Oracle® Communications Policy and Charging Rules Function
PCRF Cable Policy Software Installation Procedure

Release 11.5

E61661-01

February 2015

ORACLE®

Oracle® Communications Policy and Charging Rules Function, Cable Policy Software Installation Procedure, Release 11.5

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.

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

TABLE OF CONTENTS **3**

1. INTRODUCTION **4**

2.2 PURPOSE AND SCOPE 4
2.3 SUPPORTING DOCUMENTATION 4
2.4 ACRONYMS 5
2.5 PRE-REQUISITES 5
2.6 REQUIRED MATERIALS 7
2.7 LOGINS/PASSWORDS 8
2.8 ACRONYMS 8

3. SOFTWARE INSTALLATION AND INITIAL CONFIGURATION **9**

3.1 IPM HP RMS 9
Procedure 1: Update Servers' Firmware 9
Procedure 2: Configure Server's iLO Port 16
Procedure 3: Configure BIOS 19
3.2 TPD INSTALLATION 24
Procedure 4: Install OS of RMS Server 24
Procedure 5: Install Application Software (RMS) 30

4. CONFIGURE POLICY APPLICATION SERVERS **38**

4.2 CONFIGURE POLICY MODE 38
Procedure 6: Perform Policy Mode for Policy Servers 38
4.3 CONFIGURE NETWORK TOPOLOGY 41
Procedure 7: Perform Initial IP Configuration of Policy Servers 41
Procedure 8: CMP GUI Initial Configuration 47
Procedure 9: Add Topology Configuration for CMP Cluster 49
Procedure 10: Add MPE/BOD/MA Clusters to the Topology Configuration 56

5. SUPPORTING PROCEDURES **70**

Appendix A: Connecting to the HP DL360/380 G8 iLO Manager from a laptop 70
Appendix B: Use Remote Console of the iLO Manager to virtually mount an iso image file (HL DL360) 72
Appendix C: Use Remote Console of the iLO Manager to virtually mount an iso image file (HP DL380) 76
Appendix D: Configure SNMP 80

1. Introduction

2.2 Purpose and Scope

This document describes the procedures to install and configure Policy Server software release 11.5 for Cable Customers. This release is the first common release that supports wireless , wireline and Cable customers, configuration of the policy software components will determine the market and components that shall be running for Policy software.

Cable Policy software 11.5 can be installed on any of the following supported HP RMS hardware types:

- HP ProLiant DL360G6/G7
- HP ProLiant DL360pG8
- HP ProLiant DL380pG8

In addition to the new SUN H/W type:

- Sun Netra X3-2servers

Note: The installation screen shots and procedures of this MOP is upon DL360G6 RMS hardware.

Policy 11.5 is based on Platform 6.7 release and contains the following major components releases:

- Oracle Linux OS 6.5
- TPD 6.7
- COMCOL (In-memory DB) 6.3
- Policy components: MPE, MA, BOD and CMP 11.5

2.3 Supporting Documentation

[1] *PD001866 Formal Peer Review Process*
[2] *TR007292 Policy 9.4 Install Procedures*
[3] *TR007293 Policy 9.4 on RMS networking interconnect*
[4] *910-6929-001 HP Solutions Firmware Upgrade Pack 2.2.5*
[5] *909-2130-001 TPD Initial Product Manufacture*
[6] *910-6732-001 Platform Configuration User's Guide*
[7] *FE007452 Cable Reference Architecture*
[8] *910-6288-001 SNMP User's Guide Revision*
[9] *FD008102 Policy platform multiple modes*

2.4 Acronyms

An alphabetized list of acronyms used in the document: Table 1. Acronyms

Acronym	Definition
BIOS	Basic Input Output System
CMP	Policy Manager
DVD	Digital Versatile Disc
FRU	Field Replaceable Unit
iLO	Integrated Lights Out manager
IPM	Initial Product Manufacture – the process of installing TPD on a hardware platform
MPE	Multi-protocol Policy Engine
OS	Operating System (e.g. TPD)
PCRF	Policy and Charging Rules Function
SPP	Service Pack Proliant
TPD	Tekelec Platform Distribution
VSP	Virtual Serial Port

2.5 Pre-requisites

1. Hardware equipment ordered , installed by customer in the designated racks/enclosures and are powered on
2. Network cabling is completed and is in place. Following the network layout for all hardware types in case Direct link is configured or not:

