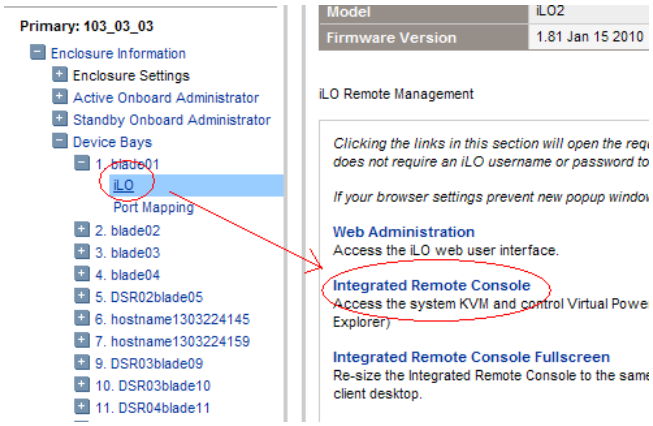
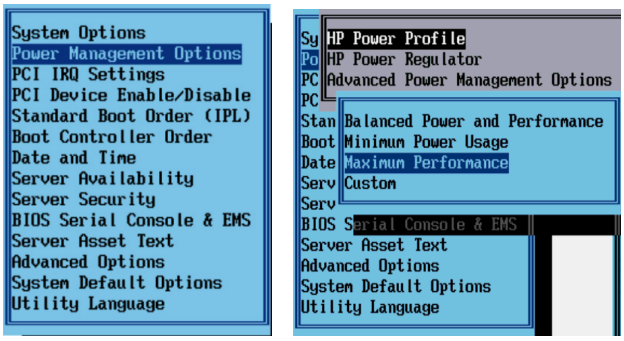
Note: Access to the HP 2.2.8 Firmware Upgrade Guide may require enablement form Oracle Support

Procedure 11: Confirm/Update Application Blade's BIOS Settings

Procedure 11: Confirm/Update Application Blade's BIOS Settings

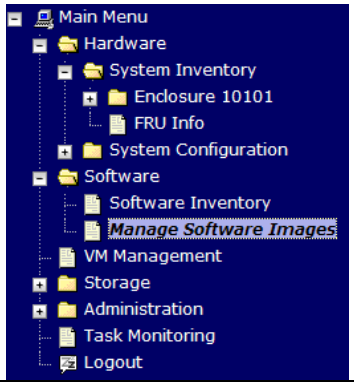
STEP #		
	This procedure will provide the steps to confirm and update the BIOS boot order on the Blade servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
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** 

Procedure 11: Confirm/Update Application Blade's BIOS Settings

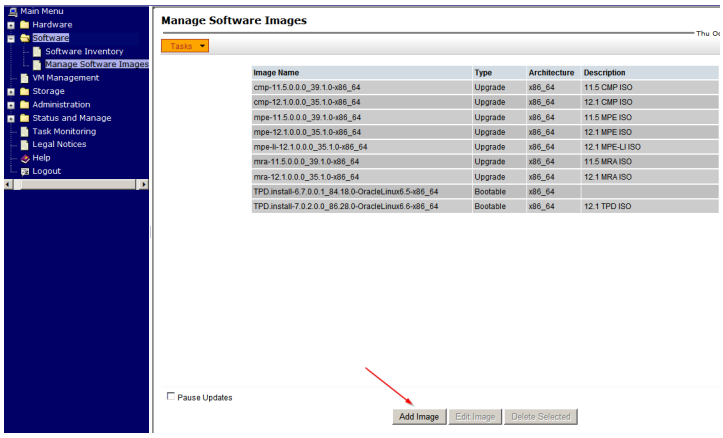
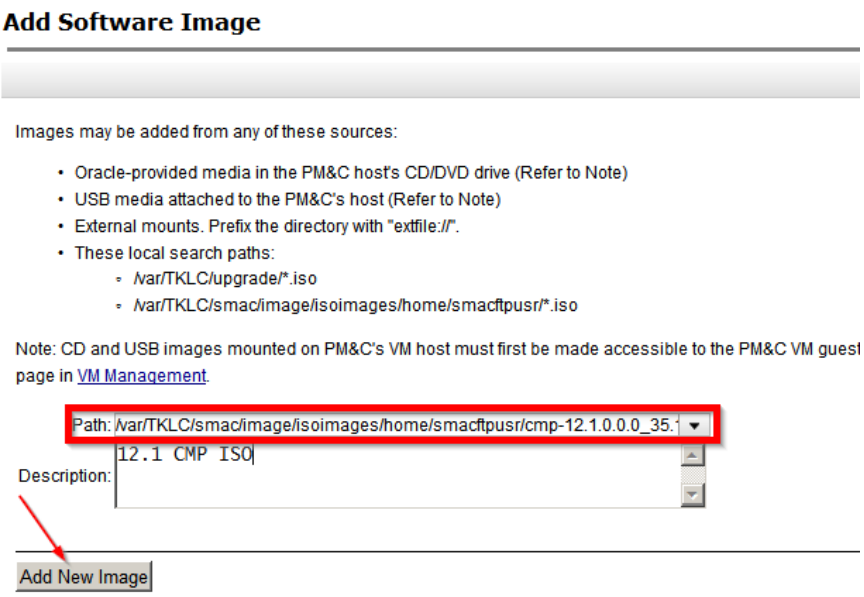
4. ☐	**OA:** Access the Blade iLO	Navigate to **Enclosure Information** -> **Device Bays** -> **<Blade 1>** -> **iLO** Click on **Integrated Remote Console**  This will launch the iLO interface for that blade. If this is the first time the iLO is being accessed, you may be prompted to install an addon 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) and after the server is powered on, as soon as you see <F9=Setup> in the lower left corner of the screen, press **F9** to access the BIOS setup 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. **You have now completed this procedure.**

Procedure 12: Loading Software Images onto the PM&C

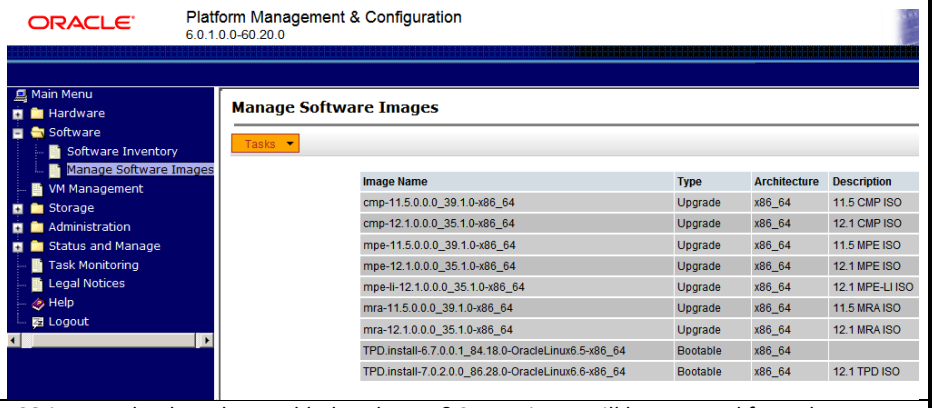
Procedure 12: Loading Software Images onto the PM&C

STEP #		
	This procedure will load the Software Images needed for the Policy Application onto the PM&C. **Needed material:** . - Application TPD ISO Image (64 bit) - Application ISO Images (cmp, mpe, [mra]) 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:** Load Application ISO image file	Insert USB Key containing Software Images into PM&C USB port. Mount the USB to /mnt/upgrade **$ sudo mount /dev/sda1 /mnt/upgrade** Verify that there is space in the /var/TKLC/upgrade directory: $ **sudo df –h** can be used for this. check. /var/TKLC/upgrade is in the /var/TKLC/ partition **$ sudo ls /var/TKLC/upgrade** Select Image to transfer: **$ sudo ls /mnt/upgrade** Copy an Application Image file to /var/TKLC/upgrade: **$ sudo cp /mnt/upgrade/<TPD or Application.iso> /var/TKLC/upgrade** - Alternative: Scp an Application ISO file to the management server and place it under **/var/TKLC/upgrade** (if networking is available) # **scp *<ISO_filename>* admusr@*<PM&C_manangement_network_ip>*:/var/TKLC/upgrade** **Note:** the user ***pmacftpusr*** can also be used to scp/sftp an ISO image to the PM&C and by default the ISO image will be placed in: **/var/TKLC/smac/image/isoimages/home/smacftpusr/**
2. ☐	**PM&C GUI:** Login	Open web browser and enter: **http://<management_network_ip>** Login as pmacadmin user.
3. ☐	**PM&C GUI:** Navigate to Manage Software Images	Navigate to **Main Menu** -> **Software** -> **Manage Software Images** 

Procedure 12: Loading Software Images onto the PM&C

4. ☐	**PM&C GUI:** Add image	Press **Add Image** button. Use the dropdown to select the image.  If the optical media was used in step 1, the device will appear as device://dev/scd0, If the ISO image file was copied over by admusr in step 1 to /var/TKLC/upgrade/ the path to var/TKLC/upgrade/*.iso is checked be default. If the image was transferred by pmacftpusr to the /var/TKLC/smac/image/isoimages/home/smacftpusr/ the path to /var/TKLC/smac/image/isoimages/home/smacftpusr/ *.iso is checked be default Select the appropriate path, adding a commnet is optional and Press the **Add New Image** button.  You may check the progress using the Task Monitoring link. Observe the green bar indicating success.

Procedure 12: Loading Software Images onto the PM&C

5. ☐	**PM&C GUI:** Verify Image Loaded	Navigate to **Main Menu** -> **Software** -> **Manage Software Images** ISO image files that have been added will now display. These files will have been moved to the PM&C repository at /var/TKLC/smac/image/repository/*.iso 
6. ☐	**PM&C GUI:** Remove image file or Media	ISO images that have been added to the PM&C repository will be removed from the /var/TKLC/upgrade directory or the /var/TKLC/smac/image/isoimages/home/smacftpusr directory. Confirm they have been removed. If still present remove them. **$ sudo ls /var/TKLC/upgrade** **$ sudo ls /var/TKLC/smac/image/isoimages/home/smacftpusr** **If DVD Media was used, remove this from the drive.**
7. ☐	**PM&C GUI:** Add additional images	Repeat this procedure to add other images. If the USB device was mounted to copy an ISO image file, the USB device can now be unmounted. **$ sudo umount /mnt/upgrade** **You have now completed this procedure.**

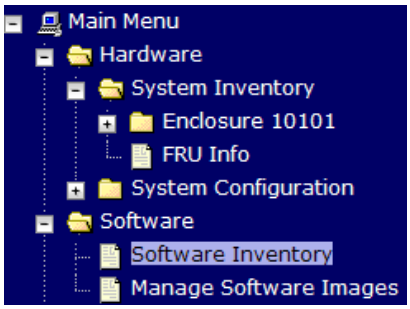
Procedure 13: IPM Blades via PM&C

Procedure 13: IPM Blades via PM&C

<table>
<tr><td>STEP #</td><td colspan="2">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.
Needed material:
- TPD Media (64-bits)

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

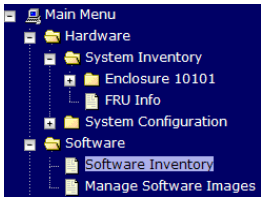
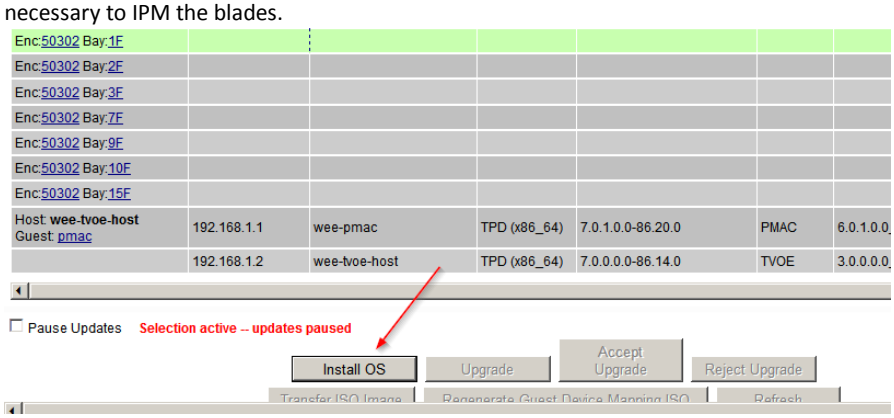
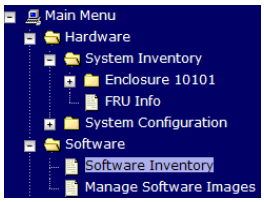
IF THIS PROCEDURE FAILS, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ASSISTANCE.</td></tr>
<tr><td>1. ☐</td><td>PM&C GUI: Verify if PM&C Contol Network is established to the blades.</td><td>Navigate to Software -> Software Inventory.
 

<table>
<tr><th>Ident</th><th>IP Address</th></tr>
<tr><td>Enc:50301 Bay:1F</td><td>192.168.1.6</td></tr>
<tr><td>Enc:50301 Bay:2F</td><td>192.168.1.12</td></tr>
<tr><td>Enc:50301 Bay:3F</td><td>192.168.1.8</td></tr>
<tr><td>Enc:50301 Bay:8F</td><td>192.168.1.5</td></tr>
<tr><td>Enc:50301 Bay:9F</td><td>192.168.1.11</td></tr>
<tr><td>Enc:50301 Bay:10F</td><td>192.168.1.10</td></tr>
<tr><td>Enc:50301 Bay:11F</td><td>192.168.1.9</td></tr>
<tr><td>Enc:50301 Bay:16F</td><td>192.168.1.7</td></tr>
</table>

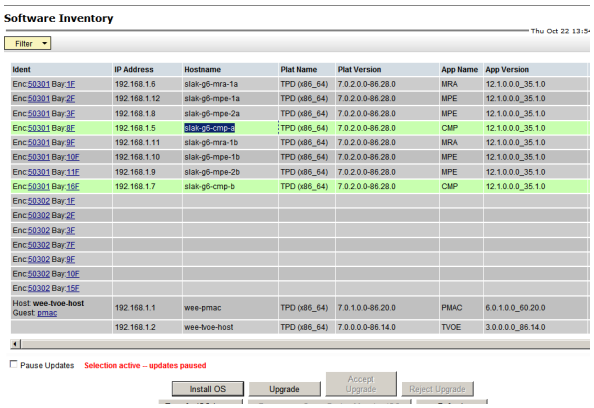
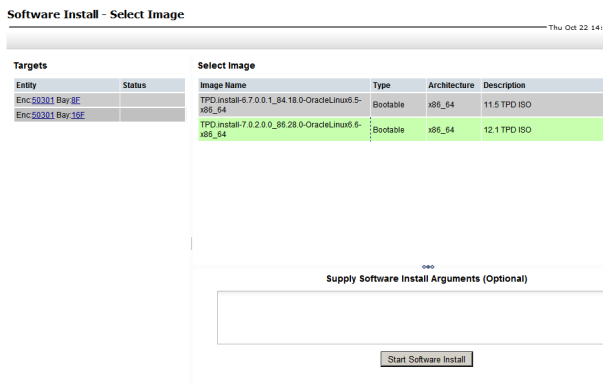
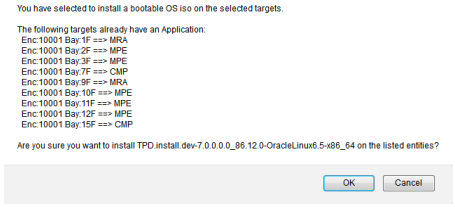
If the PM&C Control network is correctly configured, the PM&C will act as a DHCP server and provide control network addresses in the range of 192.168.1.2 – 255 to the blade servers in the managed cabinets/enclosures. PM&C always takes the address of 192.168.1.1. If the server has requested an IP address 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.
If there are IP addresses in this view, then the contol network is OK.
Proceed to step #2 if there are no IP addresses in the view.
Proceed to step #3 step if there are IP addresses in the view.</td></tr>
</table>

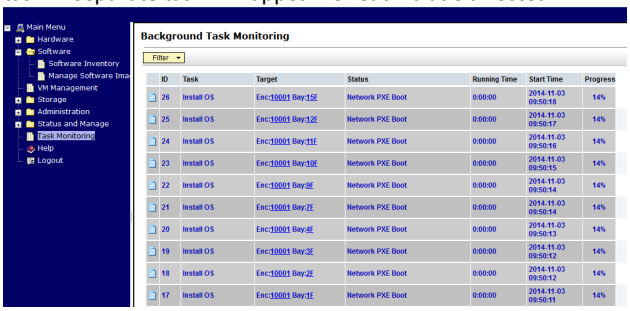
Procedure 13: IPM Blades via PM&C

2. ☐	**PM&C GUI:** Determine if Blades need to be IPM'ed - case: Software Inventory Display is "blank"	Navigate to **Software** -> **Software Inventory**.  If the display is blank, then it may be that the blades do not have an OS installed, and it is necessary to IPM the blades.  Move to the step (following) to attempt the OS install for one or more blades. NOTE: if the OS Install step fails, then it may be that the Control Network is not correctly established, and trouble shooting will be required.
3. ☐	**PM&C GUI:** Determine if Blades must be IPM'ed - case: IP Addresses and other information is shown in Software Inventory.	Navigate to **Software** -> **Software Inventory**.  If the Control network is established and the blades have an OS installed (TPD), then the PM&C gathers the current software information from the blades, and displays it in this list. • If the display shows an IP address (192.168.1.x), and PlatName = TPD, and Plat Version= xxxxx, then the blade is already installed with a version of the TPD OS. The version of TPD installed on the blades is usually not so important, as long as it is a 64 bit version and not newer than the required version for the Application.. The Application Install (Upgrade action on the PM&C GUI), to be performed in the next procedures, will automatically upgrade the TPD version on the blade to the correct version for the Application. i.e. the Application ISO includes the TPD version that the Application needs, and the Application install will automatically upgrade the blade TPD (if needed) before it installs the Application. If the version of OS installed on the blade is the same as what is required by the application, then the install will proceed more quickly because it does not need to upgrade TPD. • If the Inventory form does not not show the correct version of the TPD on the server, then the OS Install action is needed to install an appropriate version of TPD.

Procedure 13: IPM Blades via PM&C

4. ☐	**PM&C GUI:** Select Servers for OS install	Navigate to **Software** -> **Software Inventory**.  Based on the decisions of the previous steps, determine what servers need an IPM. 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.
5. ☐	**PM&C GUI:** Initiate OS Install	After selecting *Install OS,* the next screen on the left side shows the servers to be affected by this OS installation. From the list of available bootable images on the right side of the screen, select the correct TPD image to install to all of the selected servers  In this instance TPD 7.0.2.0.0_86.28.0 has been selected. See section 3.3 "Required Materials" for more information on the required release versions. Click on ***Start Software Install***, a confirmation window will pop up, click on **OK** to proceed with the install. 

Procedure 13: IPM Blades via PM&C

6. ☐	**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%".
7. ☐	**PM&C GUI:** IF OS Install fails	If the OS Install Fails, the Task status will show failed. Note the step where the Installation failed. It is also useful to login the server console (either via the iLO port, or using a local Key Board and Monitor), and try the OS Install again. Note where the console is reporting a boot problem. If the boot hangs when trying to get a DHCP address, and execute PXE boot, then the Control Network is a problem. Trouble shoot the IP networking before proceeding. **You have now completed this procedure.**

4.5 INSTALL POLICY APPLICATION SOFTWARE

The following procedures install the Policy Application software to the blade servers.

There are several Application packages (.iso) that comprise the Policy Solution.

- CMP – Manager
- MRA – Routing Agent (Also know as the PFE or Policy Front End)
- MPE – Policy Server

Important Information:

- Layout diagram for C-class enclosure(s), identifying which bays will run which Policy application.
- IP Addressing design for the Application Networks (VLAN Ids also)
- Naming assignments (hostnames for Policy Servers)
- NTP Time source for these servers
- DNS Server addresses (optional)
- SNMP Managers

CAUTION: Do not mix up the enclosures when deploying the applications.

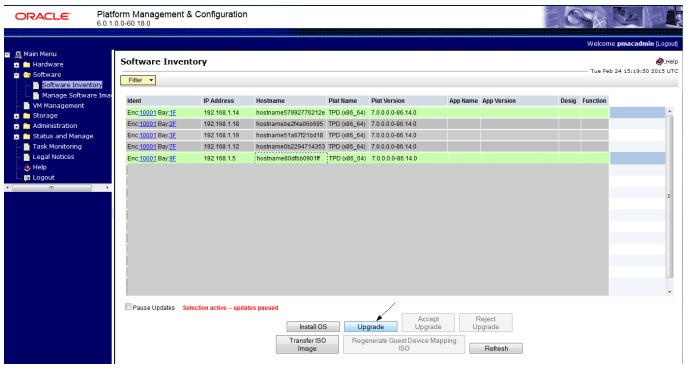
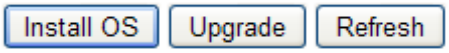
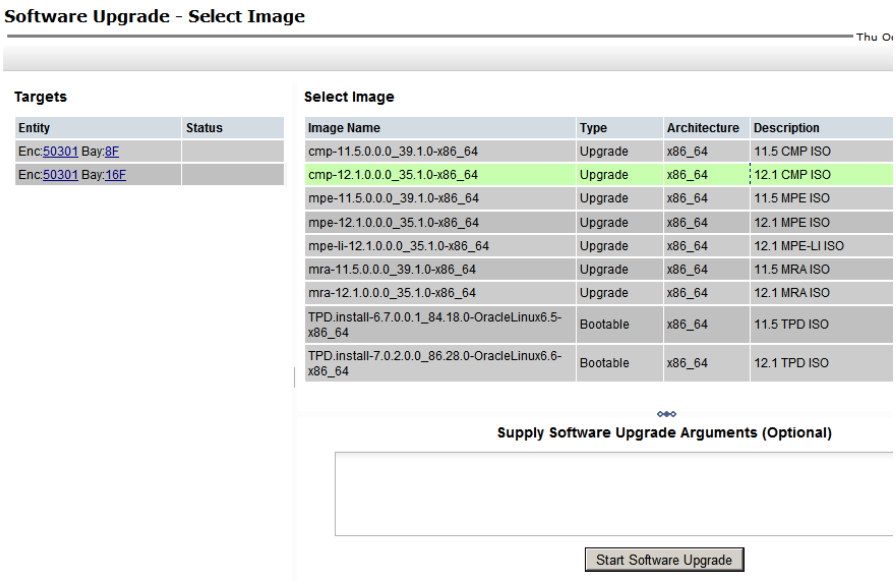
The bottom enclosure in a cabinet is identified in Oracle documentation as Enclosure 1. The Enclosure above this is Enclosure 2. However, PM&C GUI forms may list the enclosures with Enclosure 1 listed first, and Enclosure 2 listed below this in the form lists. Pay attention to this point, as it can be a source of confusion.

Procedure 14: Install the Application Software on Blades using PM&C

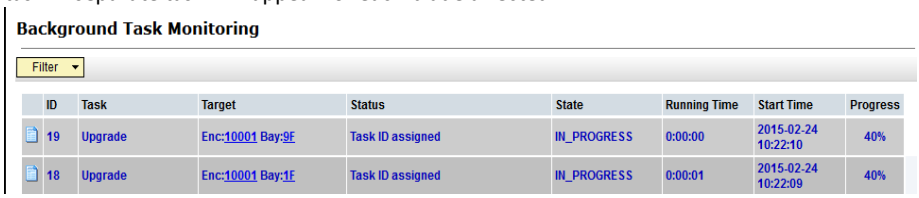
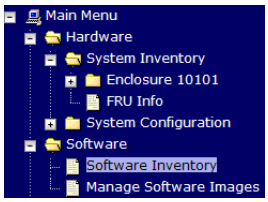
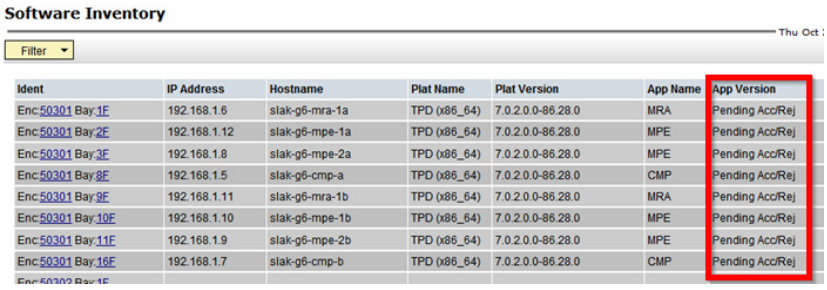
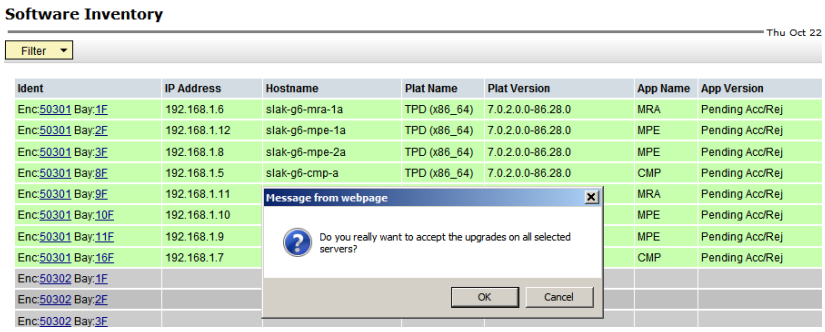
Procedure 44. Install the Application Software on Blades using PM&C

STEP #	This procedure will provide the steps to install Policy 12.1.x Application on the Blade servers. **Prerequisite**: *Procedure 13: IPM* Blades has been completed. *Loading Software Images to PM&C* has been completed. 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: **http://<management_network_ip>** Login as PM&C admin user.

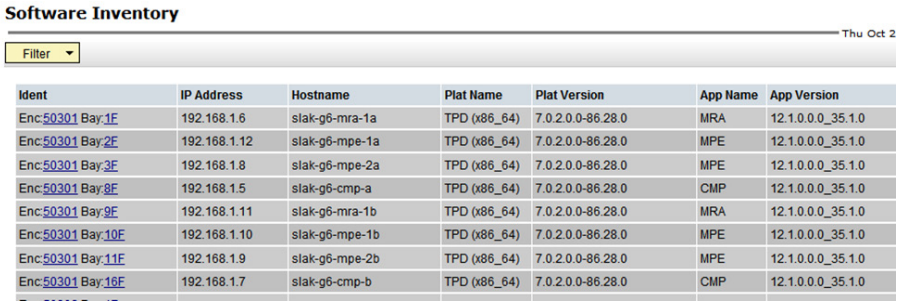
Procedure 44. Install the Application Software on Blades using PM&C

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:** Here it can be noted that 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** 
3. ☐	**PM&C GUI:** Initiate Application Install	The left side of this screen shows the servers to be affected by this OS installation. From the list of available bootable images on the right side of the screen, select one OS image to install to all of the selected servers.  Click on **Start Software Upgrade**, a confirmation window will pop up, click on **OK** to proceed with the install.

Procedure 44. Install the Application Software on Blades using PM&C

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.**
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**.  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. 

Procedure 44. Install the Application Software on Blades using PM&C

7. ☐	**Verify Application Installations**	Navigate to **Software** -> **Software Inventory**.  Software Inventory Thu Oct 2 Filter Ident / IP Address / Hostname / Plat Name / Plat Version / App Name / App Version Enc:50301 Bay:1F / 192.168.1.6 / slak-g6-mra-1a / TPD (x86_64) / 7.0.2.0.0-86.28.0 / MRA / 12.1.0.0.0_35.1.0 Enc:50301 Bay:2F / 192.168.1.12 / slak-g6-mpe-1a / TPD (x86_64) / 7.0.2.0.0-86.28.0 / MPE / 12.1.0.0.0_35.1.0 Enc:50301 Bay:3F / 192.168.1.8 / slak-g6-mpe-2a / TPD (x86_64) / 7.0.2.0.0-86.28.0 / MPE / 12.1.0.0.0_35.1.0 Enc:50301 Bay:8F / 192.168.1.5 / slak-g6-cmp-a / TPD (x86_64) / 7.0.2.0.0-86.28.0 / CMP / 12.1.0.0.0_35.1.0 Enc:50301 Bay:9F / 192.168.1.11 / slak-g6-mra-1b / TPD (x86_64) / 7.0.2.0.0-86.28.0 / MRA / 12.1.0.0.0_35.1.0 Enc:50301 Bay:10F / 192.168.1.10 / slak-g6-mpe-1b / TPD (x86_64) / 7.0.2.0.0-86.28.0 / MPE / 12.1.0.0.0_35.1.0 Enc:50301 Bay:11F / 192.168.1.9 / slak-g6-mpe-2b / TPD (x86_64) / 7.0.2.0.0-86.28.0 / MPE / 12.1.0.0.0_35.1.0 Enc:50301 Bay:16F / 192.168.1.7 / slak-g6-cmp-b / TPD (x86_64) / 7.0.2.0.0-86.28.0 / CMP / 12.1.0.0.0_35.1.0 You can now confirm that the “App Version” column no longer displays the “Pending Acc/Rej” status but rather shows the correct Application Version. **You have now completed this procedure.**

4.6 ESTABLISH NETWORKING TO CUSTOMER NETWORK

The following procedures bring up the network connections from the Policy equipment to the customer network.

4.6.1 Connect PM&C iLO to Customer Network

The PM&C iLO port is recommended to be networked as standard switchport access port direct to a customer switch. Since this is a “safe” connection from a network perspective, it may be easier to get this connection brought up by the customer.

Verify the following:

- the PM&C iLO port has the customer assigned IP address configured
- the cable from PM&C iLO port to the customer switch is in place
- the customer switch port is configured
- the customer switch port is enabled

Remotely, verify:

- http access to iLO GUI, and start the iLO Remote Console tool
- ssh access to the iLO vsp (Virtual Serial Port), and then to the PM&C Server console session

Note: from this iLO access, the following are all possible:

- console access to PM&C
- command line access to switches
- File transfer capability (via iLO Remote console “Virtual Mount” capability)
- Ssh access to all servers

The following section is used to enable access to the CMP GUI, PM&C GUI or OA GUI access

4.6.2 Connect c-Class system to Customer Network

Customer will typically configure the customer network interfaces, but shutdown the ports until the Policy system IP networking is configured and the Installation engineer confirms that the system is ready to be networked.

It is recommended to share the Policy system port configurations with the customer IT person, to allow them to verify that it meets their expectations.

When the customer opens the ports, there may be troubleshooting required of:

- Cabling
- Policy Server IP network configuration
- Customer IP network configuration

This may be easier to resolve if the Installation engineer is on site, and can trace cables and plug a laptop into a switch to run port mirroring. Issues can also be resolved remotely via the PM&C iLO connectivity, if this is in-place. It is ideal if the Installation engineer is able to sit with the customer networking person during this activity to compare configurations and discuss the issues being seen.

Note: some customers will only allow customer switch configuration changes to be implemented in a maintenance window.

Key Access points to discuss/verify with the customer:

- Customer can access the CMP GUI (accessible after initial config), all blade server iLOs, PM&C GUI and OA GUI from within their corporate network
- Customer allows Installation engineer, who is at customer premises (customer lab for example), to access product GUIs.
- Installation Engineer can access the CMP GUI, all blade server iLOs, PM&C GUI and OA GUI remotely (depends on customer security agreements)

If IP networking is NOT available, engineer can proceed to next steps, but will need to continue to work from the site where they can connect a laptop to the local switch to access these GUIs.

Installation of the OS (TPD Platform), and the Policy Software Application (CMP/MPE/MRA) in a c-Class environment has now been completed.

It will now be necessary to proceed to Section 7 “Configure Policy Application Servers” to perform the required “Initial Configurations” for each server. Steps in Section 7 will configure the IP address assignments that will be used for remote ssh access and for the servers to communication with other as required to configure the Policy Solution Network Topology.

Section 5: “Installing an HP RMS environment” & Section 6:”Installing an Oracle x5-2 RMS environment” detail the installation procedures specific only to those environments.

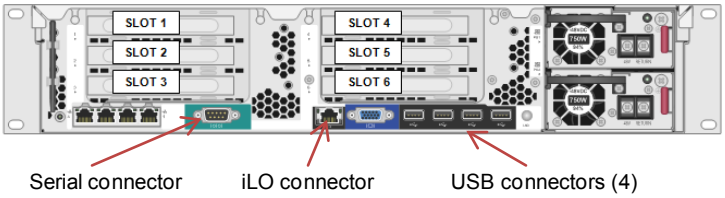
5. INSTALLING AN HP RMS ENVIRONMENT

5.1 PREPARATION PROCEDURES

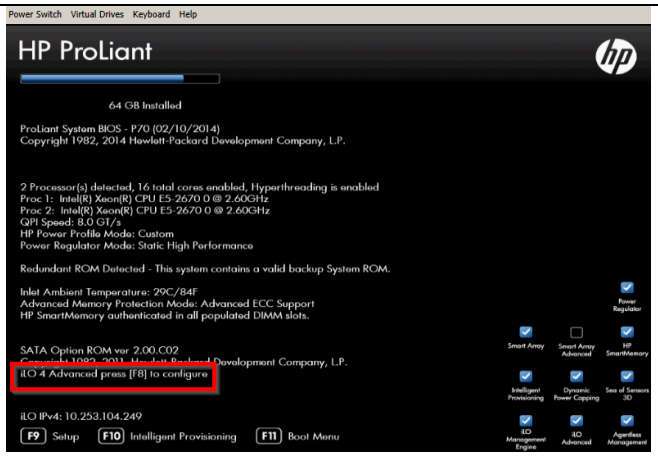
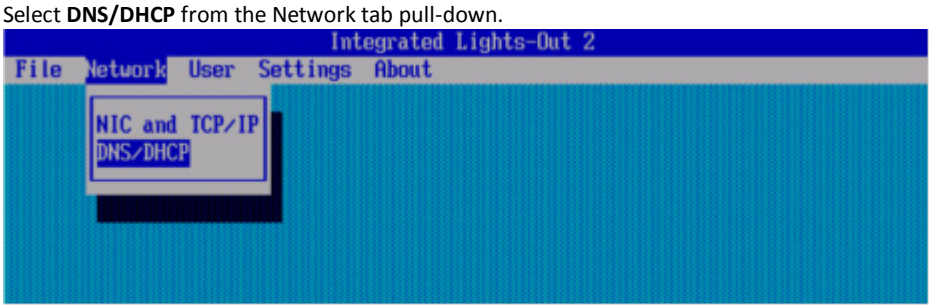
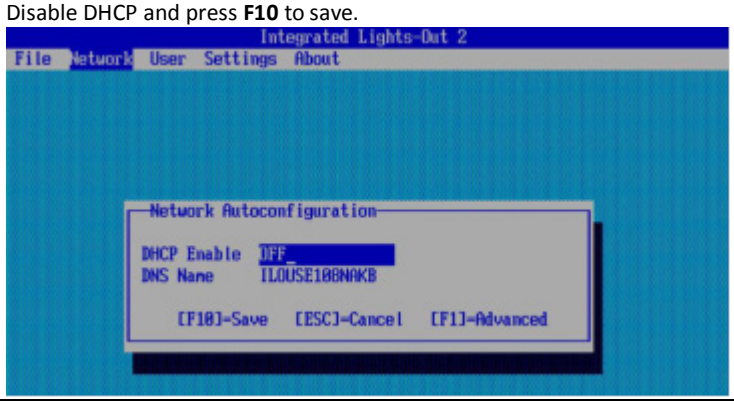
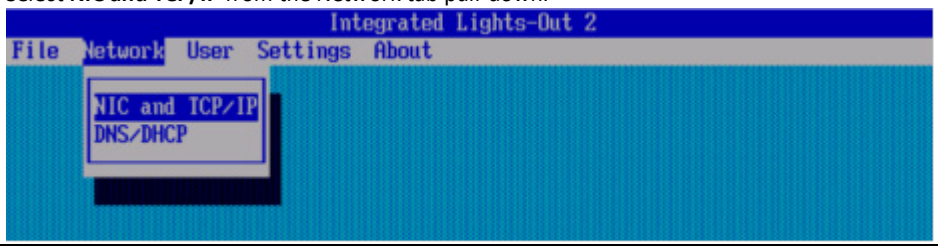
The following procedures are carried out on the HP DL380 server as example for HP RMS H/W.
For more details please refer to the supplemental procedures in Section 8 of this document. Additional information can also be found in *TPD Initial product Manufacture* as found in the reference section of this document.

Procedure 15: Configure DL380 iLO Port

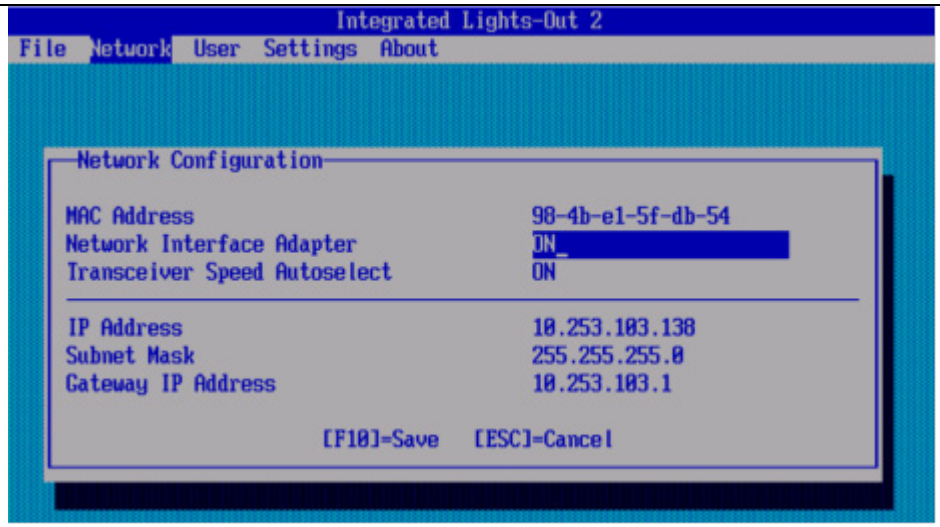
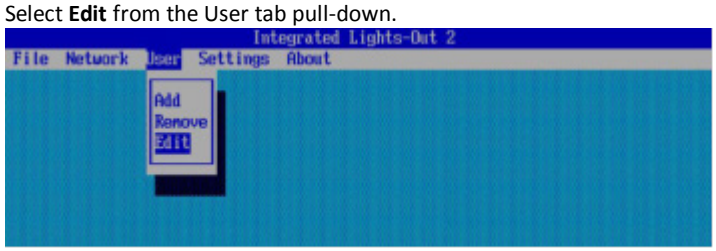
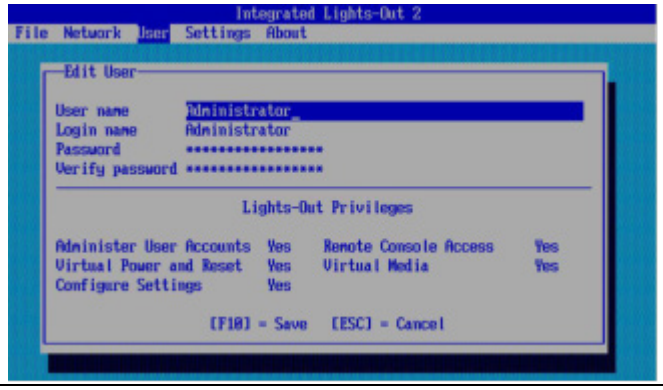
Procedure 15: Configure DL380 iLO Port

STEP #		
	This procedure will configure the iLO Port IP address from the Console Boot Menu. (It is also possible to configure the iLO Port IP address from the iLO GUI, and from a ssh session to the server. These other methods to set the iLO Port address are not covered in this procedure.) **Needed material:** - IP Addresses from the Network IP Planning document (or other customer provided document) - Local console Access (Monitor/Keyboard) - Connect laptop to server's Serial Console 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. ☐	**Console:** connect to console	Connect to the server console (refer to Section 8 "Supporting Procedures" for additional information) 
2. ☐	**Console:** reboot server	reboot the server: either press reset button, or run the command: # **shutdown -r now** [If the Policy application is running, it is recommended to stop the application before reboot of the server.]
3. ☐	**Console:** Enter iLO configuration menu	As the server is completing its POST startup, you will see the message: <Integrated Lights-Out press [F8] to configure> at the bottom of the screen. → press **F8** to access the iLO configuration menu

Procedure 15: Configure DL380 iLO Port

		
4. ☐	**Console:** Access DHCP setting form	Select **DNS/DHCP** from the Network tab pull-down. 
5. ☐	**Console:** Configure DHCP Off Press F10 to save	Disable DHCP and press **F10** to save. 
6. ☐	**Console:** Access IP address form	Select **NIC and TCP/IP** from the Network tab pull-down. 
7. ☐	**Console:** Configure IP address for iLO port	Configure the **IP address**, **netmask**, and **gateway**, and press **F10** to save.

Procedure 15: Configure DL380 iLO Port

		
8. ☐	**Console:** Access User Edit form	Select **Edit** from the User tab pull-down. 
9. ☐	**Console:** Configure Administrator password	Configure a Password for the default Administrator account, as per TR006061, and press **F10** to save. 
10. ☐	**Console:** Add root user, and password.	Select **Add** from the User tab pull-down menu and create a root user, with all privileges set to yes and the password set per TR006061. Press **F10** to save.
11. ☐	**Console:** Exit the configuration	Exit the configuration utility. Server will proceed with OS boot. **You have now completed this procedure.**

Procedure 16: Update Server Firmware

NOTE: Please refer to the HP FUP 2.2.8 upgrade documents to update the Firmware on HP RMS servers .

[4] E59721 - HP Solutions Firmware Upgrade Pack, Upgrade Guide 2.2.8

[5] E59723 - HP Solutions Firmware Upgrade Pack, Software Centric Release Notes 2.2.8

Further detail is also provided in section 3.5 "Acquiring Firmware" of this document

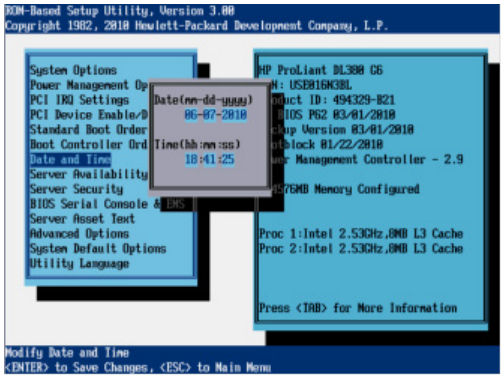
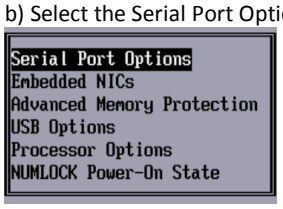
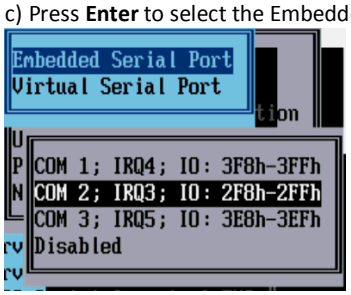
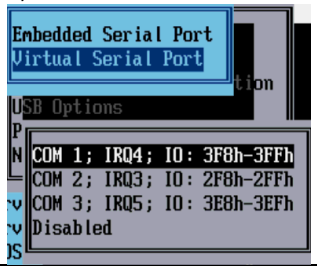
Note: Access to the HP 2.2.8 Firmware Upgrade Guide may require enablement form Oracle Support

Procedure 17: Configure BIOS

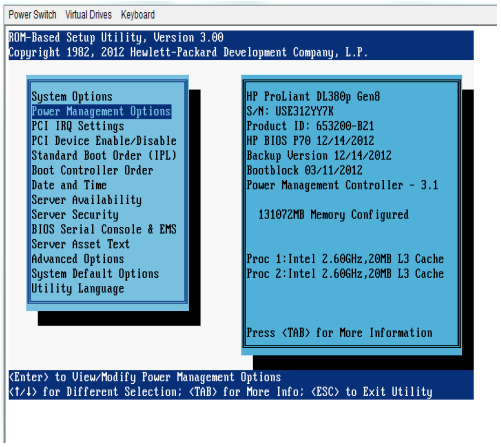
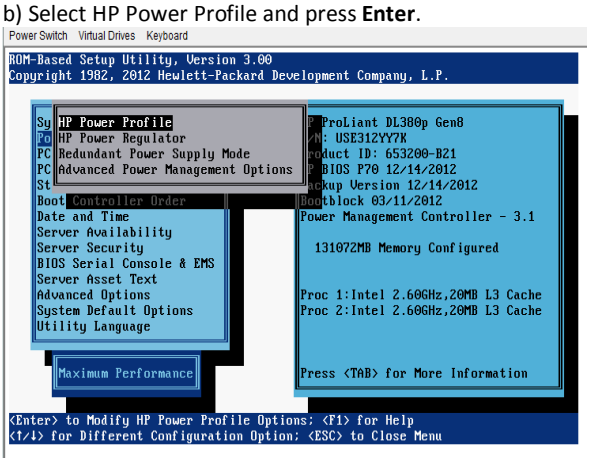
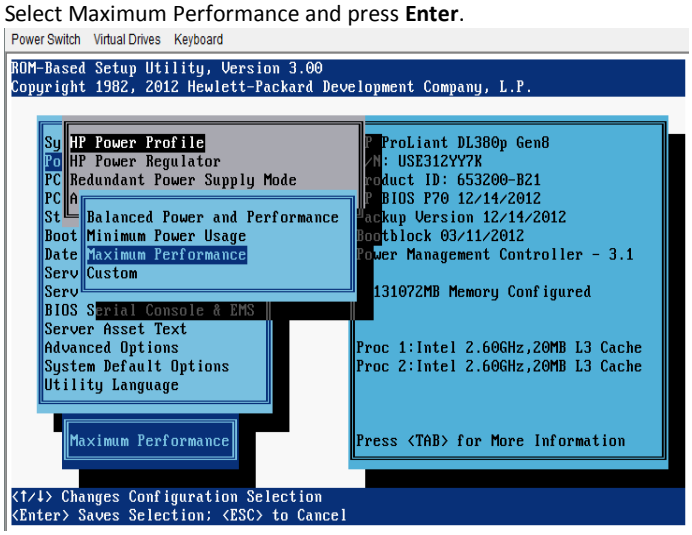
Procedure 17: Configure BIOS

STEP #	This procedure will configure the RMS BIOS. **Needed material:** - IP Addresses from the Network IP Planning document (or other customer provided document) 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. ☐	**Connect:**	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 the Remote Console - refer to Section 8 "Supporting Procedures" for additional information
2. ☐	**Console:** reboot server	reboot the server: Login as root: # **shutdown -r now** [If the Policy application is running, it is recommended to stop the application before reboot of the server.]
3. ☐	**Console:** Enter Setup configuration menu (F9)	As the server is completing its POST startup, you will see the message: To press F9 to access BIOS settings → press **F9** to access the Setup Utility

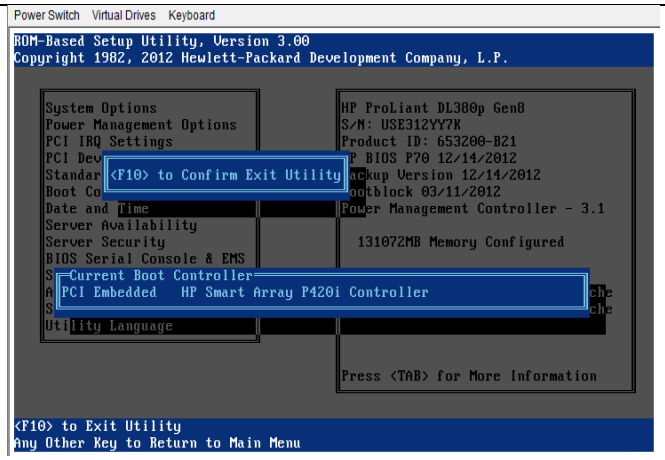
Procedure 17: Configure BIOS

4. ☐	**Console:** Select and Set Data and Time	Scroll down until you see Date and Time, and press **Enter**. Set the date and time, according to UTC, and press **Enter**. For example: 
5. ☐	**DL360 Console:** Configure Serial port for iLO (if needed)	Configure Serial Port for iLO by completing the following: a) Scroll down to the System Options and press **Enter**. b) Select the Serial Port Options and press **Enter**.  c) Press **Enter** to select the Embedded Serial Port, change the value to **COM2**, and press **Enter**.  d) Press **Enter** to select the Virtual Serial Port, change the value to **COM1**, and press **Enter**. 
6. ☐	**DL360 Console:** Select Standard Boot Order menu	Return to the main menu, select **Standard Boot Order**, and press **Enter**.
7. ☐	**DL360 Console:** Set Standard Boot Order	Validate the boot order and modify as needed. Press **Esc** to return to the main menu.

Procedure 17: Configure BIOS

8. ☐	**DL360 Console:** Select Power Management Options menu	a) Select Power Management Options and press **Enter**.  b) Select HP Power Profile and press **Enter**. 
9. ☐	**DL360 Console:** Set Power Profile to Maximum Performance	Set the Power Profile to Maximum Performance, as follows: Select Maximum Performance and press **Enter**.  Press **Esc** until you are prompted to Confirm Exit Utility.

Procedure 17: Configure BIOS

		 **You have now completed this procedure.**

5.2 SOFTWARE INSTALLATION (RMS)

Procedure 18: IPM of HP RMS Server

Procedure 18: IPM of HP RMS Server

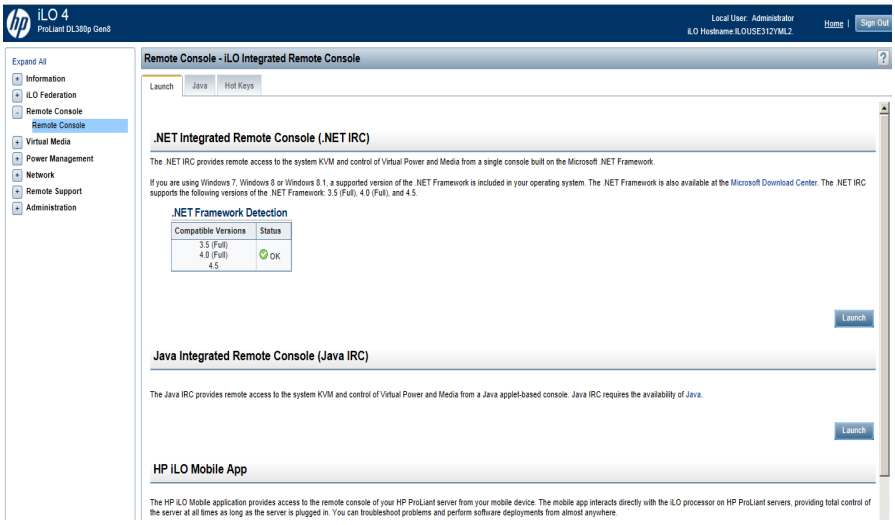
STEP #	This procedure will install system OS (IPM) of the server Refer to Section 8 "Supporting Procedures" for additional information Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. **Needed material:** - TPD ISO image file to be used for virtual mount accessible on laptop or - USB device prepared with bootable version of TPD image **NOTE**: Screenshot given in this procedure are example of DL360 G6 and different H/W displays may vary. 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 TPD ISO image file using the method described in Procedure 49: Create a Bootable USB with TPD or TVOE ISO image or other suitable method. 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 OR Use the virtual mount capability of the iLO remote console to mount the TPD ISO image file using the following procedure

Procedure 18: IPM of HP RMS Server

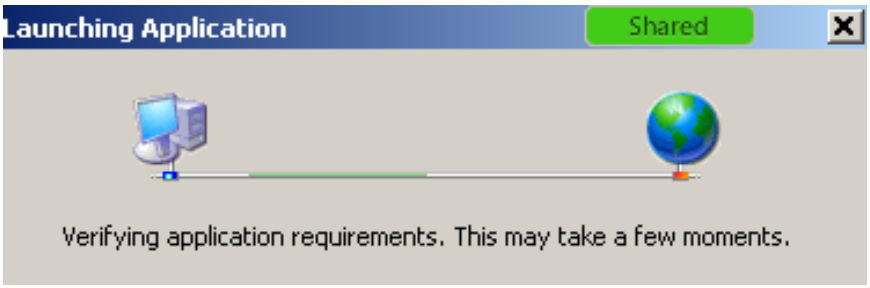
Mount the ISO image through the iLO

1. Login to the iLO console via IE/Firefox

2. Navigate to Remote Console:



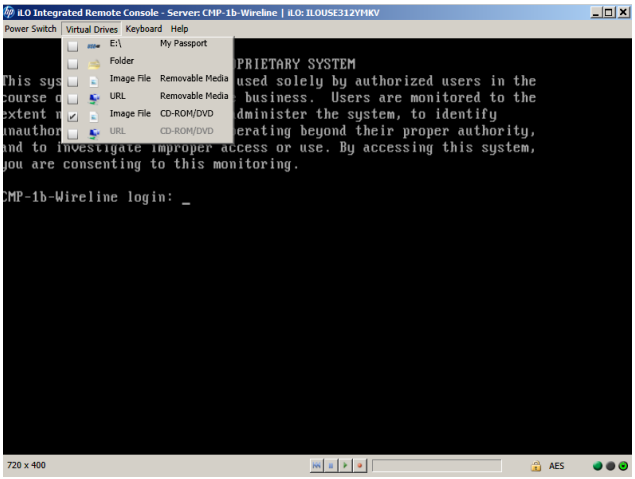
3. Click “Launch” to start the remote console, an indication “verifying application requirements” message appears:



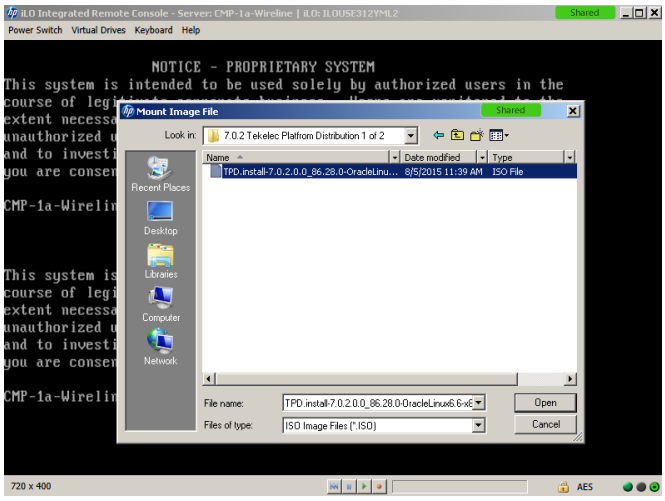
Procedure 18: IPM of HP RMS Server

4. Confirm to launch the console in the next security warning message by clicking “Run”:

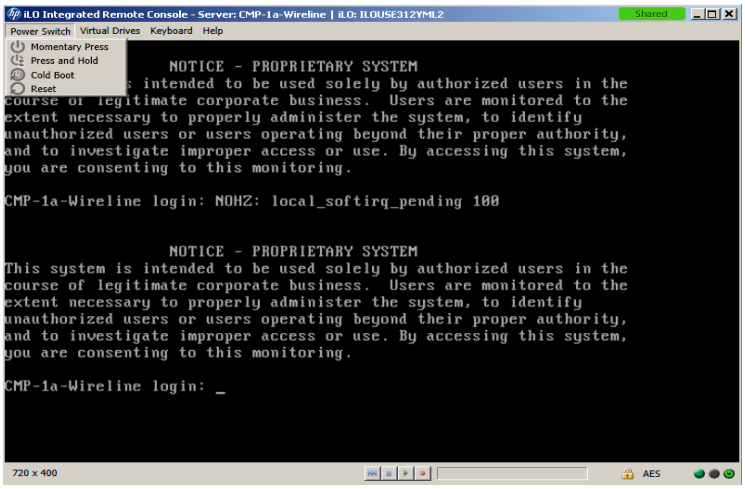
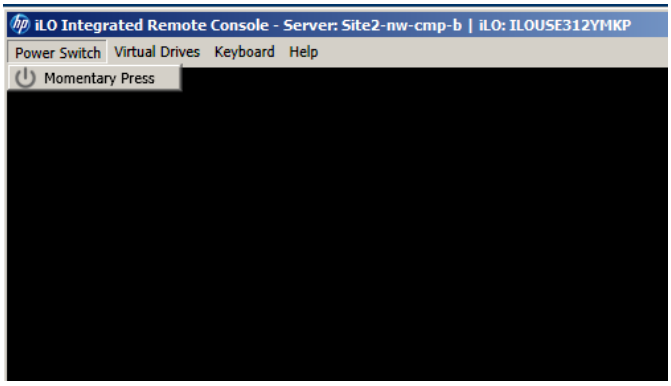
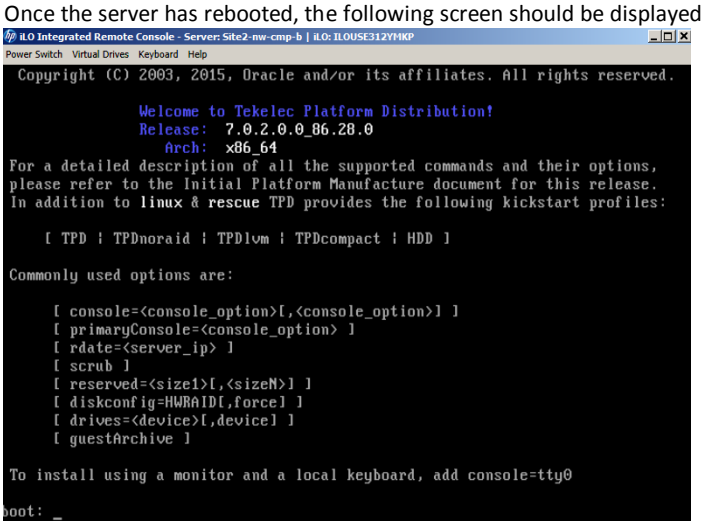
5. Select Virtual Drives menu:



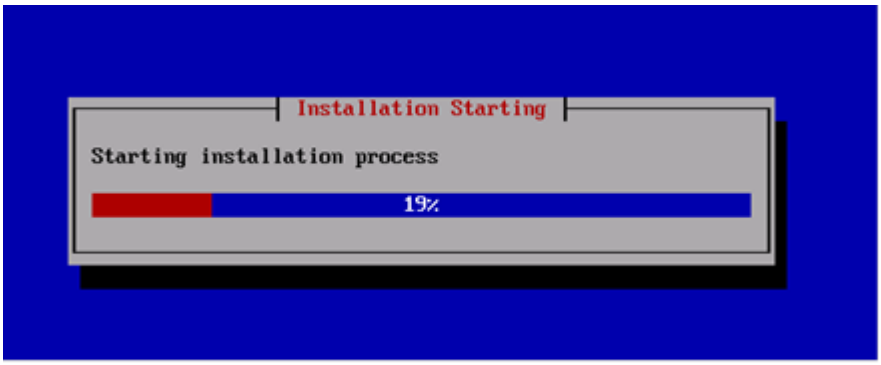
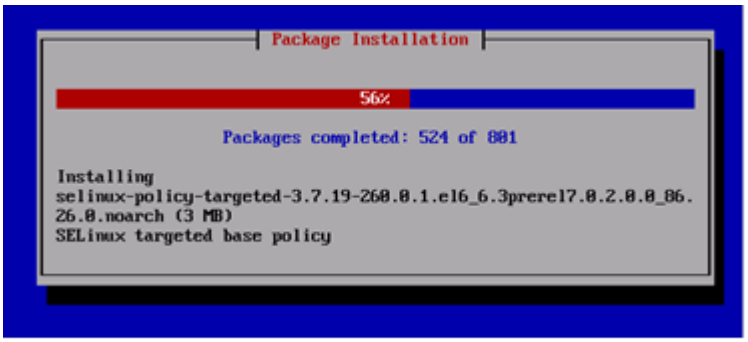
6. Select Image file CD-ROM/DVD and browse to the TPD ISO location then click open:



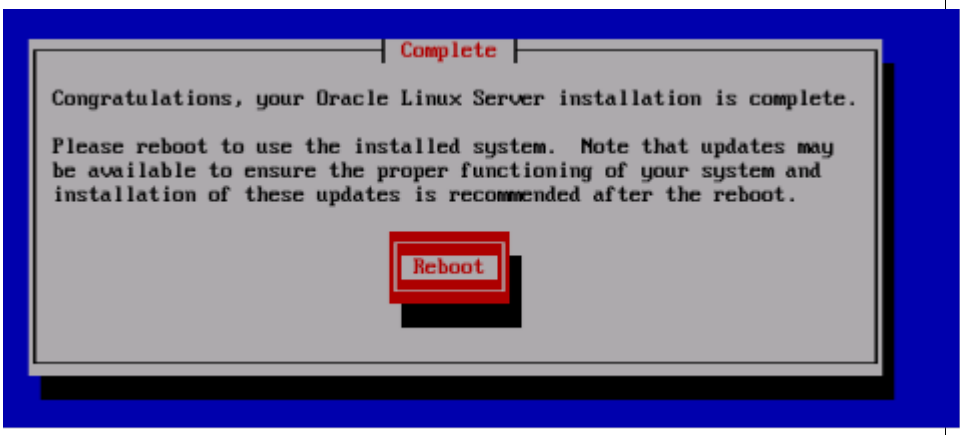
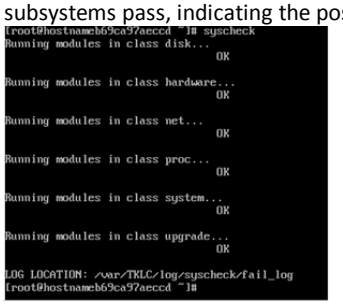
Procedure 18: IPM of HP RMS Server

2. ☐	**Console:** Boot server, wait for TPD boot: form	From the Power switch menu on the remote console, click "Momentary Press" to initate a soft shutdown.  Wait for the server to power down and the Power Switch options to display only the momentary press. Option. At this point click momentary press again to start the server.  Once the server has rebooted, the following screen should be displayed : 

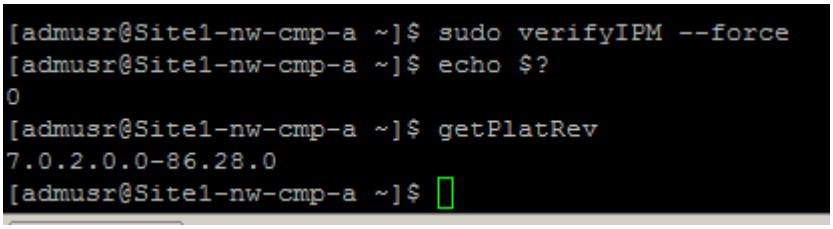
Procedure 18: IPM of HP RMS Server

3. ☐	**Console:** Enter TPD boot: command with correct options TPD install takes 20 - 40 minutes to complete	IPM the server using the following command at the boot prompt: •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 hit the carriage return and you will see something like the following screen indicating that OS is installing **Note:** If the server was previously configured with another **non-Policy Solution Application** it may be necessary to clean up Logical Disc partitions created by this Application. To perform that, use the following TPD command with scrub option at the boot prompt: boot: **TPDnoraid scrub console=tty0 diskconfig=HWRAID,force** This may take up 4 hours, depending on the disc configuration. 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: 

Procedure 18: IPM of HP RMS Server

		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 . 
4. ☐	**Console:** Press Enter to reboot	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. In the case a DVD was used as the bootable device the DVD should eject automatically. If it happens that the server boots to the bootable media again after pressing the Reboot option you should wait to be returned to the Reboot prompt as above rather than interrupting the installation process. Simply remove the bootable image that was not removed the first time and Reboot again.
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	At the login prompt, run the ***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.

Procedure 18: IPM of HP RMS Server

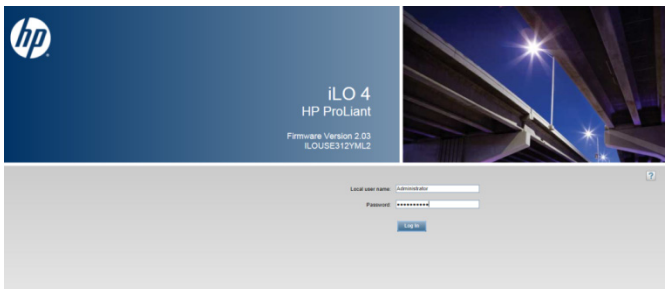
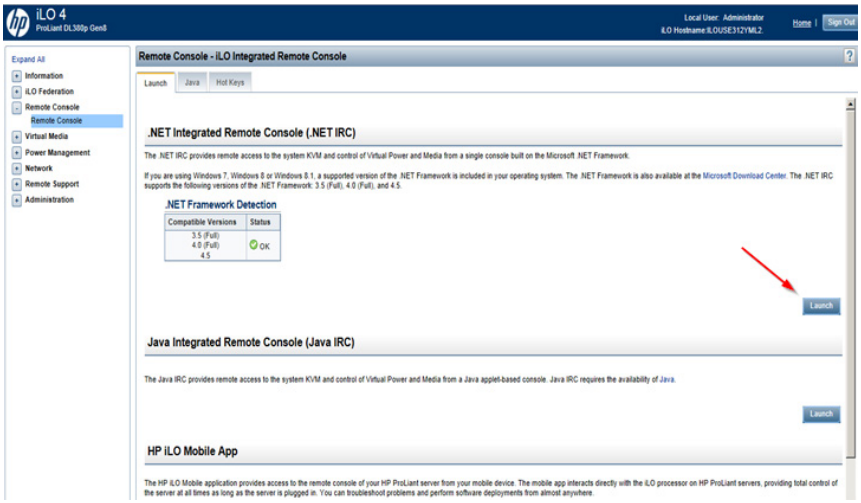
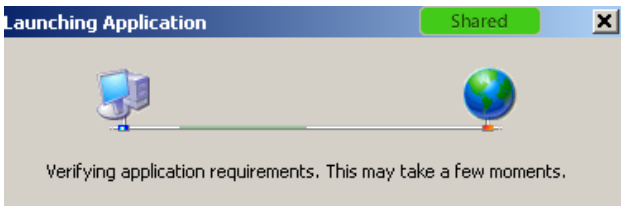
7. ☐	**Console:** Verify Install success	Verify that IPM completed successfully by checking the install logs for errors and displaying the install TPD platform version. . To do this, log in as ***admusr*** and then run the following commands: $ **sudo verifyIPM** (--force if needed) $ **sudo echo $?** (should return 0 errors) $ **sudo getPlatRev** (should return the current TPD version installed)  Previous screen shot shows no errors returned which indicates the TPD installation process is successfully completed. If errors are found, contact Oracle Customer Support. **You have now completed this procedure.**

Procedure 19: RMS Application Software Installation

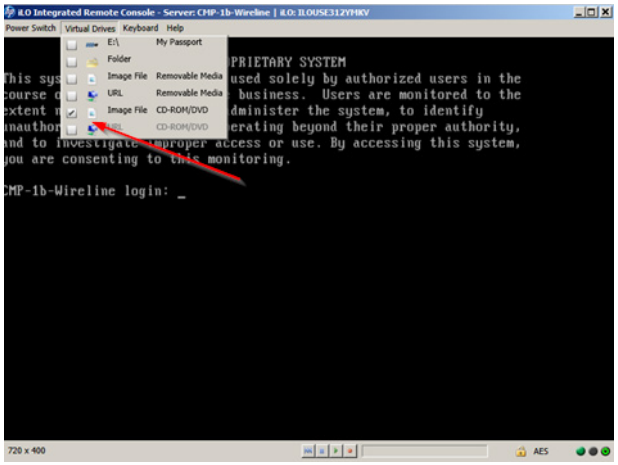
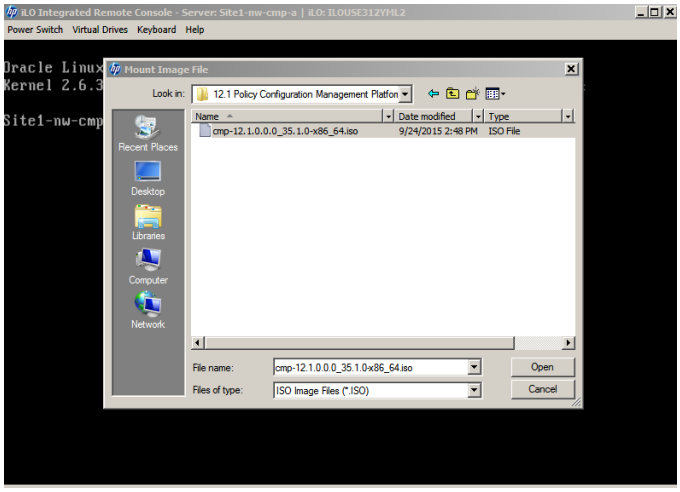
Procedure 19: ***RMS Application Software Installation***

STEP #	This procedure will install the Application Software. **Needed material:** - Application software ISO image files (cmp, mpe, and optionally mra) - See Section 3.3 "Required Materials" and Section 3.4 "Acquiring Software" for details on the required versions 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. **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. Additionally any method that places the Policy Application ISO image file in the /var/TKLC/upgrade directory of the target server is acceptable.	
1. ☐	Make the Policy Application ISO images available for installation	Copy the Policy Application ISO image file (CMP,MPE or MRA) 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 Use the virtual mount capability of the iLO remote console to mount the Policy Application ISO image file using the following procedure:

Procedure 19: ***RMS Application Software Installation***

		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. Mount the ISO image through the iLO 1. Login to the iLO console via IE/Firefox  2. Navigate to Remote Console:  3. Click "Launch" to start the remote console, an indication of verifying application requirements message appears:  4. Confirm to launch the console in the next security warning message by clicking "Run":

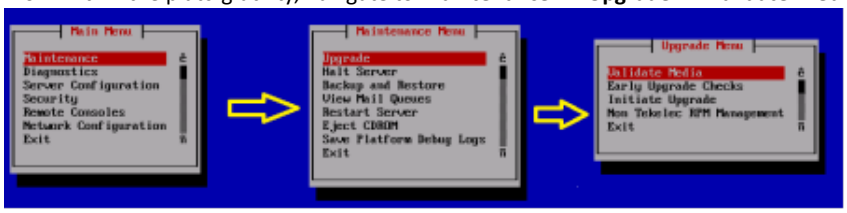
Procedure 19: ***RMS Application Software Installation***

		 5. Select Virtual Drives menu:  6. Select Image file <CD-ROM/DVD> from the drop down tab. Browse to the Policy Application ISO image file for the target serer. **Note:** Make certain that the ISO image file selected (CMP, MPE or MRA) 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.
2. ☐	**Console:** run platcfg and validate the media	Login as <admusr> if not already logged in. Start the Platcfg utility by issuing the following command:

Procedure 19: ***RMS Application Software Installation***

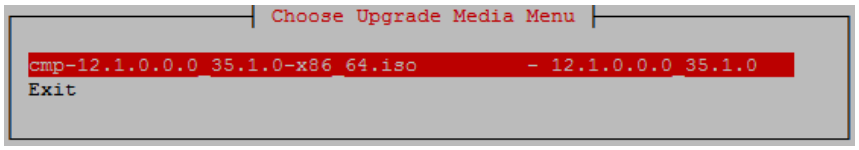
#sudo su - platcfg

From within the platcfg utility, navigate to **Maintenance ➢ Upgrade ➢ Validate Media**:



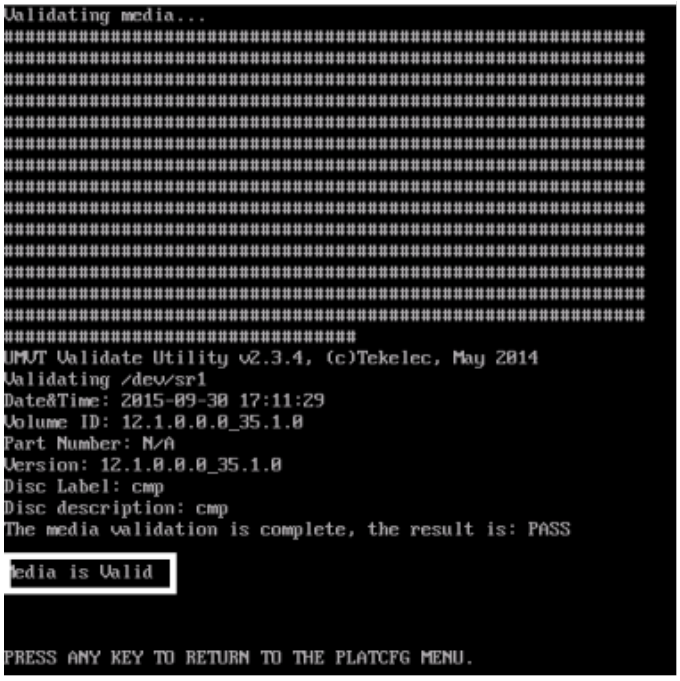
Then choose the ISO image and hit enter:

Note: Depending on the metod used the platcfg utility will search for any mounted ISOs and if successful will display the Policy Application ISO image file to install

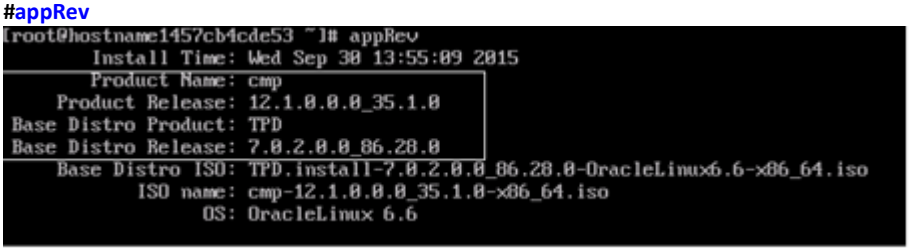
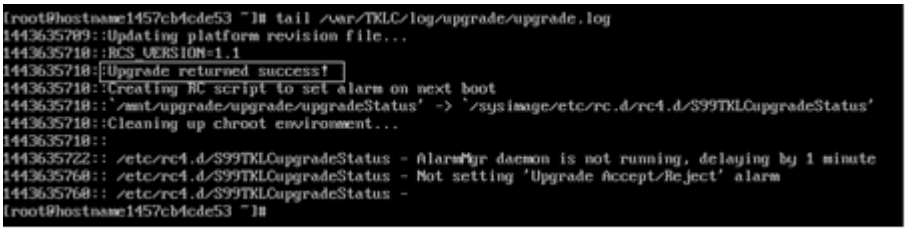


Validation progress is indicated in the console by "#" signs as shown below:

Make sure at the end of the validation process, the result is indicating "Media is Valid":



Procedure 19: *RMS Application Software Installation*

3. ☐	**Console:** Select ISO to install, and confirm Application install may take 20 Minutes – if installing with a virtual mount, it will take longer	From within the platcfg utility, navigate to **Maintenance ➢ Upgrade ➢ Initiate Upgrade**; Select the ISO image as per the previous step, and hit **ENTER** **Note:** The server will reboot twice during the installation process, Do Not Remove the media at this time.
4. ☐	**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**  Verify: • TPD revision installed • Policy application installed and its revision
5. ☐	**Console:** Verify Install success	**# tail /var/TKLC/log/upgrade/upgrade.log**  Make sure the upgrade was successful. In case UPGRADE STATUS was not successful, then inspect following log files for more details and errors occurred: • **/var/TKLC/log/upgrade/upgrade.log** • **/var/TKLC/log/upgrade/ugwrap.log**
6. ☐	**Remove Media**	Once the login prompt is displayed, installation is complete. Remove the USB device or transferred ISO image file from the server. If the installation was done by virtual media mount, disconnect the ISO file.
7. ☐	**Policy Solution servers**	This procedure needs to be followed for each Policy application component (cmp/mpe/mra) on each of the Policy Solution servers. **You have now completed this procedure.** Proceed *to* *Section 7: Configure Policy Application Servers*

6. INSTALLING AN ORACLE X5-2 RMS ENVIRONMENT

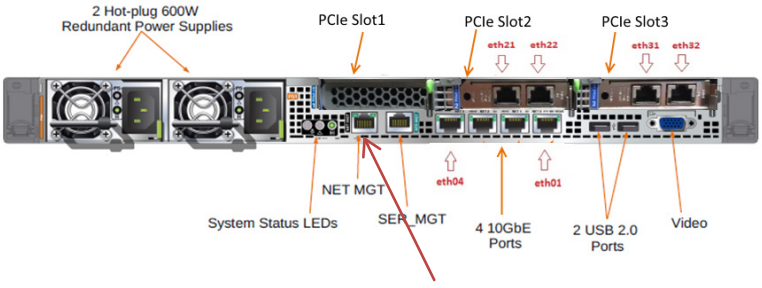
6.1 PREPARATION PROCEDURES

The following procedures are carried out on the Oracle X5-2 server as an example for Oracle RMS H/W. For more details please refer to the supplemental procedures in Section 8 of this document. Additional information can also be found in [6] *TPD Initial product Manufacture* as found in the reference section of this document.

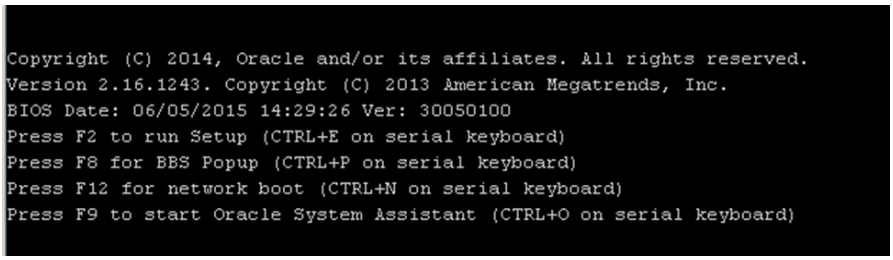
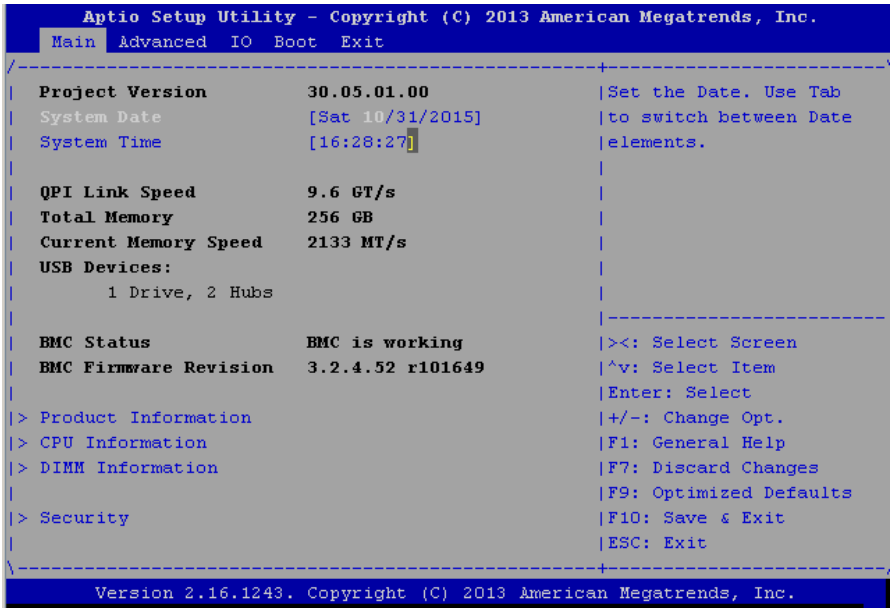
Procedure 20: Configure Initial ILOM IP address and BIOS Settings

Procedure 20: Configure Initial iLOM IP address and Bios Settings

STEP #		
	This procedure will configure the iLOM Port IP address using the BIOS setup utility accessible on bootup. **Needed material:** - IP Addresses from the Network IP Planning document (or other customer provided document) - Monitor and keyboard to connect directly to the server or - Connect laptop to serial port or 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.	

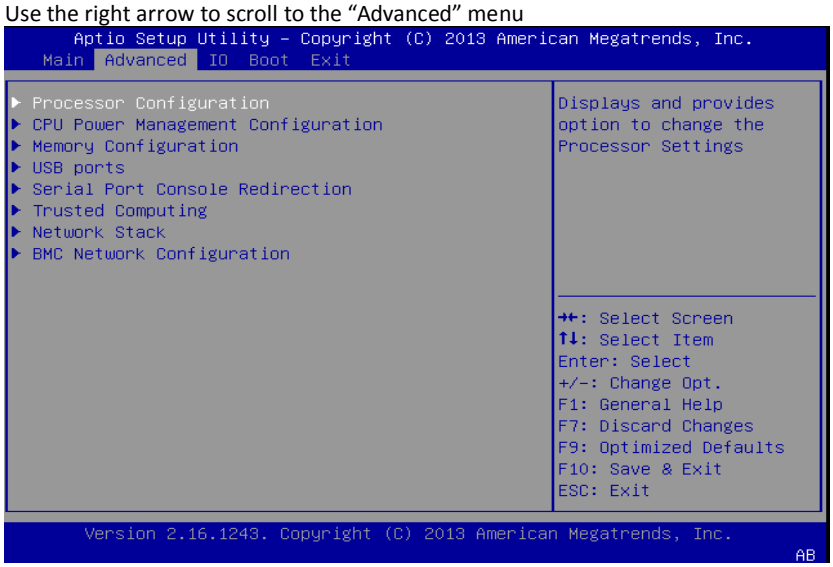
1. ☐	**Console:** connect to console	Connect to the Server:
		- using a VGA Display and USB Keyboard, or
		- using the Server Management Serial Port
		- refer to Section 8 "Supporting Procedures" for additional information
		
		 
		
		X5-2 Rear Facing Interconnections
		
		Note: To establish a serial console connection the connecting device should be set as follows:
		`Terminal Type [VT100+]`
		`Bits per second [9600]`
		`Data Bits [8]`
		`Parity [None]`
		`Stop Bits [1]`
		`Flow Control [None]`

Procedure 20: Configure Initial iLOM IP address and Bios Settings

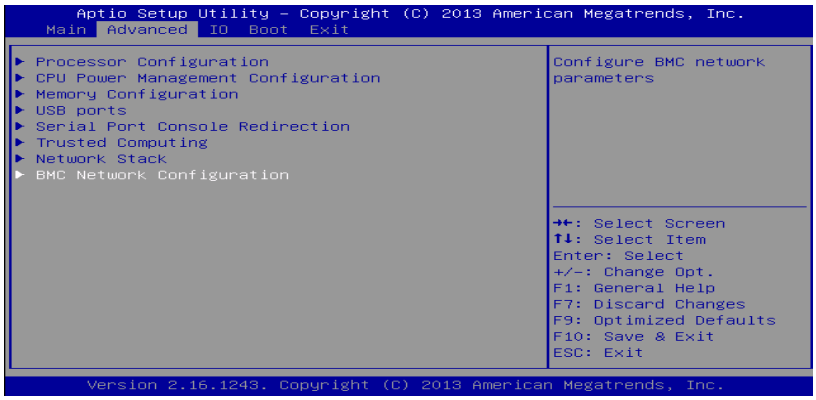
2. ☐	**Console:** Access Bios Setup Utility by powering up the server	This procedure will assign an initial IP address to the ILOM interface from the console, using the Bios setup utility. After assigning the IP address to the ILOM, future connections can be made directly to the web interface of the iLOM using a laptop directly connected to the iLOM port on the server. Alternately a web interface connection to the iLOM IP address assigned in this procedure can be used if the network connectivity has been established to support such a connection. In the case the ILOM already has a known IP address assigned but the IP address is unknown this procedure can also be used to confirm the current iLOM IP address. **Establish access to the server post startup with directly connected monitor and keyboard or serial connection from a laptop. Reset the power.** On a server without an OS installed, you will see something similar to the following as the system power up.  Copyright (C) 2014, Oracle and/or its affiliates. All rights reserved. Version 2.16.1243. Copyright (C) 2013 American Megatrends, Inc. BIOS Date: 06/05/2015 14:29:26 Ver: 30050100 Press F2 to run Setup (CTRL+E on serial keyboard) Press F8 for BBS Popup (CTRL+P on serial keyboard) Press F12 for network boot (CTRL+N on serial keyboard) Press F9 to start Oracle System Assistant (CTRL+O on serial keyboard) Use <CTRL + E> as per the instructions, to launch the Bios setup utility.
3. ☐	**Bios Setup Utility:** set initial IP address for ILOM	After rebooting the server and executing a <ctrl + E > you will be presented with the Main Bios Utility Setup screen.  Aptio Setup Utility – Copyright (C) 2013 American Megatrends, Inc. Main Advanced IO Boot Exit Project Version 30.05.01.00 | Set the Date. Use Tab System Date [Sat 10/31/2015] | to switch between Date System Time [16:28:27] | elements. QPI Link Speed 9.6 GT/s Total Memory 256 GB Current Memory Speed 2133 MT/s USB Devices: 1 Drive, 2 Hubs BMC Status BMC is working | ><: Select Screen BMC Firmware Revision 3.2.4.52 r101649 | ^v: Select Item | Enter: Select > Product Information | +/-: Change Opt. > CPU Information | F1: General Help > DIMM Information | F7: Discard Changes | F9: Optimized Defaults > Security | F10: Save & Exit | ESC: Exit Version 2.16.1243. Copyright (C) 2013 American Megatrends, Inc.

Procedure 20: Configure Initial iLOM IP address and Bios Settings

Use the right arrow to scroll to the “Advanced” menu

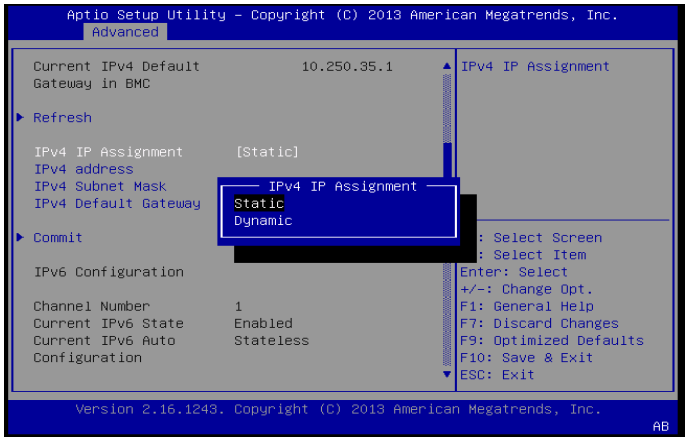


Use the down arrow to scroll to “BMC Network Configuration”:



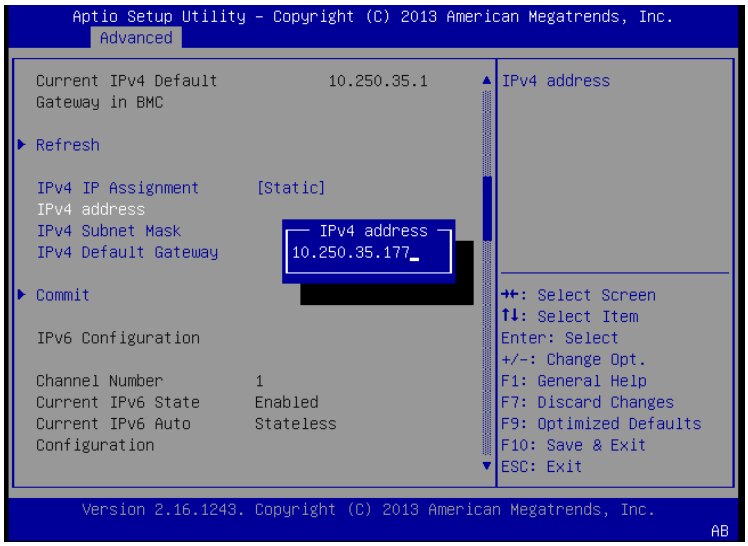
Press “Enter” then scroll down with the arrows to “IPv4 IP Assignment” (below menu item “Refresh”) and press enter:

You are prompted to choose between “Static” and “Dynamic”.



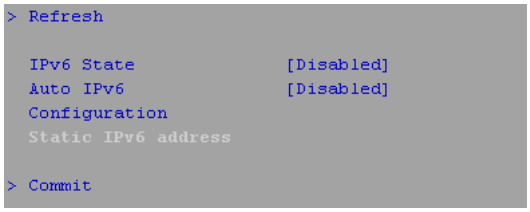
Procedure 20: Configure Initial iLOM IP address and Bios Settings

Highlight “Static” and press enter, then scroll down to “IPv4 address” and press enter to fill in the IPv4 to be assigned to the iLOM

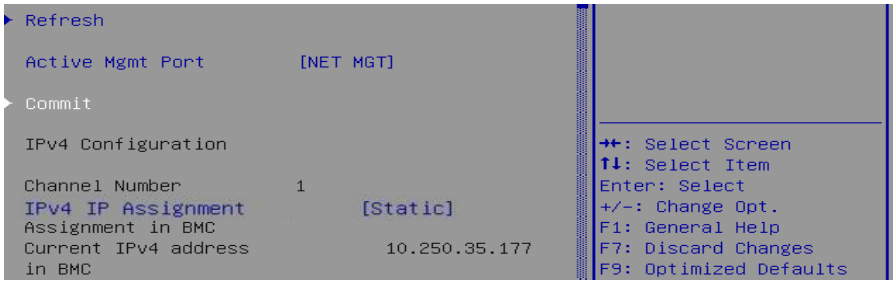


Continue in this fashion to configure “IPv4 Subnet Mask” and “IPV4 Default Gateway”.

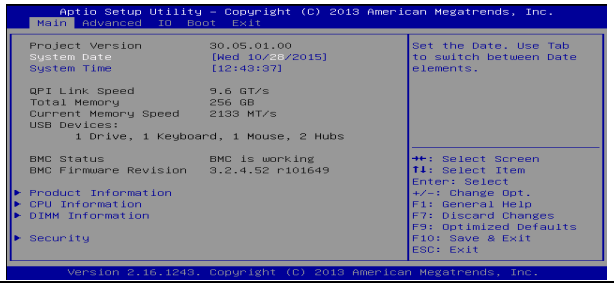
Note: By scrolling down further in the BMC configuration screen it is also possible to enable and set IPv6 address information. To set only the IPv4 address skip this step.



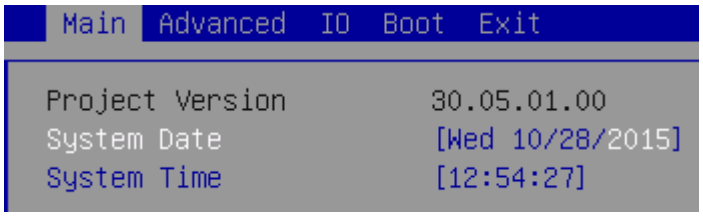
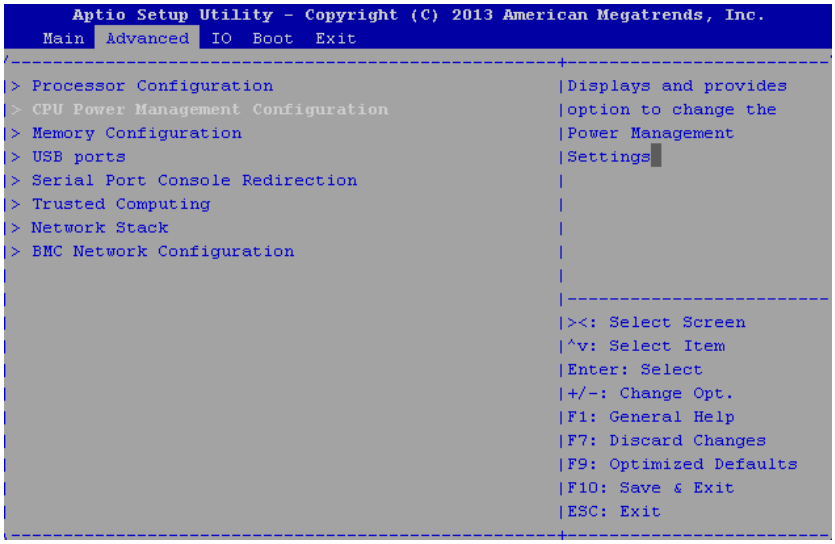
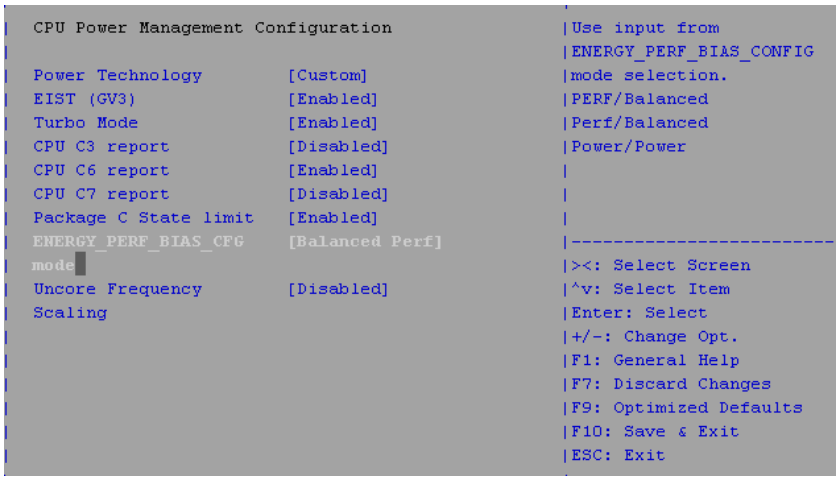
Then scroll to “Commit” and press enter to save the changes:



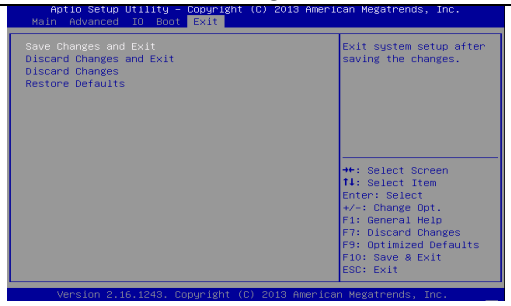
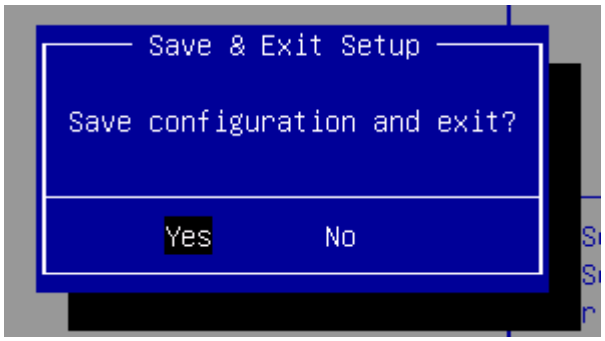
Then press ESC to exit from the network configurations screen then scroll left with the arrows To the main menu screen.



Procedure 20: Configure Initial iLOM IP address and Bios Settings

4. ☐	**Bios Setup Utility:** Set Data and Time	Use the down arrow to highlight the "System Date" then use the space bar to change the month to set it to the current month, then press enter to move to the day and set it using the space bar then same with the year:  Scroll down to the system time and follow the same way used to set the date to set the time to GMT (Greenwich Mean Time):
5. ☐	**Bios Setup Utility:** Set Performance Options	Navigate to the Advanced tab and select "CPU Power Management Configuration".  Navigate to "ENERGY_PERF_BIAS_CFG" and "Enter"  Press ESC to exit the main screen, then with the right arrow move to the "Exit" menu and press enter to save changes and exit:

Procedure 20: Configure Initial iLOM IP address and Bios Settings

		 Confirm to save configurations and exit:  **You have now completed this procedure.**

Procedure 21: Update Server Firmware

NOTE: Please refer to the Oracle X5-2 Firmware upgrade documents to update the Firmware on the Oracle RMS H/W

Further detail is also provided in section 3.5 "Acquiring Firmware" of this document

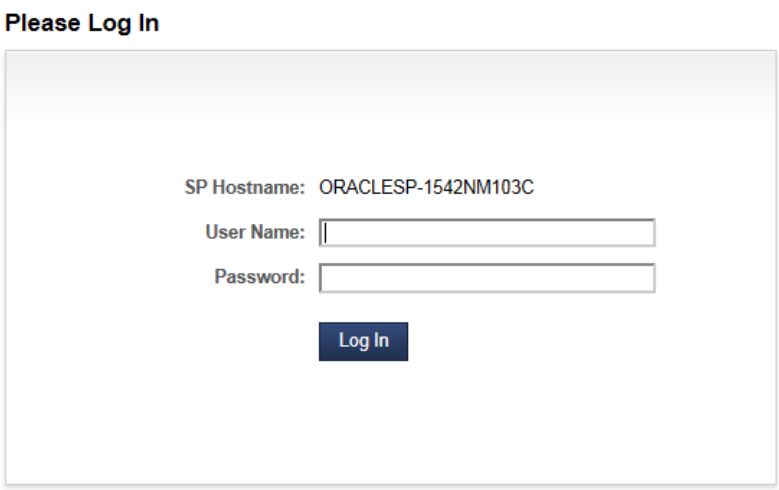
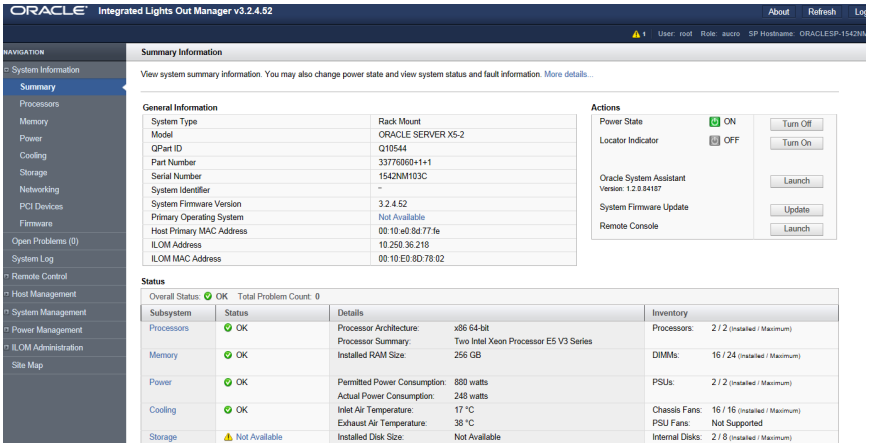
[4] E65467 - Oracle Firmware Upgrade Pack 3.1.5, Release Notes

[5] E65466 - Oracle Firmware Upgrade Pack Release 3.1.5 Upgrade Guide

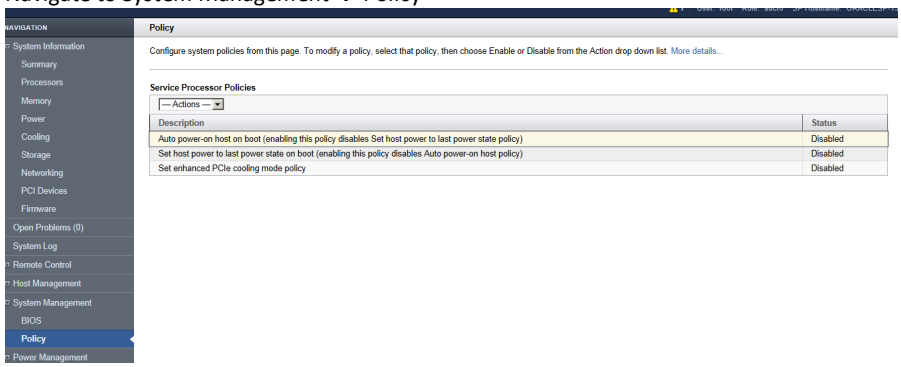
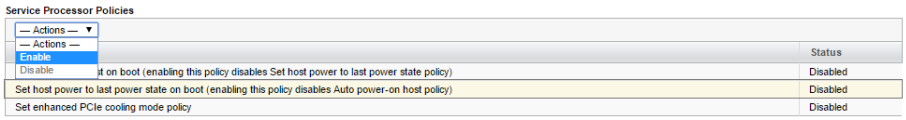
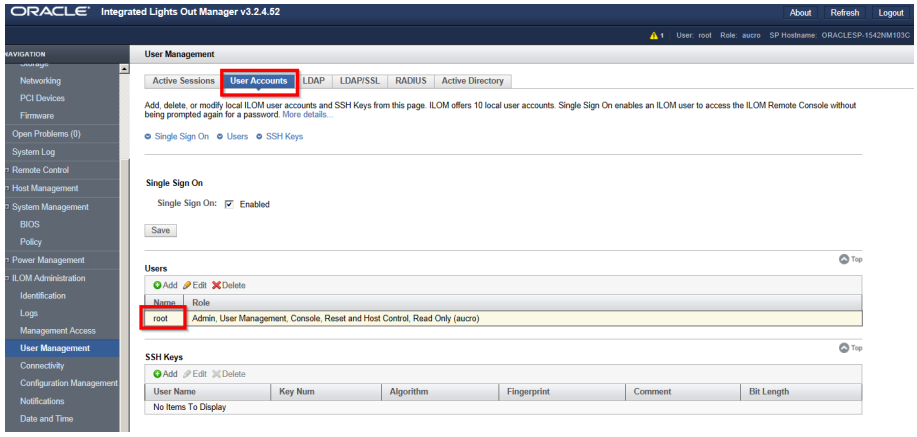
The Oracle Firmware Upgrade Pack (FUP) consists of documentation used to assist in the upgrading of Oracle rack mount servers. The pack consists of an *Upgrade Guide* and *Release Notes*. The current minimum supported release for Platform 7.0.x is 3.1.3. However, if a firmware update is required, it is recommended to use the latest available release. Firmware components can be downloaded from My Oracle Support at *https://support.oracle.com*. Refer to the appropriate FUP Release Notes for directions on how to acquire the firmware.