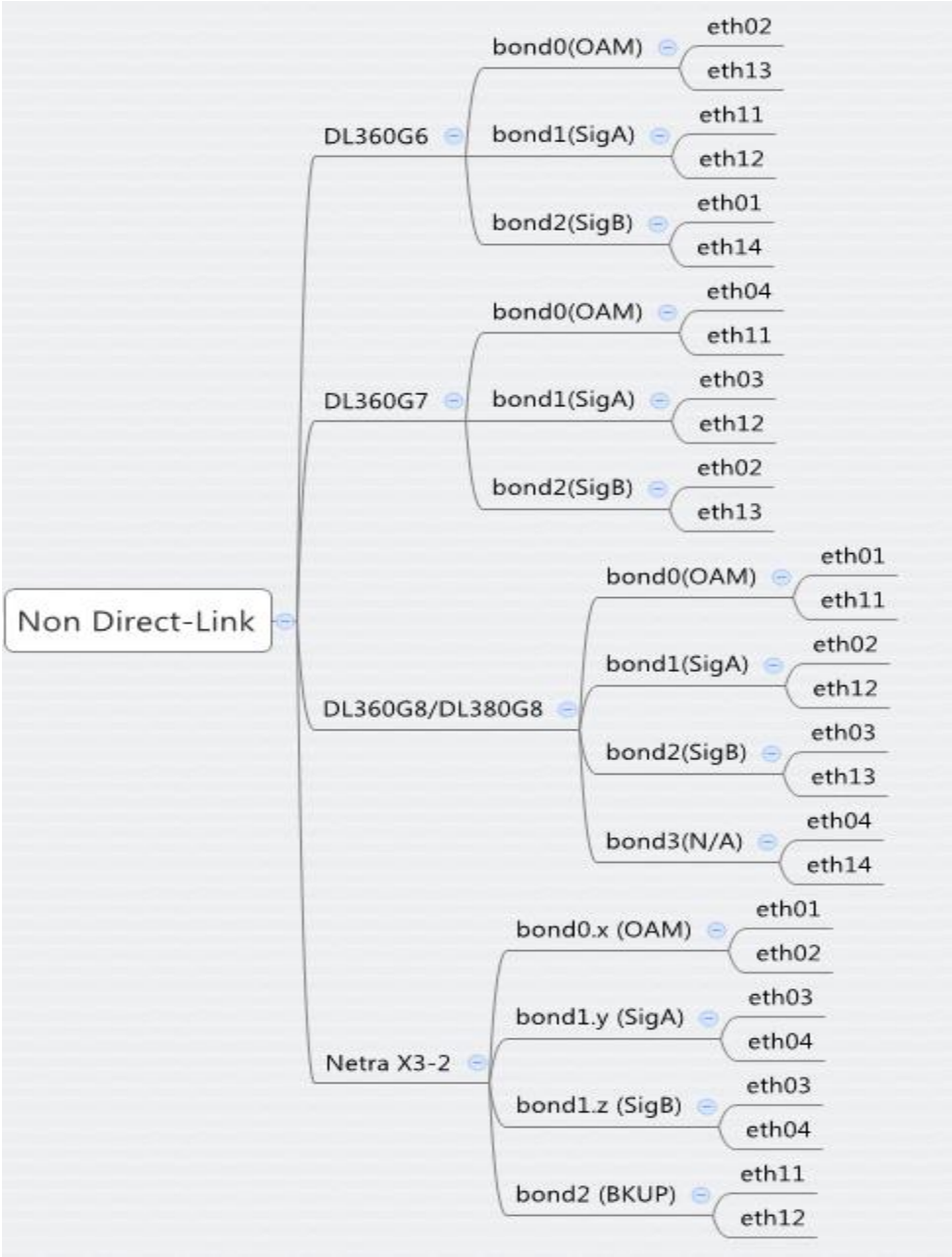


Figure 1 Network Layout for Non Direct-Link

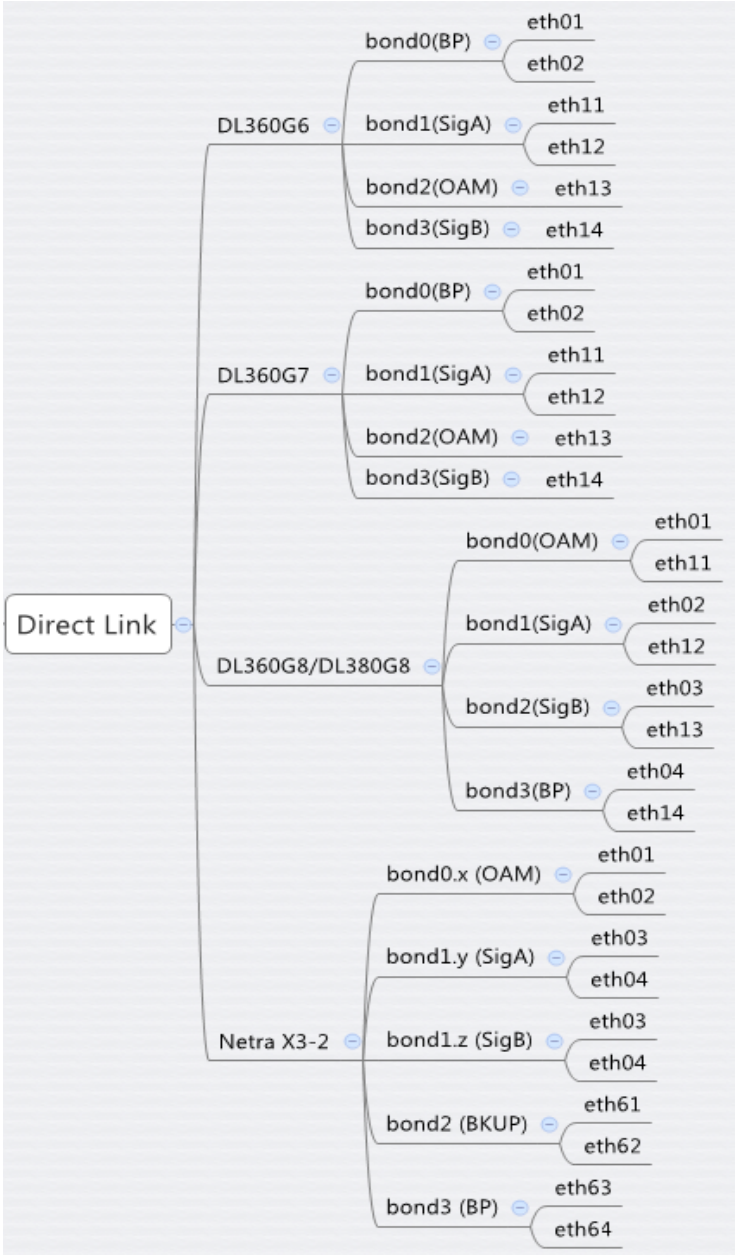


Figure 2 Network Layout for Direct-Link

2.6 Required Materials

- Firmware pack 2.2.5 , refer to reference [3] for details
- TPD 6.7 ISO image on CD/DVD/USB drive or local in the machine used in case of remote installation
- GA released version of Cable Policy components (CMP, BOD, MPE, MA) ISO images on CD/DVD/USB drive or local in the machine used in case of remote installation
- iLO https addresses for all servers

2.7 Logins/Passwords

Initial login to a HP server/module (iLO interface) 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 Tekelec Manufacturing, then the HP passwords will have been replaced with a Tekelec/Oracle configured password and noted on the plastic pull-out tab.

2.8 Acronyms

Acronym	Definition
BOD	Bandwidth on Demand
GUI	Graphical User Interface
SDM	Subscriber Data Management
HA	High Availability
IPM	Initial Program Manufacture
MA	Management Agent
MPE	Multimedia Policy Engine
CMP	Camiant Management Platform
OAM	Operation, Administration and Management
QP	QBUS Platform
SIG	Signaling Network
BIOS	Basic Input Output System
CD	Compact Disk
CSV	Comma Separated Value
DVD	Digital Versatile Disc
EBIPA	Enclosure Bay IP Addressing
FRU	Field Replaceable Unit
HP c-Class	HP blade server offering