Procedure 22: Configure Oracle X5-2 iLOM from GUI

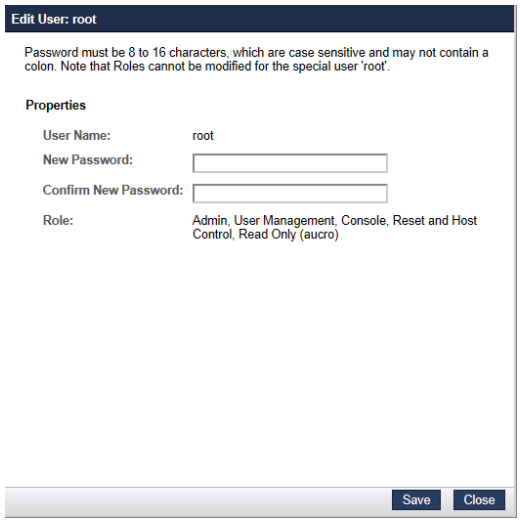
Procedure 22: Configure Oracle X5-2 iLOM From GUI

STEP #		
	This procedure will configure the RMS BIOS. **Needed material:** - Remote connection to iLOM web interface 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. ☐	**iLOM web interface:** Login to the iLOM	Login to the iLOM web interface with a browser pointed to the IP address of the ILOM interface. You will be asked for login credentials. The first time you login the password is root/changeme.  After logging in you will be presented with the Summary Information Page. 

Procedure 22: Configure Oracle X5-2 iLOM From GUI

2. ☐	**iLOM web interface :** Set the power policy	Navigate to System Management → Policy  Then highlight the "Set host power to last power state on boot" option and from the "Actions" menu select "Enable"  Confirm that status changed to "Enabled"
3. ☐	**iLOM web interface :** Change the password for root	Navigate to ILOM Administration - User Accounts 

Procedure 22: Configure Oracle X5-2 iLOM From GUI

		Select <Edit> and change the root password and add new Users if required.  Click <Save> and exit. **You have now completed this procedure.**

6.2 SOFTWARE INSTALLATION (RMS)

Procedure 23: IPM of Oracle X5-2 RMS Server

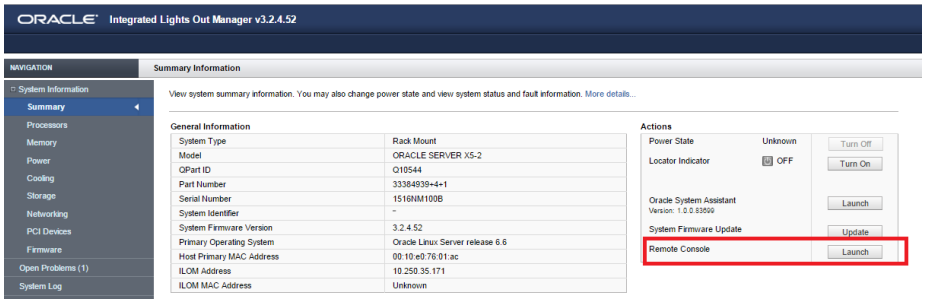
Procedure 23: IPM of Oracle X5-2 RMS Server

STEP #	This procedure will install system OS (IPM) of the server Refer to Section 8 "Supporting Procedures" for additional information 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 **Note:** Refer to Section 8 "Supporting Procedures" for additional information 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 using the method described in Procedure 48: Create a Bootable USB with TPD or TVOE ISO image or other suitable method. 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, proceed to step 2 to remotely IPM the target server using the remote console capability of the X5-2 ILOM as per the following procedure

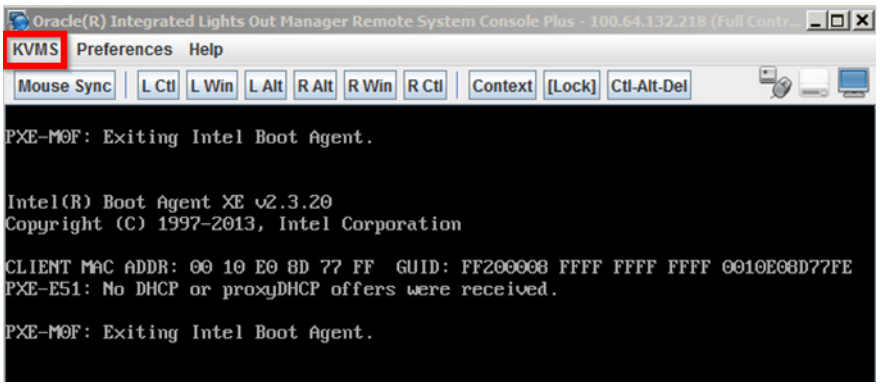
Procedure 23: IPM of Oracle X5-2 RMS Server

Login to iLOM web interface and Navigate to "System Information" → "Summary" then launch the remote console:

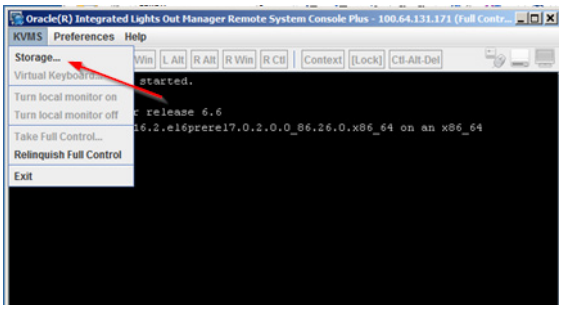
Note: This will launch the "video redirection" console which is preferred to perform these procedures



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



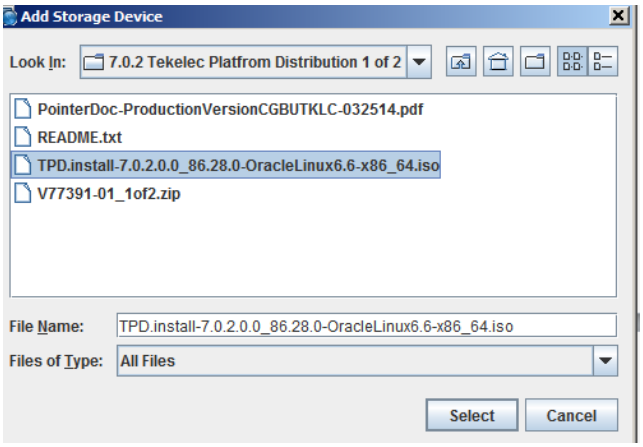
From "KVMS", click "Storage":



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

Procedure 23: IPM of Oracle X5-2 RMS Server

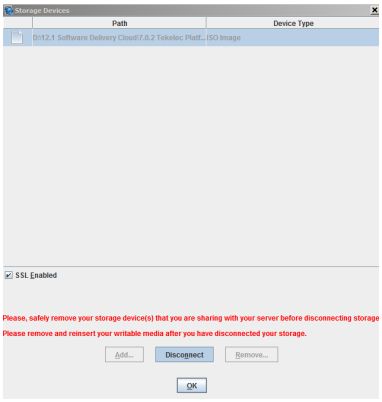
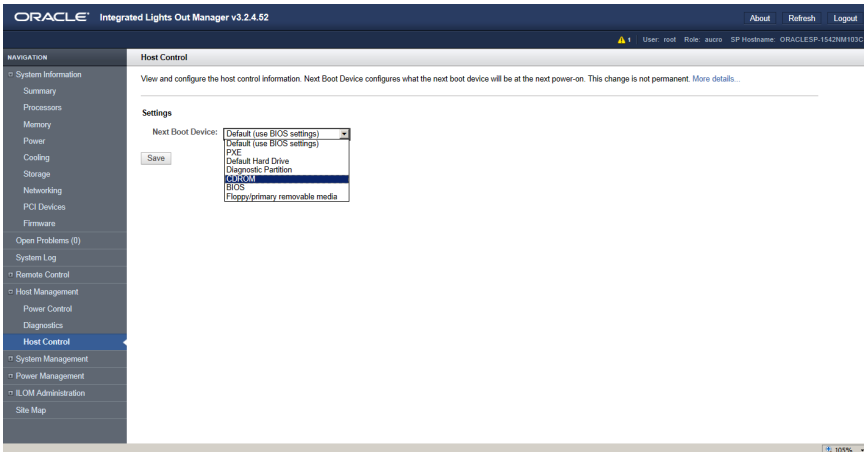
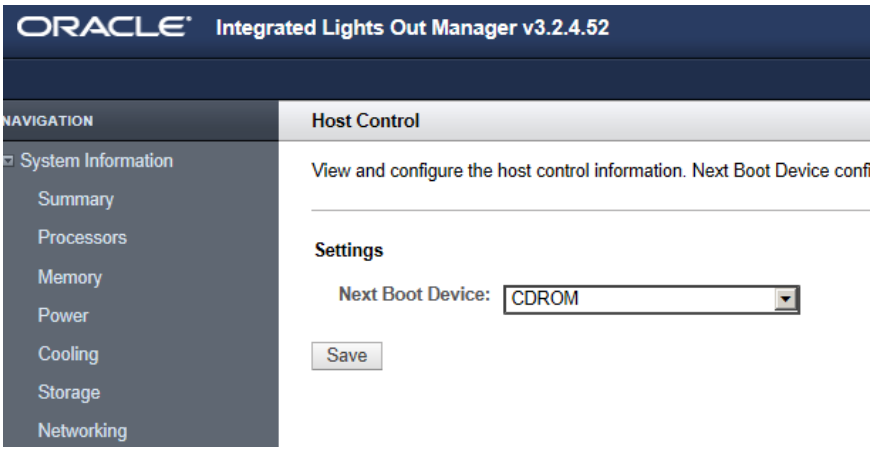
And browse to ISO image file that will be mounted and click on "Select".



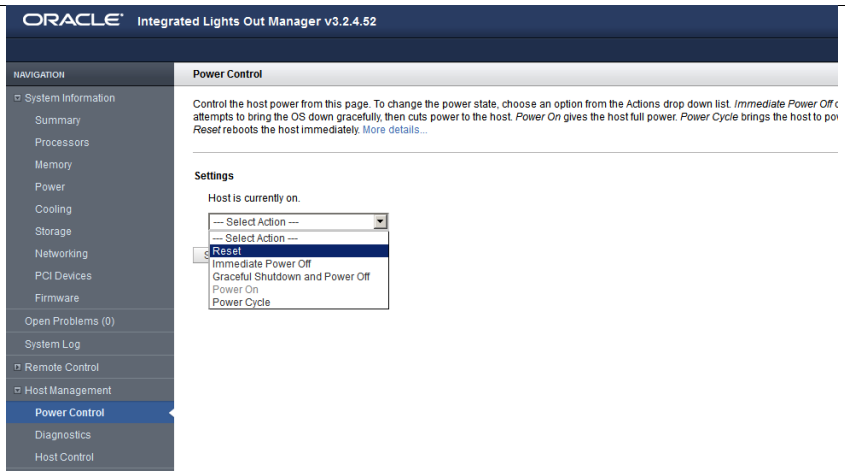
The Storage Devices form will now display the selcted ISO image file. Highlight the file and the Connect option will now be available at the bottom of the form. Click on <Connect>. And then Confirm <OK>.

The Storage Devices will indicate that the ISO image has successfully mounted/connected.

Procedure 23: IPM of Oracle X5-2 RMS Server

		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.  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.

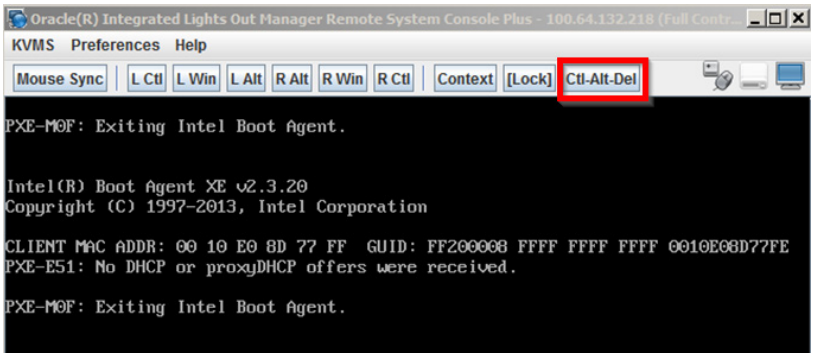
Procedure 23: IPM of Oracle X5-2 RMS Server



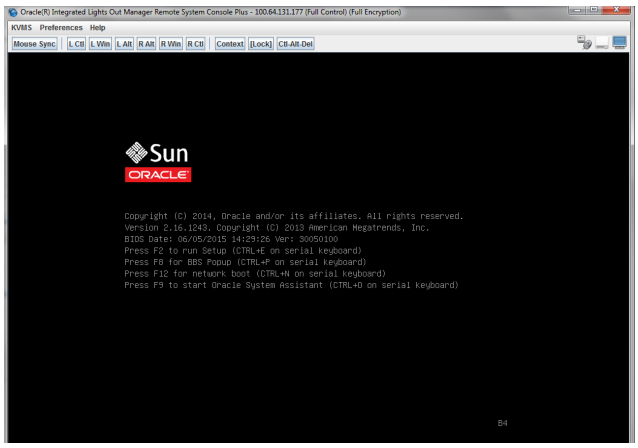
If using this method proceed to the step #3.

Alternately: The following procedure can be used to reboot the server, set the boot order using the Bios Setup Utility. As the server reboots from exiting the Bios Setup Utility it will boot to the virtually mounted ISO image. The end result will be the same in that you will be presented with the TPD install boot screen as in Step #3.

Click “Ctrl-Alt-Del” button from the remote console to reboot:

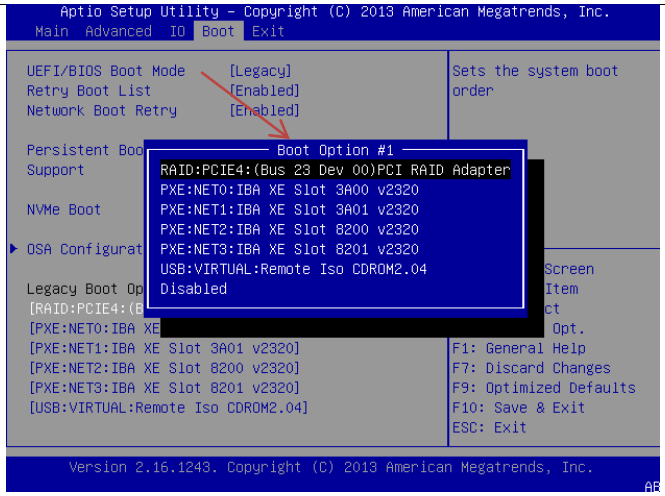


Press”F2” to open BIOS settings:



On “Boot” menu, scroll to “Legacy Boot Option Priority” then highlight the the 1st position in the boot order and press enter to display the boot #1 options.

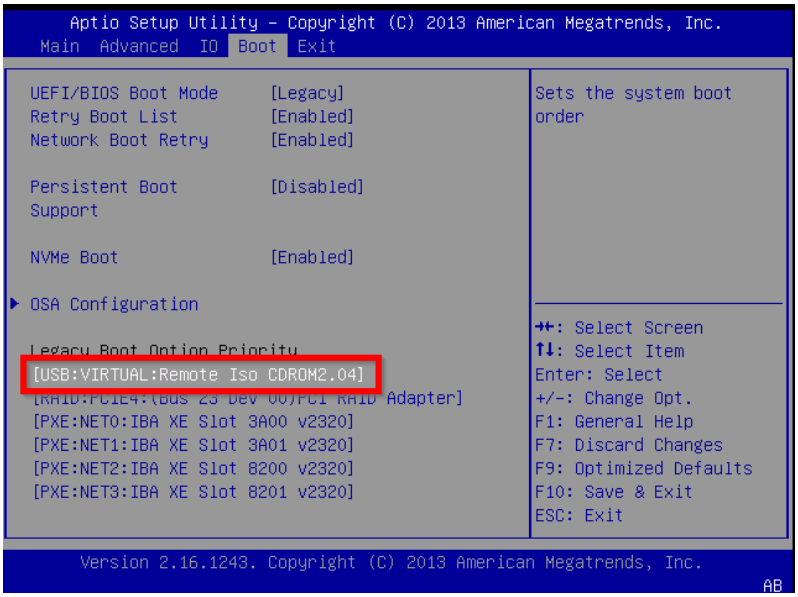
Procedure 23: IPM of Oracle X5-2 RMS Server



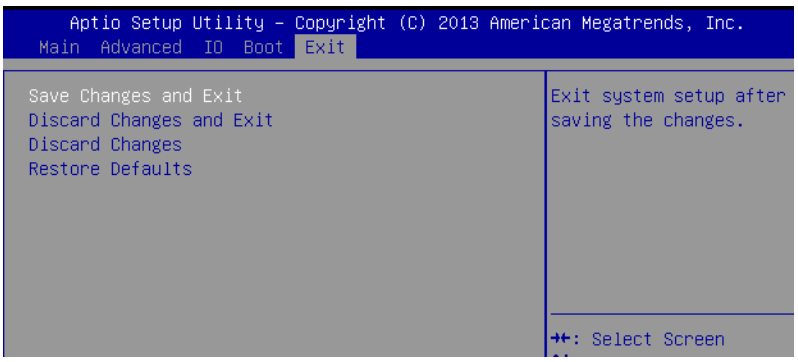
Now navigate to "USB:VIRTUAL:Remote ISO CDROM" option and press enter:

Confirm that "USB:VIRTUAL:Remote ISO CDROM" is now the 1st in order

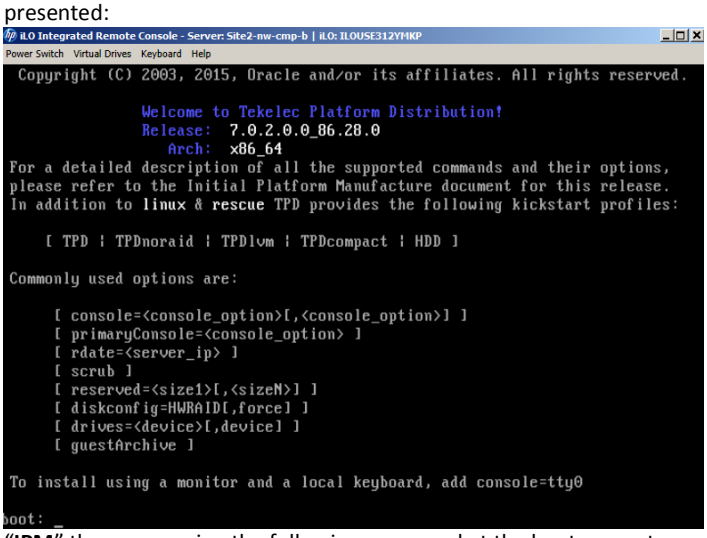
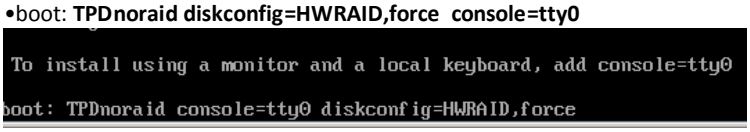
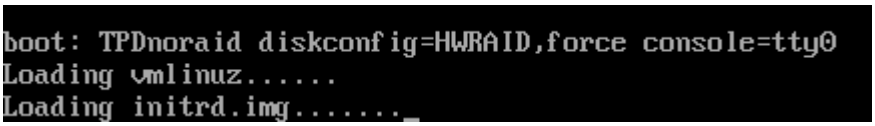
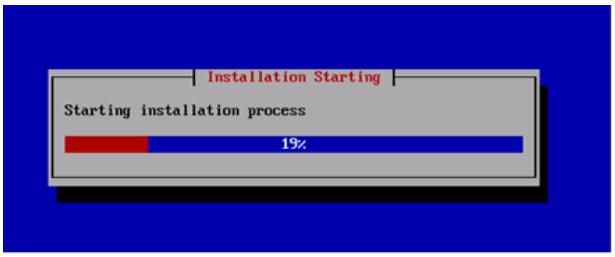
Press enter again to confirm the remote ISO option is now the first option：



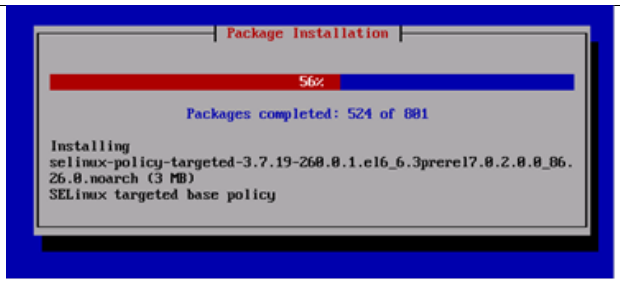
Scroll to "Exit" menu to save and exit:



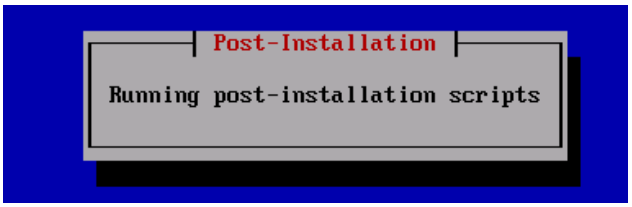
Procedure 23: IPM of Oracle X5-2 RMS Server

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:  "**IPM**" the server using the following command at the boot prompt: •boot: **TPDnoraid diskconfig=HWRAID,force console=tty0**  **Note**: If a direct connection to the serial console is being used for this step instead of the remote iLO console it is not necessary to include "console=tty0" After the command has been entered hit the carriage return and you will see something like the following screen indicating that OS is installing  **Note:** If the server was previously configured with another **non-Policy Solution Application** it may be necessary to clean up Logical Disc partitions created by this Application. To perform that, use the following TPD command with scrub option at the boot prompt: boot: **TPDnoraid scrub console=tty0 diskconfig=HWRAID,force** This may take up 4 hours, depending on the disk configuration. 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:

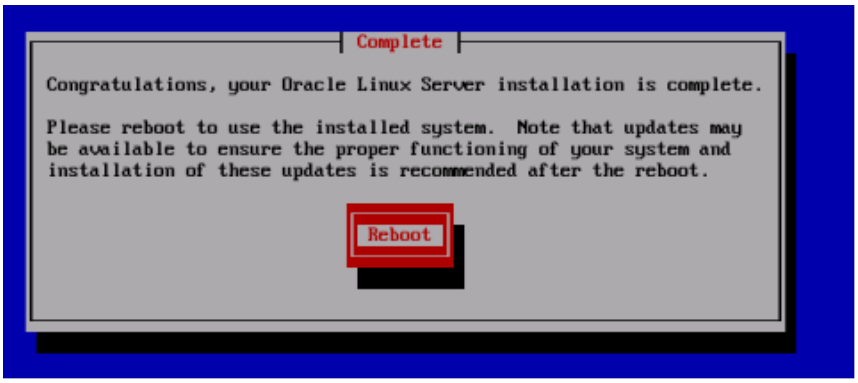
Procedure 23: IPM of Oracle X5-2 RMS Server



Then post installation scripts kick off:



After IPM the process is completed, you are prompted to press **Enter** to reboot the server. Disconnect the media used to finish installing the OS . Otherwise the server may again boot to the bootable media. If the iLO method was used to select Next Boot device: <CDROM> the server will not boot to the mounted media on the next reboot.

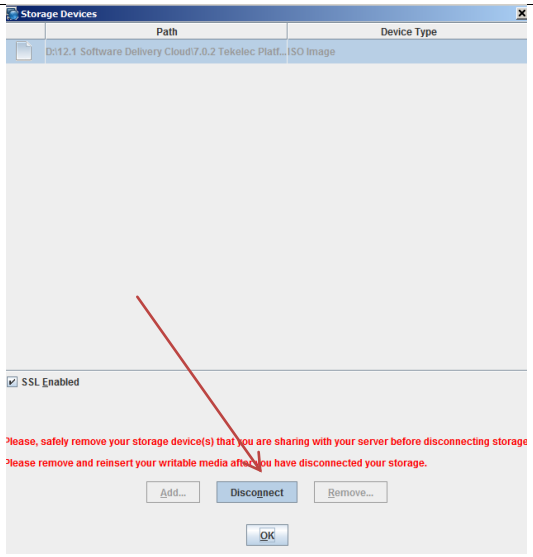
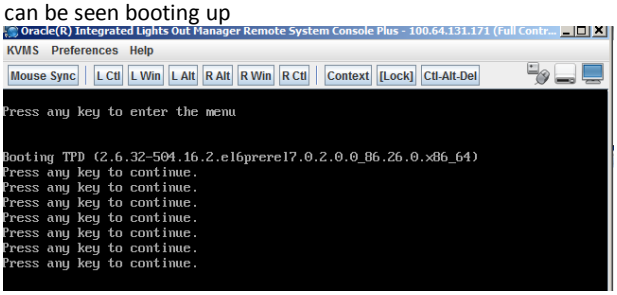
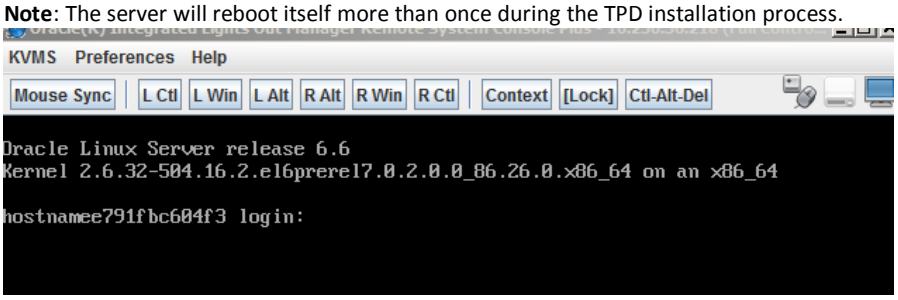


Using the iLOM's remote console, Add "Storage Devices" form, unmount the image from the ILOM remote console. Then highlighting the remote console dialog window press **Enter** to reboot the server as per the following steps. .

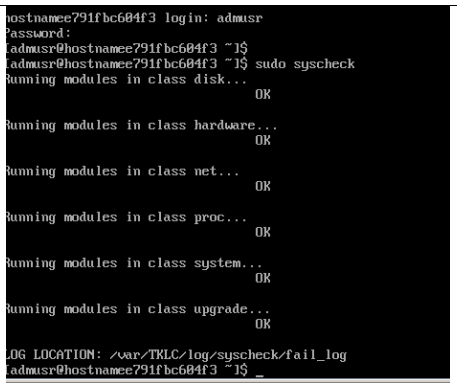
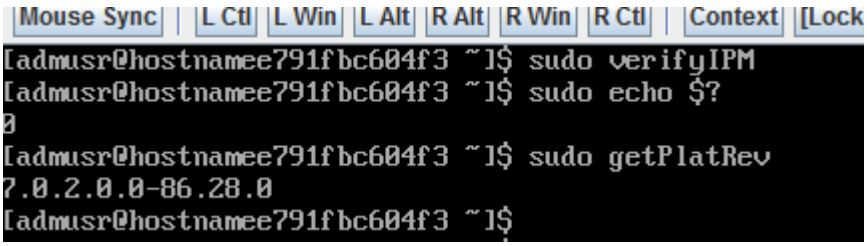
In the case a bootable USB device was used, remove the USB device

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

Procedure 23: IPM of Oracle X5-2 RMS Server

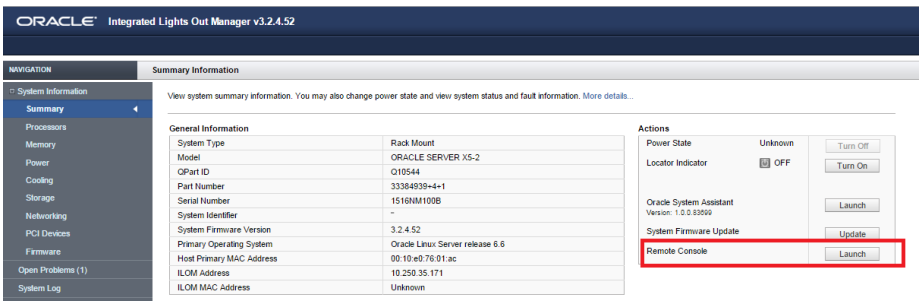
		 Then press **Enter** to boot the server from TPD and finish up the installation. The installed OS can be seen booting up 
4. ☐	**Console:** Login prompt	Once the server reboots, the login prompt is displayed. Login into the server with ***admusr.*** **Note**: The server will reboot itself more than once 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.

Procedure 23: IPM of Oracle X5-2 RMS Server

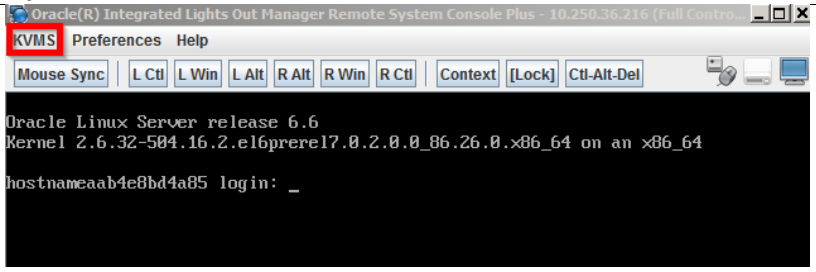
		 If any of the modules return an error, do not continue; contact Oracle Customer Support and report the error condition.
6. ☐	**Console:** Verify Install success	Verify that IPM completed successfully by checking the install logs for errors and displaying the install TPD platform version. . To do this, log in as ***admusr*** and then run the following commands: $ **sudo verifyIPM** (--force if needed) $ **sudo echo $?** (should return 0 errors) $ **sudo getPlatRev** (should return the current TPD version installed)  Previous screen shot shows no errors returned which indicates the TPD installation process is successfully completed. If errors are found, contact Oracle Customer Support. **You have now completed this procedure.**

Procedure 24: RMS Application Software Installation

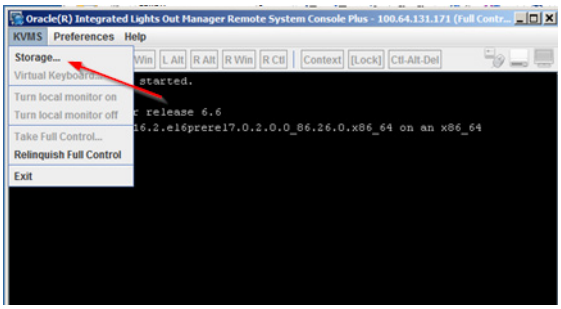
Procedure 24: ***RMS Application Software Installation***

STE P #		
	This procedure will install the Application Software. **Needed material:** - Application software ISO image files (cmp, mpe, and optionally mra) - See Section 3.3 "Required Materials" and Section 3.4 "Acquiring Software" for details on the required versions 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 or MRA)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 Login to iLOM web interface and Navigate to "System Information" → "Summary" then launch 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:	

Procedure 24: ***RMS Application Software Installation***



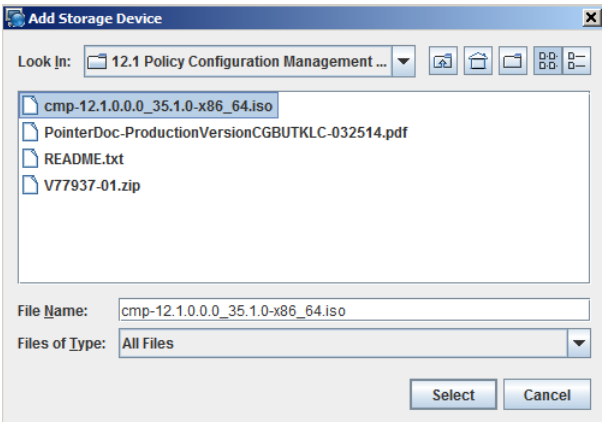
From "KVMS", click "Storage":



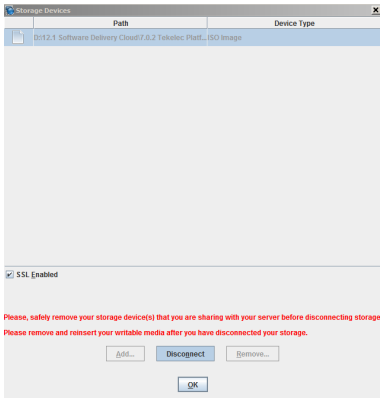
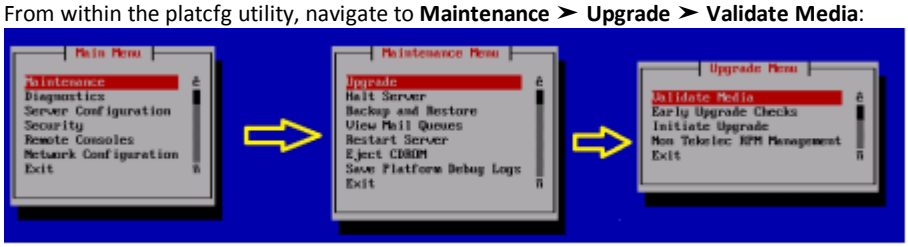
In the Storage devices form that opens up, click on the "Add" button.

And browse to ISO image file that will be mounted and click on "Select".

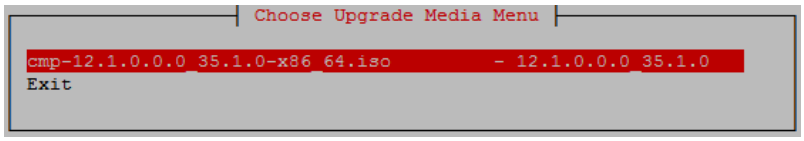
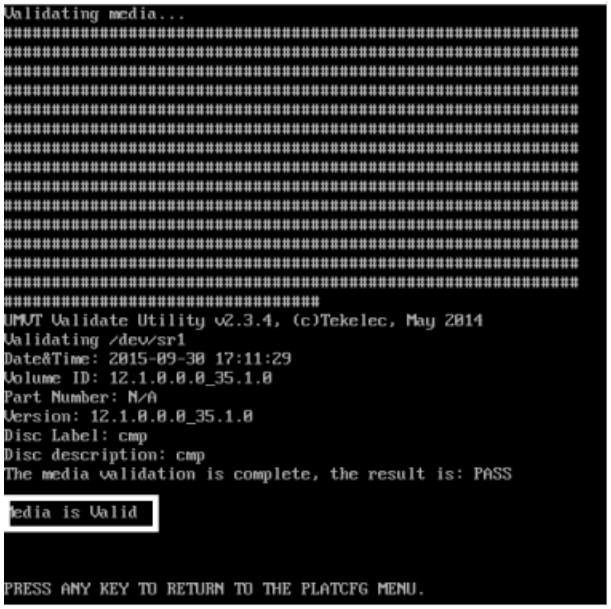
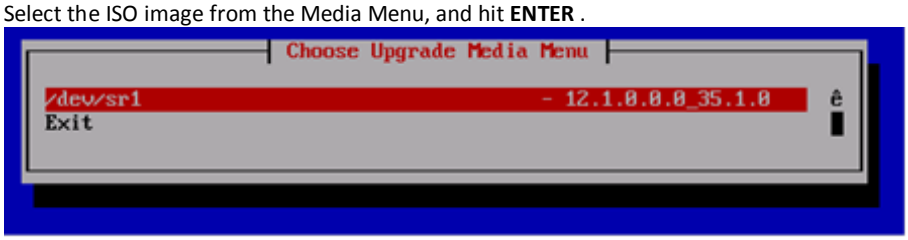
Note: For Policy applications istallation make sure to choose the correct ISO version (CMP/MPE/MRA) for the target server.



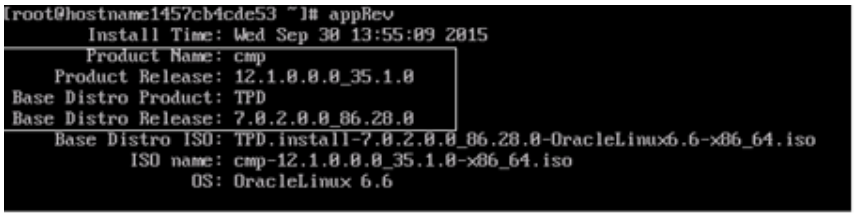
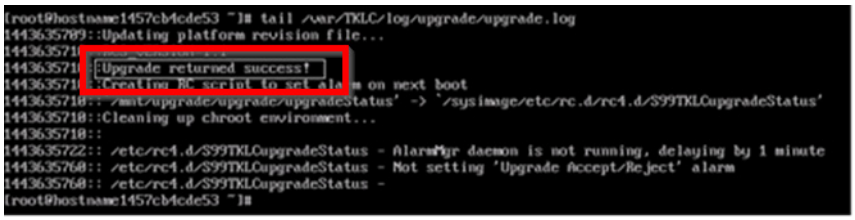
Procedure 24: ***RMS Application Software Installation***

		The Storage Devices form will now display the selcted 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>. The Storage Devices will indicate that the ISO image has successfully mounted/connected. Leave this window open. 
2. ☐	**Console:** run platcfg and validate the media	Return to the CLI prompt and Login as admusr if not already logged in. Start the Platcfg utility by issuing the following command: **#sudo su - platcfg** From within the platcfg utility, navigate to **Maintenance ➢ Upgrade ➢ Validate Media**: 

Procedure 24: ***RMS Application Software Installation***

		Then choose the ISO image and hit enter: **Note:** Depending on the method used, the platcfg utility will search for any mounted ISOs and if successful will display the Policy Management Application ISO image file to install  Validation progress is indicated in the console by "#" signs as shown below: Make sure at the end of the validation process, the result is indicating "Media is Valid": 
3. ☐	**Console:** Select ISO to install, and confirm Application install may take 20 Minutes – if installing with a virtual mount, it will take a little longer	From within the platcfg utility, navigate to **Maintenance ➢ Upgrade ➢ Initiate Upgrade**; Select the ISO image from the Media Menu, and hit **ENTER** .  **Note:** The server will reboot twice during the installation process, **do not remove** the media at this time.

Procedure 24: *RMS Application Software Installation*

4. ☐	**Console:** Verify Policy install version	After the application has completed installation log back in to the command line as admusr and confirm the installed TPD platform version and the Policy Management application version. **#appRev**  Verify: • TPD revision installed • Policy Management application installed and its revision
5. ☐	**Console:** Verify Install success	**# tail /var/TKLC/log/upgrade/upgrade.log**  Make sure the upgrade was successful. In case UPGRADE STATUS was not successful, then inspect following log files for more details: • **/var/TKLC/log/upgrade/upgrade.log** • **/var/TKLC/log/upgrade/ugwrap.log**
6. ☐	**Remove Media**	Once the login prompt is displayed, installation is complete. Remove the USB device or virtually mounted so image file from the server. If the installation was done by virtual media mount, disconnect the ISO file.
7. ☐	**Policy Solution servers**	This procedure needs to be followed for each Policy Management application component (cmp/mpe/mra) on each of the Policy Management Solution servers. **You have now completed this procedure.** Proceed *to* *Section 7: Configure Policy Application Servers*

7. CONFIGURE POLICY APPLICATION SERVERS

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.

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

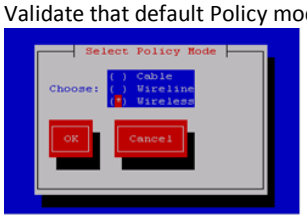
[9] E62450 - Configuration Management Platform Wireless User's Guide Release 12.1.x

[10] E62447 - Platform Configuration User's Guide Release 12.1.x

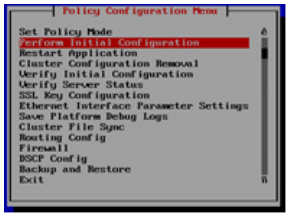
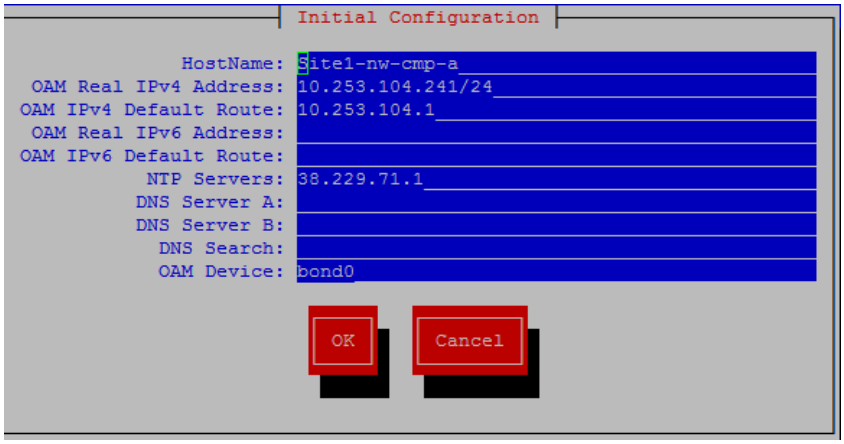
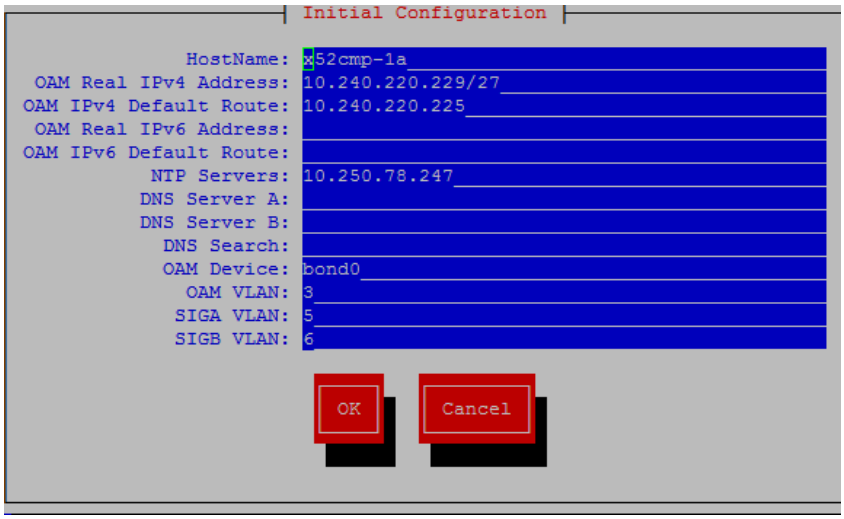
7.1 CONFIGURE NETWORK TOPOLOGY

Procedure 25: Perform Initial Configuration of Policy Servers Platcfg

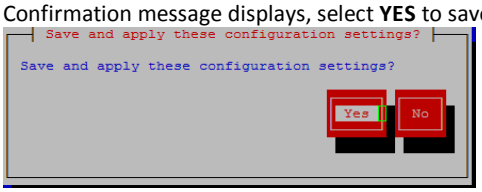
Procedure 25: Perform Initial Configuration of the Policy Servers Platcfg

STEP #	This procedure will configure the OAM Network Address of the server, and related networking. **Needed material:** - IP Addresses from the Network IP Planning document (or other customer provided document) 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 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 8.1 iLO (ILOM) Procedures
2. ☐	Verify the type of server logged in to	Login as root, via Console. # getPolicyRev –p Output will be either mra, mpe, or cmp
3. ☐	Verify Policy Mode in platcfg	Run platcfg tool: From the main menu navigate to Policy Configuration -> Set Policy Mode # su - platcfg Validate that default Policy mode “Wireless” is the one selected as shown below:  Hit “Cancel” to exit the Policy mode settings screen. Note: Policy Management 12.1.x.x only supports “Wireless Mode.

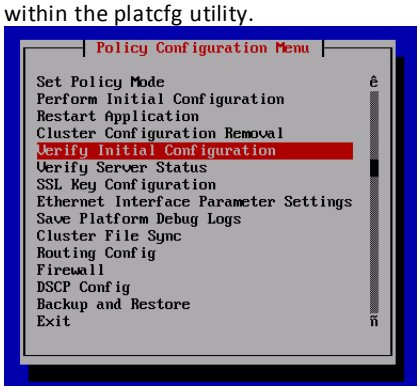
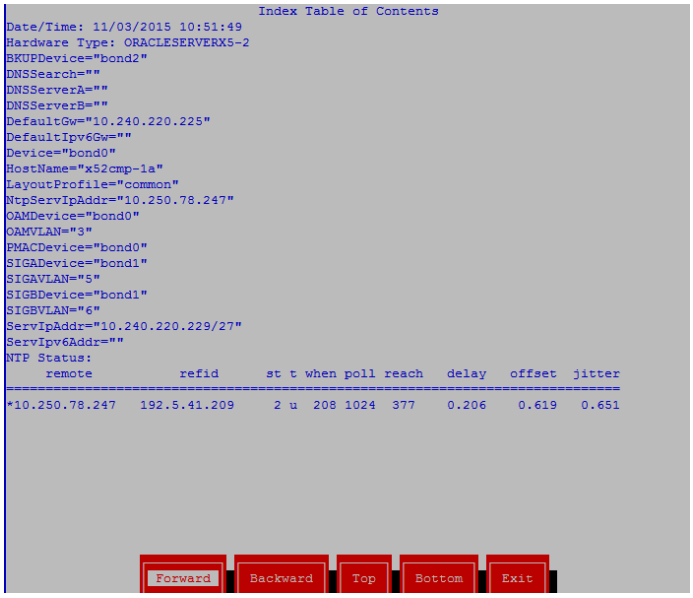
Procedure 25: Perform Initial Configuration of the Policy Servers Platcfg

4. ☐	Perform Initial Configuration	From the main menu navigate to Policy Configuration -> Perform Initial Configuration to start performing the initial configuration of the server:  **Note:** HP RMS Hardware presents the following screen (No vlans need to be configured) The configuration in this snapshot is only an example. Actual configuration should be in accordance with network design requirments. See the table below for additional detail on the configurable fields.  **Note:** C-class server blades and Oracle X5-2 RMS Hardware present the following screen (Vlans need to be configured according to network design requirements) 

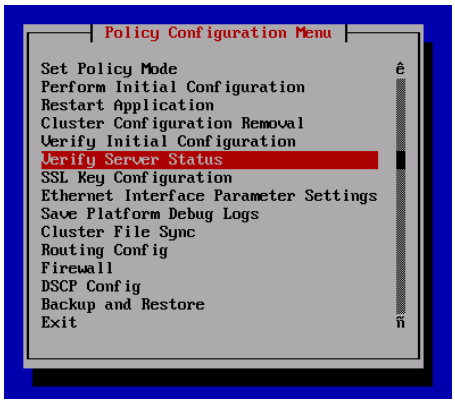
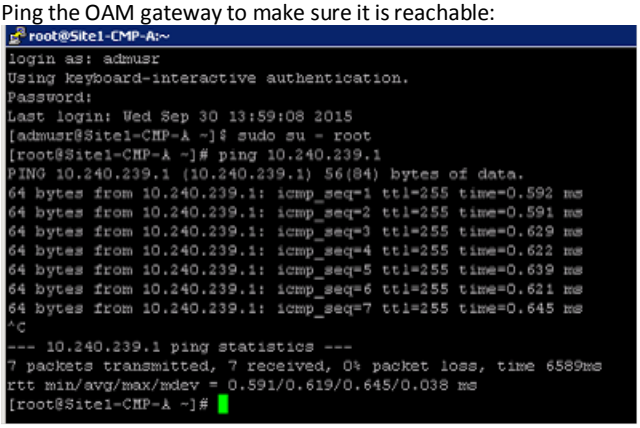
Procedure 25: Perform Initial Configuration of the Policy Servers Platcfg

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. • **OAMVLAN**--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** --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. 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.

Procedure 25: Perform Initial Configuration of the Policy Servers Platcfg

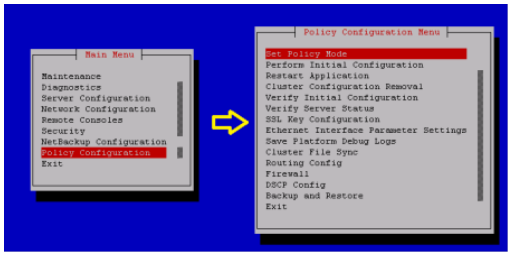
6. ☐	**Verify Config**	From the main menu navigate to Policy Configuration -> **Verify Initial Configuration** from within the platcfg utility.  A display similar to the following is shown.  **Note**: The NTP status may not have updated. This is normal behavior. You may need to hit <enter> on the Forward button to view the NTP status.

Procedure 25: 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 initialization are present.

Procedure 25: 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`
		`==============================================================================`
		`*10.250.32.10    192.5.41.209     2 u    5   64    1    0.255   -0.483   0.034`
		`[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.

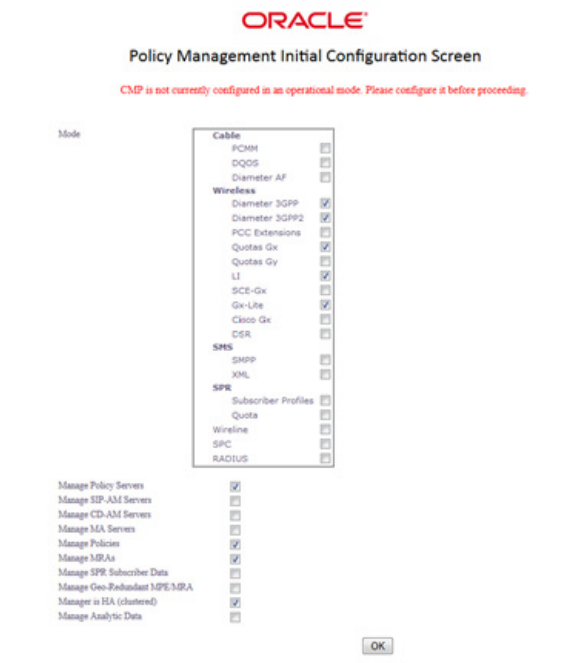
10. ☐	**Repeat on additional servers**	Repeat this procedure on all Policy components' servers that are planned for service. If solution is geo-redundant, this procedure need to be performed on site1 and site2 Policy servers  **You have now completed this procedure**

Procedure 26: Perform Initial Configuration of the Policy Servers CMP GUI

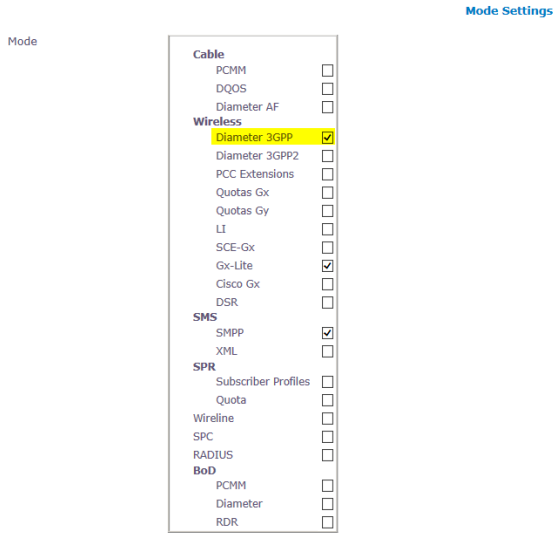
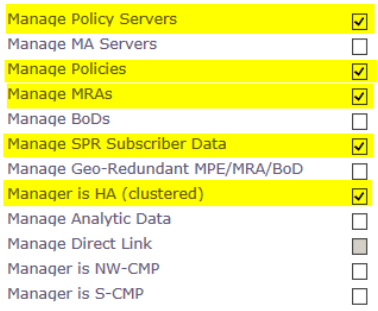
This procedure will perform initial configuration of the CMP GUI on a newly installed environment.

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.

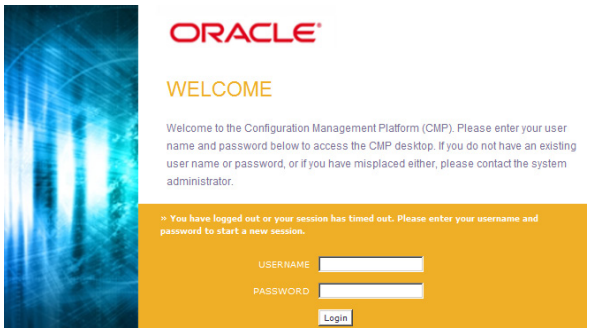
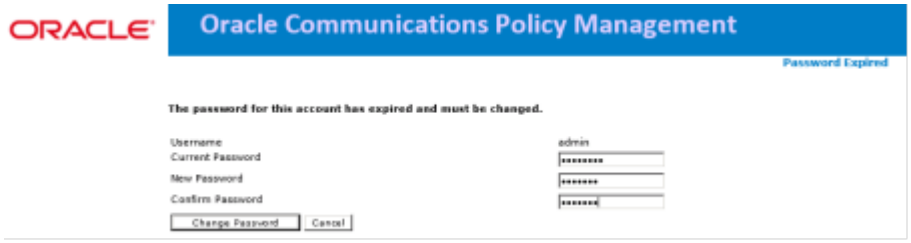
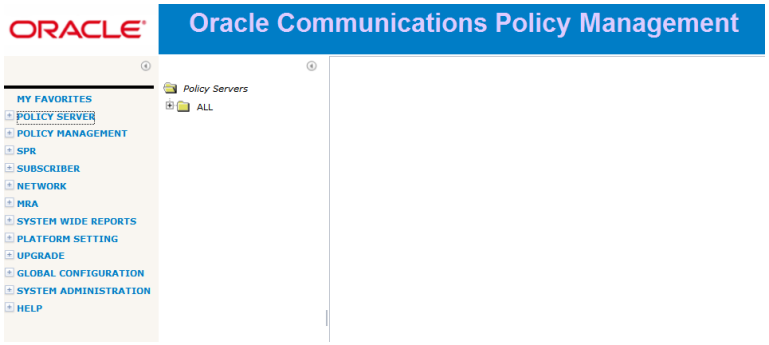
Procedure 26: Perform Initial Configuration of the Policy Servers CMP GUI

STE P #		
	This procedure will configure the CMP at the Active site (CMP Site 1). **Pre-requisite:** - 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 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
2. ☐	Set CMP Mode in 1st selected CMP	Once connected to the CMP GUI for the 1st time the , the 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 OK. The following page provides a sample selection.  [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.

Procedure 26: Perform Initial Configuration of the Policy Servers CMP GUI

3.	Set CMP Mode in 1st selected CMP	Below is an example of a configuration that will provide basic functionality for a Policy 12.1.x wireless solution. The wireless mode of operation will have already been confirmed in earlier procedures. [Checkboxes are for example only). In most cases, the Geo-Redundant MPE/MRA option will not be needed.] **For the greater detail please refer to "The Mode Settings Page" in the following document (as found in the reference section of this document).** [9] E62450 - Configuration Management Platform Wireless User's Guide Release 12.1.x   **Notes:** • ***Diameter 3GPP, 3GPP2*** and ***GxLite*** enable the functionality required to support these protocols in a Policy Management Solution • ***LI*** is used if the MPE installation used the LI (Lawful Intercept) version of the mpe ISO image. To use this option the LI version of the MPE ISO image must have been installed on the MPEs in the Policy Management Solution • ***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. **Note:** The mode selections on this form depend on the customer deployment and should conform

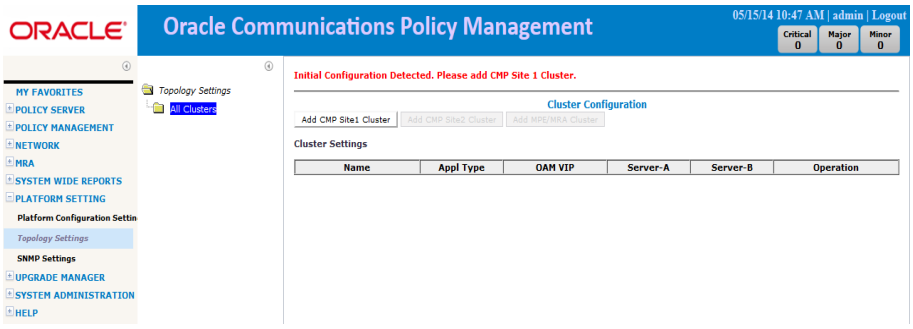
Procedure 26: Perform Initial Configuration of the Policy Servers CMP GUI

		with the engineering team responsible for the planned Policy Management Solution deployment. **Note:** ***Manager is NW CMP*** & ***Manager is S-CMP*** are specific to a "Tiered CMP System" deployment. For the procedure to deploy a Tiered CMP System see Tiered CMP SYSTEM
4. ☐	Login to CMP GUI	After finishing the policy mode selection and pressing "OK", login screen below would be displayed:  If 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 surrogate Aggregation switch (temporary) may be needed during installation.
5. ☐	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 hit "Change Password" button.
6. ☐	Verify that the CMP GUI is displayed, with expected menus.	 **You have completed this procedure**

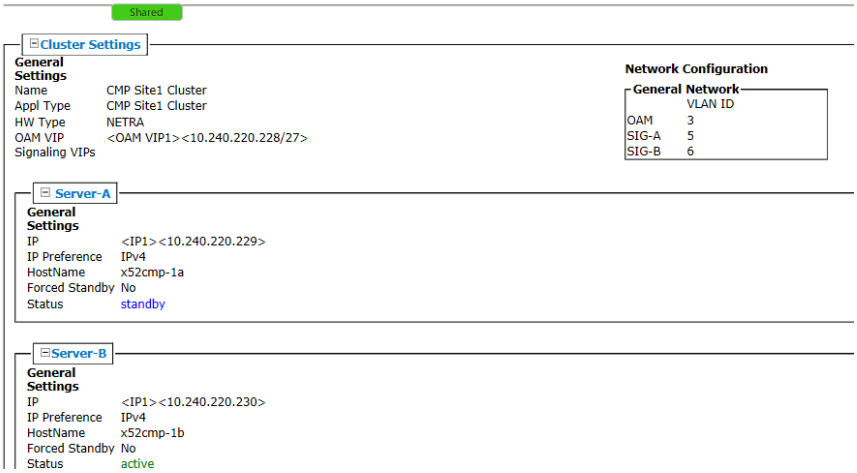
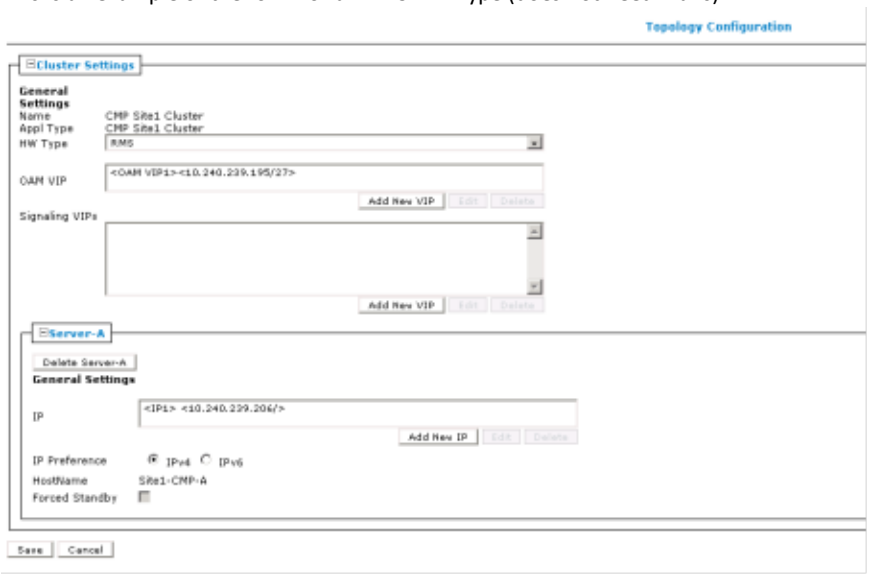
Procedure 27: CMP Site1 Cluster Topology Configuration

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

Procedure 27: CMP Site1 Cluster Topology Configuration

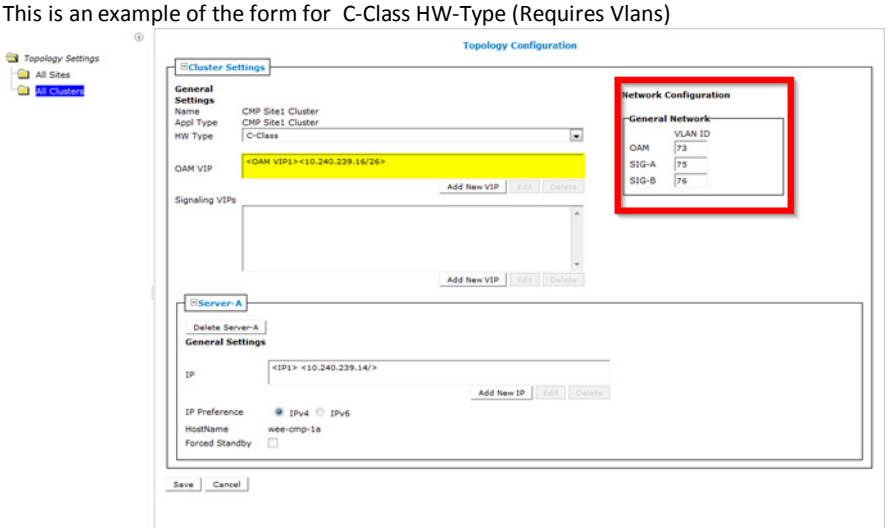
STEP #		
	This procedure will perform configure the CMP at the Active site (CMP Site 1) For additional detail please refer to the following (as per the reference section in this document). **[10]** **E62450 - Configuration Management Platform Wireless User's Guide Release 12.1.x** Note: The recommended 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 and MRA clusters — Enter MPE and MRA cluster settings on the active CMP server on the primary site. **4.** For geo-redundancy (optional), configure additional sites for MPE and MRA 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. **Pre-requisite:** - 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. ☐	**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. 

Procedure 27: CMP Site1 Cluster Topology Configuration

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 the determine whether Vlans are required. For c-Class 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. • RMS Hardware-Type does not require Vlans. • VM Hardware-Type is for Virtualized Solutions and is covered in the 12.1.x Virtual Install Guide and are not referenced here. This is an example of the form for a NETRA HW Type for Oracle and Netra x5-2 Servers (Requires Vlans)  Shared Cluster Settings General Settings Name CMP Site1 Cluster Appl Type CMP Site1 Cluster HW Type NETRA OAM VIP <OAM VIP1><10.240.220.228/27> Signaling VIPs Network Configuration General Network VLAN ID OAM 3 SIG-A 5 SIG-B 6 Server-A General Settings IP <IP1><10.240.220.229> IP Preference IPv4 HostName x52cmp-1a Forced Standby No Status standby Server-B General Settings IP <IP1><10.240.220.230> IP Preference IPv4 HostName x52cmp-1b Forced Standby No Status active This is an example of the form for an RMS HW Type (does not need Vlans)  Topology Configuration Cluster Settings General Settings Name CMP Site1 Cluster Appl Type CMP Site1 Cluster HW Type RMS OAM VIP <OAM VIP1><10.240.239.195/27> Add New VIP Edit Delete Signaling VIPs Add New VIP Edit Delete Server-A Delete Server-A General Settings IP <IP1> <10.240.239.206/> Add New IP Edit Delete IP Preference IPv4 IPv6 HostName Site1-CMP-A Forced Standby Save Cancel

Procedure 27: CMP Site1 Cluster Topology Configuration

This is an example of the form for C-Class HW-Type (Requires Vlans)



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:

- **C-Class** (default)
- **C-Class(Segregated Traffic)** (for a configuration where Signaling and other networks are separated onto physically separate equipment)
- **NETRA** (for a Netra server)
- **RMS** (for a rack-mounted server)
- **VM** (for a virtual machine)

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

Network VLAN IDs (appears if you selected **C-Class**, **C-Class(Segregated Traffic)**, or **NETRA**) Enter the Operation, Administration, and Management (OAM), SIG-A, and (optionally) SIG-B virtual LAN (VLAN) IDs, in the range 1–4095. The defaults are 3 for the OAM Virtual IP (VIP) and server IP, 5 for the SIG-A VIP, and 6 for the SIG-B VIP.

Note: If vlan IDs were designated in the initial config using platcgf they can be reused here to match the initial configuration

— Complete the OAM VIP

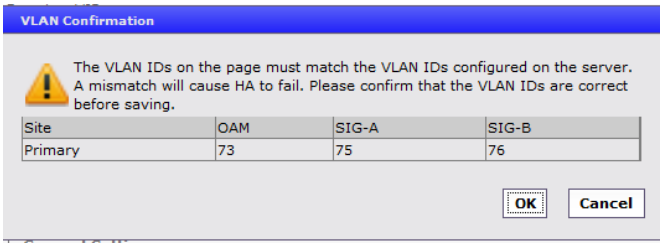
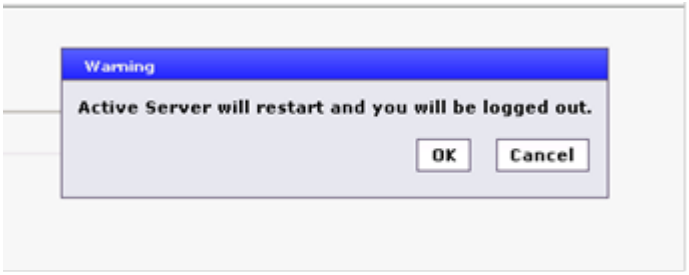
OAM VIP (required) — The OAM VIP is the IP address the CMP uses to communicate with a Policy Management cluster. Enter up to two OAM VIP addresses (one IPv4 and one IPv6) and their masks. Enter the address in the standard dot format and the subnet mask in CIDR notation from 0–32 (IPv4), or standard 8-part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

— Complete Signaling VIP if applicable

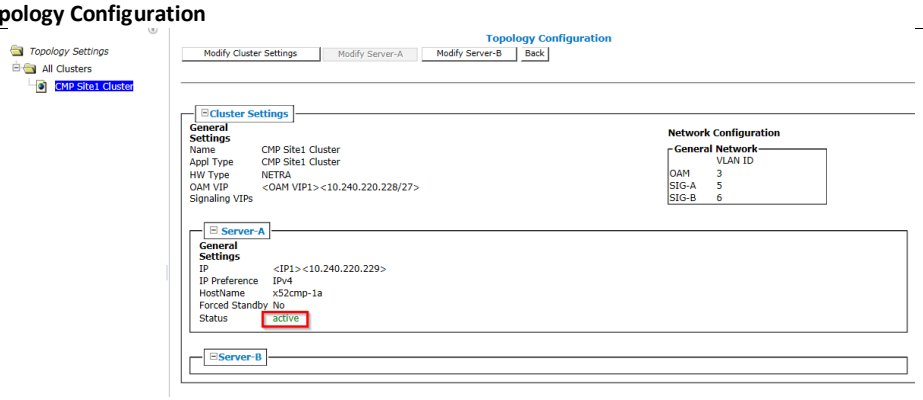
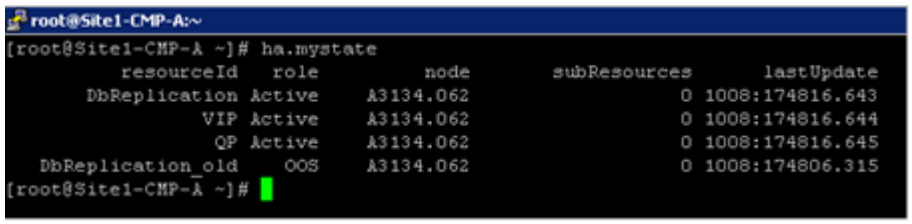
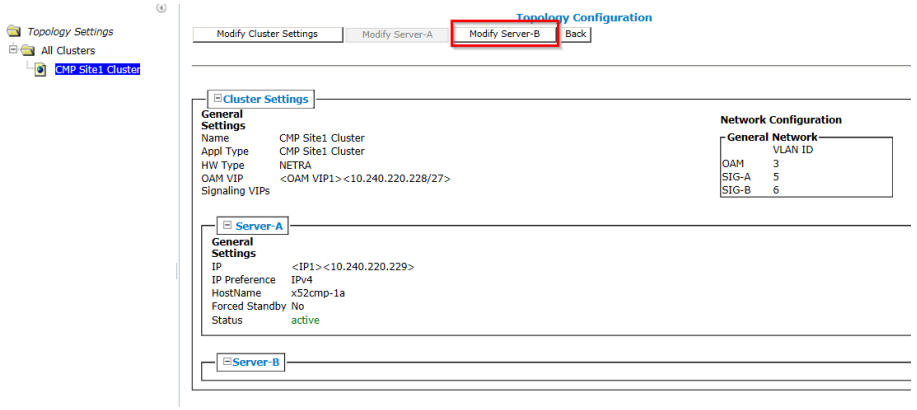
Signaling VIP 1 through **Signaling VIP 4** (optional) — Enter up to four IPv4 or IPv6 addresses and masks of the signaling virtual IP (VIP) addresses; for each, select **None**, **SIG-A**, or **SIG-B** to indicate whether the cluster will use an external signaling network. You must enter a Signaling 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

Procedure 27: CMP Site1 Cluster Topology Configuration

		—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 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 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 point 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**

Procedure 27: CMP Site1 Cluster Topology Configuration

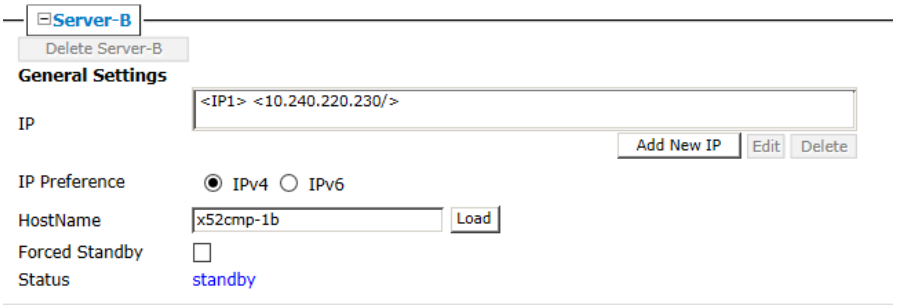
		 Verify the configured CMP server is now in "Active" state
4 ☐	**IF the CMP VIP is not available…**	SSH to the CMP Real IP address of the CMP server to confirm the server role is "active" as shown below # ha.mystate  NOTE: "DbReplication_old" with role "OOS" is not an indication of a problem and can be ignored. 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.

Procedure 27: CMP Site1 Cluster Topology Configuration

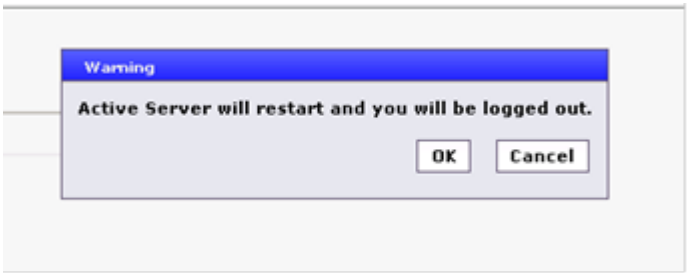
- Server-B Hostname — hostname for the second server. This hostname must exactly match the hostname configured in platcfg (same as uname -n). Alternatively, you may highlight the server IP then hit "Load" button for the system to automatically look up the server name from initial configuration

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.

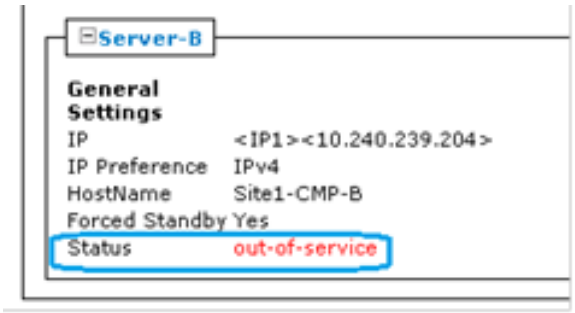
Example of Site1 CMP Cluster Server B Topology Configuration



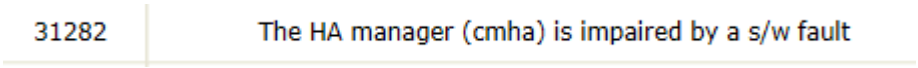
Select "save" then "OK" on the following confirmation message.



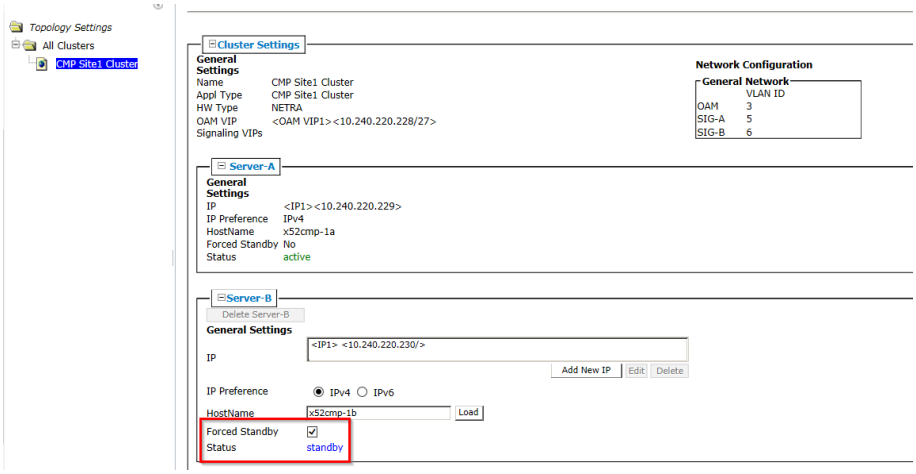
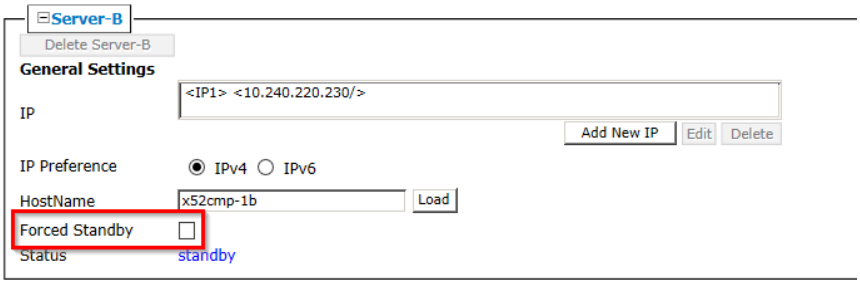
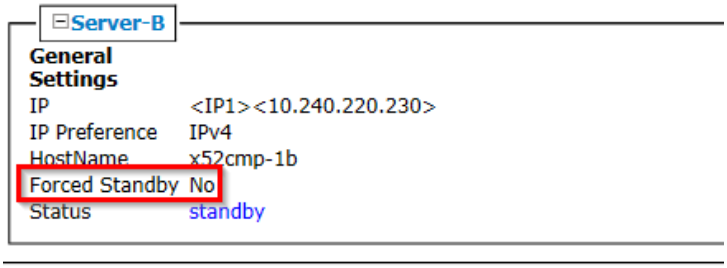
The server status will be "out-of-service" for few minutes and that is expected until the cluster forms:



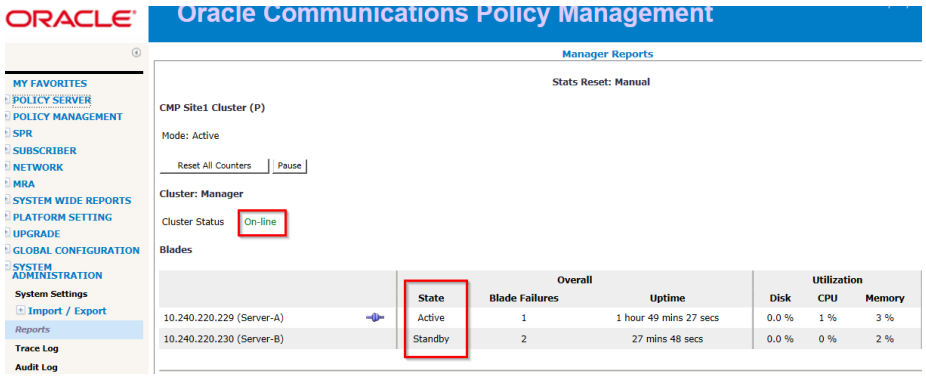
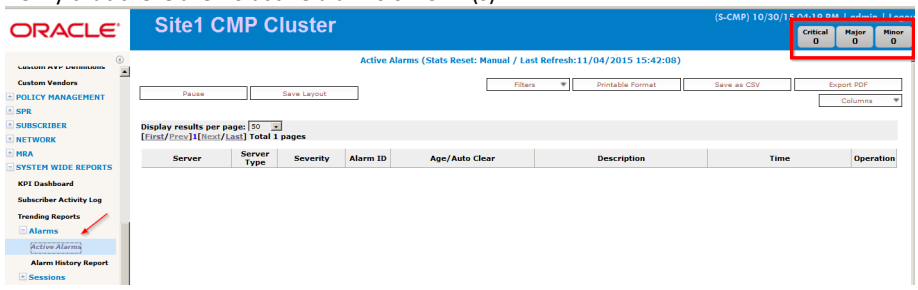
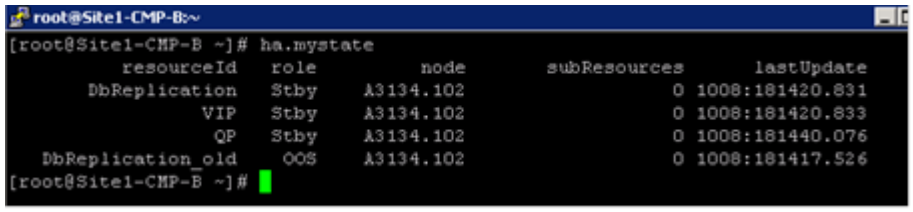
Note: Wait for any Alarms, such as the following, to clear.



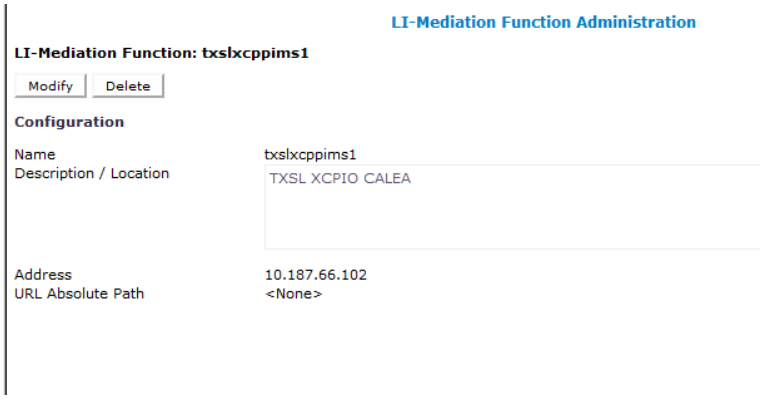
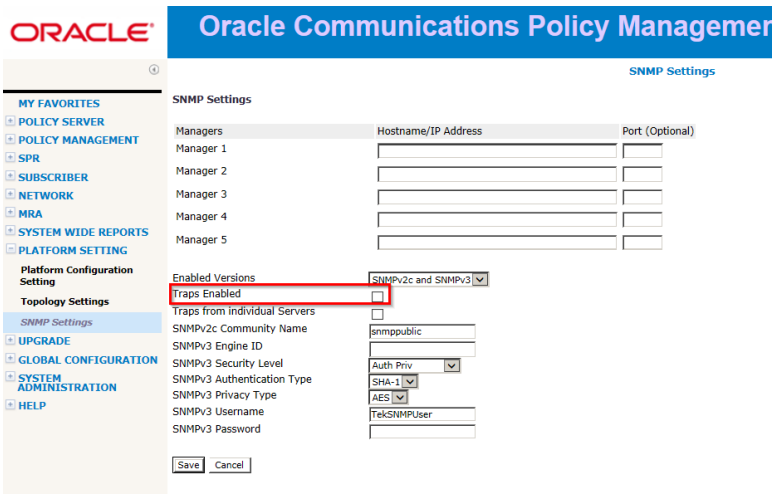
Procedure 27: CMP Site1 Cluster Topology Configuration

6. ☐	**Verify Server B is added**	**Menu → Topology → CMP Site 1 Cluster**  Verify status is: • Forced Standby = yes (automatically set upon entering CMP server-B information) • Status = standby (after refreshing the page) (Wait a minute, if needed, for the status to become stable.)
7. ☐	**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 

Procedure 27: CMP Site1 Cluster Topology Configuration

8. ☐	**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 "online": 
9. ☐	**GUI: Verify CMP cluster**	SYSTEM WIDE REPORTS → Active Alarms Verify that there are no active alarms on CMP(s). 
10. ☐	**GUI: 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
11. ☐	**GUI: Configure LI Mediation Functions**	If the Policy Management Solution will be using Lawful Intercept than the "mpe-li" ISO will have been used to install the MPEs and the "LI" mode will have been selected in the Initial Configuration of the Policy Management Servers. If this is the case the LI Mediation Function must be enabled on the CMP. If the Policy Management Solution is not using the "LI" function there is no need to perfrom this procedure. **Note:** In order to access the LI Mediation Function, you must log into the CMP GUI as user "liadmin".

Procedure 27: CMP Site1 Cluster Topology Configuration

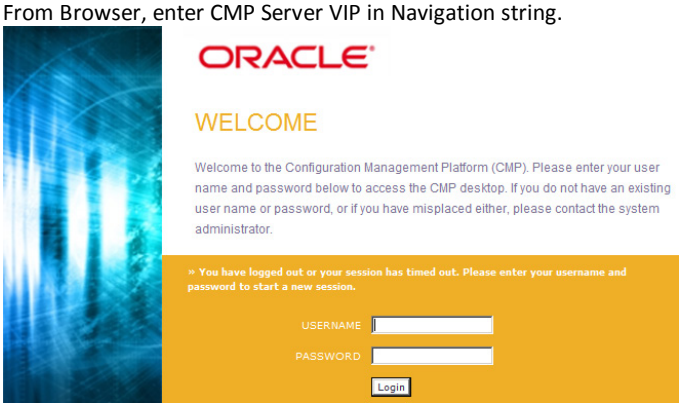
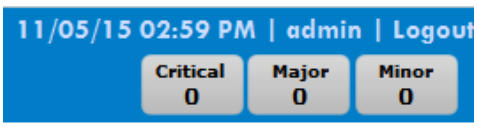
		Log into the CMP as *liadmin* and navigate to Policy Server -> LI Mediation Function -> and click on 'Create LI-Mediation Function' Outputs below are examples only. 
12. ☐	**GUI: Add SNMP Servers**	PLATFORM SETTING → SNMP Settings Make the appropriate configuration for SNMP destination, version and community string and then select save.  NOTE: De-select the checkbox for "traps enabled" until ready to go live. **You have completed this procedure**

Procedure 28: Topology Configuration of Additional Clusters

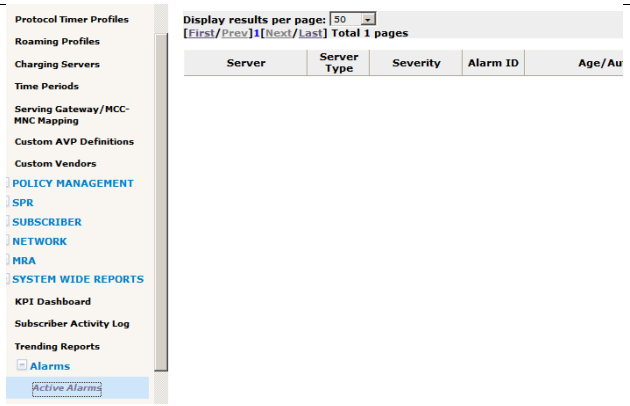
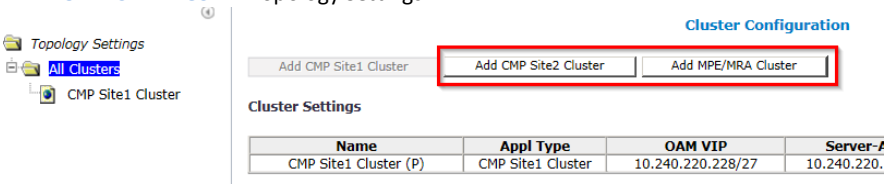
This procedure will configure the management relationships between the Active site CMP cluster and the other servers (MPEs/MRAs), and their cluster assignments. After this, the status of the servers will be available from the CMP GUI. The Geo-site CMP cluster is also configured in this way

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.

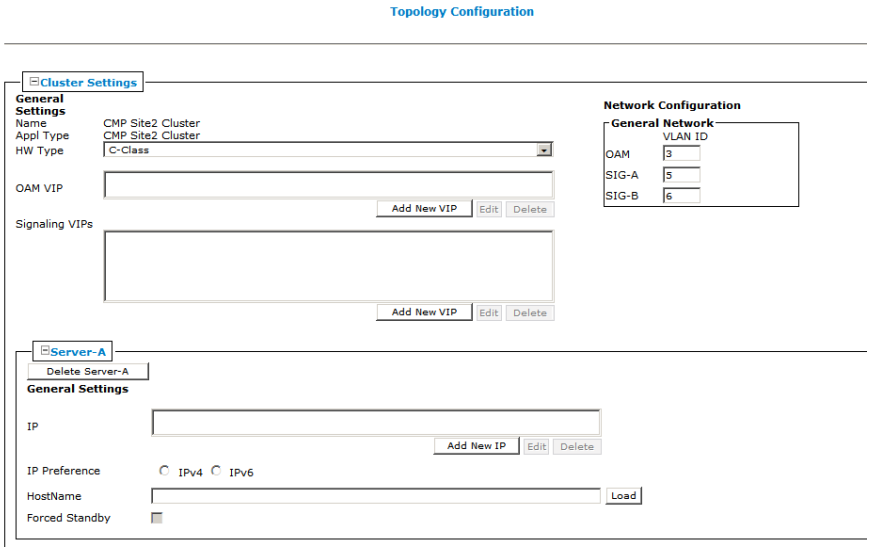
Procedure 28: Topology Configuration of Additional Clusters

STEP #		
	This procedure will configure the management relationships between the CMPs and the other servers (MPEs/MRAs), 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. **Pre-requisite:** - 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 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.  View of Alarms from CMP GUI upper right banner

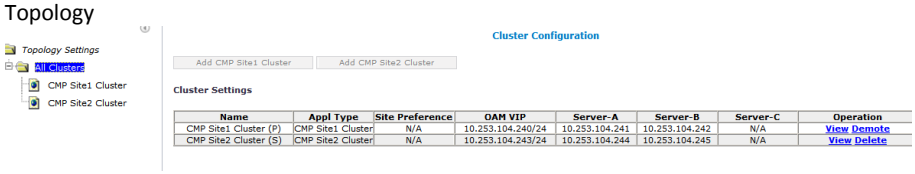
Procedure 28: Topology Configuration of Additional Clusters

		 View of Alarms from System Wide Reports -> Active Alarms IMPORTANT: In Policy 12.1.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. ☐	**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. For a Geo-Redundant CMP Cluster select : • Add CMP Site 2 Cluster For a MPE or MRA cluster select: • Add MPE/MRA Cluster **Note:** For a Geo-Redundant MRA/MPE cluster the option "**Manage Geo-Redundant MPE/MRA/BoD**" will need to have been selected in the Initial Configuration of the Policy Server
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. 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. *Review Procedure 27 step 2* if there are questions about the fields provided in the form. The initial form will configure the Cluster OAM VIP and the Server-A Real IP address. To datafill the hostname click on the <Load> button. **Note:** CMPs are not typically configured with Signaling VIPs

Procedure 28: Topology Configuration of Additional Clusters



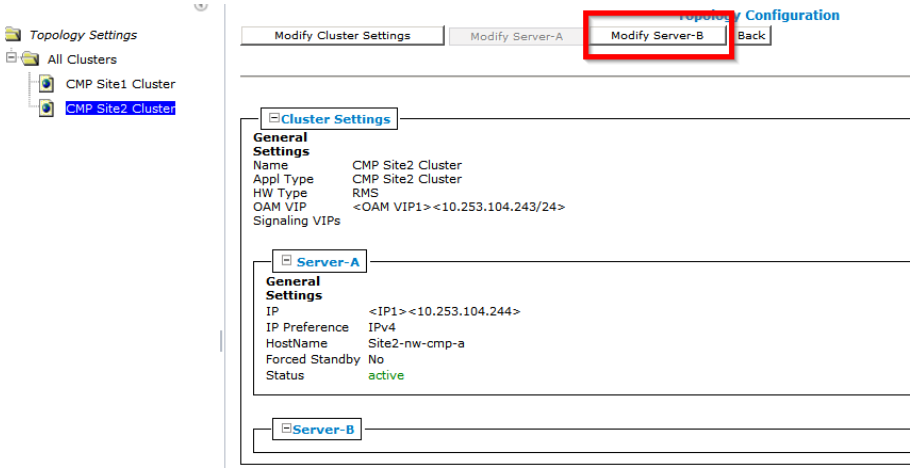
When completed save the form. The Geo –Redundant CMP Site2 Clsueter is now visible in the Topology



5. ☐ **Add SITE 2 CMP Cluster-Server-B**

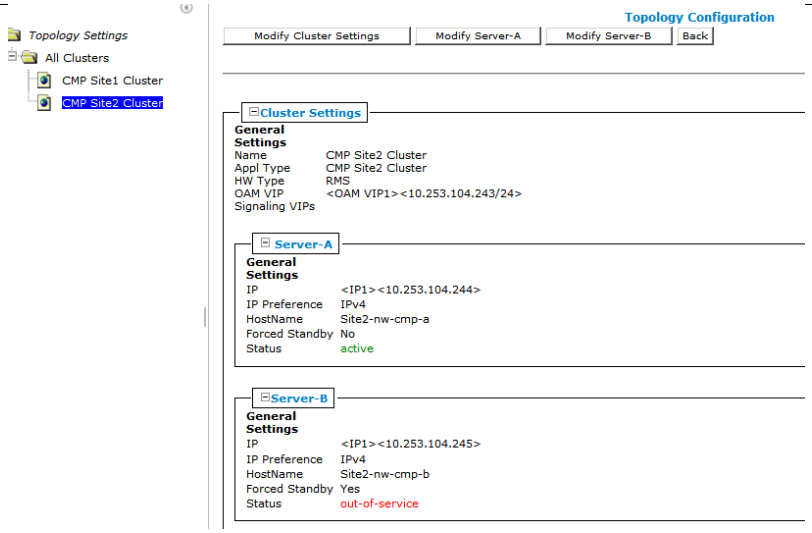
CMP-Site2 Cluster will need Server-B added to complete the cluster configuration. From the topology settings page click on CMP Site2 Cluster.

Click on Modify server-B.

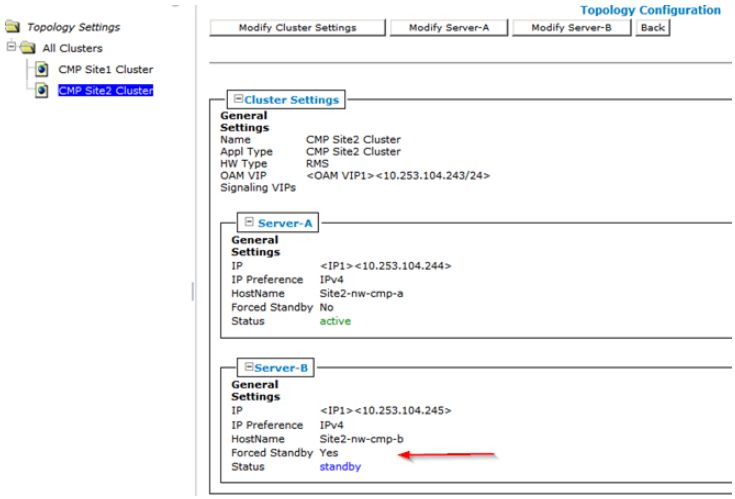


Datafill the form for Server-B accordingly and <Save>.

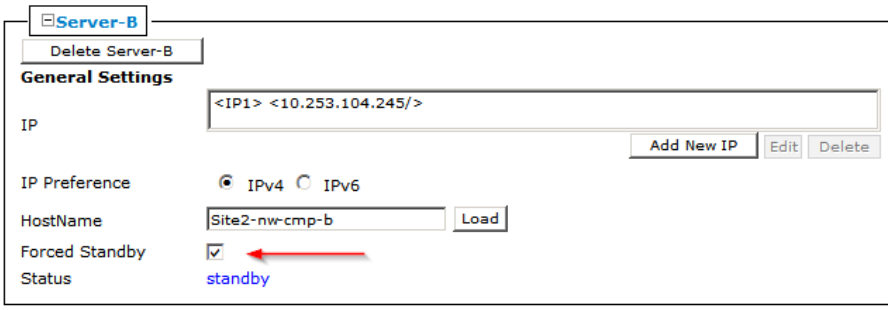
Procedure 28: Topology Configuration of Additional Clusters



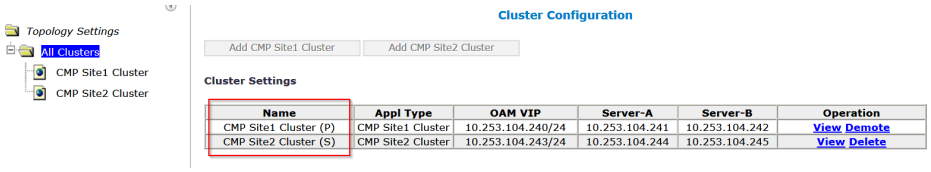
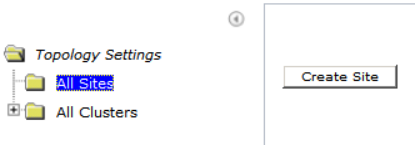
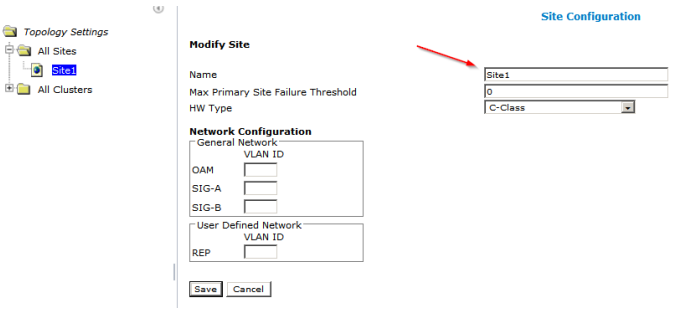
Note: Initally several alarms will be generated. Wait for all the alarms to clear - then refresh the view of the toplogy screen to confirm that the CMP Site2 Cluster is now <standby>.



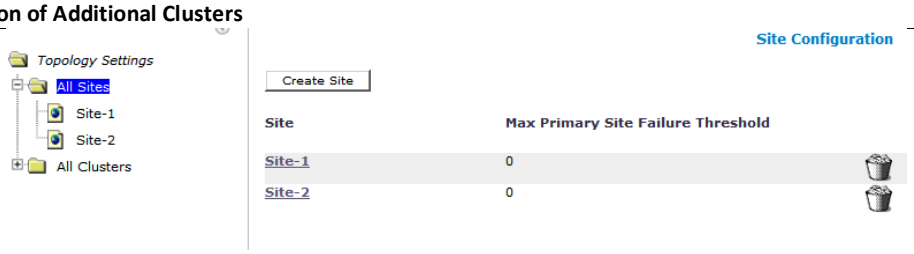
Return to topology configuration for the CMP Site2 Cluster and click on the < Modify Server-B> again to **uncheck** the Forced Standby state of Server-B by unchecking the Forced Standby box. <Save> the configuration



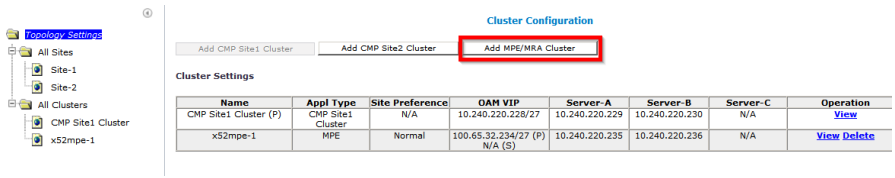
Procedure 28: Topology Configuration of Additional Clusters

		When the Geo-Redundat Site 1 and Site-2 clustersconfugration has been completed the CMP Site-1 Cluster will be marked with a (P) for primary and the CMP Site-2 Cluster wiil be marked with an (S) for secondary.  **The CMP Site2 Cluster Configuration is now complete.**
6. ☐	**Create and name Site-1 and Site-2** **NOTE:** This step is to be done once only.	**MPE and MRA clusters** can be dispersed between a primary site and a secondary site. This provides Geo-Redundancy for the MPE/MRA 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 MRA/MPE cluster the option "**Manage Geo-Redundant MPE/MRA/BoD**" will need to have been selected in the Initial Configuration of the Policy Server 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 MPE/MRA/BoD**" 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  When completed multiple sites can now be viewed in the Topology. MPEs/MRAs will be added to these sites at the time the topology for these servers is created.

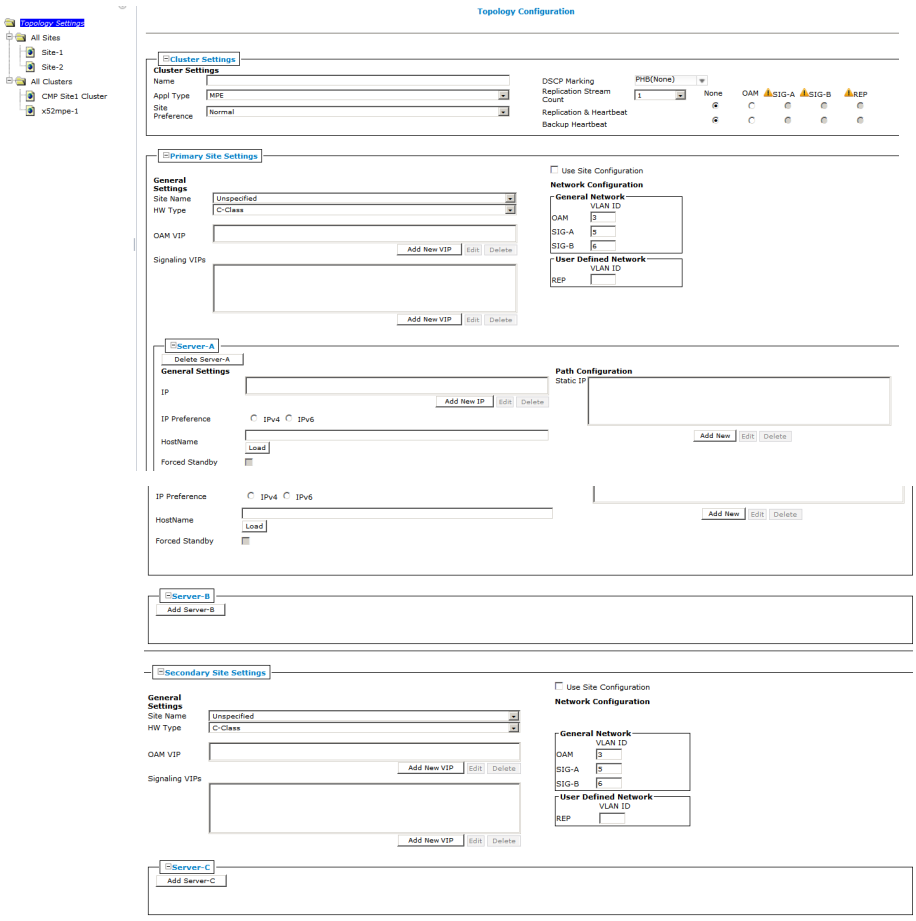
Procedure 28: Topology Configuration of Additional Clusters



7. ☐	**Add MPE/MRA Cluster**	PLATFORM SETTINGS → Topology Settings



Click on <Add MPE/MRA Cluster>. In the Topology Configuration form, enter the information for this cluster.