iLO	Integrated Lights Out manager
IE	Internet Explorer
IPM	Initial Product Manufacture – the process of installing TPD on a hardware platform
OA	HP Onboard Administrator
OS	Operating System (e.g. TPD)
PM&C	Platform Management & Configuration
RMM2	Intel Remote Management Module 2 – PP-5160 Lights out Management
RMS	Rack Mount Server
SFTP	SFTP Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
TPD	Tekelec Platform Distribution
VSP	Virtual Serial Port

Table 2 Acronyms

3. Software Installation and Initial Configuration

3.1 IPM HP RMS

Procedure 1: Update Servers' Firmware

Procedure 1. Update Servers' Firmware

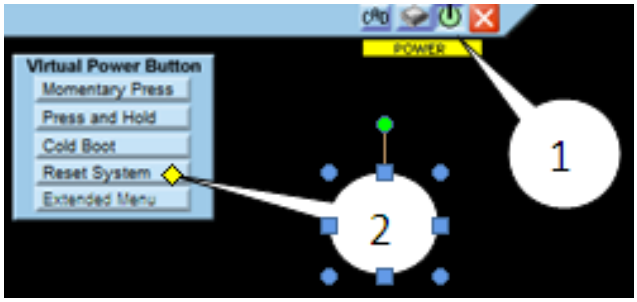
S T E P #	This procedure will update the RMS servers' firmware to HP SPP (Service Pack Proliant) 2.2.5 Servers that are shipped to site may have different shipping dates. Consequently servers may have different versions of firmware depending on ship dates. This procedure will bring all the servers, regardless of when they may have been shipped, up to a standardized baseline. **Needed material:** - HP Firmware 872-2488-106-2.2.5_10.37.0-FW_SPP.iso (HP Service Pack for ProLiant 2.2.5)	
1. ☐	**Server's iLO Manager Remote Console:** Launch the remote console	Reference the procedures at the end of this document (Appendix B or C) based on the hardware used to start the remote console of the server via iLO web interface page

Procedure 1. Update Servers' Firmware

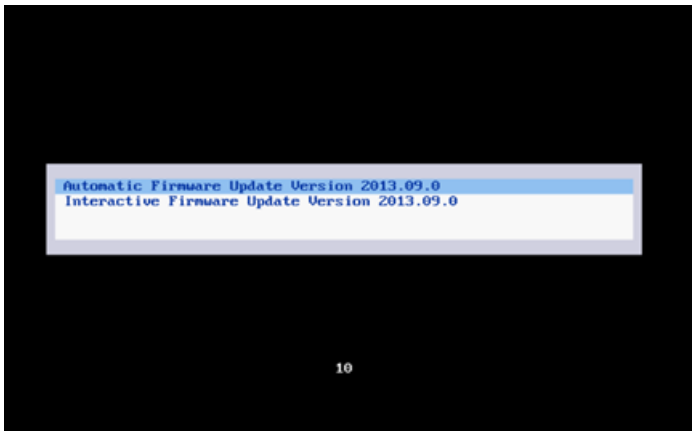
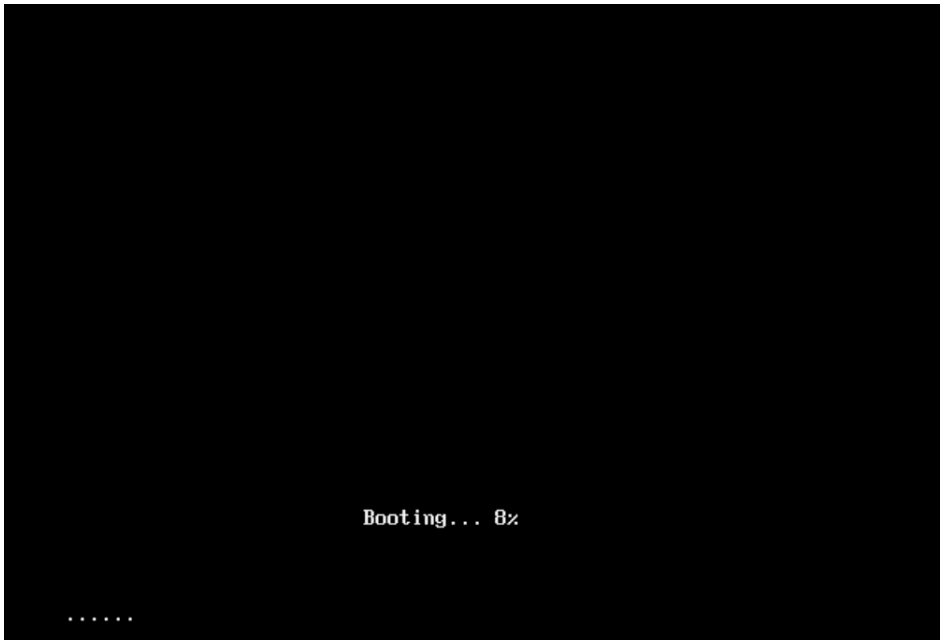
2. ☐	**Server's iLO Manager Remote Console:** System Health Check for ProLiant Servers	HP RMS Servers have been delivered to site with pre-installed software and firmware. This procedure beigns by accessing the cli using the remote console of the iLO and running a "syscheck" before confirming the updated firmware. A "syscheck" will have already been performed during hardware verification.
		
		1. Access the command prompt using iLO's remote console and login to the server as "*root*" then switch to the root user:
		
		`[root@yhu-cmp ~]# syscheck`
		
		2. Verify system health is normal by running the **syscheck** command.
		
		`[root@yhu-cmp ~]# syscheck`
		`Running modules in class disk...`
		`OK`
		`Running modules in class hardware...`
		`OK`
		`Running modules in class net...`
		`OK`
		`Running modules in class proc...`
		`OK`
		`Running modules in class system...`
		`OK`
		`Running modules in class upgrade...`
		`OK`
		`LOG LOCATION: /var/TKLC/log/syscheck/fail_log`
		`[root@yhu-cmp ~]#`
		
		If all checks return "***OK***" then proceed with next step, but in case of failures, the failed tests and reasons need to be analyzed and corrected before continuing. Contact Tekelec/oracle support if needed.

3. ☐	**Server's iLO Manager Remote Console:** Check the iso image md5sum	Be sure to validate all image files with the md5sum command to assure the output key is the same as the one provided with the original software. For example: md5sum 872-2488-106-2.2.5_10.37.0-FW_SPP .iso should return MD5 Signature: **c25beedb09375a23077bd32301a81014**
4. ☐	**Server's iLO Manager Remote Console:** Mount the firmware iso image file	Mount the firmware iso image according to the steps outlined in Appendix B or C based on the hardware used