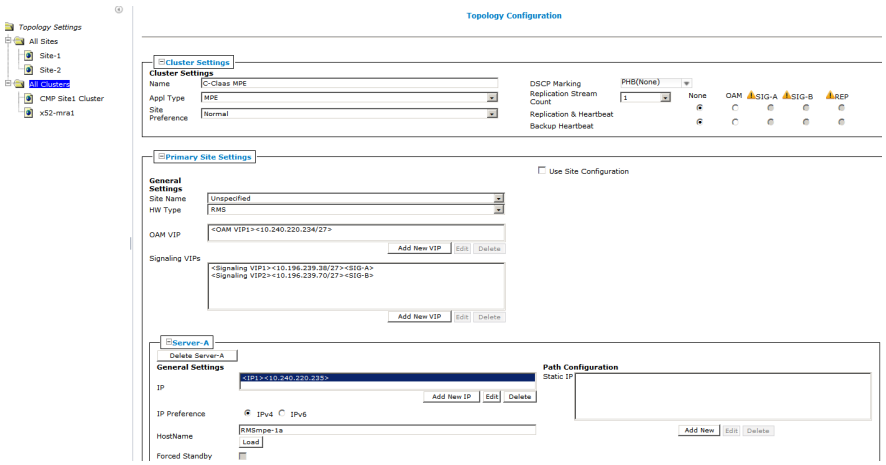


Procedure 28: Topology Configuration of Additional Clusters

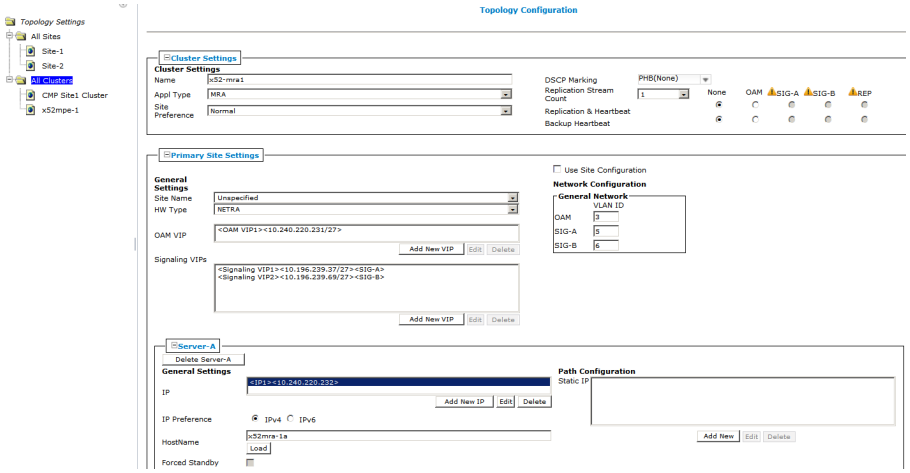
		It is allowed to add both Server-A, Server-B and Server-C in this form at the same time **Note:** Here it is determined whether the cluster that will be added to the topology will be an MPE cluster or a MRA cluster. **Note:** These settings are only an example of a likely configuration. An actual deployment will be specific to customer requirements. Define the Cluster Settings 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 **MRA** c) **Site Preference** – NORMAL DSCP Marking = NONE Replication Stream Count = 1 through 8 Replication and Heartbeat = REP Backup Heartbeat = OAM Define the Primary 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) • **C-Class (Segregated Traffic)** (for a configuration where Signaling and other networks are separated onto physically separate equipment) • **NETRA** (for a Netra server) • **RMS** (for a rack-mounted server) • **VM** (for a virtual machine) **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 At least one signaling VIP is required. Define the general network configuration for the C-Class, C-Class segregated, or 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

Procedure 28: Topology Configuration of Additional Clusters

Example of an MPE Cluster configuration of HW Type RMS

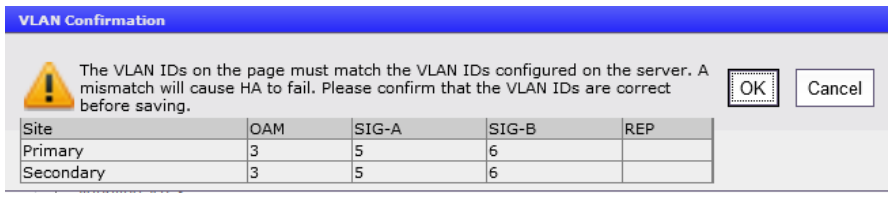


Example of an MRA cluster configuration of HW Type Netra

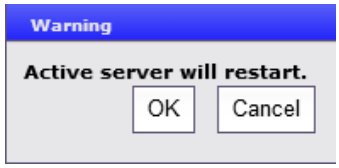


<**Save**> the topology configuration

Confirm the vlan configuration if the hardware type requires vlans

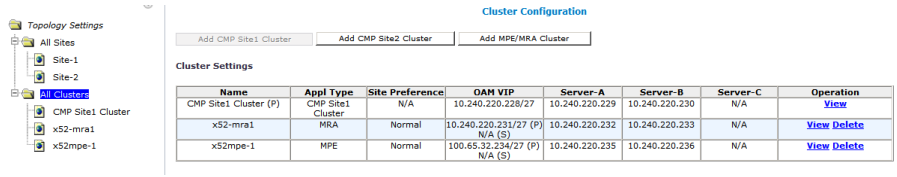


Click <**OK**> to confirm



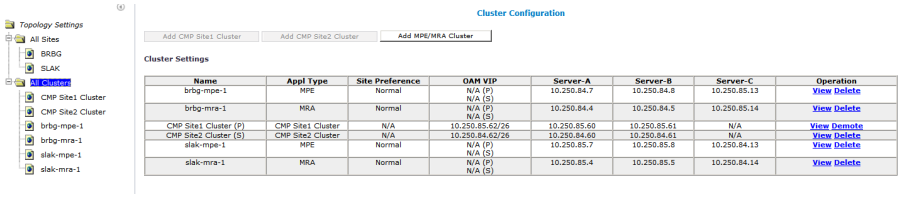
Procedure 28: Topology Configuration of Additional Clusters

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



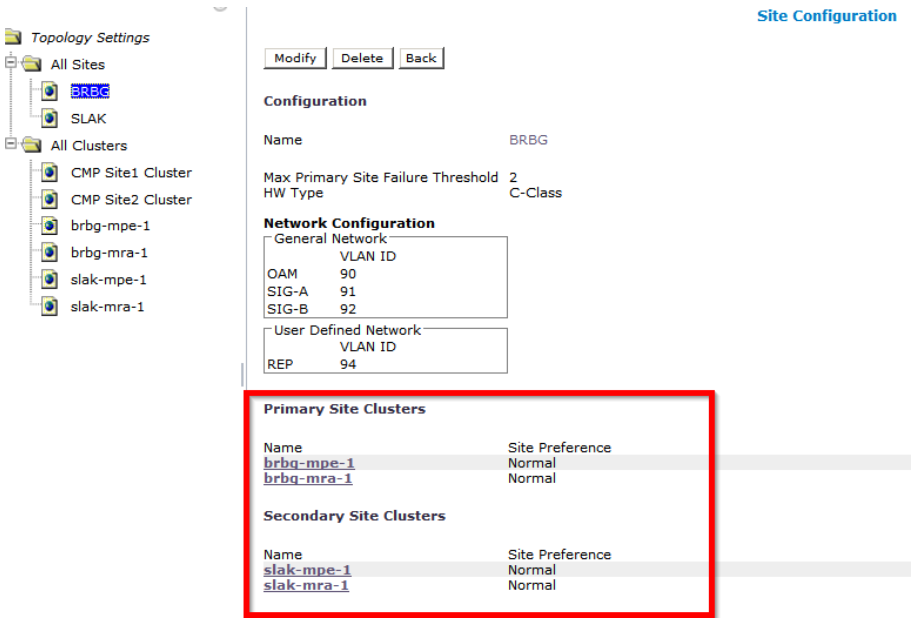
Note: Initally several alarms will be generated. Wait for all the alarms to clear - then refresh the view of the topology screen to confirm that the newly added MRA/MPE now shows an "active" and a "standby" status for Server-A and Server-B. If there was a Server-C added for to the MPE/MRA cluster topology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

Here is an example of a **Geo-Redundant Policy System in a c-Class environment** with <Site 1> and <Site 2 CMP> Clusters and several MPE and MRA components

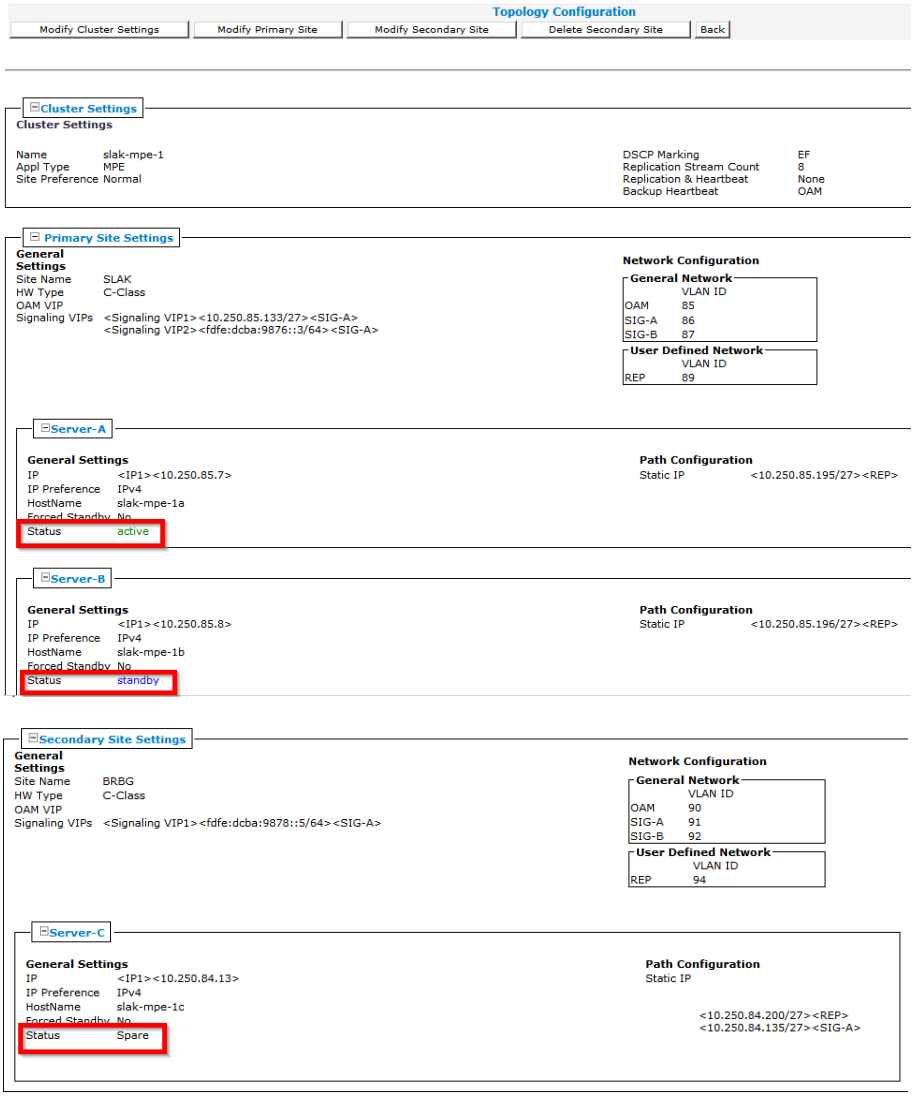


The MPEs and the MRAs have been assigned to the sites <BRBG> and <SLAK> per design of the topology.

Note: CMP clusters are associated with <CMP Site 1 cluster > and <CMP Site 2 Cluster> upon creation. Only the MPEs and MRAs are associated directly to the customized sites populated in "All Sites".



Procedure 28: Topology Configuration of Additional Clusters

		The Geo-Redundant configuration of the MPE cluster with a Spare server-C can be seen here.  Topology Configuration Modify Cluster Settings | Modify Primary Site | Modify Secondary Site | Delete Secondary Site | Back Cluster Settings Cluster Settings Name slak-mpe-1 Appl Type MPE Site Preference Normal DSCP Marking EF Replication Stream Count 8 Replication & Heartbeat None Backup Heartbeat OAM Primary Site Settings General Settings Site Name SLAK HW Type C-Class OAM VIP Signaling VIPs <Signaling VIP1><10.250.85.133/27><SIG-A> <Signaling VIP2><fdfe:dcba:9876::3/64><SIG-A> Network Configuration General Network VLAN ID OAM 85 SIG-A 86 SIG-B 87 User Defined Network VLAN ID REP 89 Server-A General Settings IP <IP1><10.250.85.7> IP Preference IPv4 HostName slak-mpe-1a Forced Standby No Status active Path Configuration Static IP <10.250.85.195/27><REP> Server-B General Settings IP <IP1><10.250.85.8> IP Preference IPv4 HostName slak-mpe-1b Forced Standby No Status standby Path Configuration Static IP <10.250.85.196/27><REP> Secondary Site Settings General Settings Site Name BRBG HW Type C-Class OAM VIP Signaling VIPs <Signaling VIP1><fdfe:dcba:9878::5/64><SIG-A> Network Configuration General Network VLAN ID OAM 90 SIG-A 91 SIG-B 92 User Defined Network VLAN ID REP 94 Server-C General Settings IP <IP1><10.250.84.13> IP Preference IPv4 HostName slak-mpe-1c Forced Standby No Status Spare Path Configuration Static IP <10.250.84.200/27><REP> <10.250.84.135/27><SIG-A> **Note:** If the topology configuration is performed at a time when there is no network connectivity between the CMP and the MRA/MPE 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. 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.
8. ☐	**Repeat the previous step for additional clusters**	**A list of Clusters to be configured can be added to this step as a reminder.**

Procedure 28: Topology Configuration of Additional Clusters

9. ☐	**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.
10. ☐	**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.
11. ☐	**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.***

Procedure 29: SSH Key Exchanges to all Servers in the Topology

After you perform the initial configurationof all the servers, and the topology has been set up correctly, SSH keys must be exchanged.

Procedure 29: SSH Key Exchanges to all the Servers in the Topology

STEP #	**Pre-requisite:** - CMP Site 1 cluster is configured and GUI available - MPE/MRAs for one or more sites are added to the CMP Topology 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 1A:**
	Execute Key Exchanges to MPE/MRAs
		Ssh to the **active** server at CMP Site 1 Cluster . The CLI command <ha.mystate> can be used to determine if the server is the active server in the HA cluster.
		
		$sudo qpSSHKeyProv.pl --prov
		
		Enter the Password of admusr
		`^C[admusr@x52cmp-1a ~]$ sudo qpSSHKeyProv.pl --prov`
		
		`The password of admusr in topology:`
		`Connecting to admusr@x52mpe-1b ...`
		`Connecting to admusr@x52mra-1b ...`
		`Connecting to admusr@x52mpe-1a ...`
		`Connecting to admusr@x52mra-1a ...`
		`Connecting to admusr@x52cmp-1a ...`
		`Connecting to admusr@x52cmp-1b ...`
		
		`[1/6] Provisioning SSH keys on x52mpe-1b ...`
		
		`[2/6] Provisioning SSH keys on x52mra-1b ...`
		
		`[3/6] Provisioning SSH keys on x52mra-1a ...`
		
		`[4/6] Provisioning SSH keys on x52mpe-1a ...`
		
		`[5/6] Provisioning SSH keys on x52cmp-1a ...`
		
		`[6/6] Provisioning SSH keys on x52cmp-1b ...`
		
		`SSH keys are OK.`

Procedure 29: SSH Key Exchanges to all the Servers in the Topology

2. ☐	**Ssh to CMP Site 1A:** Check Key Exchanges to MPE/MRAs	Ssh to the **B server** at CMP Site 1. **$sudo qpSSHKeyProv.pl --check --verbose** Enter the Password of admusr

```
[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 ~]$
```

After the topology has been setup and SSH keys have been correctly exchanged, it is possible that some server in the topology changes its keys. This case happens when:

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

In any of the above scenarios this procedure should be executed again. The SSH provisioning utility will recheck the existing ssh key exchanges in the entire topology and provision any key exchanges not yet executed. It is OK to run the command multiple times, even if keys were previously exchanged.

This procedure has been completed.

Procedure 30: Configure IP Routing on the MPE and MRA

On the MPE and MRA servers, the default route is initially configured to route all traffic via the OAM interface for remote servers. This is done to facilitate clustering and topology configurations. However, in many (most) networking environments, it is necessary to route signaling traffic (Diameter) via the Signaling interfaces of the servers and switches, and OAM traffic (replication, configuration, Alarms, Reports) via the OAM network. This requires routing configurations on the servers.

This procedure will guide you through configuring the required static routes on the MPE and MRA servers, to provide separation of OAM and Signaling traffic.

The recommended method to provide this separation is:

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

  Note: Adminstration of the MPEs and MRAs 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 SigA network.

In this way, traffic to other Signaling points in the network will follow the Default route over the SigA network.

Note that this should only be done for the MPE and MRA, as the CMP should retain the default route on the OAM interface.

This procedure is specific to the recommended method. Other routing configurations may be desired, depending on the customer needs. This procedure will illustrate the basic steps for making routing configurations on the MPE and MRA servers.

Procedure 30: Configure IP Routing on the MPE and MRA to separate OAM and Signaling traffic

STE P #	This procedure will configure the IP routing on the MPE and MRA to separate OAM and Signaling traffic. Specifically, it will change the Default route to the SigA network, and add static Routes for the OAM network. **Pre-requisite:** - Ssh access to the MPE and MRA servers - During this procedure it is recommended that access to the server iLO remote console is always available to get back into the server in case a route change impacts remote access. - Using SSH from the CMP to access the MRA/MPE servers will minimize the possibility of losing connectivity while performing 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. ☐	**Preparations:** Identify the Static OAM Routes for MPEs and MRAs	Determine the static routes that will be required on the OAM interface, once the default route is moved. As a minimum you will need the following static routes: • Site 1 and 2 CMP OAM network (if not co-located) • Server-C for geo-redundant MPE/MRA clusters • NTP server • DNS server • SNMP trap destination • Remote backup archives • External syslog servers • Any host you wish the MPE/MRA server to access over the OAM network i.e. routes to mates in a geo-redundant setup. While it is preferred to configure static host routes for each destination, fewer network routes may be used to maintain network connectivity.

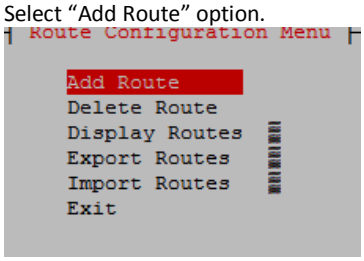
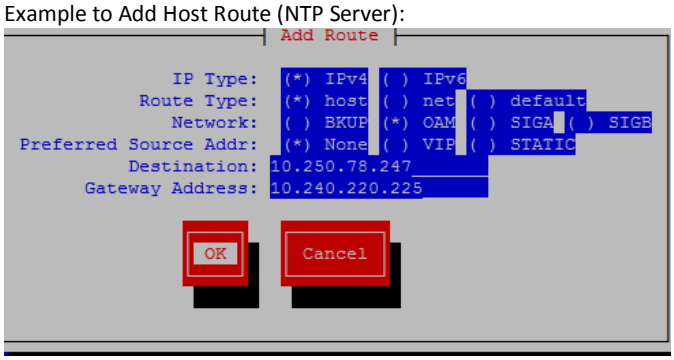
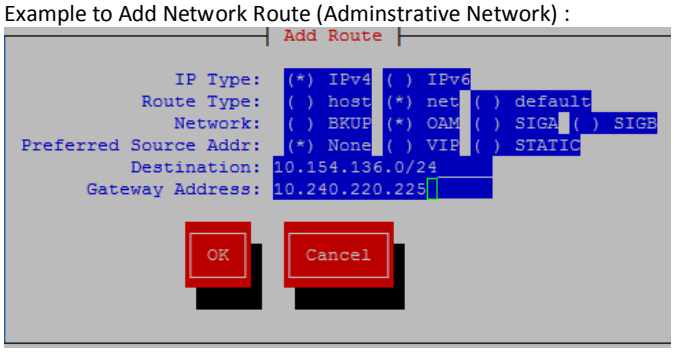
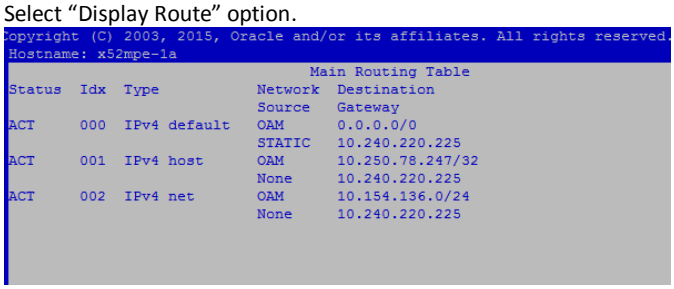
Procedure 30: Configure IP Routing on the MPE and MRA to separate OAM and Signaling traffic

2. ☐	**Ssh:** root login	Ssh to a CMP server, and then ssh to the standby server of the MPE or MRA cluster to be configured.
		
		`[admusr@x52cmp-1a ~]$ ssh admusr@10.240.220.235`
		`FIPS integrity verification test failed.`
		`Password:`
		`Last login: Wed Nov 11 10:46:33 2015 from 10.240.220.229`
		`[admusr@x52mpe-1a ~]$`
		
		Note: after this routing change, it may not be possible to ssh directly to the MPE and MRA server OAM interface, since the Default route will no longer be set to use the OAM Network. Thus, ssh access to the MPE and MRA servers OAM addresses must be via the CMP servers.

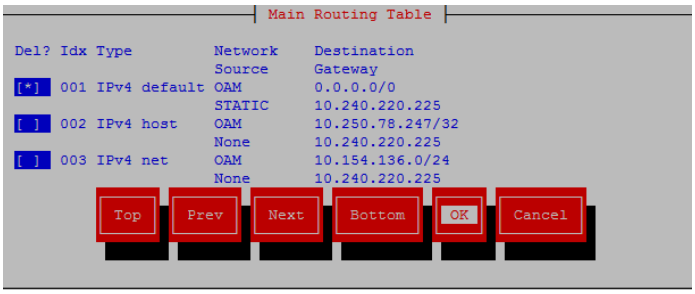
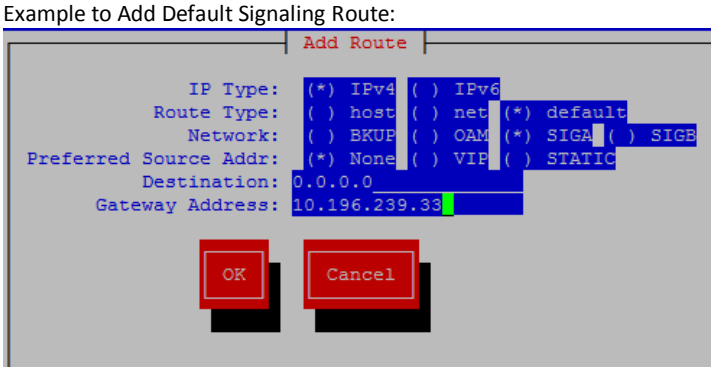
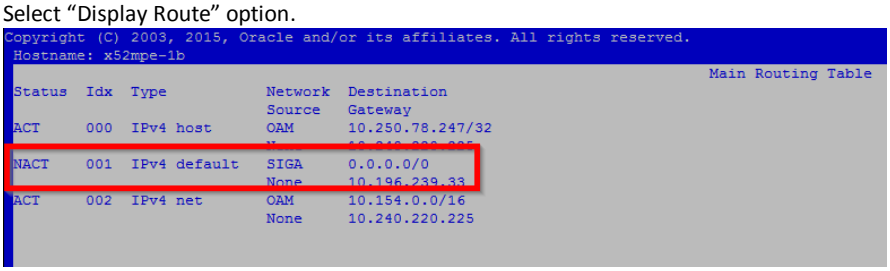
3. ☐	**Ssh:** Verify if server is Standby	$sudo **ha.mystate**
		`[admusr@x52mra-1a ~]$ sudo ha.mystate`
		`resourceId role node subResources lastUpdate`
		`DbReplication Stby C0516.004 0 1107:172936.457`
		`VIP Stby C0516.004 0 1107:172936.459`
		`QP Stby C0516.004 0 1107:172954.524`
		`DbReplication_old OOS C0516.004 0 1107:172859.000`
		`[admusr@x52mra-1a ~]$`
		If this server is not standby, ssh to the other server of the cluster

4. ☐	**Platcfg:** Access Routing Config tool	$sudo **su - platcfg** Select Policy Server Configuration → Routing Config Policy Configuration Menu Set Policy Mode Perform Initial Configuration Restart Application Cluster Configuration Removal Verify Initial Configuration Verify Server Status SSL Key Configuration Ethernet Interface Parameter Settings Save Platform Debug Logs Cluster File Sync Routing Config Firewall DSCP Config Backup and Restore Exit **Note:** it is not recommended to use other routing configuration methods, like netAdm or configuring routes directly from the CLI.

Procedure 30: Configure IP Routing on the MPE and MRA to separate OAM and Signaling traffic

5. ☐	**Platcfg:** Add OAM Routes	Select "Add Route" option.  Add the OAM static routes as planned in step 1. **Note:** If the route changes requred is large, it is possible to use the import/export functionality of the platcfg utiility to modify the routing as needed. **Note:** Use the space bar to select and tab to navigate Example to Add Host Route (NTP Server):  Example to Add Network Route (Adminstrative Network) : 
6. ☐	**Platcfg:** Verify - Display Routes	Select "Display Route" option.  Verify Routes are created as expected. In this snapshot one host route and one network route has been added. The default gateway still points to the OAM Interface.

Procedure 30: Configure IP Routing on the MPE and MRA to separate OAM and Signaling traffic

7. ☐	**Platcfg:** Delete OAM Default Route	Select "Delete Route" option. Delete the current Default Route.  **Note:** This step will break the OAM network connectivity to the server, except via the CMP servers. If the connection is lost, Ssh to the CMP, and then ssh to server. It may also be possible to use the iLO remote console if needed.
8. ☐	**Placfg:** Add Default route via Sig Network	Select "Add Route" option. Add the Default routes via the SigA Gateway. Example to Add Default Signaling Route:  Note: On the standby server the default route will be Inactive. This is expected. The default route will activate if the standby server becomes the active server in the HA cluster.
9. ☐	**Platcfg:** Verify - Display Routes	Select "Display Route" option.  Verify Routes are created as expected.
10. ☐	**Ssh:** Reboot the server	Re-boot the server to assure that the default route change is made, and the routes are stable across a boot
11. ☐	**Ssh:** Verify – PING or tracert to servers	Log back into the server with the newly addred routes and changed default gateway and ping, traceroute or ssh to the servers defined in Step 1 to confirm the target servers are reachable.

Procedure 30: Configure IP Routing on the MPE and MRA to separate OAM and Signaling traffic

12. ☐	**Ssh:** Switchover to make configured server Active, and other server Standby	Ssh to the Active server of the cluster as root. The following command will cause the currently active server to become the standby server in order that the route configuration can be executed while the this server is Standby.
		
		$sudo **service qp_procmgr restart**
		`[admusr@x52mra-1b ~]$ sudo ha.mystate`
		`resourceId role node subResources lastUpdate`
		`DbReplication Active C0516.026 0 1111:191952.754`
		`VIP Active C0516.026 0 1111:191952.756`
		`QP Active C0516.026 0 1111:191952.757`
		`DbReplication_old OOS C0516.026 0 1111:184956.639`
		`[admusr@x52mra-1b ~]$ sudo service qp_procmgr restart`
		`Stopping qp_procmgr: [ OK ]`
		`Starting qp_procmgr: [ OK ]`
		`[admusr@x52mra-1b ~]$ sudo ha.mystate`
		`resourceId role node subResources lastUpdate`
		`DbReplication Stby C0516.026 0 1111:192539.574`
		`VIP Stby C0516.026 0 1111:192537.547`
		`QP Stby C0516.026 0 1111:192545.543`
		`DbReplication_old OOS C0516.026 0 1111:184956.639`
		`[admusr@x52mra-1b ~]$`
		
		Repeat steps 4 – 11 of this procedure on the the server that is now “standby”. If the cluster is geo-redundant this procedure should also be performed on the “spare” C-Server. This procedure has now been completed for this cluster.

13. ☐	**Ssh:**Repeat this procedure for additional clusters	This procedure should be performed on all MRA and MPE clusters in the topology.

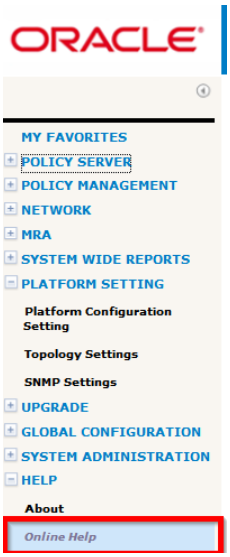
7.2 POST TOPOLOGY CONFIGURATION TASKS

The following description provides an "Overview of the Main Tasks" applicable to configuring the MPE (Policy Server) and MRA (Policy Front End) components, after the Policy Management Solution's Topology Configuration has been completed per the previous procedures in section 7.1 of this document. Note that additional information on these tasks are reviewed in greater detail in the 12.1.x CMP Wireless User's Guide.

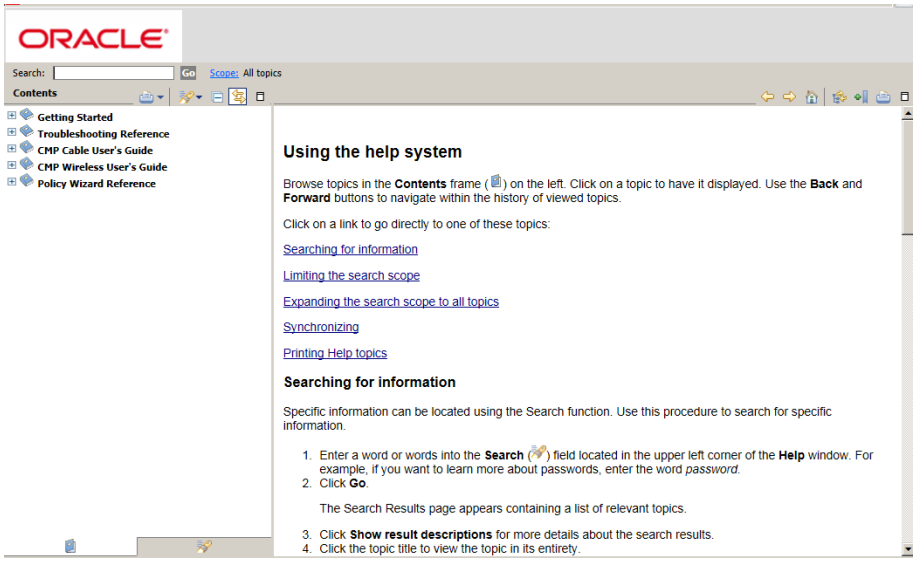
[10]E62450 - Configuration Management Platform Wireless User's Guide Release 12.1.x

In Policy 12.1.x, the Wireless User's Guide is provided with the CMP product, and available as On-line help.

In the CMP Menu navigate to On-Line Help.



Below is the Help system welcome screen:



Note: The references in this section are from the CMP Wireless User's Guide Release 12.1.x

Overview of Main Tasks

The major tasks involved in using MPE devices are configuration, defining network elements, defining manageable devices, managing subscribers, and administering authorized CMP users. The configuration tasks are a series of required steps that must be completed in the following order:

1. Configure the topology, which defines the addresses and interconnections of Policy Management clusters in your network. These steps are described in *Configuring the Policy Management Topology*.

2. Configure policy server profiles for MPE devices. This step is described in *Managing Multimedia Policy Engine Devices*.

3. Configure protocol routing, which enables a Policy Management device to forward requests to other Policy Management devices for further processing. This step is described in *Configuring Protocol Routing*.

4. Configuring advanced device settings, which include expert settings, service overrides, and load shedding options. This step is described in *Configuring Advanced Device Settings*.

The element and profile definition tasks you need to perform depend on what exists on your network. They can be defined in any order at any time as needed. The full set of tasks is as follows:

- Create network element profiles, including protocol options, for each network element with which Policy Management devices interact. This task is described in *Managing Network Elements*.

- Specify which Policy Management device will interact with which network elements. This task is described in *Managing Multimedia Policy Engine Devices* and *Managing Policy Front End Devices*.

- Define protocol timer profiles, which configure the Diameter response timeout values for specific applications and the different message types within an application. This task is described in *Managing Protocol Timer Profiles*.

- Define charging servers, which are applications that calculate billing charges for a wireless subscriber. This task is described in *Managing Charging Servers*.

- Map serving gateways to mobile country codes (MCCs) and mobile network codes (MNCs). This task is described in *Mapping Serving Gateways to MCCs/MNCs*.

- Configure Policy Front End (also called Multi-Protocol Routing Agent or MRA) devices, which are Policy Management devices that can route requests to MPE or other MRA devices. This task is described in *Managing Policy Front End Devices*.

- Configure subscriber profile repositories and manage entity states, quotas, pools, tiers, and entitlements. These tasks are described in *Managing Subscriber Profile Repositories* and *Managing Subscribers*.

The management and administrative tasks, which are optional and performed only as needed, are as Follows:

- View reports on the function of the Policy Management systems in your network. This task is

described in *System-Wide Reports*.

- Manage CMP users, accounts, access, authorization, and operation. These tasks are described in *System Administration*.
- Upgrade software using the Upgrade Manager. These tasks are described in *Upgrade Manager*.

7.3 *CONFIGURE POLICY SERVERS (AND MRAS)*

The previous section provides an overview of all the main tasks to be performed after the Policy Management Solution topology configuration has been completed. This section will only cover procedures to configure the Policy Servers (and optionally MRAs) to a minimum level to execute a test call. Additional details can be found in the CMP Wireles User's Guide. For more information refer to the CMP Wireless User's Guide.

[10]E62450 - Configuration Management Platform Wireless User's Guide Release 12.1.x

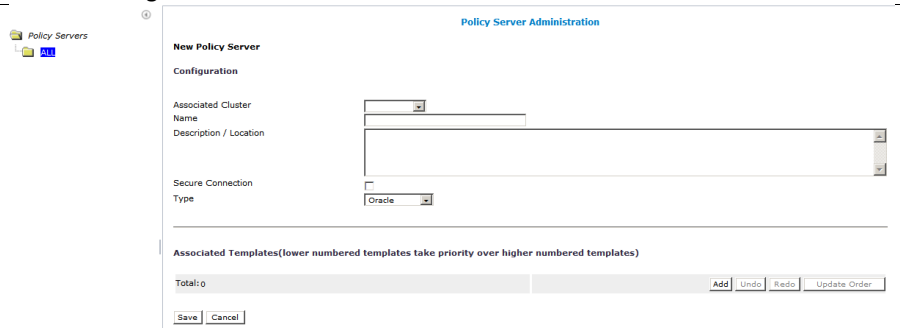
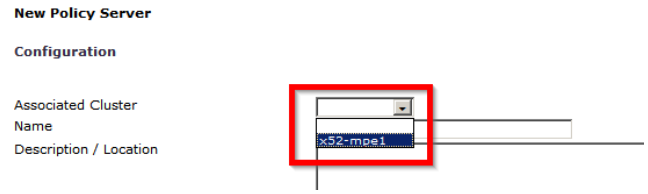
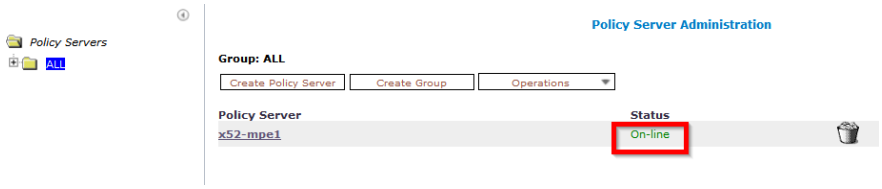
Procedure 31: Adding MPE and MRA to CMP Menu

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

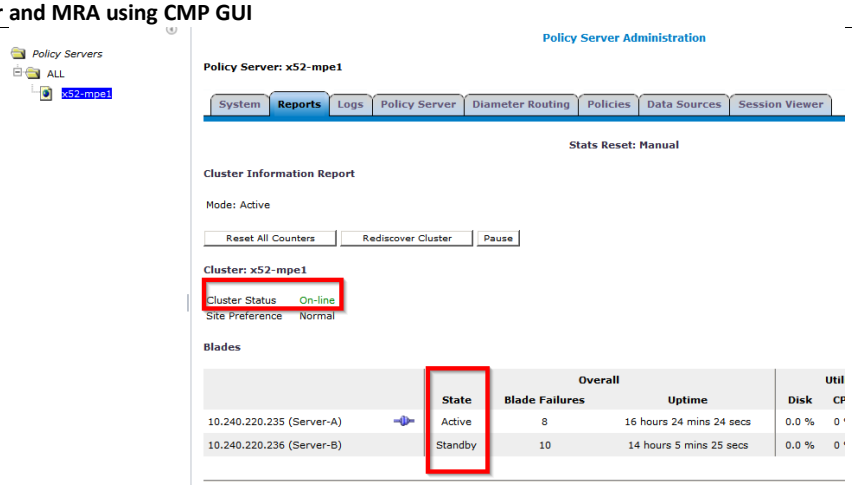
Procedure 31: Configure Policy Server and MRA using CMP GUI

STEP #		
	This procedure will perform the configuration of MPE/Policy Server and MRA applications **Pre-requisite:** - 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 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:

Procedure 31: Configure Policy Server and MRA using CMP GUI

		 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.  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

Procedure 31: Configure Policy Server and MRA using CMP GUI

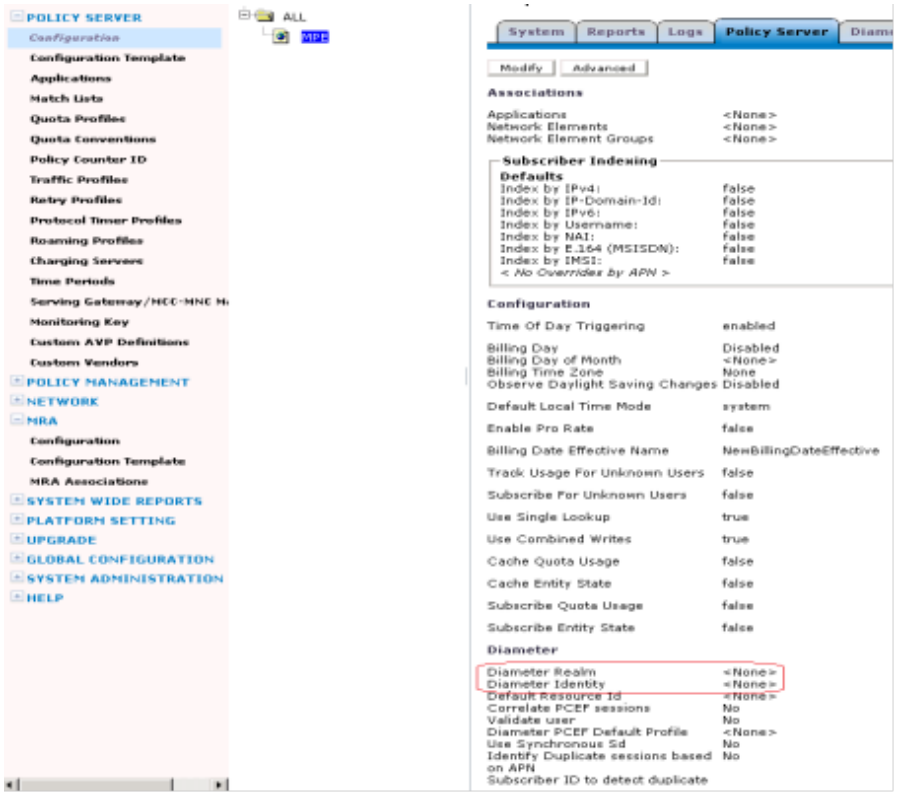


Validate that MPE cluster status is On-line and that both Active and Standby servers displayed correctly

3. ☐ **Diameter configurations for MPE**

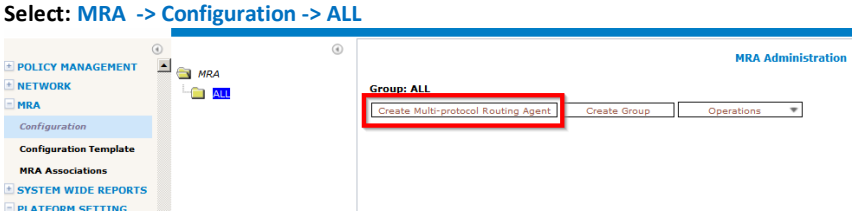
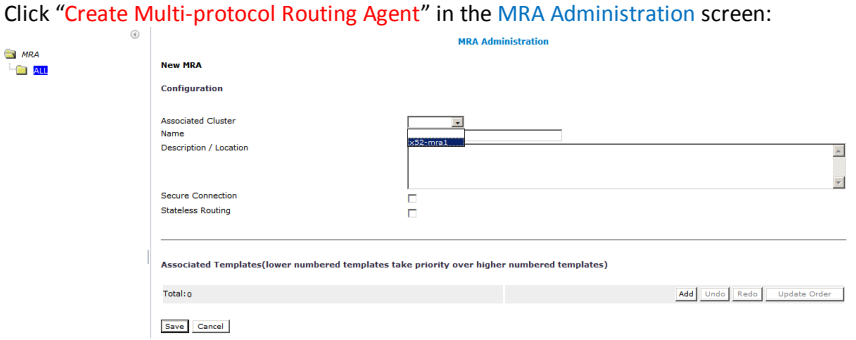
Select: Policy Server -> Configuration -> MPE -> Policy Server tab

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.

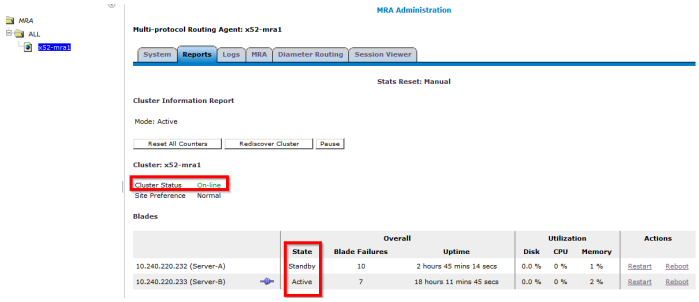
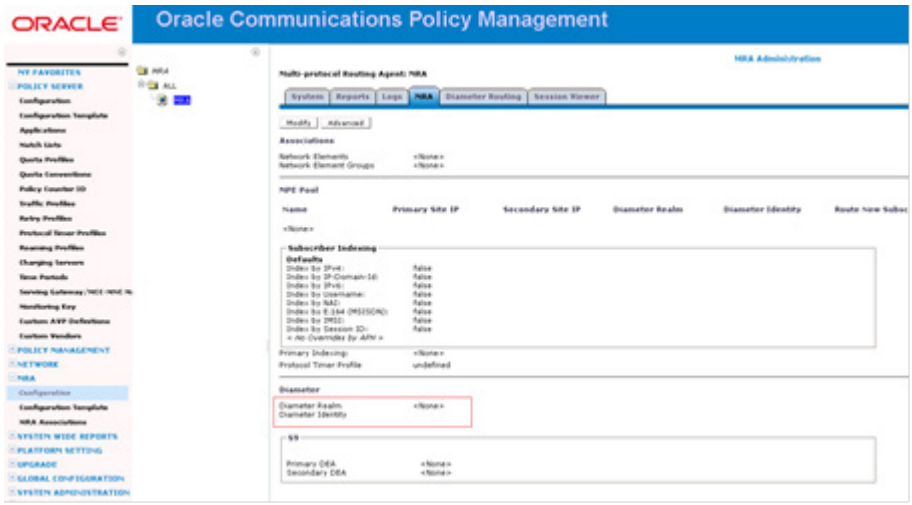


To define these diameter parameters, click the “Modify” button on top of page then fill in the diameter Realm and Identity that your network will be using and click “Save”:

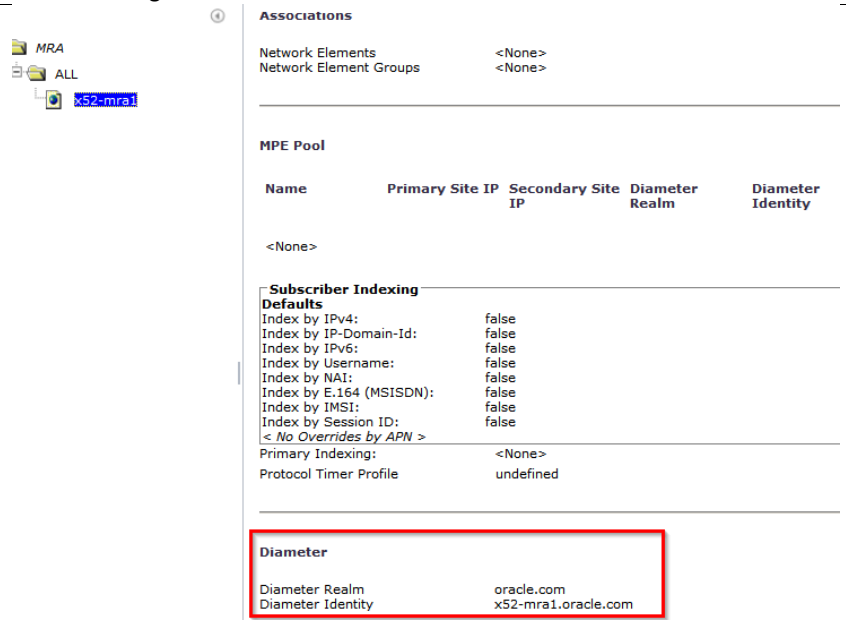
Procedure 31: Configure Policy Server and MRA using CMP GUI

		<table><tr><th>Attribute</th><th>Description</th></tr><tr><td>Diameter Realm</td><td>The domain of responsibility (for example, galactel.com) for the MPE device.</td></tr><tr><td>Diameter Identity</td><td>The fully qualified domain name (FQDN) of the MPE device (for example, mpe3.galactel.com).</td></tr></table> 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":

Procedure 31: Configure Policy Server and MRA using CMP GUI

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 configurations 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”:

Procedure 31: Configure Policy Server and MRA using CMP GUI

		 **You have completed this procedure:**

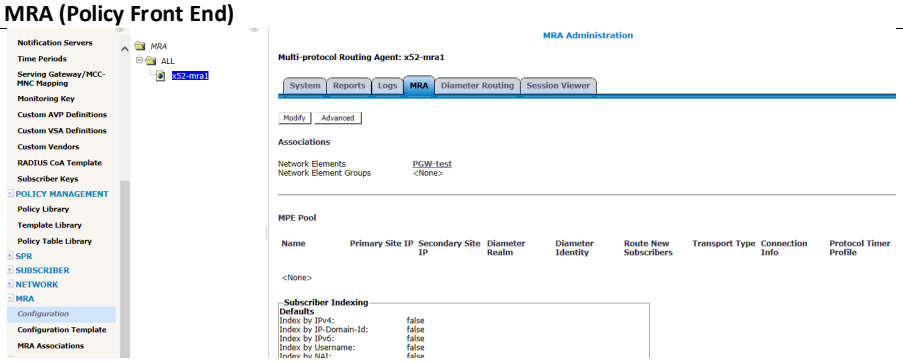
Procedure 32: Configure MPE Pool on MRA (Policy Front End)

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.

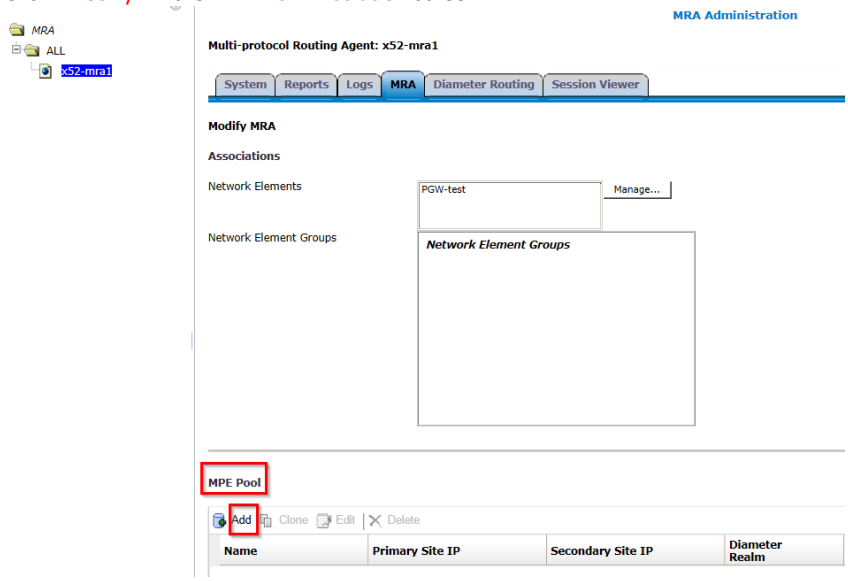
Procedure 32: Configure MPE Pool on MRA (Policy Front End)

STEP #	This procedure will add the MPE clusters to the MPE Pool of the MRA (Policy Front End) **Pre-requisite:** - 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

Procedure 32: Configure MPE Pool on MRA (Policy Front End)

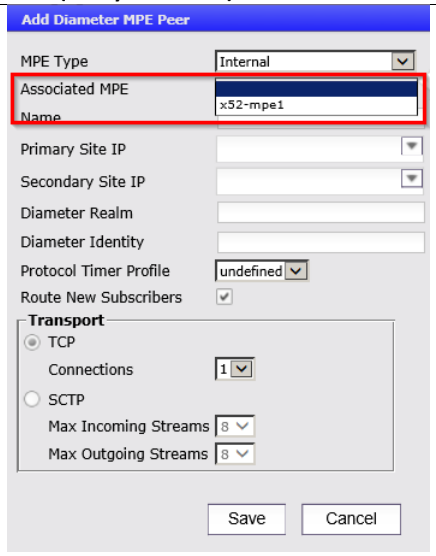


Click "Modify" in the MRA Administration screen:



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

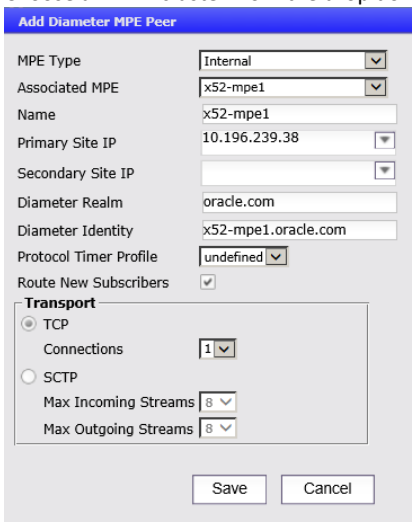
Procedure 32: Configure MPE Pool on MRA (Policy Front End)



Click the "Associated MPE" drop down on the Add Diameter Peer form:

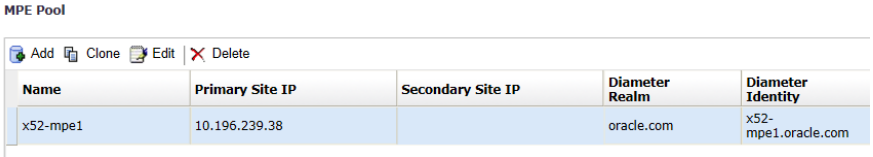
MPE clusters previously configured in the CMP topology and added to the CMP menu will be listed here.

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 as per step 3 in Procedure 32



The added MPE cluster now appears in the MPE Pool form. Navigate to the bottom of the form and click "Save" again.