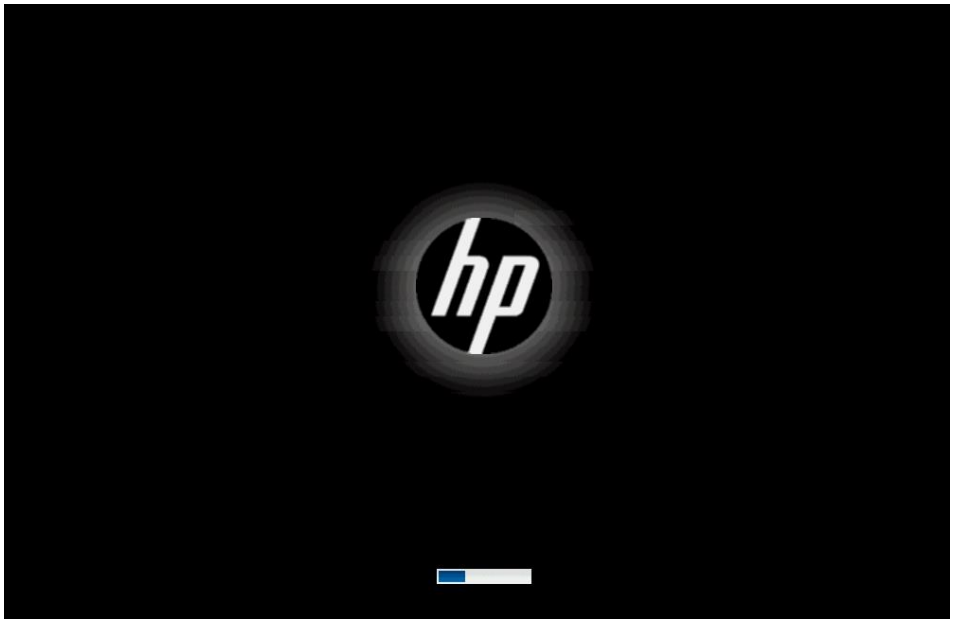
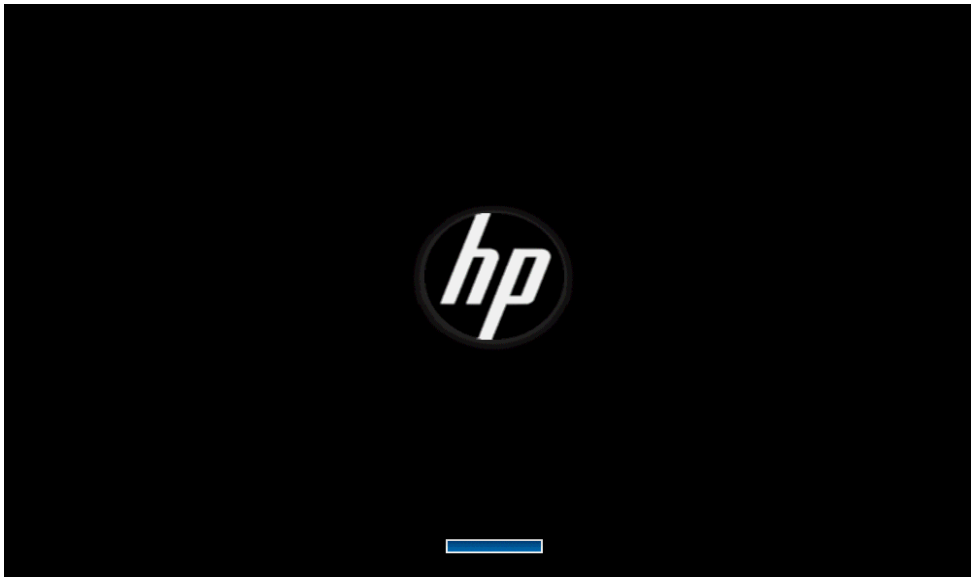
Procedure 1. Update Servers' Firmware

5. ☐	**Server's Remote Console:** Reboot the server	In the remote console, log into the server as root if needed, and run: # **shutdown –r now** Alternatively a **reset** for the server to reboot can be performed from the remote console as follows: 

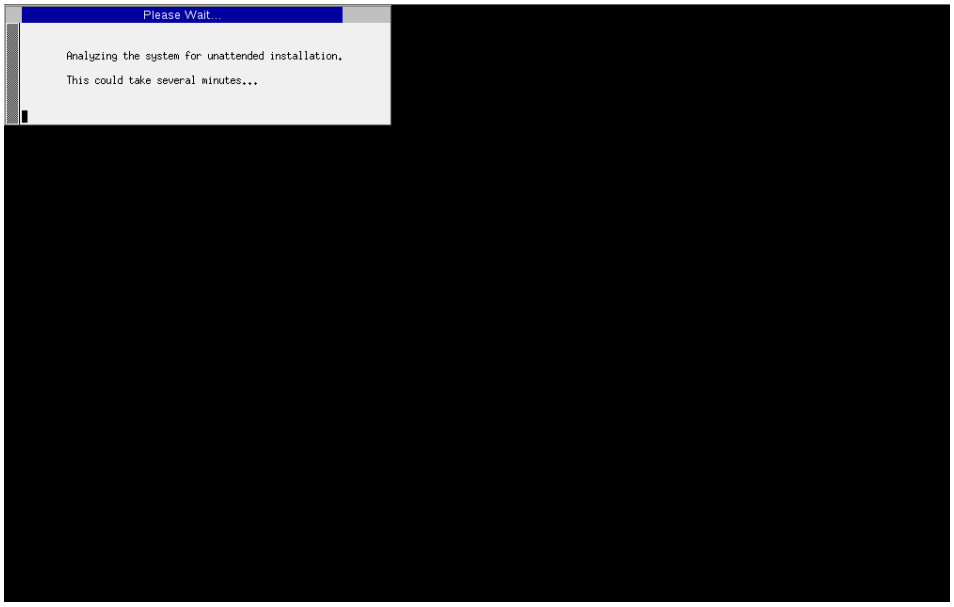
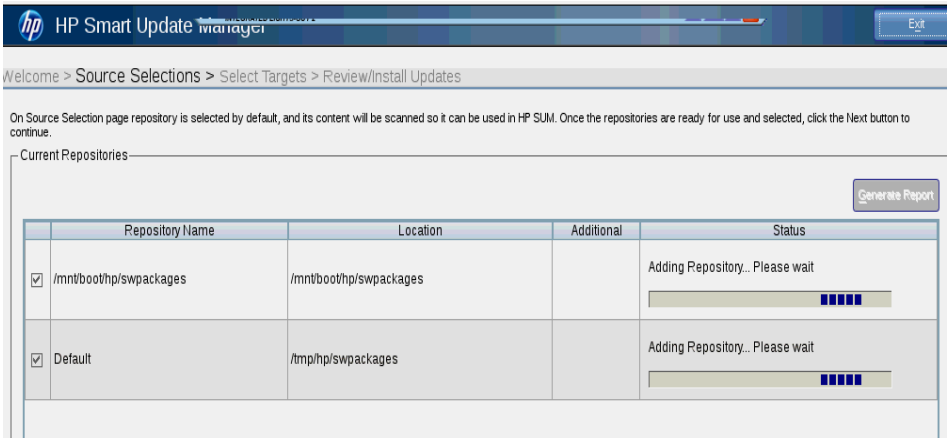
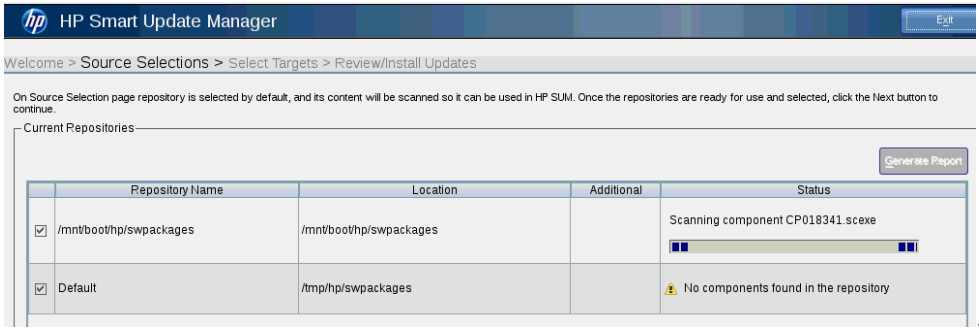
Procedure 1. Update Servers' Firmware