Procedure 32: Configure MPE Pool on MRA (Policy Front End)

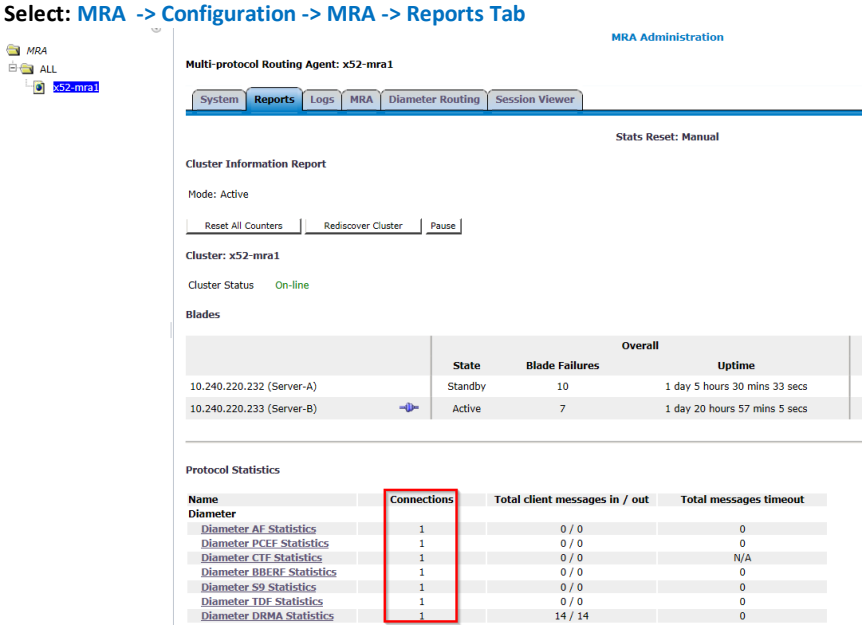
The added MPE cluster can now be seen in the MPE Pool

MPE Pool

Name	Primary Site IP	Secondary Site IP	Diameter Realm	Diameter Identity	Route New Subscribers	Transport Type	Connection Info
x52-mpe1	10.196.239.38		oracle.com	x52-mpe1.oracle.com	true	TCP	Connections : 1

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

Select: MRA -> Configuration -> MRA -> Reports Tab



Logs can be noted on the MPE that the Diameter connection between the MRA and the MPE has been established.

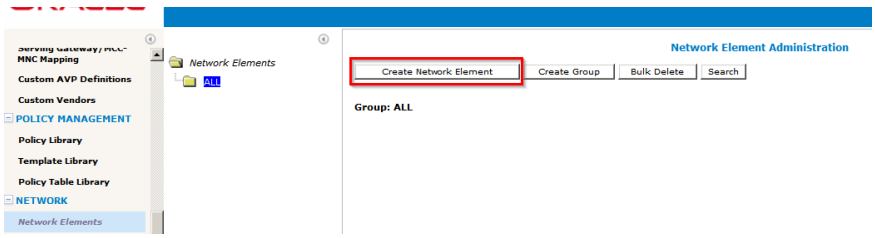
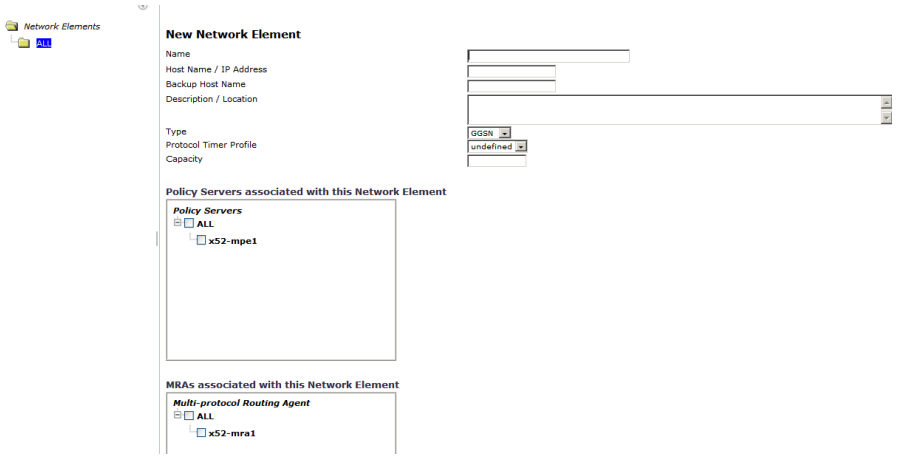
1401 Warning Diameter:Transport connection opened with peer 10.196.239.38:3868
1404 Info Diameter:Sent CER [705897686:1266001557] to x52-mpe1.oracle.com (10.196.239.38:3868)
1413 Info Diameter:Received CEA [705897686:1266001557] DIAMETER_SUCCESS (2001) from x52-mpe1.oracle.com(10.196.239.38:3868) in 0 ms
1407 Notice Diameter:Peer x52-mpe1.oracle.com(10.196.239.38:3868) status changed from INITIAL to OKAY

You have completed this procedure.

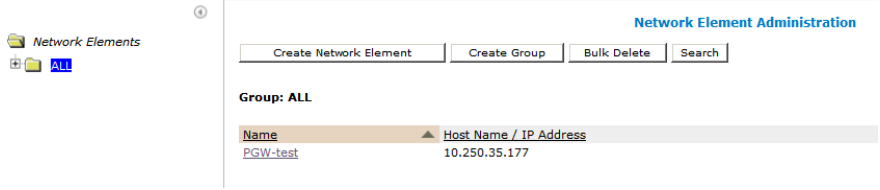
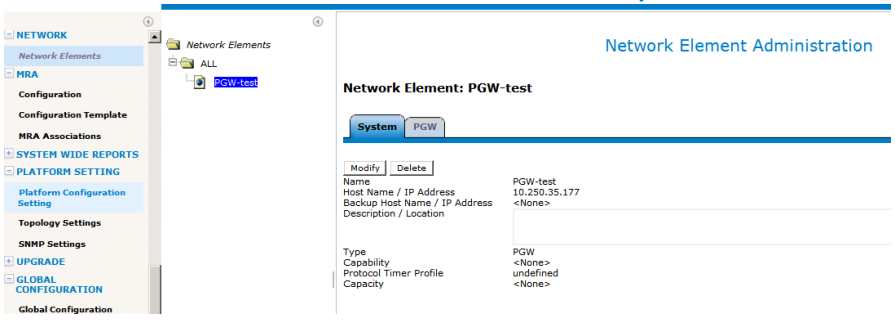
Procedure 33: Define and Add Network Elements

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

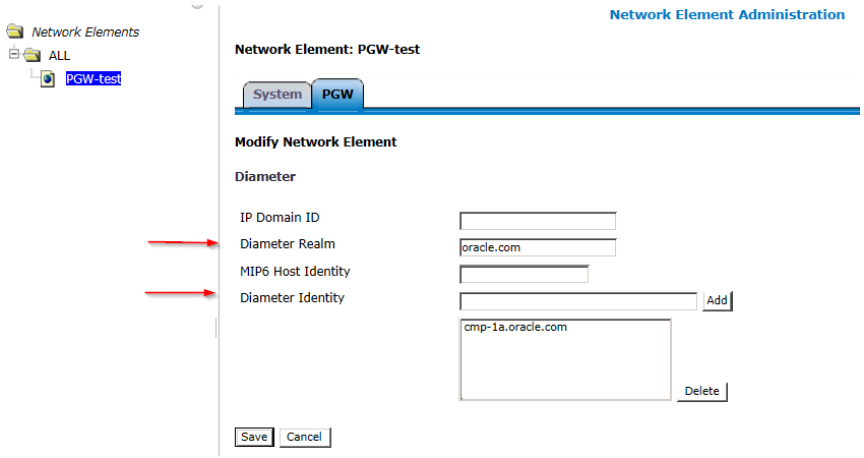
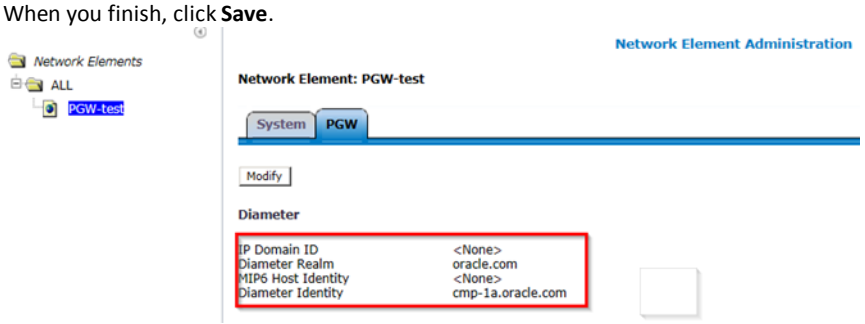
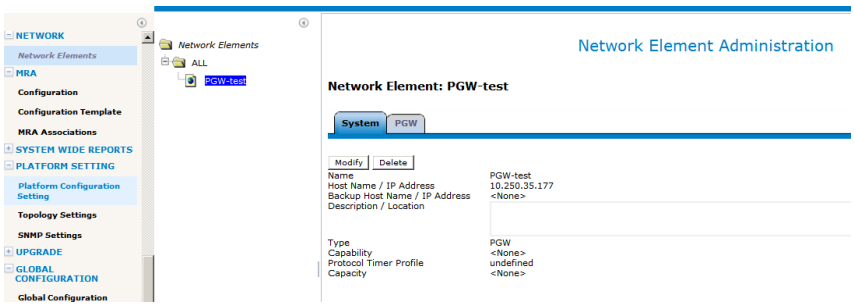
Procedure 33: Define and Add Network Elements

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. **Pre-requisite:** - 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: Network -> Network Elements -> All**  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 supported types are: **Note:** This list varies depending on the configuration of the CMP system.

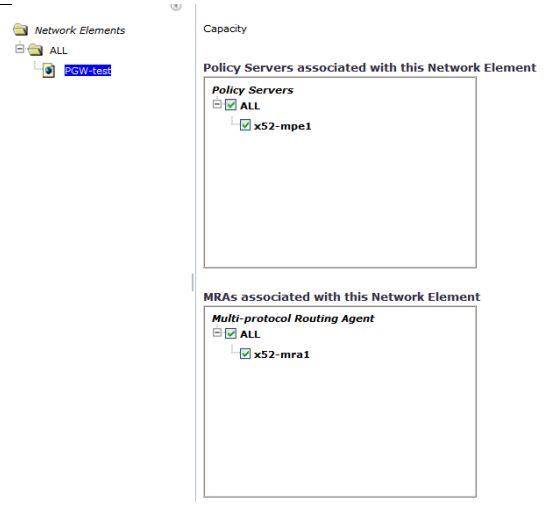
Procedure 33: Define and Add Network Elements

		• **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**. For this example a "PGW" Network Element has been defined. **New Network Element** Name: PGW-test Host Name / IP Address: 10.250.35.177 Backup Host Name: Description / Location: Type: PGW Protocol Timer Profile: undefined Capability: Time-Tariff Capacity: 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 (from the IP address assigned to the Network Element during creation) 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.

Procedure 33: Define and Add Network Elements

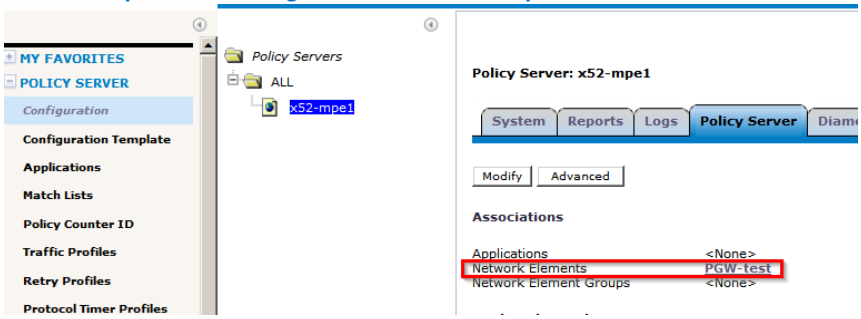
		Click on the <PGW> tab of the network element to assign the Diameter Identity that will be used to authenticate to the Policy Management System. Click "Modify"  **Note:** This tab is dependent on the Network Element "**Type**" that was configured during the previous step. In this example the Network Element "**Type**" used is a "**PGW**" (Packet Gateway) which will be used to establish a Diameter connection to the Policy Management System (to the MPE in an MPE only system or to the MRA (Policy Front End) in a Policy Management System that includes MPEs and MRAs). On the PGW tab, datafill the Diameter Realm and Identity that will be assigned to the Network Element. This should match the configuration that will be configured on the Gateway Device, in this case, the PGW. 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.

Procedure 33: Define and Add Network Elements



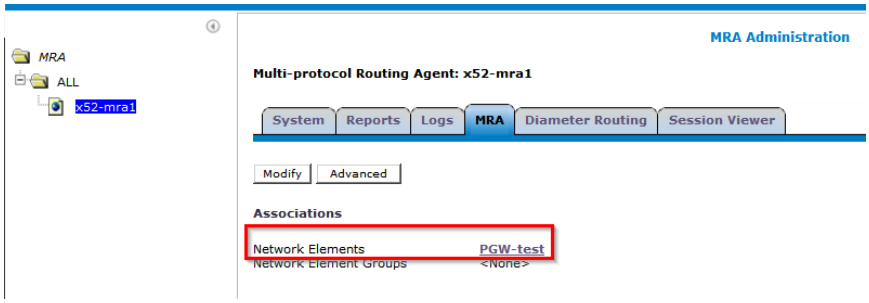
When you finish, click **Save**.

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

Note: MRAs are optional. If no MRAs are present in the Policy Management System there is no need to deploy a network element to an MRA.

You have completed this procedure.

7.3.1 Load Policies and related Policy Data

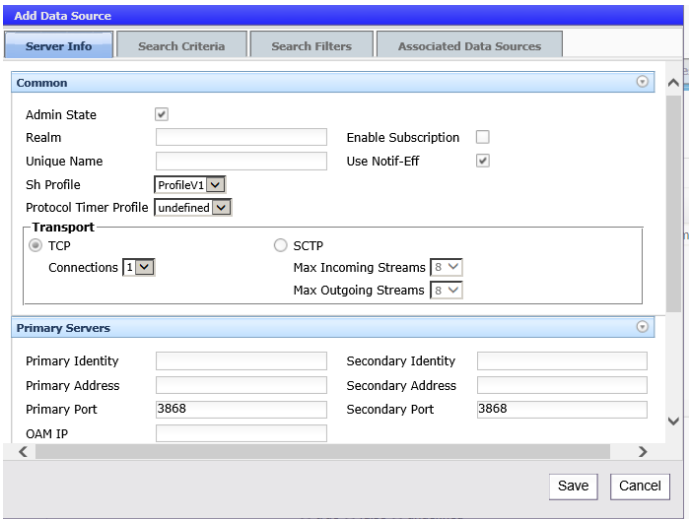
This step is optional. Policies are not required to process a test call but for the purpose of verification, a basic Policy can be installed manually, or using an import action and an xml file. The policy must be deployed to the MPE which will process the test call.

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.

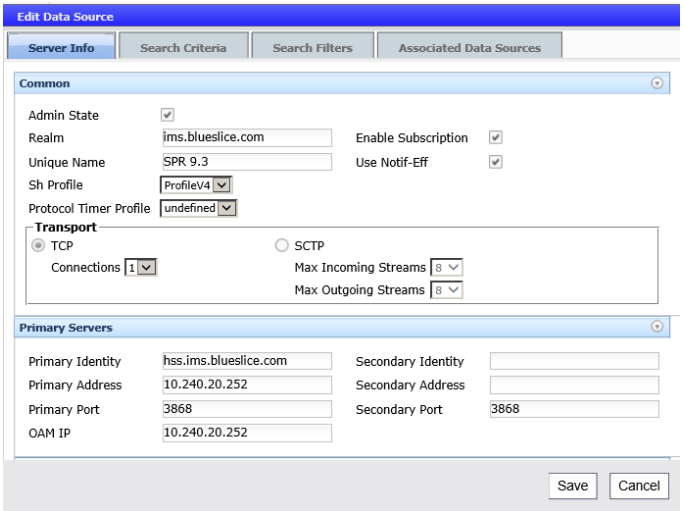
Create new session
where the request is creating a new session
send notification to trace log with `*new session created policy triggered*` and severity `*Critical*`
continue processing message

7.3.2 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.



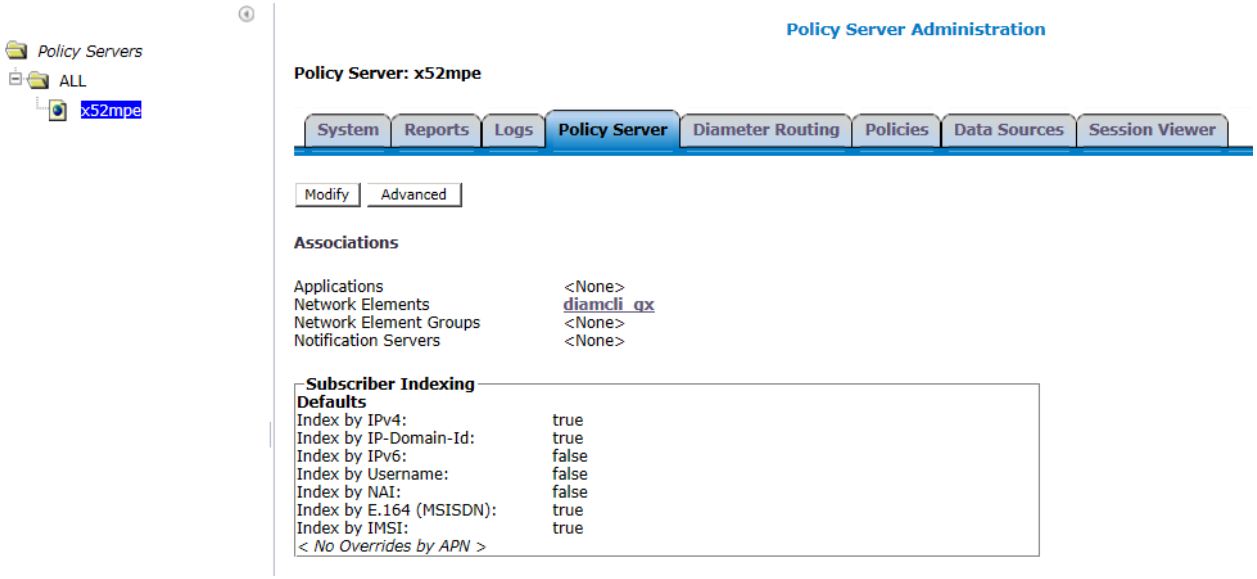
Here is a sample configuration. This form will be specific to the customer site.



7.3.3 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 was created in Procedure 33: Define and Add Network Elements. 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.



7.4 *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

[11]E62458 -SNMP User's Guide

Additional Procedures can be referenced from the following document

[10]E62447 - Platform Configuration User's Guide Release 12.1.x

Chapter 3: Performing Initial Server Configuration

- Configuring Routing on Your Server
- Configuring Firewall Settings

Chapter 4: Managing Certificates

Chapter 5: Synchronizing Files

Chapter 7: Performing System and Server Backups and Restores

7.5 TIERED CMP SYSTEM

A “Tiered CMP System” uses the feature “Multi-Level OAM” to deploy CMPs clusters as either a NW-CMP (Network CMP) or S-CMP (System-CMP). The NW-CMP manages a number of CMPs in S-CMP mode. A CMP in S-CMP mode will manage individual MPE/MRA instances.

For additional information please reference the CMP Wireless User’s Guide R12.1.x

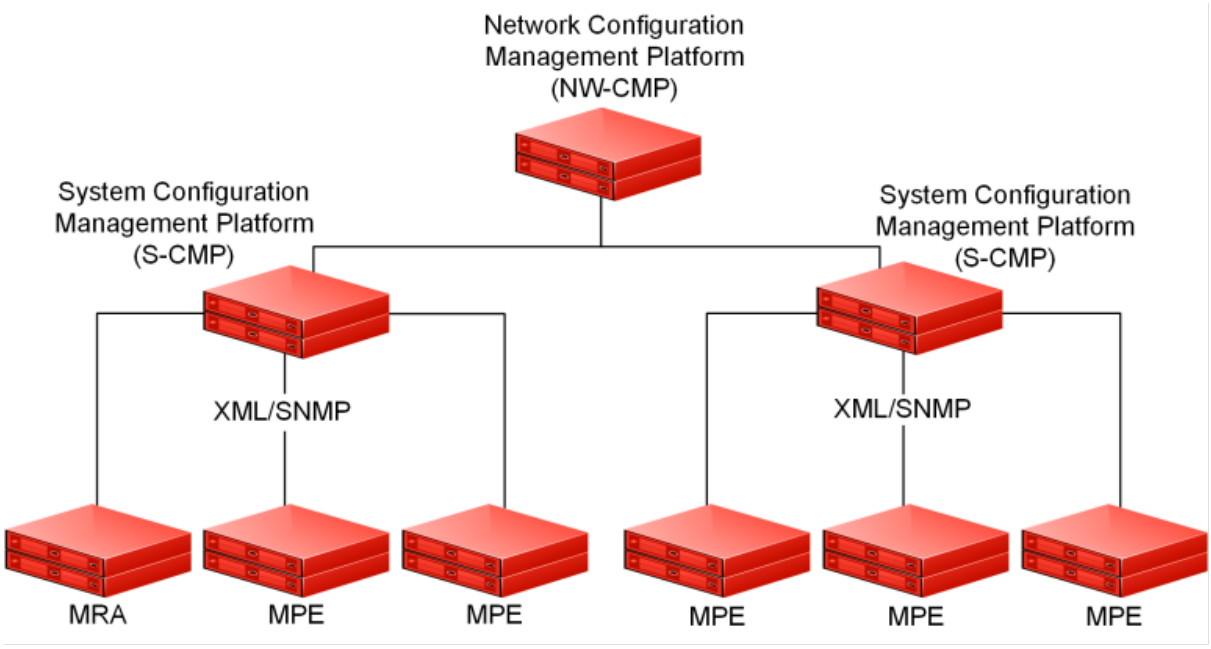
E62450 - Configuration Management Platform Wireless User's Guide Release 12.1.x

The Oracle Communications Policy Management Network Configuration Management Platform provides centralized management for systems containing multiple CMP servers. This configuration is a tiere

d configuration that uses two types of CMP servers: Network Configuration Management Platform (NW-CMP) and System Configuration Management Platform (S-CMP). The NW-CMP server manages the entire system by managing one or more S-CMP servers. The NW-CMP sends configuration updates to the S-CMP servers, and the S-CMP configures MPE and MRA devices.

The NW-CMP server configures Network tier objects. Examples of Network tier objects are policies, network elements, and configuration templates. After the Network tier objects are configured on the NW-CMP, the objects are distributed to S-CMP servers. On the S-CMP the Network tier objects can be associated with MRA or MPE servers. Network tier objects cannot be created, modified, or deleted on S-CMP servers.

The S-CMP servers configure System tier objects. System tier objects are MPE and MRA devices. These objects are used to apply configurations to individual servers. The MPE and MRA configurations can change individual server configuration parameters or associate Network tier objects with an MPE or MRA device. The figure below shows the structure of a Network Configuration Management Platform system.



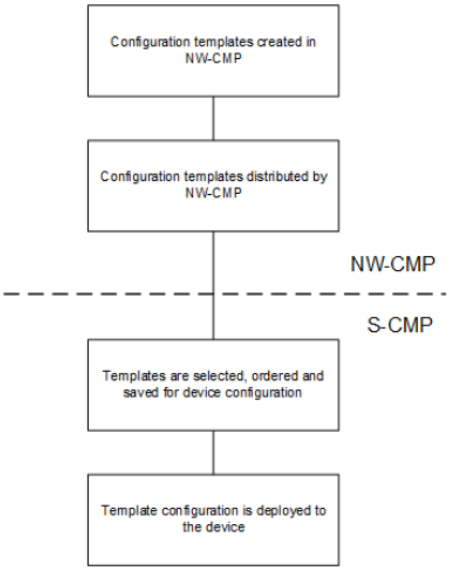
Device Configuration in a Network CMP

Configuration of MPE and MRA servers in a tiered CMP configuration can be done manually or with configuration templates. In a manual configuration, the Network tier objects are created on the NW-CMP server and then associated with individual MPE or MRA servers using S-CMP servers. While the manual configuration method takes advantage of the network-wide configuration capability, it requires significant configuration of individual servers and can have consistency problems.

Using configuration templates is a more efficient and consistent method of configuring MPE and MRA servers across the entire CMP system. Since configuration template objects are configured at the Network tier, all configuration templates are created and distributed by an NW-CMP server. Configuration templates are only viewable on S-CMP servers. When using configuration templates, the configuration of parameters and the association of configuration objects are consistent across all devices in the CMP system. After a configuration template is created on the NW-CMP server, the template is distributed to all S-CMP servers and is available for configuring individual servers.

It is recommended that a global configuration template is created for each server type. The global configuration template is then distributed from the NW-CMP server to all S-CMP servers. Then the global template is associated with the appropriate server. This results in a single global configuration template object used network-wide on all servers of the same type. Since all the servers are associated with the same global objects, applying a configuration change from the NW-CMP server becomes as simple as making a change either in a configuration template or in another global object (such as a policy) referenced by this configuration template. Any change to the configuration template is immediately propagated from the NW-CMP server through the S-CMP servers to all associated servers.

To simplify the association of a configuration template to devices, virtual configuration templates can be used. A Virtual Configuration template is a configuration template that consists of a reference to a standard configuration template. Any place the virtual configuration template is used, it is replaced by the definition of the standard configuration template. The virtual configuration template can make changes to configuration of servers as easy as changing the virtual configuration template reference from one standard configuration template to another standard configuration template.



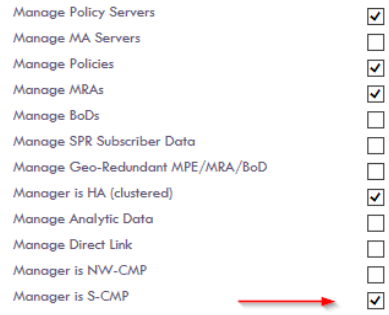
Device Configuration Flow Using Configuration Templates

Procedure 34: Building a Tiered CMP System

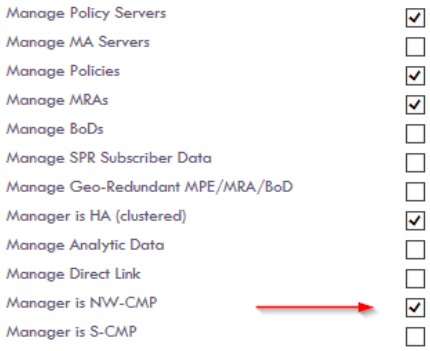
Procedure 34: Building a Tiered CMP System

STEP #		
	This procedure will review how to build a Tiered CMP System (Multi-Level OAM). Many of the procedures are the same as for a Non-Tiered CMP system. For additional detail please refer to the following (as per the reference section in this document). **E62450 - Configuration Management Platform Wireless User's Guide Release 12.1.x** **Pre-requisites:** - Network access to the NW-CMP and S-CMPs OAM IP address, to bring up a web Browser GUI (http) - Installed CMP Clusters available to be configured as NW-CMPs and S-CMPs 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. ☐	Install Servers to be used in the System Topology	**These steps are the same as for a Non-Tiered CMP System** Follow the installation methods in this document as described in the section that corresponds to the hardware environment. • INSTALLATION (AND NETWORKING) IN A C-CLASS ENVIRONMENT • INSTALLING AN HP RMS ENVIRONMENT • INSTALLING AN ORACLE X5-2 RMS ENVIRONMENT **Note:** The main difference between a "Non-Tiered CMP System" and a "Tiered CMP System" is that the number of CMP servers that need to be installed will correspond to number of S-CMPs **plus** the NW-CMPs per the network design. The CMP ISO application is the same for both NW-CMP and S-CMPs. These two types of clusters will be differentiated during the Initial Configuration of the mode options of the CMP Servers via the CMP GUI.
2. ☐	Configure Servers to be used in the Network Topology	**These steps are fundamantally the same as for a Non-Tiered CMP System unless otherwise noted in this procedure. Proceed with the procedures in the referenced section and refer back to this procedure as appropriate.** Referenced Section: • CONFIGURE POLICY APPLICATION SERVERS Procedure 25: Perform Initial Configuration of Policy Servers Platcfg **No change** Procedure 26: Perform Initial Configuration of the Policy Servers CMP GUI In this procedure, when the CMP GUI is accessed for the first time in a new installation, during mode selection, mark the checkbox that corresponds to the role that CMP will play. For the **S-CMP** select the checkbox for "M**anager is S-CMP"**

Procedure 34: Building a Tiered CMP System



For the **NW-CMP**, select the checkbox for "**Manager is NW-CMP**"



Note: For other Mode Selections refer to Procedure 26: Perform Initial Configuration of the Policy Servers CMP GUI

Note: If neither NW-CMP or S-CMP is selected, the CMP configuration will default to the legacy CMP of a Non-Tiered System.

Note: Once the mode options have been selected and saved with the option "Manager is S-CMP" selected, the mode option settings on the S-CMP will be grayed out. This is because the mode options will be controlled at the NW-CMP and pushed to the S-CMPs once the S-CMPs have been added to the NW-CMP.

Important: If the mode selection of the CMP has been accessed for the purpose of changing an existing "Non-Tiered" CMP to a "Tiered" S-CMP, and the Non-Tiered CMP has configured data to be preserved, it is advisable to create and save a system backup off server.

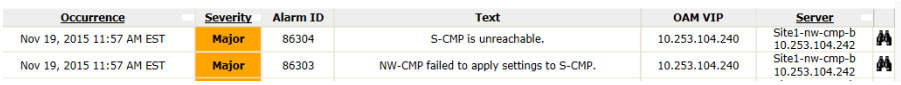
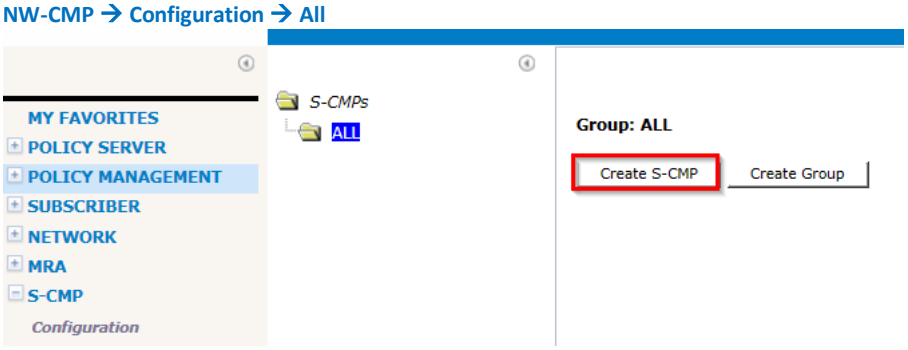
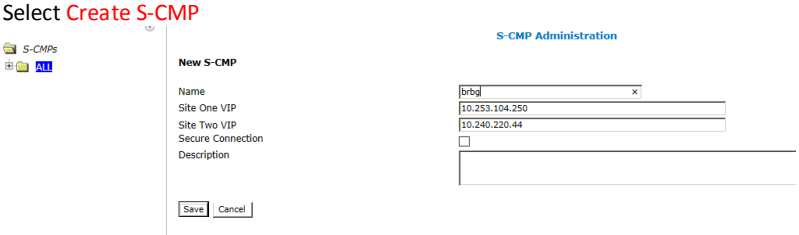
Procedure 27: CMP Site1 Cluster Topology Configuration
No Change

Procedure 28: Topology Configuration of Additional Clusters
No Change

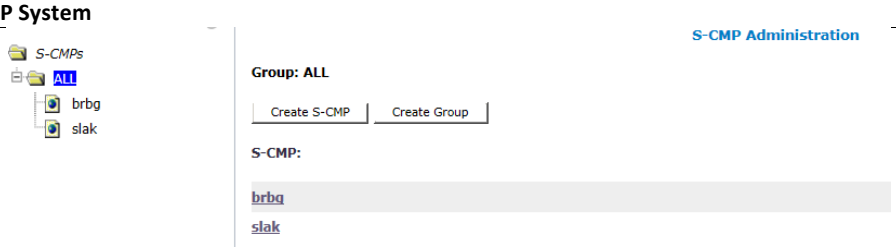
Procedure 29: SSH Key exchanges to all servers in the topology
This procedure will need to be executed from the "Active" server of the "SITE-1 NW-CMP" cluster. Additionally, this procedure should be executed from the "Active" server of each "SITE-1 S-CMP" cluster

Procedure 30: Configure the IP routing on the MPE and MRA
No Change

Procedure 34: Building a Tiered CMP System

		Procedure 31: Adding MPE and MRA to CMP Menu **No Change** **Note:** In Procedure 32, "Diameter Realm" and "Diameter Identity" are manually configured for both the MRA and the MPE. It is possible to define the "Diameter Realm" from the NW-CMP in a Multi-Tier configuration but the "Diameter Identity" must be configured on the S-CMP as this field will be unique to each S-CMP. Procedure 32: Configure MPE Pool on MRA (Policy Front End) **No Change** **Note:** MRAs in a Policy System are optional. If the system will not be using MRAs this step can be skipped. After completing Procedure 33, further configuration of the newly added MPEs and MRAs will be performed from the NW-CMP using configuration templates.
3. ☐	Login to the NW-CMP Gui and Add S-CMPs	**Starting with Procedure 33 the methodology used to complete the system installation is different for a "Tiered CMP System" than a "Non-Tiered CMP System". Proceed as follows:** **Note:** The NW-CMP will expect that the S-CMPs are reachable and that a connection can be established from the NW-CMP to the S-CMP to complete this step. If the S-CMPs are not reachable, or if the CMP being connected to is not configured as a "S-CMP" there will be associated alarms.  Login to the NW-CMP GUI using the VIP address. **NW-CMP → Configuration → All**  Select Create S-CMP  In the "New-S-CMP" form datafill a <Name> and the <Site1 VIP>. If the S-CMP has a geo-redundant Site 2 CMP add the Site 2 VIP as well. Select Save.

Procedure 34: Building a Tiered CMP System



The S-CMP is now added to the NW-CMP.

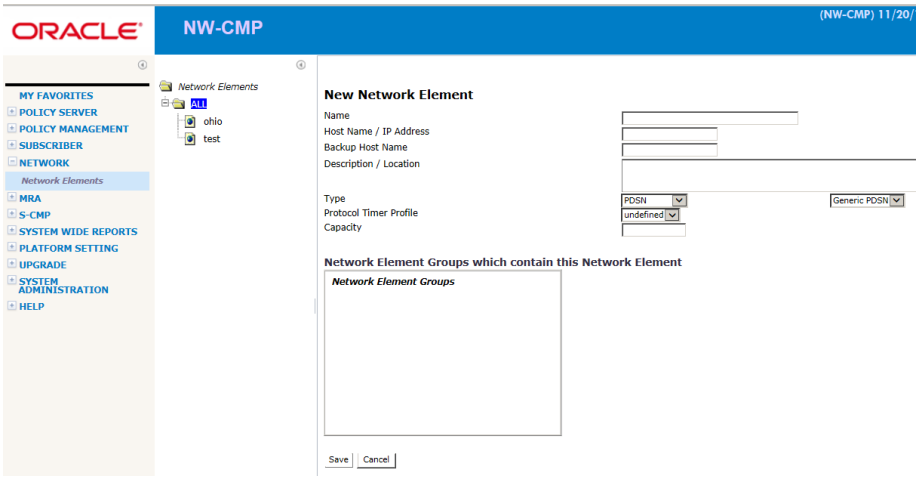
Repeat this for each S-CMP that will be associated with the NW-CMP

4. ☐ NW-CMP: Create Network Element

Note: In this step the creation of a Network Element is used as an example. There are several different configurations that can be completed on the NW-CMP and pushed to S-CMP in the same fashion as the Network Elements. For a more comprehensive review of which parameters can be configured on the NW-CMP and pushed to the S-CMPs and which parameters can only be configured on the S-CMP, refer to the section "**Network CMP Tier Capabilities"** in the Configuration Management Platform Wireless User's Guide Release 12.1.x

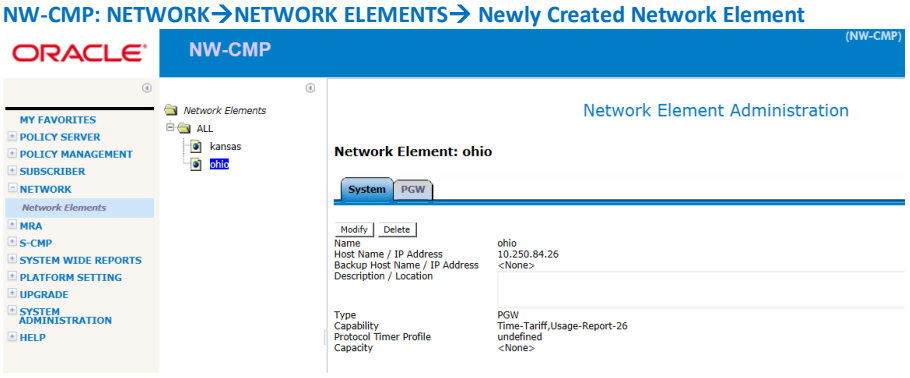
To create the Network Element on the NW-CMP follow steps 1 & 2 as in Procedure 34: Define and Add Network Elements. The NW-CMP will automatically push the created Network Element to all the S-CMPs it manages.

NW-CMP: NETWORK→NETWORK ELEMENTS→ All



Datafill the network Element form and "Save" the configuration

NW-CMP: NETWORK→NETWORK ELEMENTS→ Newly Created Network Element

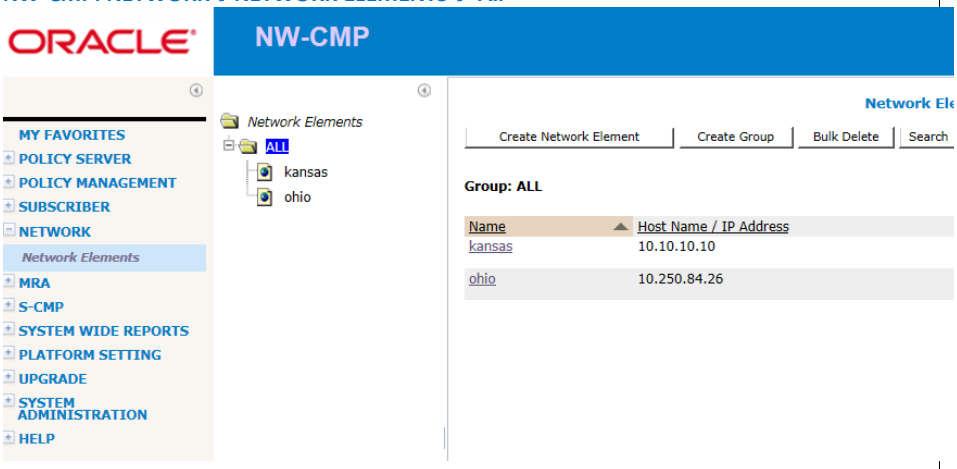


Network Element named "**ohio**" created on the NW-CMP.

Procedure 34: Building a Tiered CMP System

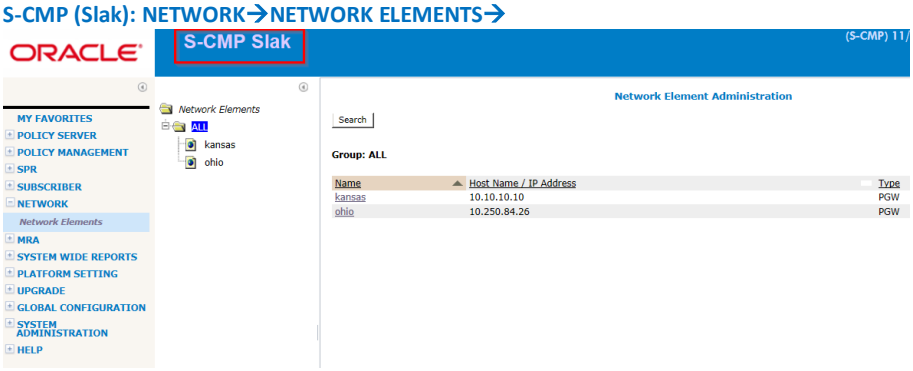
Repeat this step for any required additional Network Elements

NW-CMP: NETWORK→NETWORK ELEMENTS→ All



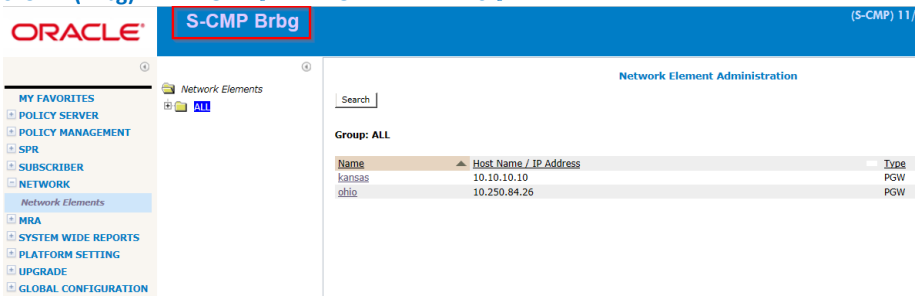
Now confirm that the newly configured Network Element(s) have been automatically pushed to the S-CMPs

S-CMP (Slak): NETWORK→NETWORK ELEMENTS→



Network Element named "**ohio**" created on the S-CMP (Slak).

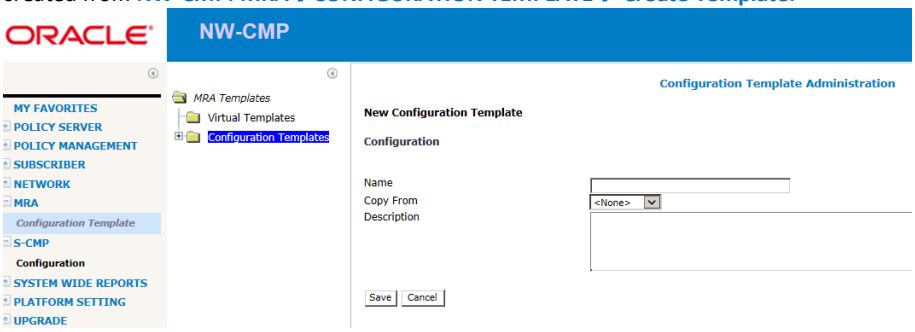
S-CMP (Brbg): NETWORK→NETWORK ELEMENTS→



Network Element named "**ohio**" created on the S-CMP (Brbg)

Procedure 34: Building a Tiered CMP System

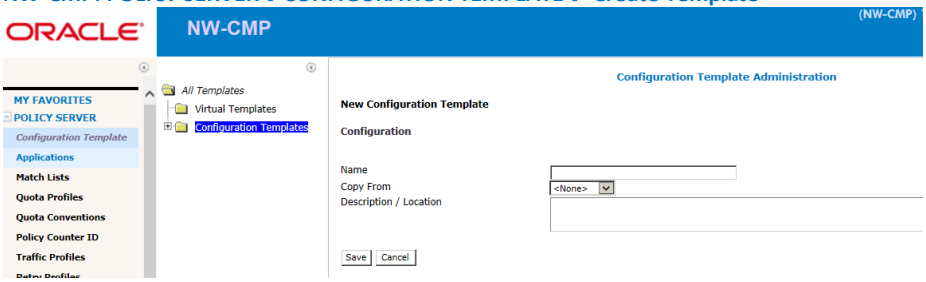
5. ☐	NW-CMP: Create MPE or MRA Template to deploy Network Element	**Note:** In this example a Configuration Template **for the MPE** is created. If the Policy System will include **MRAs** (Policy Front End) the procedure to create, push and apply Configuration Templates for the **MRA** is similar except that for the MRAs, the Configuration Templates are created from **NW-CMP: MRA→CONFIGURATION TEMPLATE→ Create Template.**



Create a Confguration Template for the MPE

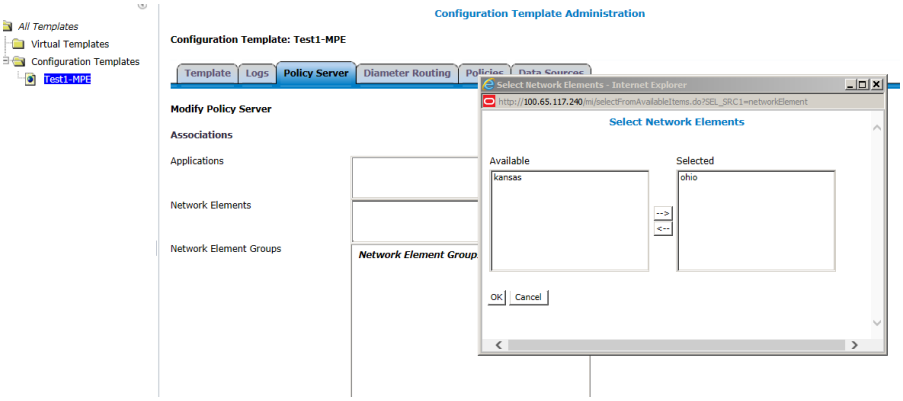
The NW-CMP can be used to create a template that will be automatically pushed to the S-CMPs in the same fashion that the Network Elements were created on the NW-CMP and automatically pushed to the S-CMPs.

NW-CMP: POLICY SERVER→CONFIGURATION TEMPLATE→ Create Template



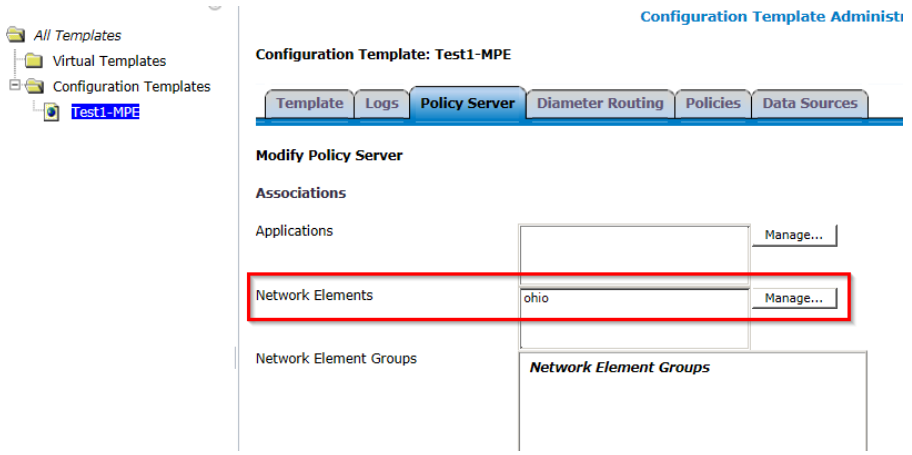
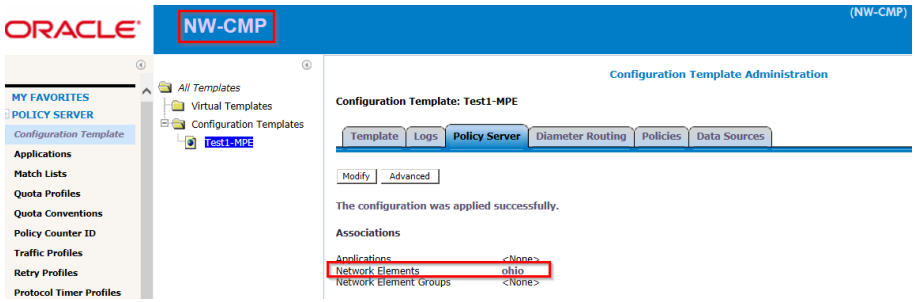
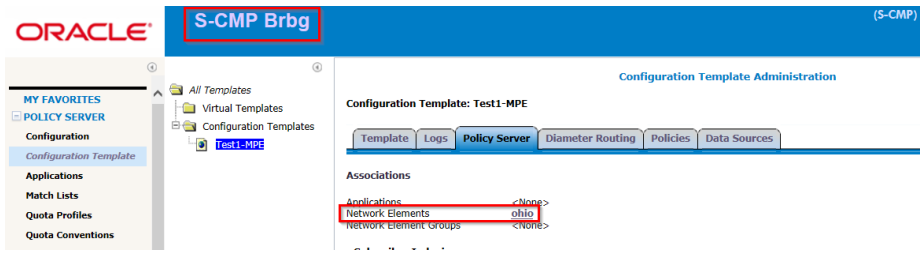
Datafill the "Create Template" form with a name and "Save". Only <name> is a required field at this point.

Open the newly created template and navigate to the Policy Server tab
NW-CMP: POLICY SERVER→CONFIGURATION TEMPLATE→ Created Template→Policy Server tab



Select: Modify and then click on <Manage> "**Network Elements**" . This opens a dialog to associate any required Network Elements for the target MPE

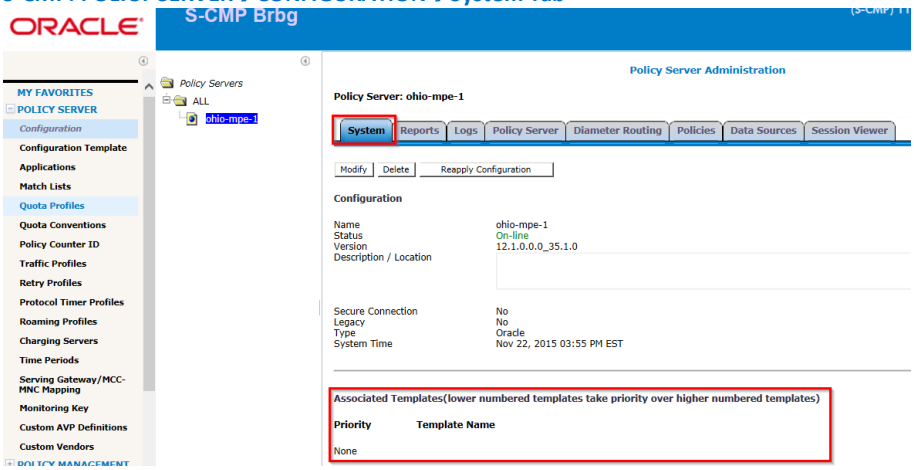
Procedure 34: Building a Tiered CMP System

		Select the required Network Element that will be associated to the target MPE click on "OK"  Now "Save" the new Configuration Template  The Configuration Template has now been completed. The configuration template will be automatically pushed to the S-CMP where the Configuration Template can be applied to the target MPE.
6. ☐	S-CMP: Apply Configuration Template to target MPE	On the S-CMP check the Configuration Template that has been pushed from the NW-CMP to the S-CMP to confirm the newly created Network Element on the Policy Server tab . **S-CMP: POLICY SERVER→CONFIGURATION TEMPLATE** 

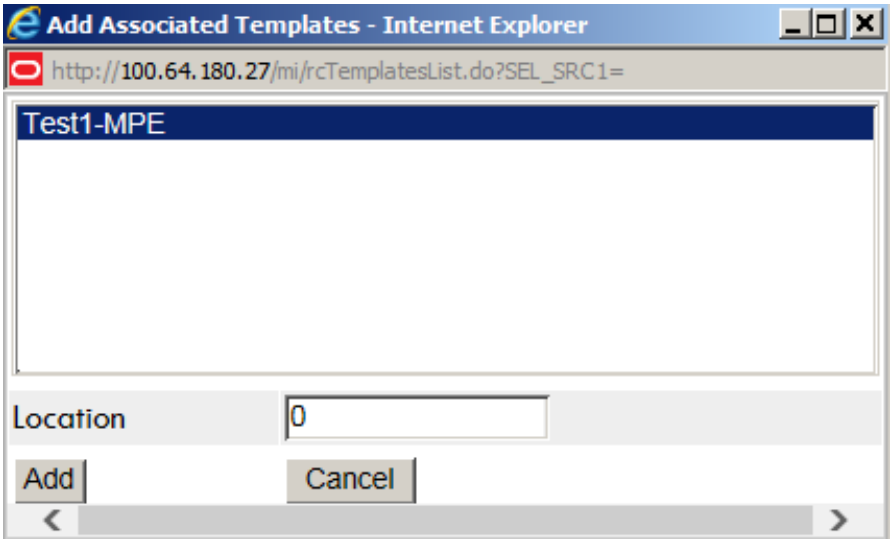
Procedure 34: Building a Tiered CMP System

Now apply the configuration template to the target MPE on the S-CMP using the system tab of the target MPE.