6. ☐	**Server's Remote Console:** Initial splash screens	The server will reboot from the mounted HP Service Pack for ProLiant 2.2.5 ISO image and following boot prompt shall be displayed:  Press **[Enter]** to select the **Automatic Firmware Update** procedure or wait for 30 seconds then the system will automatically proceed via the default Automatic Firmware Update highlighted option Screen shall display booting progress percentage as follows: 

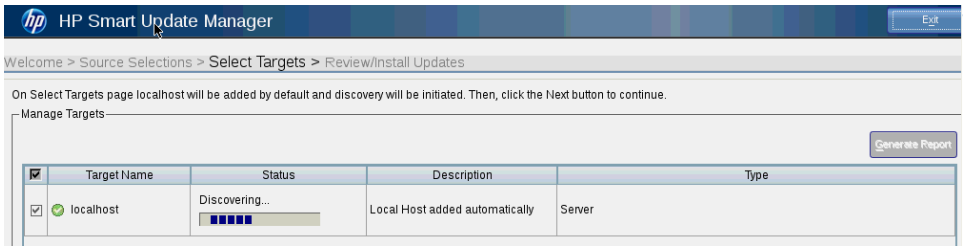
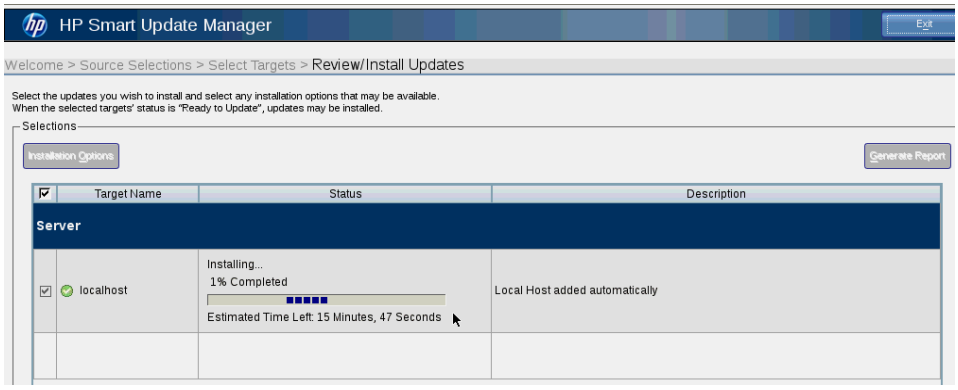
Procedure 1. Update Servers' Firmware

7. ☐	**Server's Remote Console:** System analysis	Once the system has booted to the firmware installation image, a system scan of the server in which it will identify all of the firmware components that are eligible for upgrade. This process may take 10-20 minutes up to more than thirty mins depending on the speed of the network connection being used. *The entire upgrade can take up to more than two hours with a very slow network connection but the upgrade will eventually complete*. **Be patient and do not attempt to interrupt the process.**   When the previous splash screen progress bar completes you will see the console session go blank for several minutes. **Be patient and do not attempt to interrupt the process.**

Procedure 1. Update Servers' Firmware

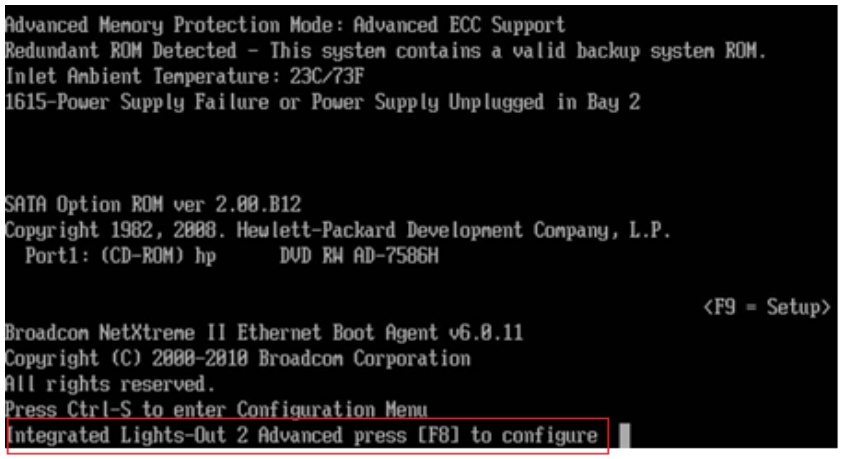
8. ☐	**Server's Remote Console:** System analysis (continued) Smart Upgrade Manager launches	 Smart Upgrade Manager launches and sources selections are being collected and added to repository:  Some components may not need upgrade as the following example snapshot indicates: 

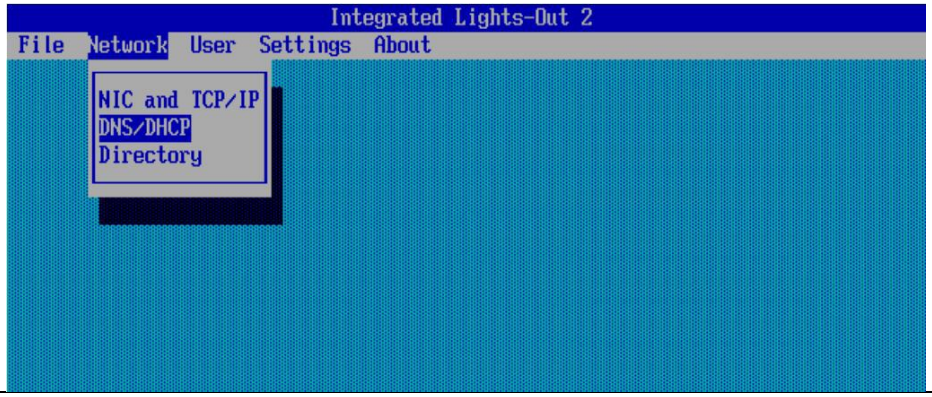
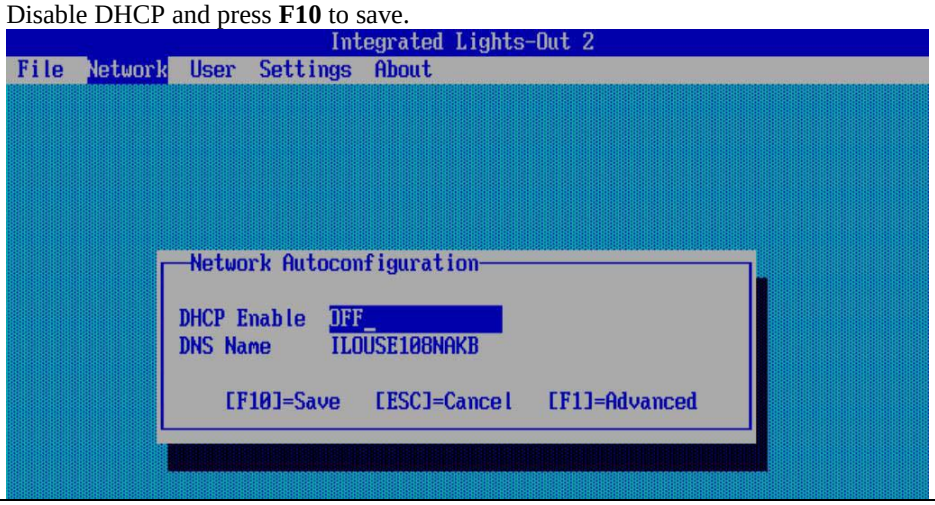
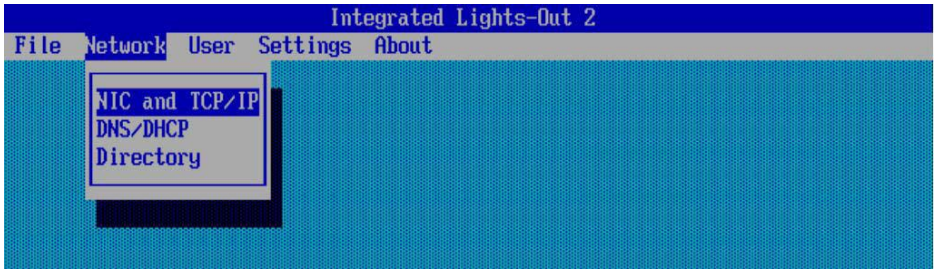
Procedure 1. Update Servers' Firmware