S-CMP: POLICY SERVER→CONFIGURATION→System Tab



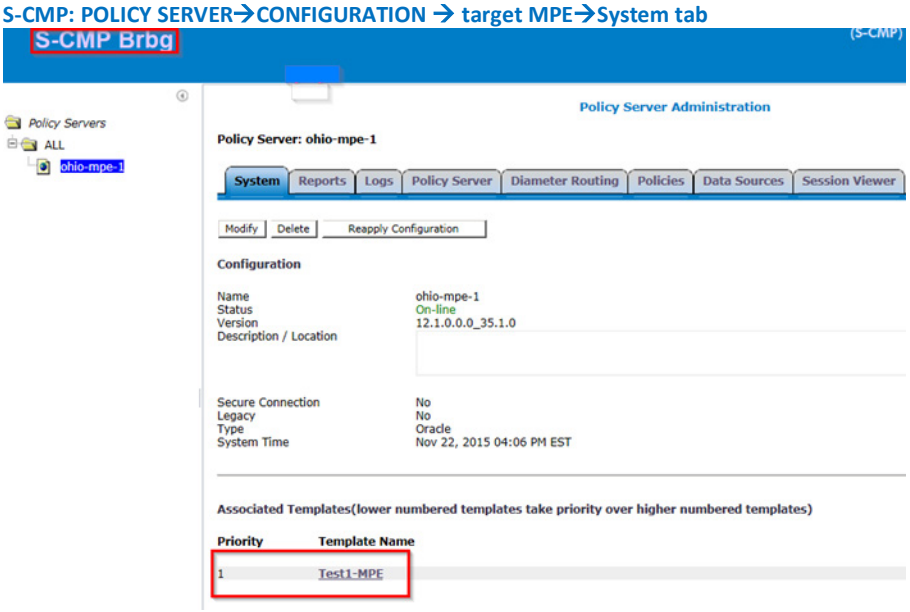
Select: "Modify" on the system tab and then click "Add" for "Associated Templates".



Procedure 34: Building a Tiered CMP System

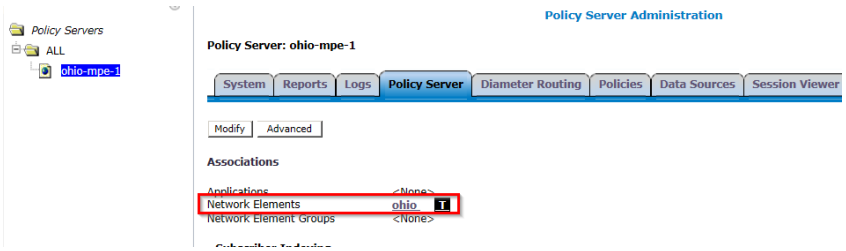
Confirm the Configuration Template to be applied to the target MPE and select "Save." This will associate any configurations included in the Configuratopn Template to the corresponding MPE.

S-CMP: POLICY SERVER→CONFIGURATION → target MPE→System tab



Now confirm the Network Element from the Configuration Template shows as "deployed" on the Policy Server tab of the target MPE.

S-CMP: POLICY SERVER→CONFIGURATION → target MPE→Policy Server tab



Note: When an object is associated wioth a target MPE using a configuration Template the symbol "T" is dislayed next to the object to indicate the source of the object is from a Configuration Template

In this fashion the NW-CMP can be used to manage configurations across a large number of S-CMPs.

You have completed this procedure.

8. SUPPORTING PROCEDURES AND INFORMATION

The following procedures and information may be referenced during installation, or may provide useful alternative methods for performing certain steps.

8.1 ILO (ILOM) PROCEDURES

This section contains procedures for iLO Access and Configuration. The examples provided below are for HP servers and in some case for Oracle X-5-2 servers. Generally procedures are similar for HP Servers and Oracle X5-2 servers. In some case examples are provided for both systems. Below is a reference to documentation that provides additional detail for both HP Servers and Oracle X5-2 servers.

Further detail is also provided in the following document as found in the reference section of this document

[6] E53017 - TPD Initial Product Manufacture

Procedure 5: Change iLO IP address from Console HP DL380

Below is a procedure to set the iLO IP address to a desired value using console access

If the server has been purchased from Oracle , then the iLO IP address may already be set to the production standard value (192.168.100.5). This procedure can also be used to confirm if a network address has already been assigned. The user can access the iLO GUI, and change the iLO address to a customer/site specific value using the iLO IP address configuration form.

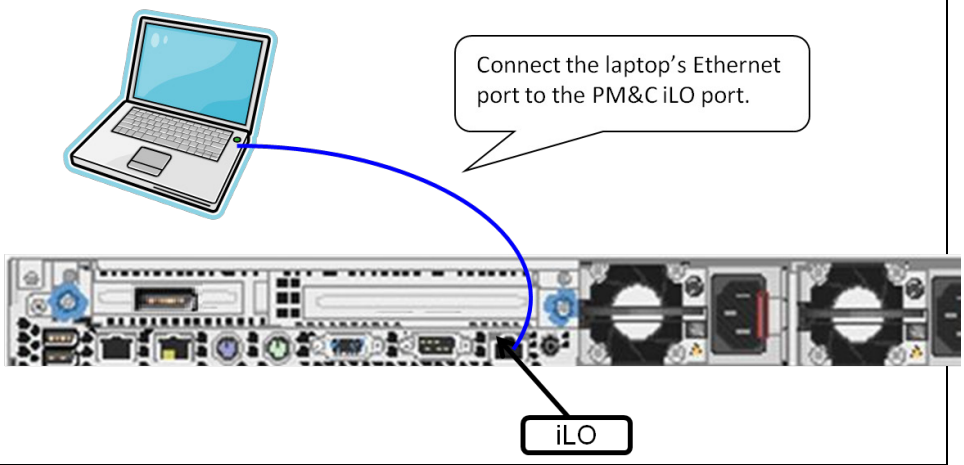
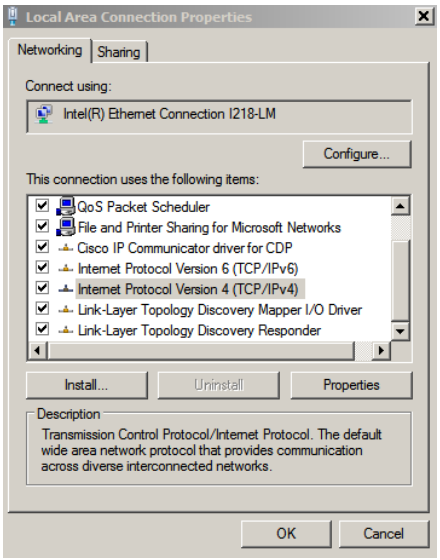
Procedure 35: Set/change iLO IP address via Console

STE P #	This procedure will Set/change iLO IP address via Console, on a DL380 server **Needed material:** IF THIS PROCEDURE FAILS, CONTACT ORACLE TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1. ☐	**Connect to the Server**	Connect to the Server: - using a VGA Display and USB Keyboard, or - using the Server iLO port and iLO Web Interface (to access Remote Console) (Note: default IP address on the iLO port is _192.168.100.5_)
2. ☐	**Boot the Server**	▪ Restart or power up the server. ▪ Press the **F8** key when prompted during POST. The iLO RBSU runs. A dialog is provided
3. ☐	**Set the IP address and other iLO Parameters**	▪ Select **Network ->DNS/DHCP**, press the **Enter** key, and then select **DHCP Enable**. Press the spacebar to turn off DHCP. Be sure that DHCP Enable is set to **Off**, and save the changes. ▪ Select **Network ->NIC ->TCP/IP**, press the **Enter** key, and enter the appropriate information in the **IP Address**, **Subnet Mask**, and **Gateway IP Address** fields. ▪ Save the changes. ▪ Exit iLO RBSU. The changes take effect when you exit iLO 3 RBSU.
4. ☐	**Verify IP address by Login to iLO port**	Follow procedure to login to the iLO Port using configured IP address.

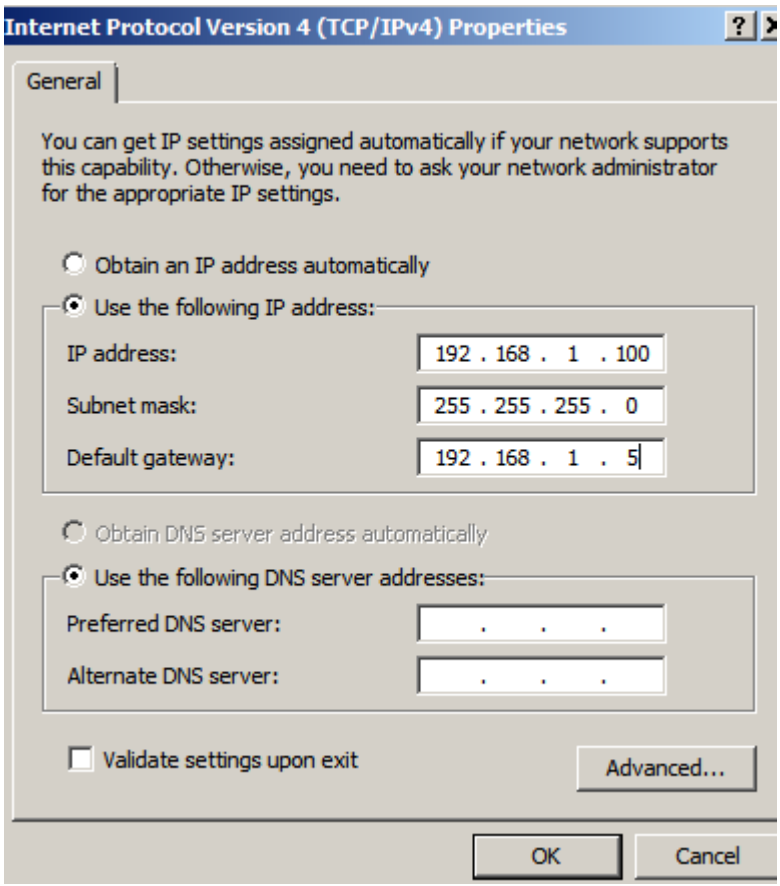
Procedure 6: Connect Laptop to iLO Port

This procedure contains the steps to connect a laptop to the iLO via a directly cabled Ethernet connection.

Procedure 36: Connect Laptop to iLO port

Step	Procedure	Result
1. ☐	Connect the laptop's Ethernet port directly to the PM&C iLO port using a standard Cat-5 cross-over cable.	
2.	Access the laptop network interface card's TCP/IP "Properties" screen.	Windows 7 • Go to Control Panel • Click on *Network and Sharing Center* • Click on *Change Adapter Settings* • Right click Local Area Connection and select "Properties" • Select "Internet Protocol (TCP/IP)" and select "Properties" 

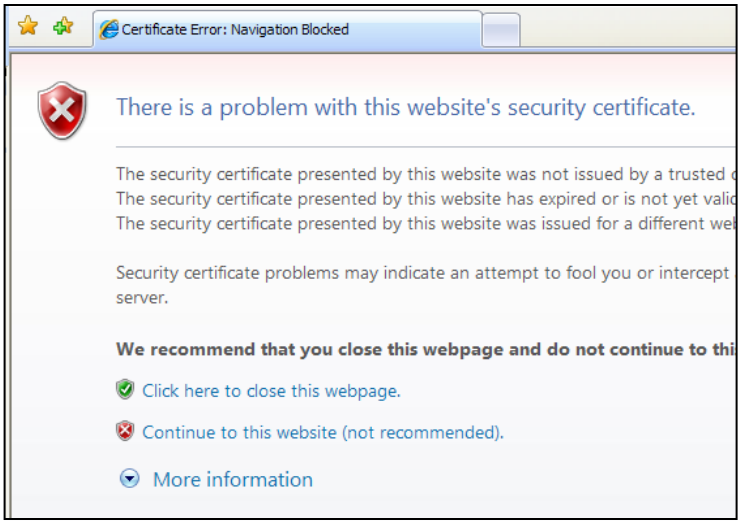
Procedure 36: Connect Laptop to iLO port

3.	Set the **IP address** to: 192.168.100.100 the **Subnet mask** to: 255.255.255.0 and the **Default gateway** to: 192.168.100.5 click **"OK"**. 2) Click **"Close"** from the network interface card's main "Properties" screen	The expectation for this IP addressing scheme is that the iLO Management Interface IP address has been set previously to the 192.168.100.5/24. The IP addressing scheme to use on the laptop that will be making the iLO connection should correspond according to the IP address assigned to iLO Management interface. 
THIS PROCEDURE HAS BEEN COMPLETED		

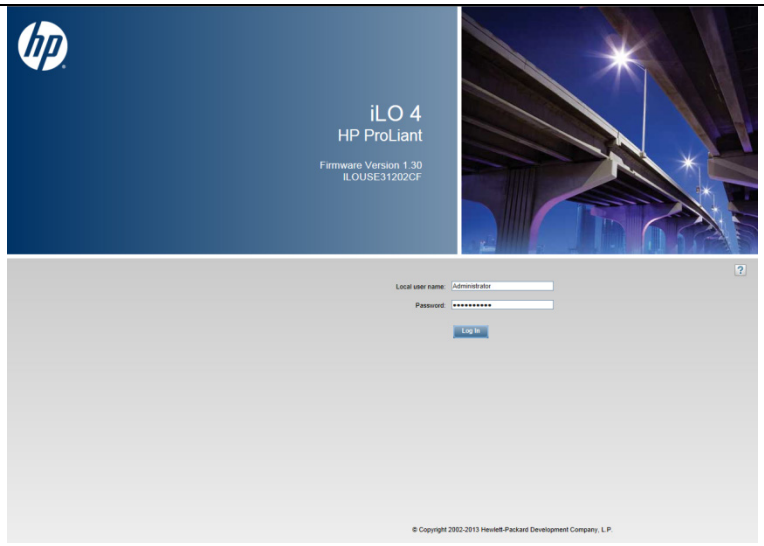
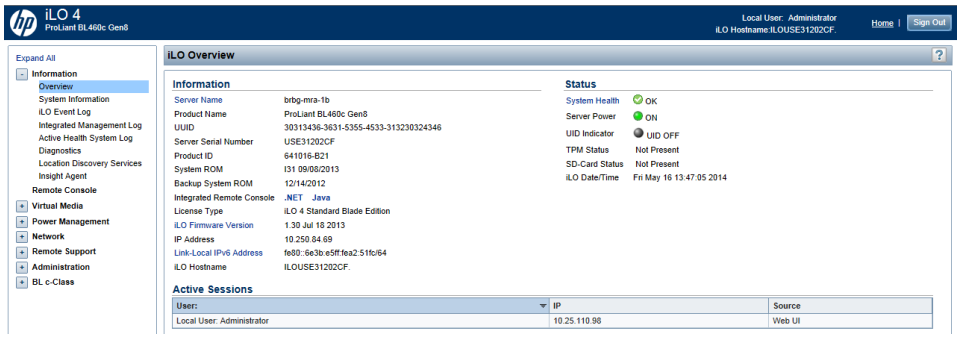
Procedure 7: Access the HP iLO GUI

This procedure contains the steps to access the HP iLO GUI.

Procedure 37: Access the HP iLO GUI

Step	Procedure	Result
1. ☐	Launch Internet Explorer and "Go To" 192.168.100.5 (manufacturing default) or customer IP set during installation.	
2. ☐	Internet Explorer may display a warning message regarding the Security Certificate.	
3. ☐	Select the option to "Continue to the website (not recommended)"	

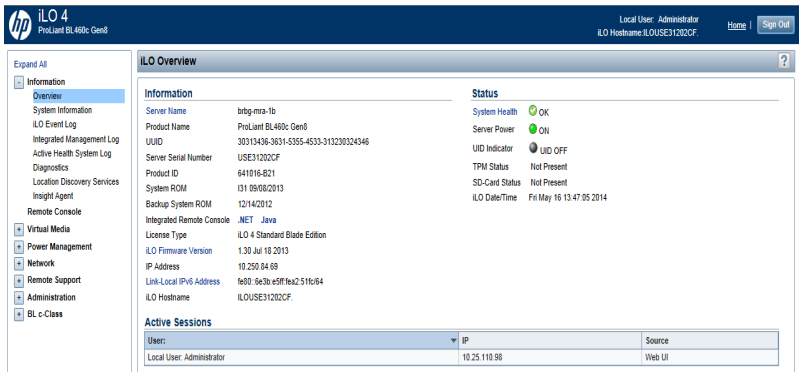
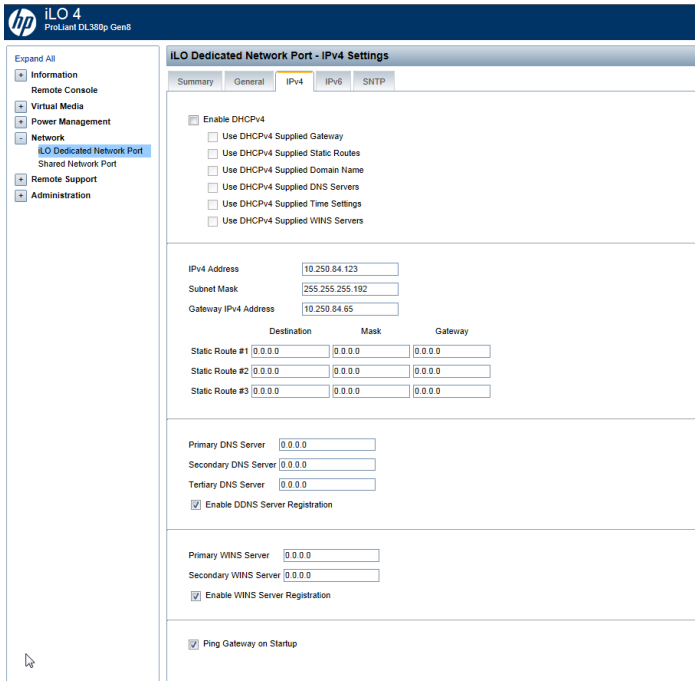
Procedure 37: Access the HP iLO GUI

4. ☐	Log in as user "**Administrator**"	
5. ☐	The HP iLO Home page is displayed.	
THIS PROCEDURE HAS BEEN COMPLETED		

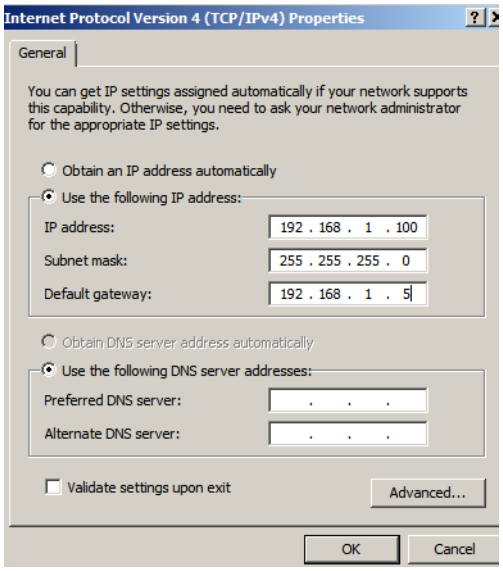
Procedure 8: Changing the HP iLO address from the iLO GUI

This procedure will set the IP address of the iLO to the customer's network so that it can be accessed by Oracle support.

Procedure 38: Changing the HP iLO address from the iLO GUI

Step	Procedure	Result
1. ☐	Launch the HP iLO GUI	The home page will be displayed 
2. ☐	iLO GUI configuration	Navigate to Network→iLO Dedicated network port→IPv4 TAB Change the **IP Address**, **Subnet Mask** and **Gateway IP Address** to the values supplied in the IP Site Survey. Hit **Submit**. NOTE: You will lose access after you hit the Submit button. 

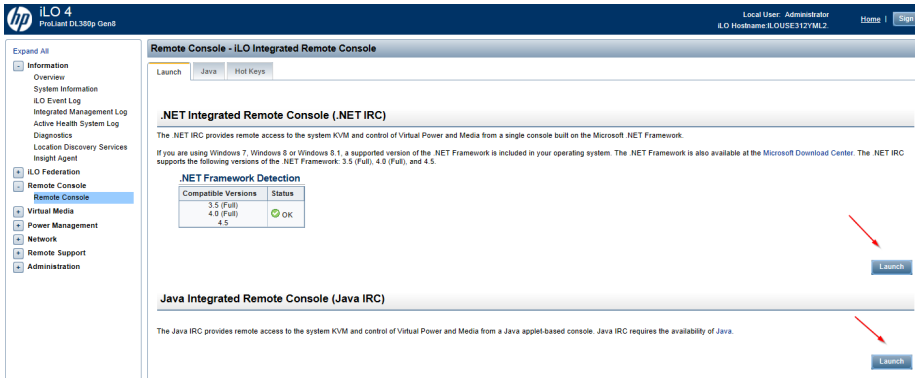
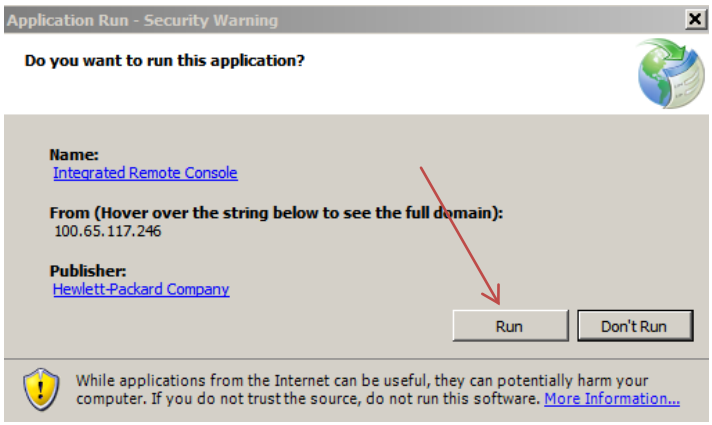
Procedure 38: Changing the HP iLO address from the iLO GUI

3. ☐	Reset IP configuration on laptop	If using a laptop, **re**set the PC's network configuration, updating the IP configuration in network 
4. ☐	Reconnect to iLO with newly configured IP address	 **Note:** Use the newly configured IP address
THIS PROCEDURE HAS BEEN COMPLETED		

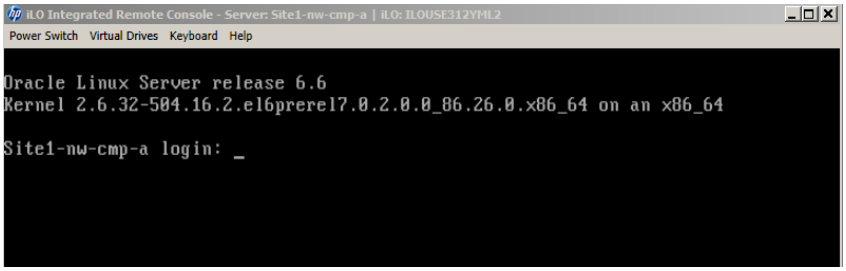
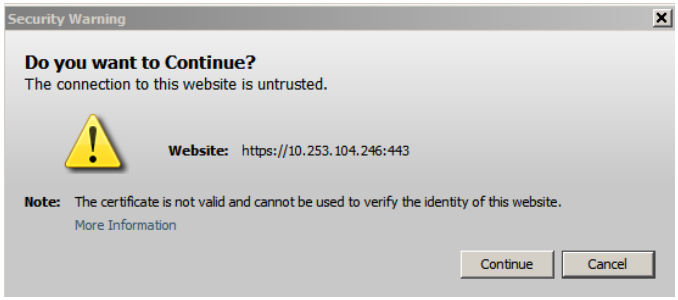
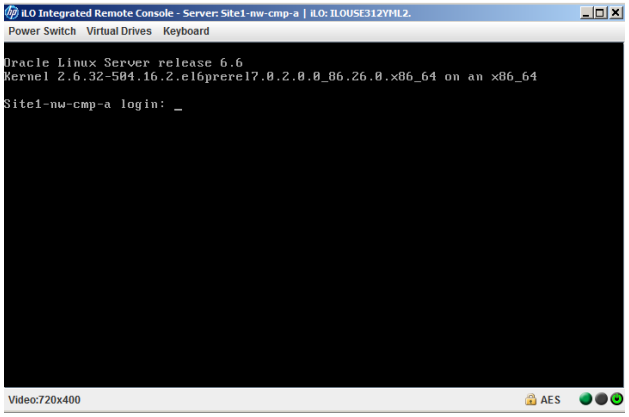
Procedure 9: Launching the Remote Console from the HP iLO GUI

This procedure will Launch the Remote Console after having connected to the HP iLO interface as per the procedures in this section.

Procedure 39: Launching the Remote Console from the HP iLO GUI

Step	Procedure	Result
1. ☐	HP iLO Gui	Navigate to Remote Console -> Remote Console  **Note**: There are two modes that can be selected
2. ☐	HP iLO Gui	Select the ***.net Integrated Remote Console*** **Note for Firefox users:** Firefox requires an Add-on to launch .NET applications. Visit the Firefox Add-on website to download the latest version of the Microsoft .NET Framework Assistant. **Note for Chrome users:** Chrome requires an extension to launch .NET applications. As a workaround select one of the following instead: • Integrated .NET IRC application with another browser • Standalone .NET IRC application available from hp.com • Integrated Java-based Remote Console (Java IRC) • iLO Mobile Application to access the iLO Remote console Confirm "run" when prompted 

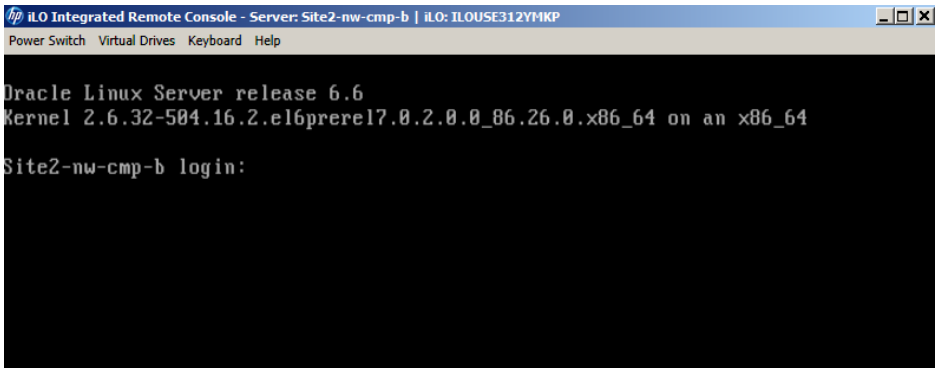
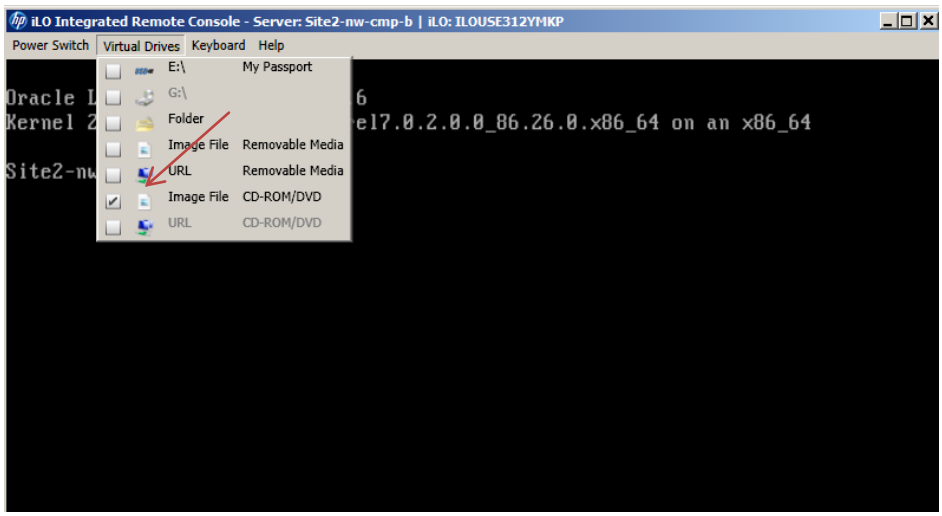
Procedure 39: Launching the Remote Console from the HP iLO GUI

3. ☐	Remote Console Login (.net)	The remote console will present the login screen to the CLI of the installed OS. Login with *admusr* to access the CLI prompt. **Note:** For keystrokes to register on the Remote Console window, the window may need to be selected/highlighted with the mouse pointer while typing. 
4. ☐	HP iLO Gui	Alternately, a second option to launch the remote Remote Console is to select the ***Java Integrated Remote Console*** from the remote console window as seen in step #1. **Note:** The Java IRC provides remote access to the system KVM and control of Virtual Power and Media from a Java applet-based console. Java IRC requires the availability of Java. **Note:**The java console will take some before this prompt to appear and also for the remote console to launchs Confirm "continue " when prompted 
5. ☐	Remote Console Login (java)	The remote console will present the login screen to the CLI of the installed OS. Login with *admusr* to access the CLI prompt. **Note:** An advantage of this console is that the console size can be adjusted. 
THIS PROCEDURE HAS BEEN COMPLETED		

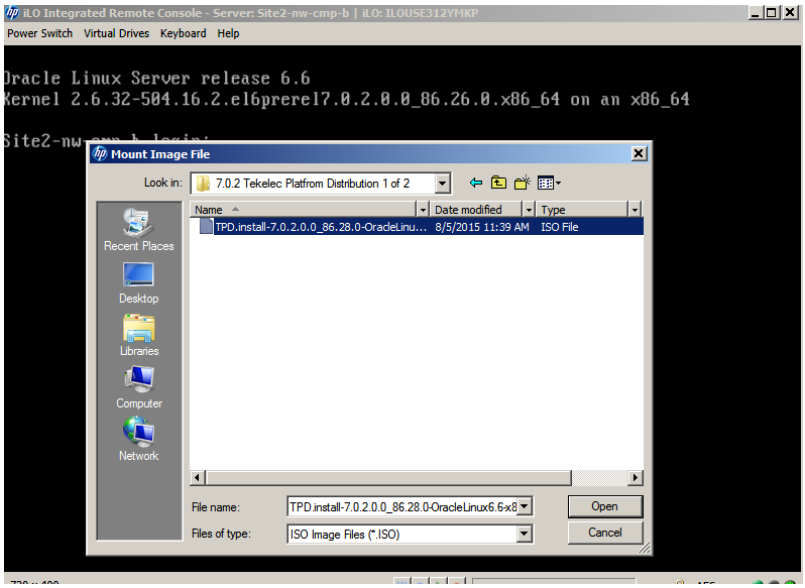
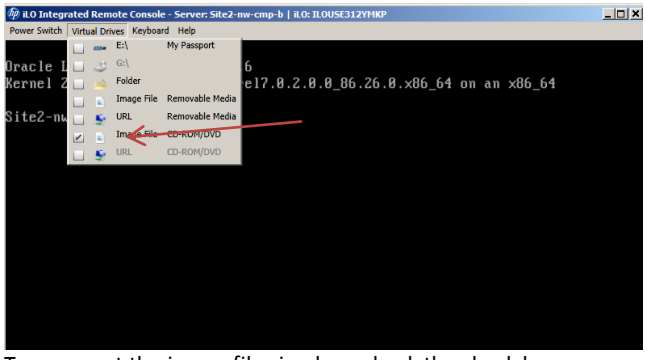
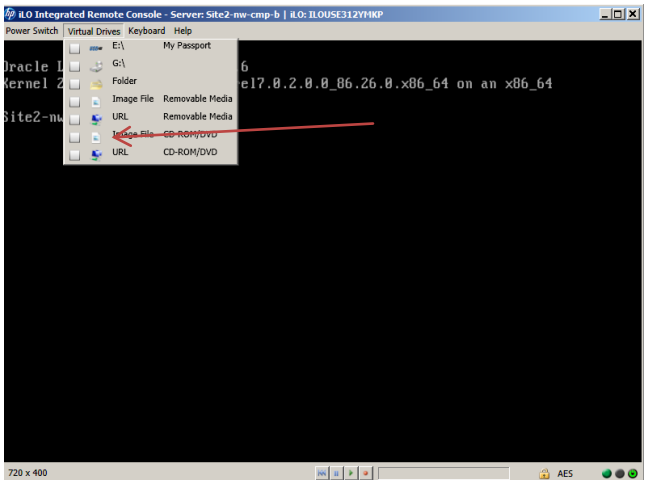
Procedure 10: Virtual Mount an ISO image file from the HP iLO GUI

This procedure contains the steps to mount an ISO image file from the remote console of the iLO interface.

Procedure 40: Virtual Mount an ISO image file from the HP iLO GUI

Step	Procedure	Result
1. ☐	Launch the remote console	Launch the remote console. In this example the .net console is used. 
2. ☐	Remote Console	Select “Virtual Drives”. From the drop down tab, check the box “Image File CD-ROM/DVD. 

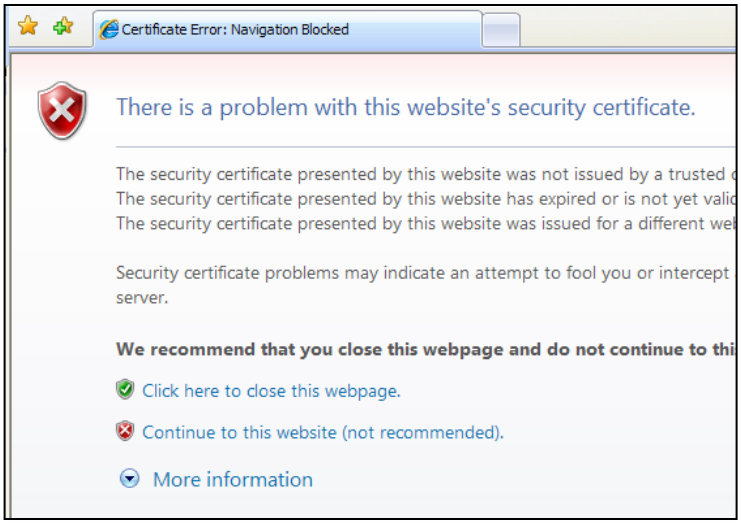
Procedure 40: Virtual Mount an ISO image file from the HP iLO GUI

3. ☐	Remote Console	You will be prompted to browse to the file you want to "virtual mount". In this case a TPD Platform ISO image file has been selected 
4. ☐	Remote Console	Open the selected ISO image file. You can confirm the image file is mounted if the checkbox is still checked.  To unmount the image file simply uncheck the check box. 
THIS PROCEDURE HAS BEEN COMPLETED		

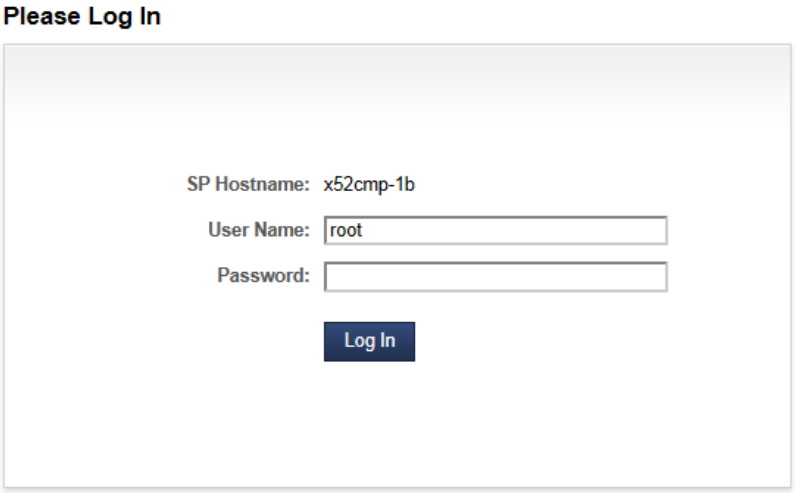
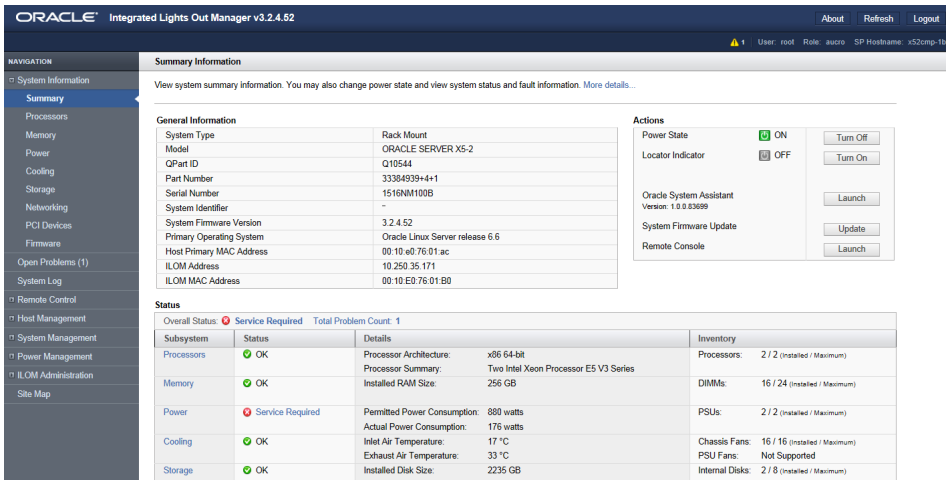
Procedure 11: Access the Oracle X5-2 iLO GUI

This procedure contains the steps to access the HP iLO GUI.

Procedure 41: Access the Oracle X5-2 iLO GUI

Step	Procedure	Result
1. ☐	Launch Internet Explorer and "Go To" 192.168.100.5 (manufacturing default) or customer IP set during installation.	
2. ☐	Internet Explorer may display a warning message regarding the Security Certificate.	
3. ☐	Select the option to "Continue to the website (not recommended)"	

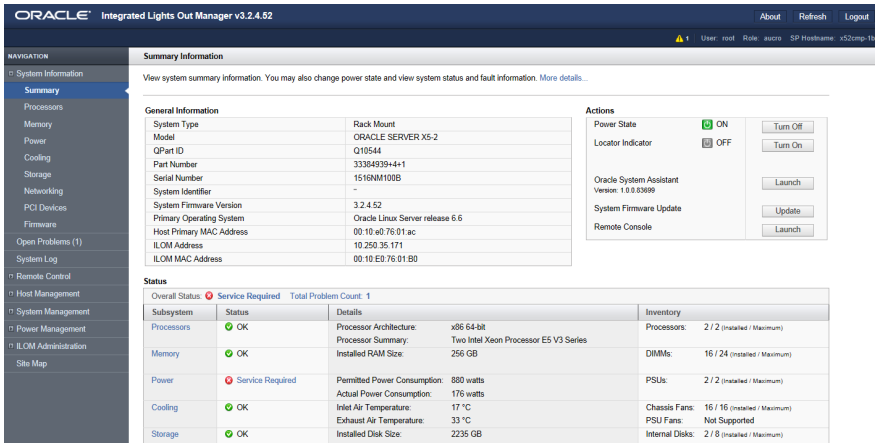
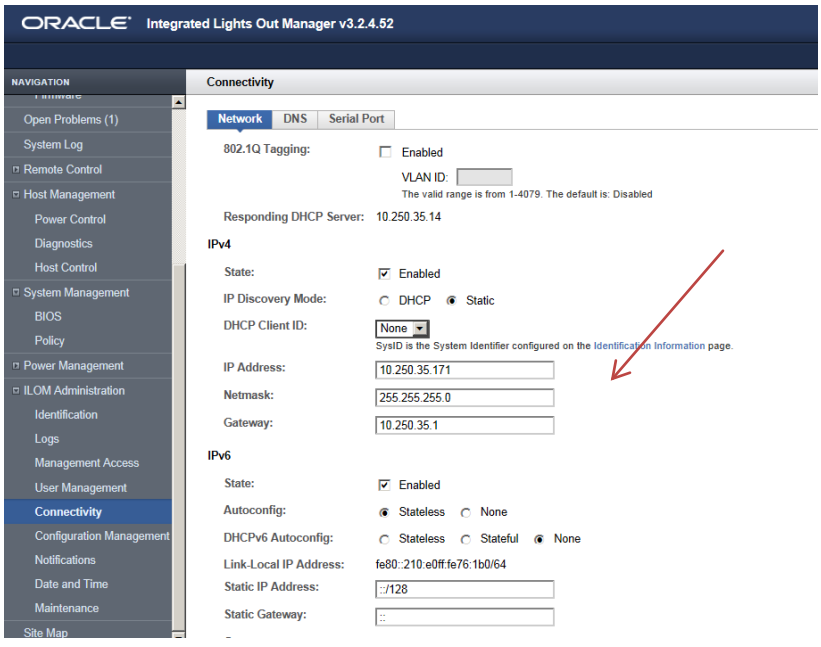
Procedure 41: Access the Oracle X5-2 iLO GUI

4. ☐	Log in as user "**Root**".	Fresh Install default password is *changeme* 
5. ☐	The X5-2 iLOM Home page is displayed.	
THIS PROCEDURE HAS BEEN COMPLETED		

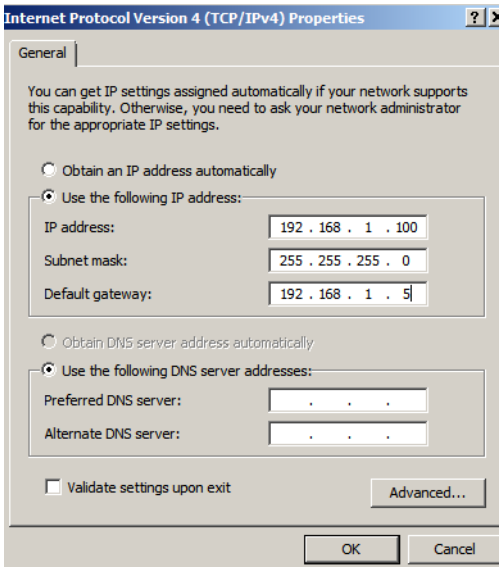
Procedure 12: Changing the Oracle X5-2 iLO address from the iLO GUI

This procedure will set the IP address of the iLO to the customer's network so that it can be accessed by Oracle support.

Procedure 42: Changing the Oracle X5-2 iLO address from the iLO GUI

Step	Procedure	Result
1. ☐	Launch the X5-2 iLOM GUI	The home page will be displayed 
2. ☐	iLOM GUI configuration	Navigate to Network→ iLOM Administration ->Connectivity Change the **IP Address**, **Subnet Mask** and **Gateway IP Address** to the values supplied in the IP Site Survey. Hit **Save**. NOTE: You will lose access after you hit the "Save" button. 

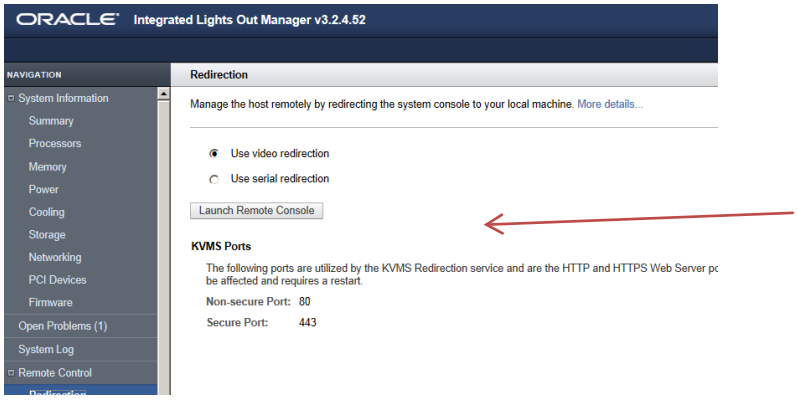
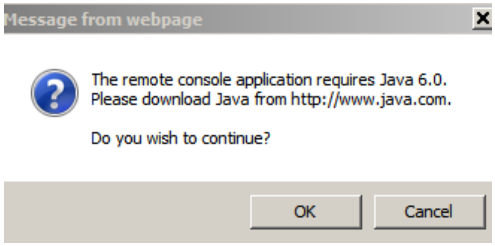
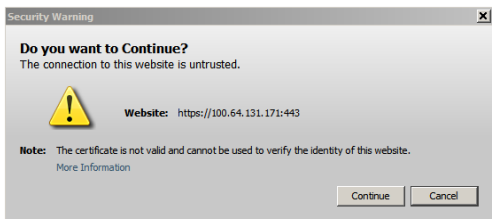
Procedure 42: Changing the Oracle X5-2 iLO address from the iLO GUI

3. ☐	Reset IP configuration on laptop	If using a laptop, **re**set the PC's network configuration, updating the IP configuration in network 
4. ☐	Reconnect to iLOM with newly configured IP address	 **Note:** Use the newly configured IP address
THIS PROCEDURE HAS BEEN COMPLETED		

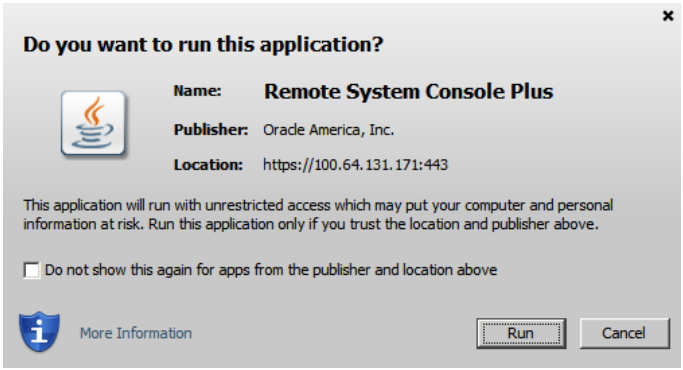
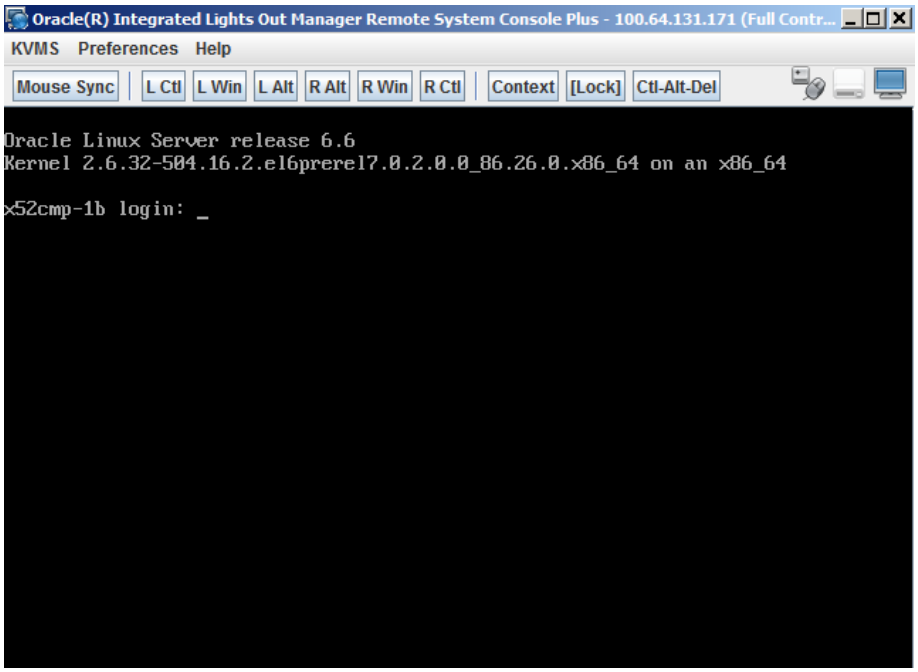
Procedure 13: Launching the Remote Console from the Oracle X5-2 iLO GUI

This procedure will Launch the Remote Console after having connected to the HP iLO interface as per the procedures in this section.

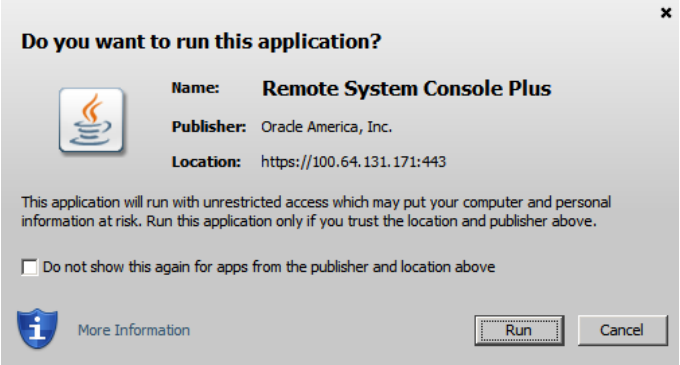
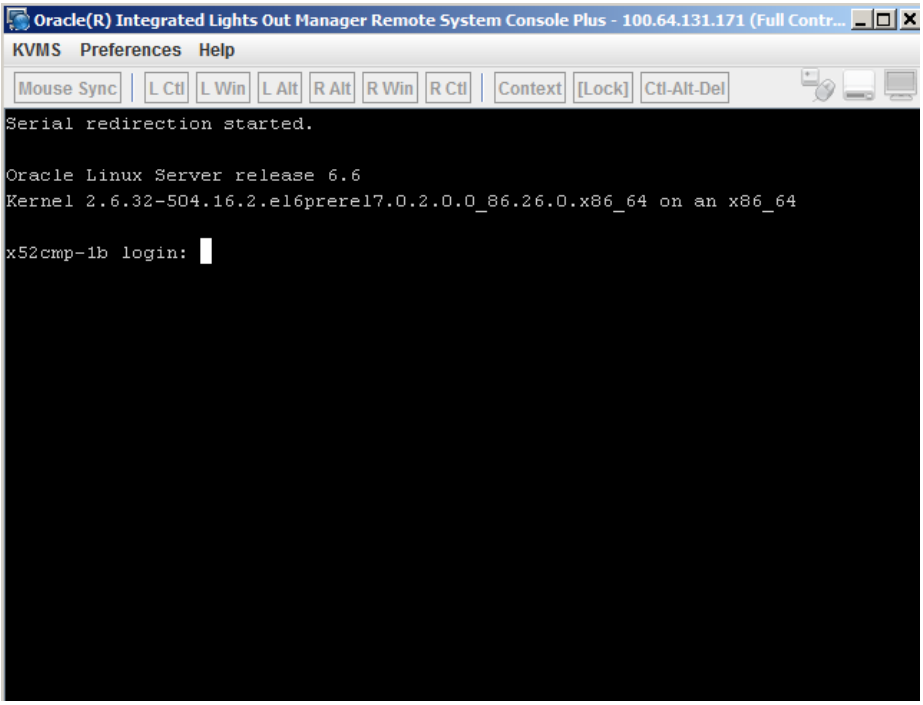
Procedure 43: Launching the Remote Console from the Oracle X5-2 iLO GUI

Step	Procedure	Result
1. ☐	HP iLO Gui	Naviagte to Remote Control -> Redirection  **Note**: There are two modes that can be selected
2. ☐	X5-2 iLOM GUI	Select the ***Use video redirection*** Confirm "OK" or "continue" if prompted  

Procedure 43: Launching the Remote Console from the Oracle X5-2 iLO GUI

3. ☐	Remote Console (video redirection)	Select "run"  The remote console will present login screen to the CLI of the installed OS. Login with *admusr* to access the CLI prompt. 

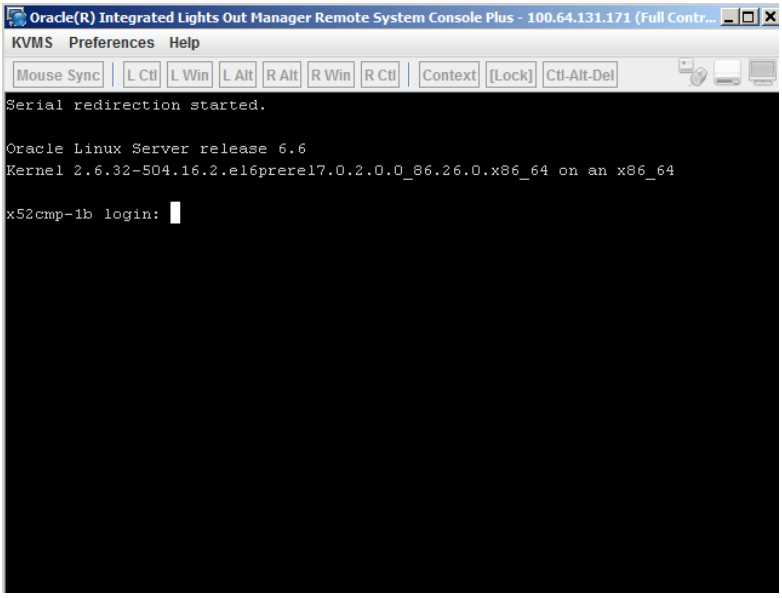
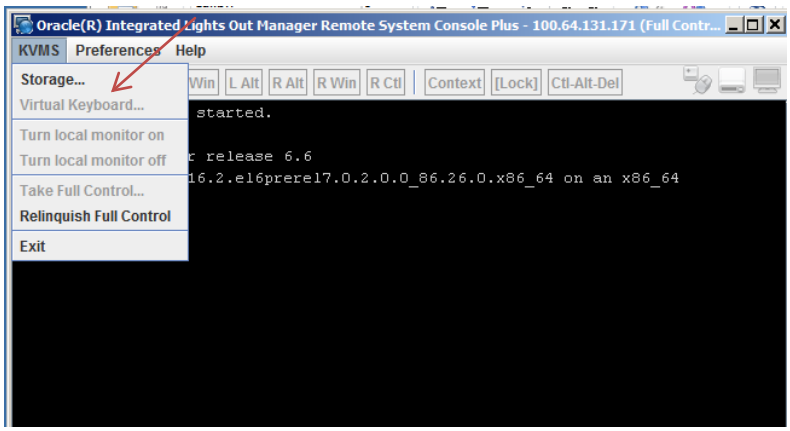
Procedure 43: Launching the Remote Console from the Oracle X5-2 iLO GUI

4. ☐	X5-2 iLOM GUI	Or *Select* ***Use serial redirection*** Click through the dialog boxes Confirm "continue " when prompted 
5. ☐	Remote Console Login (java)	The remote console will present login screen to the CLI of the installed OS. Login with *admusr* to access the CLI prompt. **Note:** Press Enter to get the CLI prompt to display. 
THIS PROCEDURE HAS BEEN COMPLETED		

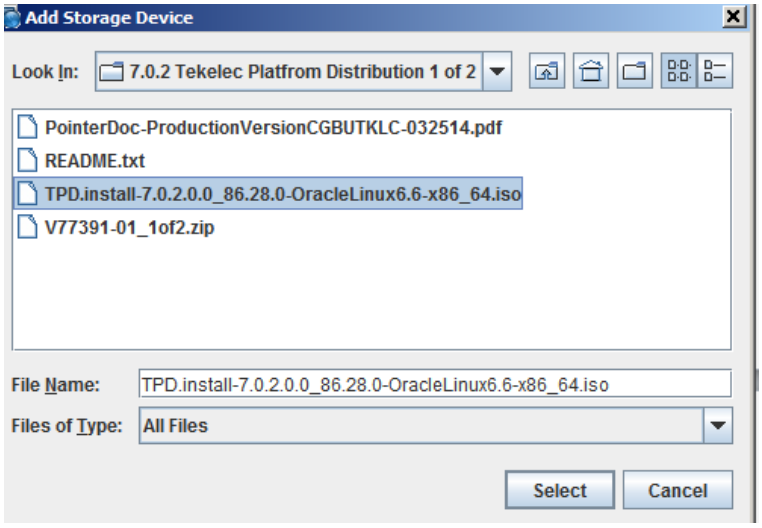
Procedure 14: Virtually Mount an ISO image file from the Oracle X5-2 iLO GUI

This procedure contains the steps to mount an ISO image file from the remote console of the iLO interface. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

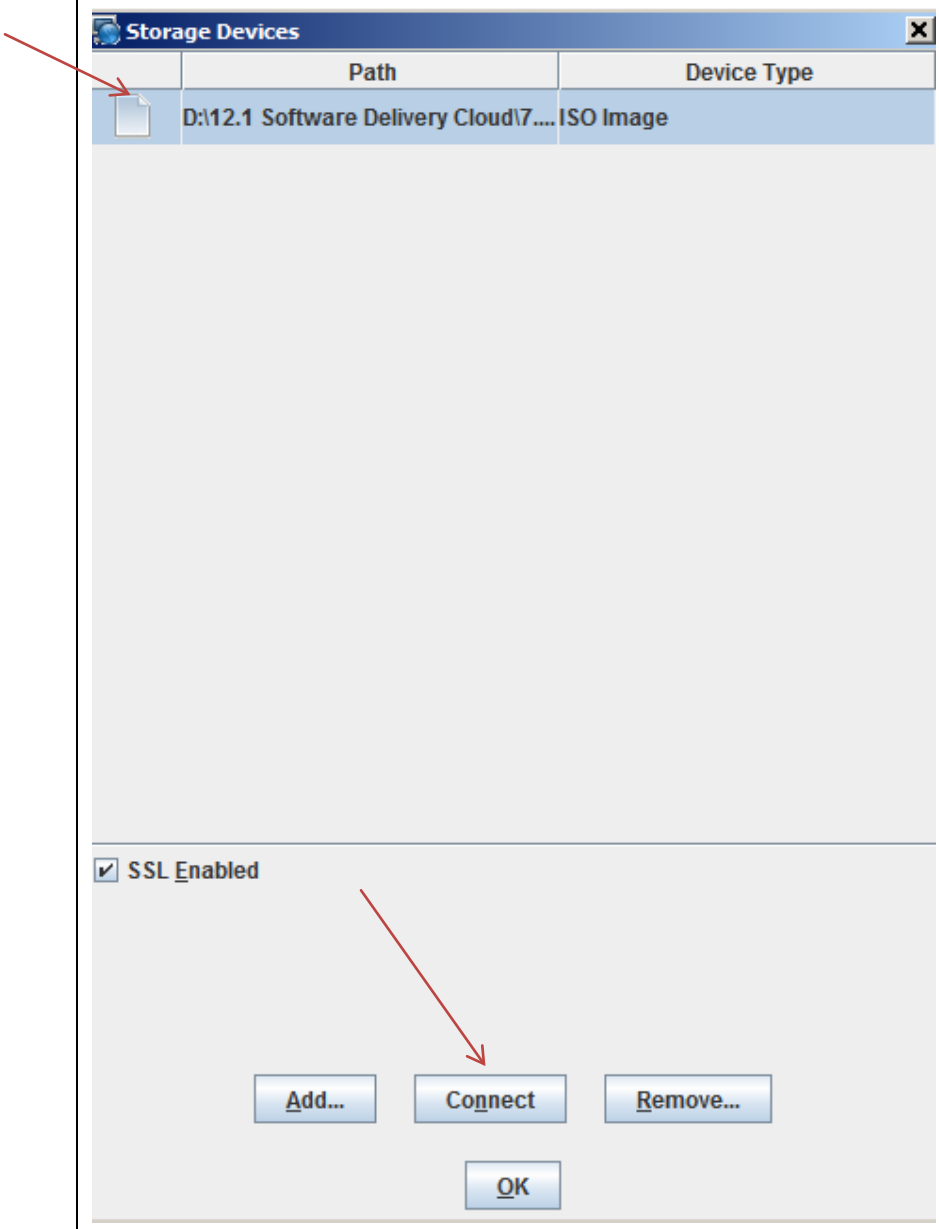
Procedure 44: Virtually mount an ISO image file from the Oracle X5-2 iLO GUI

Step	Procedure	Result
1. ☐	Launch the remote console	Launch the remote console. 
2. ☐	Remote Console	Select “KVMS” and from the drop down tab, select Storage. 

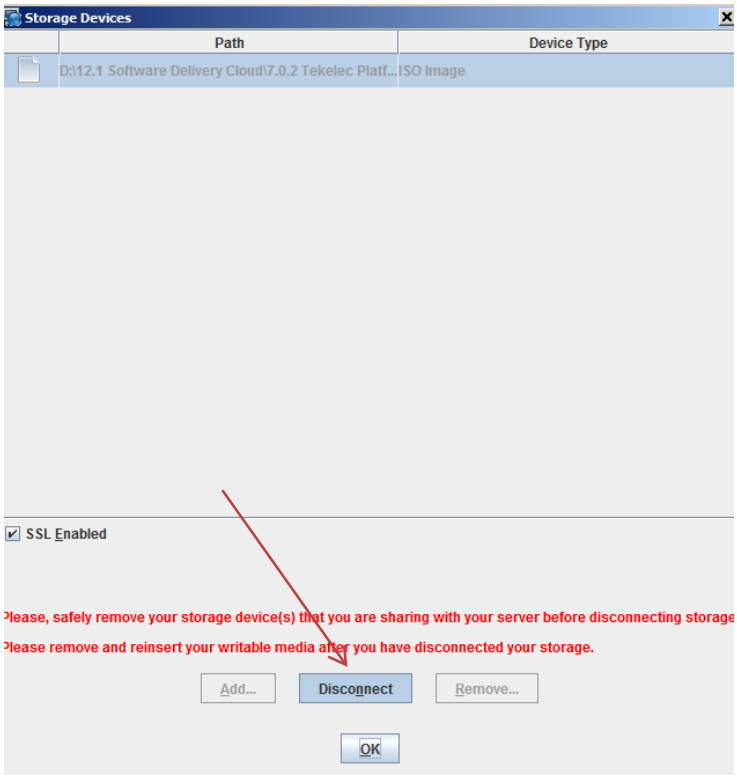
Procedure 44: Virtually mount an ISO image file from the Oracle X5-2 iLO GUI

3. ☐	Remote Console	In the form that opens up, click on the "Add" button. And browse to ISO image file that will be mounted and click on "Select". 

Procedure 44: Virtually mount an ISO image file from the Oracle X5-2 iLO GUI

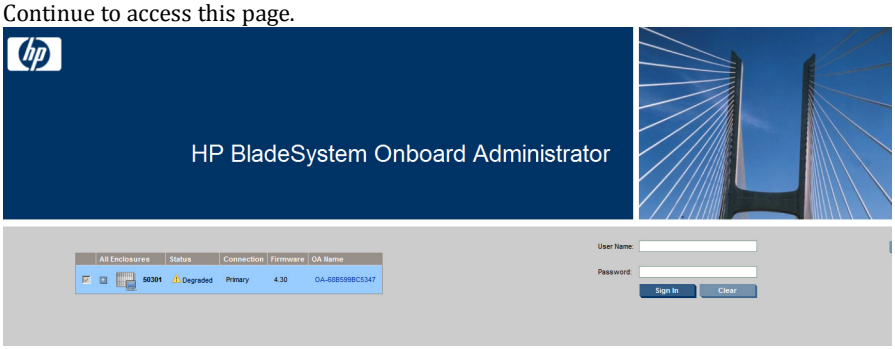
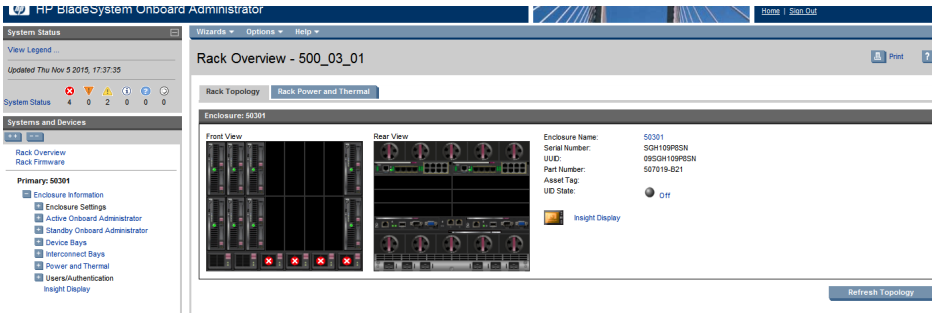
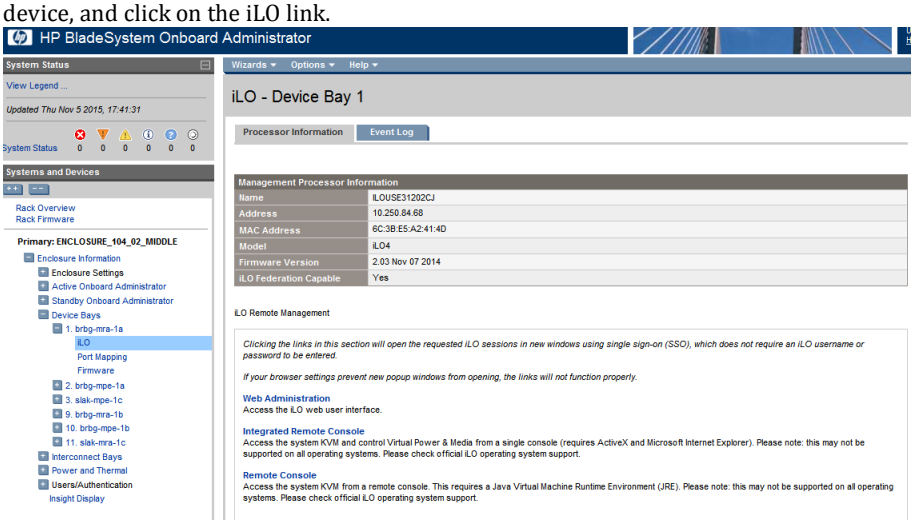
4. ☐	Remote Console	You will see the path to the selected file populated in the form. Highlight the ISO image and the buttons at the bottom of the form become available. Click on "connect" to complete mounting the ISO image file. 

Procedure 44: Virtually mount an ISO image file from the Oracle X5-2 iLO GUI

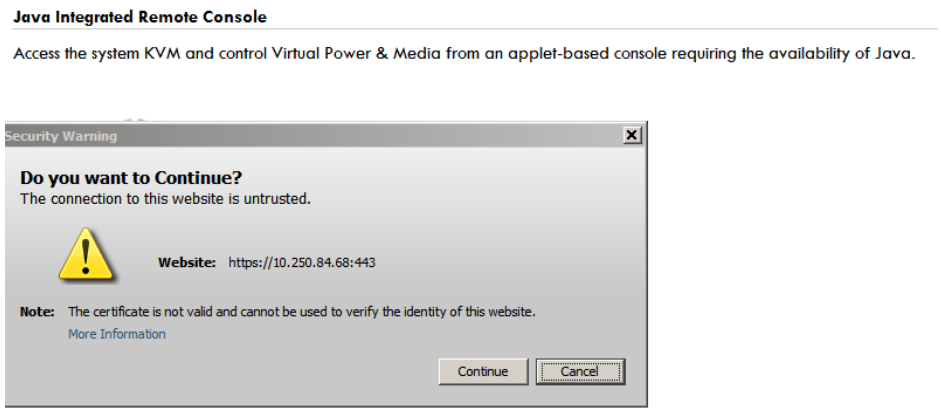
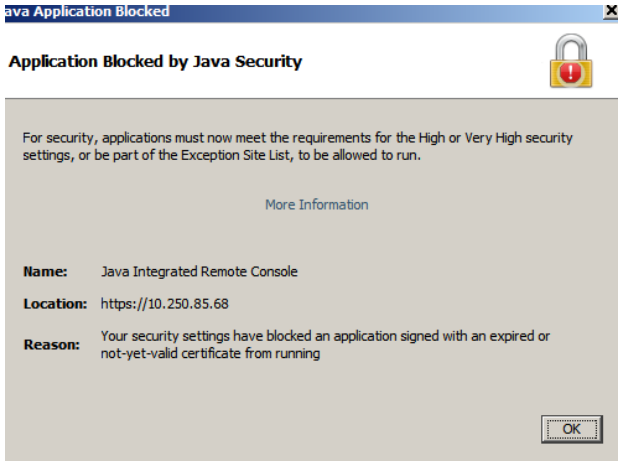
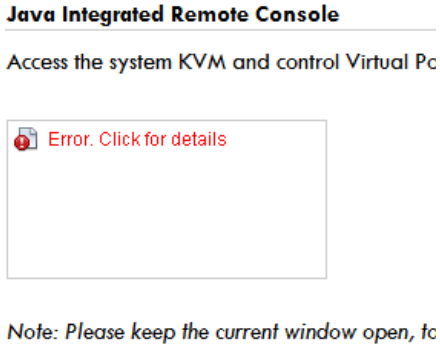
5. ☐	Remote Console	Once the iso image file is successfully "connected" you will be presented with the screen below indicating that the iso image is now mounted.  To unmount the image file select the file and click on "Remove"
THIS PROCEDURE HAS BEEN COMPLETED		

Procedure 45: Launching the Remote Console using the OA (c-Class)

Procedure 45: Launching the Remote Console using the OA (c-Class)

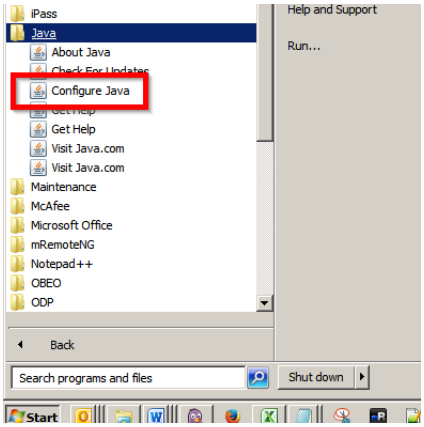
1. ☐	**Web Browser:** Access Onboard Administrator Login (must be Active OA)	Open a web browser and navigate to the OA IP address. Note that you be prompted with a warning for security certificates, because the certificate is self-signed. You must select Continue to access this page. 
2. ☐	**Web Browser:** 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. 

Procedure 45: Launching the Remote Console using the OA (c-Class)

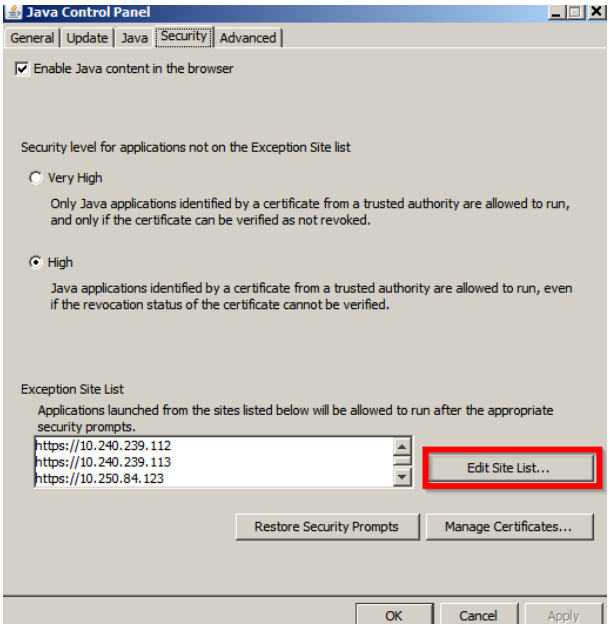
4. ☐	**Web Browser:** Click the remote Console link	Click the Remote Console link, and a new browser window opens. You may be prompted with a security certificate warning, as well as a warning about running content from an untrusted site. Click though the prompts.  You must select Continue or Yes to proceed.
5. ☐	**Web Browser**: If Java security error encountered	If the following error is encountered check your java security setting on the laptop and add the IP address of the target iLO to the exceptions list (see below)  

Procedure 45: Launching the Remote Console using the OA (c-Class)

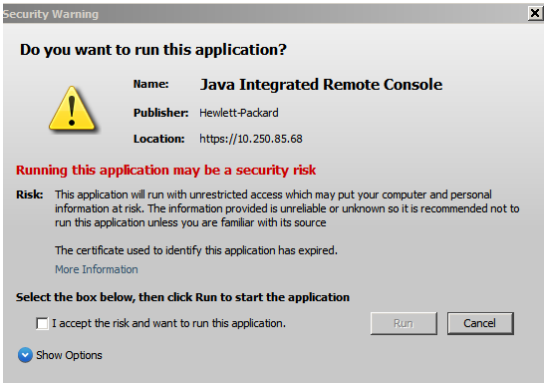
Find the Java application in programs on the client workstation and open "Configure Java"



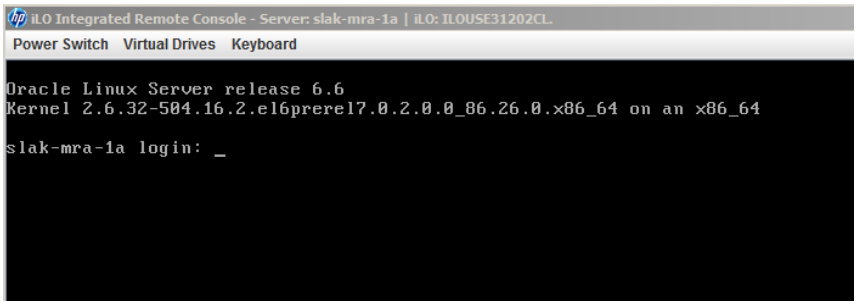
Go to the Security tab and click on <Edit Site List> and add the IP address of the target iLO.



Establish a new session and retry launching the console. When presented with the following screen click the I accept checkbox and then <run>.



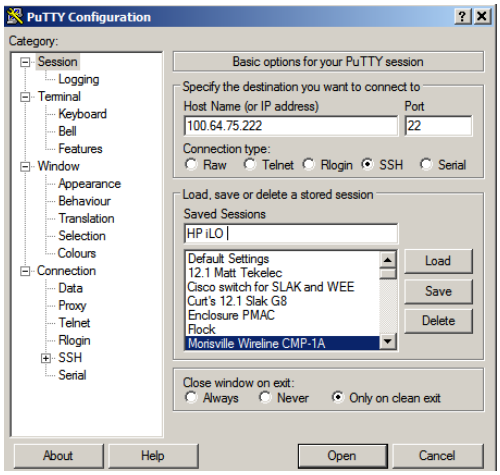
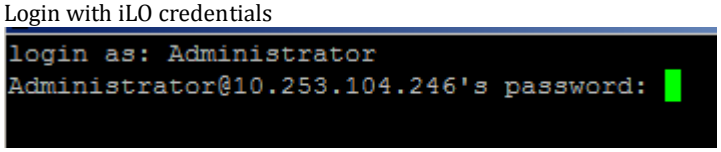
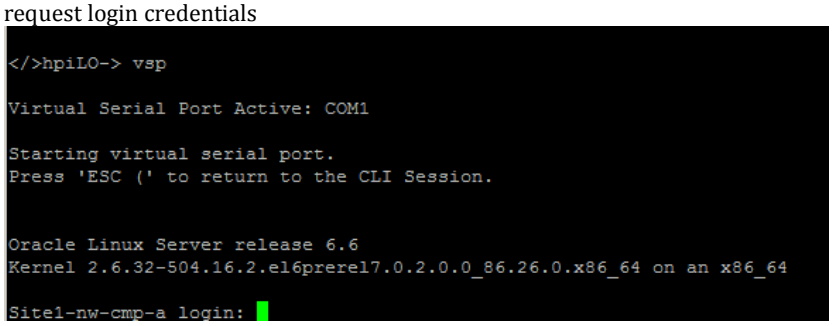
Procedure 45: Launching the Remote Console using the OA (c-Class)

		After a few moments, the Console window will open.  **You have completed this procedure.**

Procedure 46: SSH to the HP iLO and access the OS CLI

This procedure will access the Linux OS CLI by using ssh to connect to the HP iLO

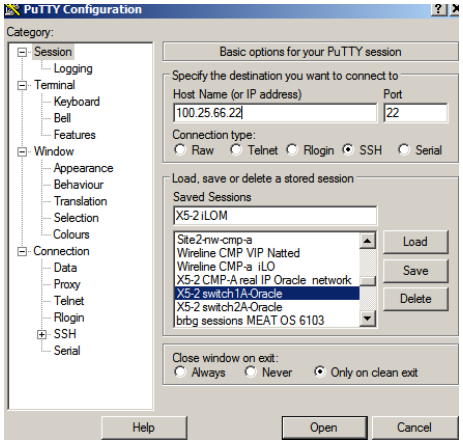
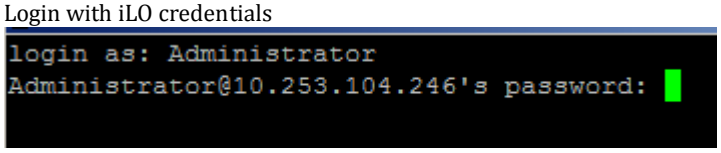
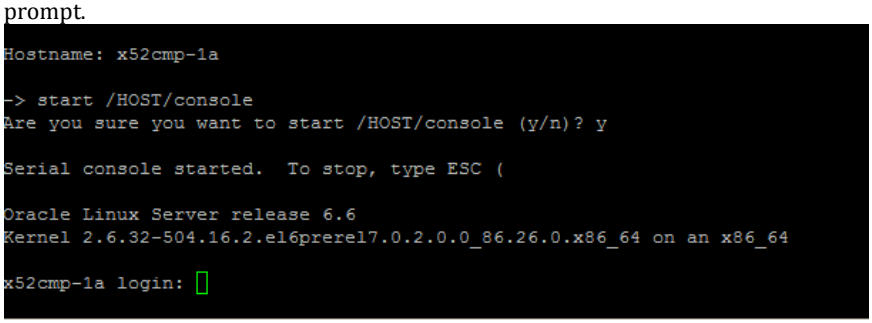
Procedure 46: SSH to the HP iLO and access the OS CLI

Step	Procedure	Result
1. ☐	**Open an SSH session to iLO IP address**	Using an ssh client such as putty, begin an SSH session to the iLO IP address of the target HP server.  Login with iLO credentials  At the HP iLO prompt use the command <**vsp**>. The host OS of the target server will now request login credentials  Login to host OS **You have completed this procedure.**

Procedure 47: SSH to the Oracle X5-2 iLOM and access the OS CLI

This procedure will access the Linux OS CLI by using ssh to connect to the X5-2 iLOM

Procedure 47: SSH to the Oracle X5-2 iLOM and access the OS CLI

Step	Procedure	Result
1. ☐	**Open an SSH session to iLOM IP address**	Using an ssh client such as putty, begin an SSH session to the iLO IP address of the target HP server.  Login with iLO credentials  At the X5-2 iLOM prompt use the command <**start /HOST/console**>. Confirm your intention to start a console session and you will be presented with a the host OS login prompt.  Login to host OS **You have completed this procedure.**

8.2 ADDITIONAL PROCEDURES

Procedure 48: Create a Bootable USB with TPD or TVOE ISO image

Procedure 48: Create a Bootable USB drive with TPD or TVOE ISO image

1. ☐	**View Topology Settings**	**Copying the USB image to a USB flash drive to achieve a Bootable Image:** For Tekelec Platform Distribution (TPD) and TVOE where bootable USB media is required for system installation, the following instructions are provided to Copy the USB image for TPD and /or TVOE to a USB Flash Drive in a manner that yields a bootable image for use on the system. 1) Run fdisk to determine what devices exist PRIOR to plugging in the USB device # fdisk -l | grep "Disk /dev" Disk /dev/sda: 300.0 GB, 299966445568 bytes Disk /dev/sdb: 1499.8 GB, 1499830990848 bytes Disk /dev/mapper/vgroot-plat_root: 1073 MB, 1073741824 bytes Disk /dev/mapper/vgbuild-home: 1499.8 GB, 1499828584448 bytes Disk /dev/mapper/vgroot-plat_var: 1073 MB, 1073741824 bytes Disk /dev/mapper/vgroot-plat_usr: 4294 MB, 4294967296 bytes Disk /dev/mapper/vgroot-plat_tmp: 1073 MB, 1073741824 bytes 2) Insert USB drive 3) Run fdisk again to determine how the USB device was enumerated (/dev/sdc in this example) # fdisk -l | grep "Disk /dev" Disk /dev/sda: 300.0 GB, 299966445568 bytes Disk /dev/sdb: 1499.8 GB, 1499830990848 bytes Disk /dev/mapper/vgroot-plat_root: 1073 MB, 1073741824 bytes Disk /dev/mapper/vgbuild-home: 1499.8 GB, 1499828584448 bytes Disk /dev/mapper/vgroot-plat_var: 1073 MB, 1073741824 bytes Disk /dev/mapper/vgroot-plat_usr: 4294 MB, 4294967296 bytes Disk /dev/mapper/vgroot-plat_tmp: 1073 MB, 1073741824 bytes Disk /dev/mapper/vgroot-plat_var_tklc: 4294 MB, 4294967296 bytes Disk /dev/mapper/vgroot-scratchpad: 287.9 GB, 287863472128 bytes Disk /dev/sdc: 2044 MB, 2044723200 bytes 4) Run dmesg to confirm how the USB device was enumerated # dmesg | tail -20 usb 1-5: Manufacturer: Generic usb 1-5: SerialNumber: F8F3A1CA usb 1-5: configuration #1 chosen from 1 choice Initializing USB Mass Storage driver... scsi3 : SCSI emulation for USB Mass Storage devices usb-storage: device found at 2 usb-storage: waiting for device to settle before scanning usbcore: registered new interface driver usb-storage USB Mass Storage support registered. usb-storage: device scan complete scsi 3:0:0:0: Direct-Access Generic Flash Disk 8.07 PQ: 0 ANSI: 2 sd 3:0:0:0: Attached scsi generic sg4 type 0

Procedure 48: Create a Bootable USB drive with TPD or TVOE ISO image

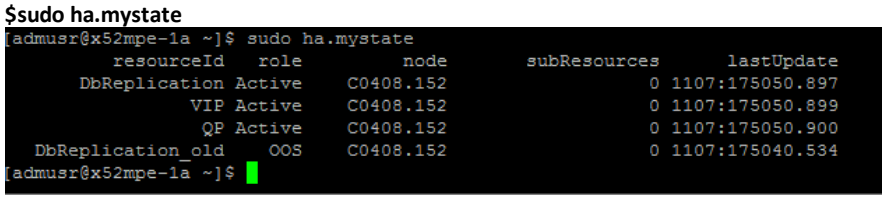
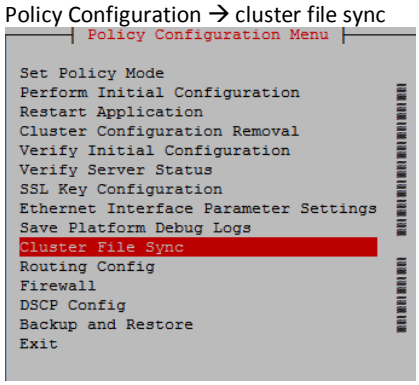
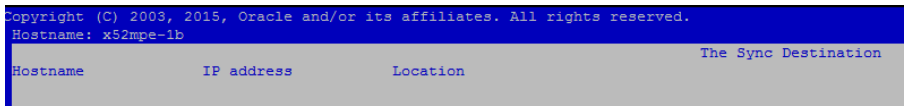
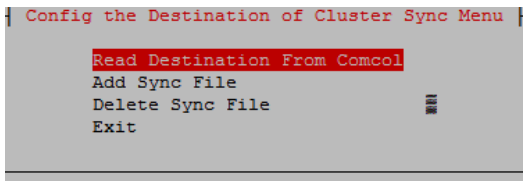
		sd 3:0:0:0: [sdc] 3993600 512-byte logical blocks: (2.04 GB/1.90 GiB) sd 3:0:0:0: [sdc] Write Protect is off sd 3:0:0:0: [sdc] Mode Sense: 03 00 00 00 sd 3:0:0:0: [sdc] Assuming drive cache: write through sd 3:0:0:0: [sdc] Assuming drive cache: write through sdc: sdc1 sd 3:0:0:0: [sdc] Assuming drive cache: write through sd 3:0:0:0: [sdc] Attached SCSI removable disk 5) Run fdisk command on the newly enumerated device name to determine the partition name (sdc1 in this example) # fdisk -l /dev/sdc Disk /dev/sdc: 2044 MB, 2044723200 bytes 31 heads, 30 sectors/track, 4294 cylinders Units = cylinders of 930 * 512 = 476160 bytes Sector size (logical/physical): 512 bytes / 512 bytes I/O size (minimum/optimal): 512 bytes / 512 bytes Disk identifier: 0x3fb6f5c2 Device Boot Start End Blocks Id System /dev/sdc1 2 4295 1996040 6 FAT16 6) Use the dd command to copy the image to the USB device (to the device and not the partition) # dd if=TPD.install-6.5.1_82.28.5-CentOS6.4-x86_64.usb of=/dev/sdc 2306305+0 records in 2306305+0 records out 1180828160 bytes (1.2 GB) copied, 504.454 s, 2.3 MB/s 7) Remove USB drive and reinsert it. Run dmesg again to determine name. # dmesg | tail -20 usb 1-5: Product: Mass Storage usb 1-5: Manufacturer: Generic usb 1-5: SerialNumber: F8F3A1CA usb 1-5: configuration #1 chosen from 1 choice scsi4 : SCSI emulation for USB Mass Storage devices usb-storage: device found at 3 usb-storage: waiting for device to settle before scanning usb-storage: device scan complete scsi 4:0:0:0: Direct-Access Generic Flash Disk 8.07 PQ: 0 ANSI: 2 sd 4:0:0:0: Attached scsi generic sg4 type 0 sd 4:0:0:0: [sdc] 3993600 512-byte logical blocks: (2.04 GB/1.90 GiB) sd 4:0:0:0: [sdc] Write Protect is off sd 4:0:0:0: [sdc] Mode Sense: 03 00 00 00 sd 4:0:0:0: [sdc] Assuming drive cache: write through sd 4:0:0:0: [sdc] Assuming drive cache: write through sdc: unknown partition table sd 4:0:0:0: [sdc] Assuming drive cache: write through sd 4:0:0:0: [sdc] Attached SCSI removable disk ISO 9660 Extensions: Microsoft Joliet Level 3 ISO 9660 Extensions: RRIP_1991A

Procedure 48: Create a Bootable USB drive with TPD or TVOE ISO image

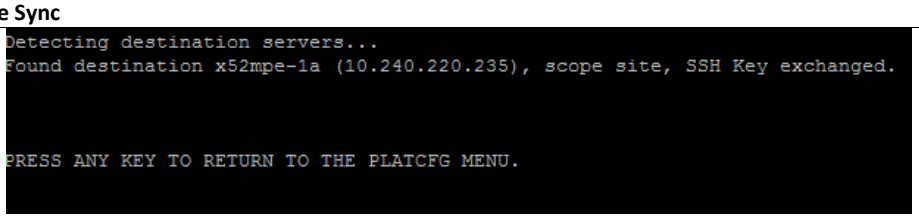
		8) Mount the partition on the USB device to the /media mount point (use partition name and not device) # mount /dev/sdc1 /media 9) Verify the USB contents look as expected (example below is from TPD) # lsf /media total 835588 drwxr-xr-x 5 root root 4096 Dec 31 1969 ./ dr-xr-xr-x. 29 root root 4096 Jan 11 17:10 ../ drwxr-xr-x 3 root root 4096 Jan 11 14:22 images/ -r-xr-xr-x 1 root root 32768 Jan 11 13:22 ldlinux.sys* drwxr-xr-x 2 root root 4096 Jan 11 14:22 syslinux/ -rwxr-xr-x 1 root root 855554048 Jan 11 14:22 TPD.install-6.5.1_82.28.5-CentOS6.4-x86_64.iso* -rwxr-xr-x 1 root root 32229 Jan 11 14:22 TPD.ks* drwxr-xr-x 4 root root 4096 Jan 11 14:22 umvt/ 10) Mount the ISO image (may be different for non-TPD USB images) from the USB image to another mount point mount -o loop /media/TPD.install-6.5.1_82.28.5-CentOS6.4-x86_64.iso /mnt/upgrade 11) Run command to validate the ISO image # /mnt/upgrade/upgrade/.validate/validate_cd Validating cdrom... UMVT Validate Utility v2.2.2, (c)Tekelec, June 2012 Validating /media/TPD.install-6.5.1_82.28.5-CentOS6.4-x86_64.iso Date&Time: 2014-01-14 17:53:31 Volume ID: tklc_000-0000-000_Rev_A_82.28.5 Part Number: 000-0000-000_Rev_A Version: 82.28.5 Disc Label: TPD Disc description: TPD The media validation is complete, the result is: PASS CDROM is Valid 12) Unmount the ISO image # umount /mnt/upgrade 13) Unmount the USB device # umount /media **You have completed this procedure**

Procedure 49: Perform a Cluster File Sync

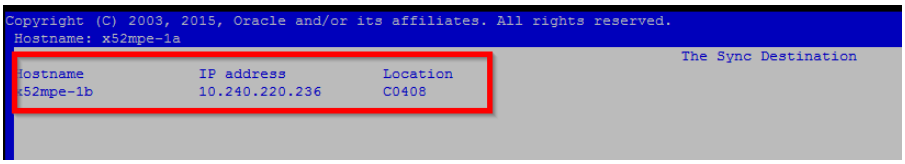
Procedure 49: Perform a Cluster File Sync

STEP #		
	This procedure will perform a cluster file sync from the active blade to the standby blade of an HA cluster **Pre-requisite:** - HA Cluster has been completed in the Cluster Topology Configuration in the CMP GUI - SSH Key exchanges to all servers in the topology has been completed 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: Platcfg**: Perform cluster sync from active server in the cluster to HA mate	Ssh to the active server of the target cluster, and login as admusr and cconfirm that the ssh session is on the active server. **$sudo ha.mystate**  **Note: Cluster file syncs should always be performed from the active mate in the cluster to the standby mate and not the other way around.** **$sudo su – platcfg** Policy Configuration → cluster file sync  From the “Cluster Configuration SyncMenu” select “Show Sync Destination”. On a newly installed server the destination will be empty.  Navigate to “Cluster Sync Config” -> “Read Destination from Comcol”  Select “Read Destination from Comcol”. Press any key to return to platcfg menu. After some time you will be returned to the platcfg menu.

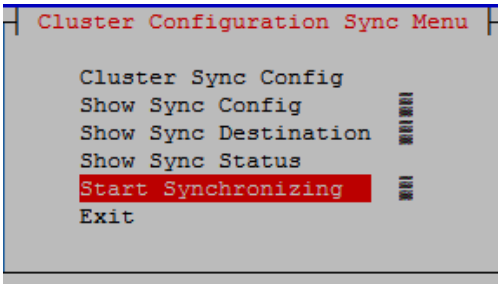
Procedure 49: Perform a Cluster File Sync



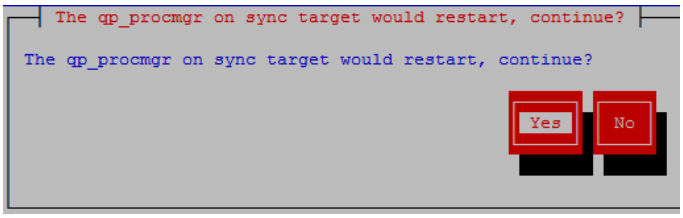
In the platcfg menu navigate to "Show Sync Destination" and confirm the hostname is now populated .



From the Cluster Configuration Sync Menu select "Start Synchronizing".

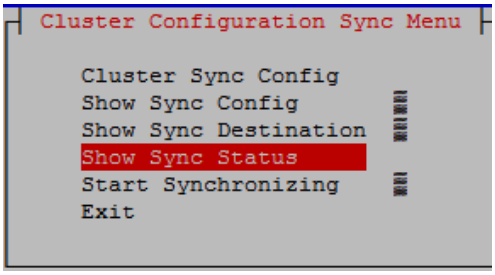


And confirm when prompted



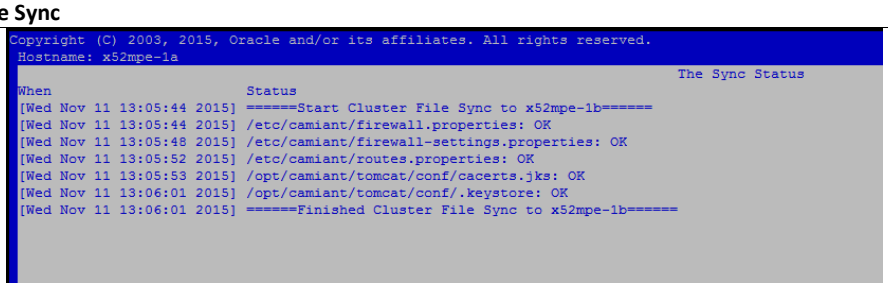
Wait to be returned to the platcfg menu.

In the Cluster Configuration Sync Menu select "Show Sync Status"



And Confirm success.

Procedure 49: Perform a Cluster File Sync

		 Exit the Platcfg utility and return to cli prompt. **You have completed this procedure**

8.3 C-CLASS: MANUFACTURING IP NETWORKING CONFIGURATION

This section describes the IP address configuration of the network interfaces that are applied during Oracle manufacturing setup. These addresses are configured for use by manufacturing for the purpose of diagnostics prior to shipping devices to a customer site.

These network IP addresses are expected to be changed once the devices are deployed at the customer site.

8.3.1 Management VLAN

Network — 192.168.100.0

Netmask — 255.255.255.0

VLAN 2-VIP (Gateway) — 192.168.100.1

Switch 1A — 192.168.100.2

Switch 1B — 192.168.100.3

PM&C Server — 192.168.100.4 bond 0.2

PM&C iLO — 192.168.100.5

First HP C7000 Enclosure		Second HP C7000 Enclosure	
HP c7000 OA 1	192.168.100.6	HP c7000 OA 1	192.168.100.28
HP c7000 OA 2	192.168.100.7	HP c7000 OA 2	192.168.100.29
HP Enclosure 1 Blade 1 iLO	192.168.100.10	HP Enclosure 2 Blade 1 iLO	192.168.100.30
HP Enclosure 1 Blade 2 iLO	192.168.100.11	HP Enclosure 2 Blade 2 iLO	192.168.100.31
HP Enclosure 1 Blade 3 iLO	192.168.100.12	HP Enclosure 2 Blade 3 iLO	192.168.100.32
HP Enclosure 1 Blade 4 iLO	192.168.100.13	HP Enclosure 2 Blade 4 iLO	192.168.100.33
HP Enclosure 1 Blade 5 iLO	192.168.100.14	HP Enclosure 2 Blade 5 iLO	192.168.100.34
HP Enclosure 1 Blade 6 iLO	192.168.100.15	HP Enclosure 2 Blade 6 iLO	192.168.100.35
HP Enclosure 1 Blade 7 iLO	192.168.100.16	HP Enclosure 2 Blade 7 iLO	192.168.100.36

HP Enclosure 1 Blade 8 iLO	192.168.100.17	HP Enclosure 2 Blade 8 iLO	192.168.100.37
HP Enclosure 1 Blade 9 iLO	192.168.100.18	HP Enclosure 2 Blade 9 iLO	192.168.100.38
HP Enclosure 1 Blade 10 iLO	192.168.100.19	HP Enclosure 2 Blade 10 iLO	192.168.100.39
HP Enclosure 1 Blade 11 iLO	192.168.100.20	HP Enclosure 2 Blade 11 iLO	192.168.100.40
HP Enclosure 1 Blade 12 iLO	192.168.100.21	HP Enclosure 2 Blade 12 iLO	192.168.100.41
HP Enclosure 1 Blade 13 iLO	192.168.100.22	HP Enclosure 2 Blade 13 iLO	192.168.100.42
HP Enclosure 1 Blade 14 iLO	192.168.100.23	HP Enclosure 2 Blade 14 iLO	192.168.100.43
HP Enclosure 1 Blade 15 iLO	192.168.100.24	HP Enclosure 2 Blade 15 iLO	192.168.100.44
HP Enclosure 1 Blade 16 iLO	192.168.100.25	HP Enclosure 2 Blade 16 iLO	192.168.100.45
HP 6120XG switch Bay 1	192.168.100.26	HP 6120XG switch Bay 1	192.168.100.46
HP 6120XG switch Bay 2	192.168.100.27	HP 6120XG switch Bay 2	192.168.100.47
Third HP C7000 Enclosure		**Manufacturing Test Computer IP Addresses**	
HP c7000 OA 1	192.168.100.48	192.168.100.250	
HP c7000 OA 2	192.168.100.49	192.168.100.251	
HP Enclosure 1 Blade 1 iLO	192.168.100.50	192.168.100.252	
HP Enclosure 1 Blade 2 iLO	192.168.100.51	192.168.100.253	
HP Enclosure 1 Blade 3 iLO	192.168.100.52	192.168.100.254	
HP Enclosure 1 Blade 4 iLO	192.168.100.53		
HP Enclosure 1 Blade 5 iLO	192.168.100.54		
HP Enclosure 1 Blade 6 iLO	192.168.100.55		
HP Enclosure 1 Blade 7 iLO	192.168.100.56		
HP Enclosure 1 Blade 8 iLO	192.168.100.57		
HP Enclosure 1 Blade 9 iLO	192.168.100.58		
HP Enclosure 1 Blade 10 iLO	192.168.100.59		
HP Enclosure 1 Blade 11 iLO	192.168.100.60		
HP Enclosure 1 Blade 12 iLO	192.168.100.61		
HP Enclosure 1 Blade 13 iLO	192.168.100.62		
HP Enclosure 1 Blade 14 iLO	192.168.100.63		
HP Enclosure 1 Blade 15 iLO	192.168.100.64		
HP Enclosure 1 Blade 16 iLO	192.168.100.65		
HP 6120XG switch Bay 1	192.168.100.66		
HP 6120XG switch Bay 2	192.168.100.67		

8.3.2 HP RMS Management Addresses

Network — 192.168.100.0

Netmask — 255.255.255.0

Switch VIP (Gateway) — 192.168.100.1

Switch 1A — 192.168.100.2

Switch 1B — 192.168.100.3

NOTE: 22 DL360 (1U) Servers allowed in one Cabinet.

HP RMS Cabinet	
Server	**iLO IP Address**
A	**192.168.100.10**
B	**192.168.100.11**
C	**192.168.100.12**
D	**192.168.100.13**
E	**192.168.100.14**
F	**192.168.100.15**
G	**192.168.100.16**
H	**192.168.100.17**
J	**192.168.100.18**
K	**192.168.100.19**
L	**192.168.100.20**
M	**192.168.100.21**
N	**192.168.100.22**
P	**192.168.100.23**
Q	**192.168.100.24**
R	**192.168.100.25**
S	**192.168.100.26**
T	**192.168.100.27**
U	**192.168.100.28**
V	**192.168.100.29**
W	**192.168.100.30**
X	**192.168.100.31**

8.3.3 Application Default IP Addresses

Internal

	XMI	IMI	XSI-1	XSI-2
NetID	192.168.101.0	192.168.101.64	192.168.101.128	192.168.101.192
NetMask	255.255.255.192	255.255.255.192	255.255.255.192	255.255.255.192
Switch A	192.168.101.2	192.168.101.66	192.168.101.130	192.168.101.194
Switch B	192.168.101.3	192.168.101.67	192.168.101.131	192.168.101.195
Switch VIP	192.168.101.1	192.168.101.65	192.168.101.129	192.168.101.193
Uplink Port	-	-	-	-
VLAN ID	3	4	5	6
VRRP ID	3	4	5	6
Default Gateway	192.168.101.1	192.168.101.65	192.168.101.129	192.168.101.193

8.3.4 External Default IP Addresses

	XMI	IMI	XSI-1	XSI-2
NetID	192.168.102.0	192.168.102.64	192.168.102.128	192.168.102.192
NetMask	255.255.255.192	255.255.255.192	255.255.255.192	255.255.255.192
Switch A	192.168.102.2	192.168.102.66	192.168.102.130	192.168.102.194
Switch B	192.168.102.3	192.168.102.67	192.168.102.131	192.168.102.195
Switch VIP	192.168.102.1	192.168.102.65	192.168.102.129	192.168.102.193
Uplink Port	-	-	-	-
VLAN ID	3	4	5	6
VRRP ID	3	4	5	6
Default Gateway	192.168.102.1	192.168.102.65	192.168.102.129	192.168.102.193

Appendix A. DISCREPANCY LIST

The following form may be used to document discrepancies (variations, issues that will require additional follow up at post-installation).

Discrepancy List

Date	Procedure and Step	Description of Discrepancy	Resolution Responsibility	Resolution Date:

Appendix B. ACCESSING ORACLE'S CUSTOMER SUPPORT SITE

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*. When calling, make the selections in the sequence shown below 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 **2** for Non-technical issue

You will be connected to a live agent who can assist you with MOS registration and provide Support Identifiers. Simply mention you are an Oracle Customer new to MOS. MOS is available 24 hours a day, 7 days a week, 365 days a year.