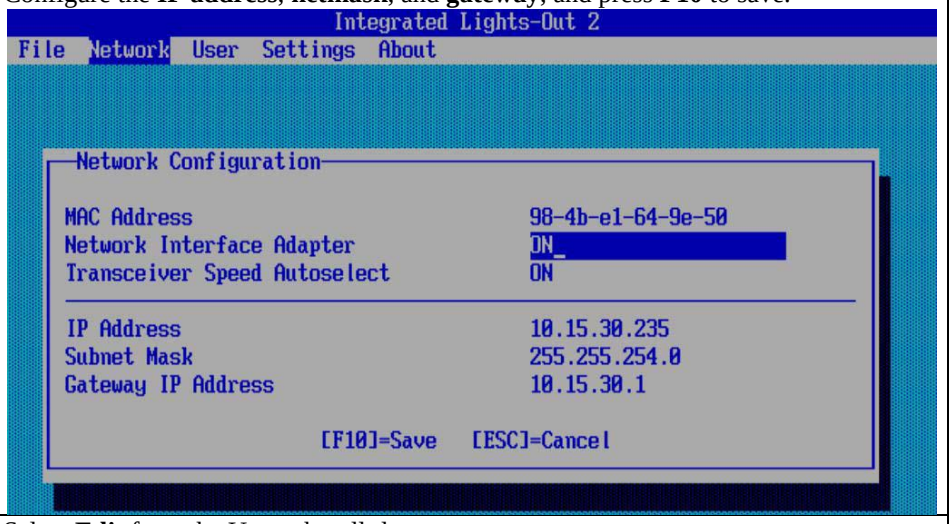
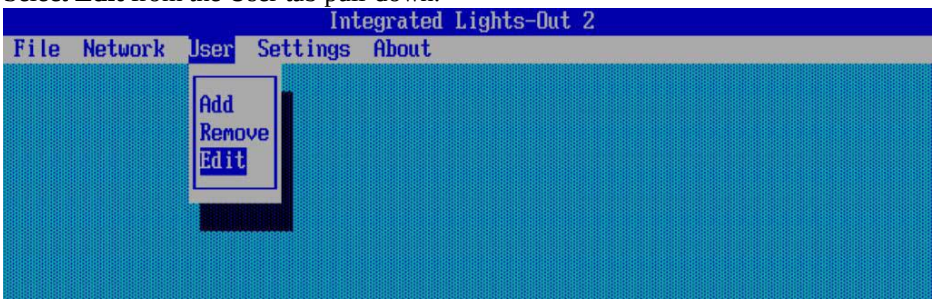
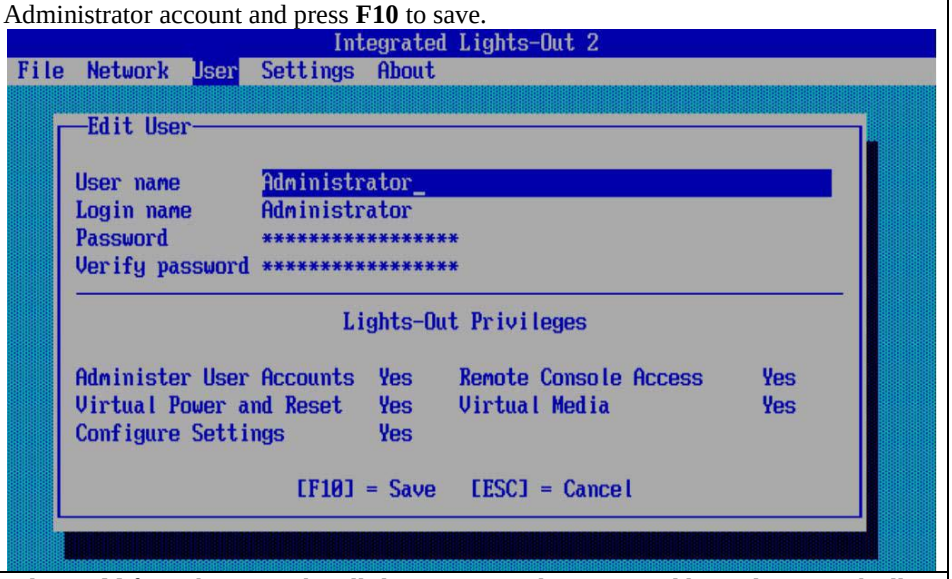
9. ☐	**Server's Remote Console:** Select Targets AND INSTALLATION	Once analysis and sources selection phase is completed, the HP Smart Upgrade Manager will begin select the targets firmware components eligible for upgrade  Then actual installation of components to be upgraded is started:  **Note**: The server will reboot after the firmware upgrade has been completed. **You must unmount the iso image in the remote console menu or the server will reboot into the firmware upgrade iso once again and attempt to repeat the upgrade.**
THIS PROCEDURE HAS BEEN COMPLETED		

Procedure 2: Configure Server's iLO Port

Procedure 1: Configure Server's iLO Port from Boot Menu

S T E P #	This procedure will configure the iLo Port IP address from the Console Boot Menu. Note: Initial iLO configuration will have been performed by Tekelec/Oracle. This configuration (ip address and user access) can be confirmed using the plastic tab located on the front of the server Note: It is also possible to change the ip address and setup user accounts from within the iLO GUI once the initial configuration has been performed and the user is logged into the iLO GUI. This procedure only covers the initial configuration in the case iLO access needs to be configured for the first time. **Needed material:** - IP Addresses from the Network IP Planning document (or other customer provided document) - Console Access (Monitor/Keyboard) or via remote access to server's iLO	
1. ☐	**Server's Console or iLO web page:** connect to console	Connect to the console locally or via iLO web page remotely
2. ☐	**Server's Console:** reboot server	reboot the server: either use button press, or via the command: # **shutdown -r now**
3. ☐	**Server's Console:** Enter iLo configuration menu	As the server is completing its POST startup, you will see the message: <Integrated Lights-Out 2 Advanced press [F8] to configure> in case DL360 HW is used  OR <iLO4 Advanced press [F8] to configure> in case DL380 HW is used at the bottom of the screen.

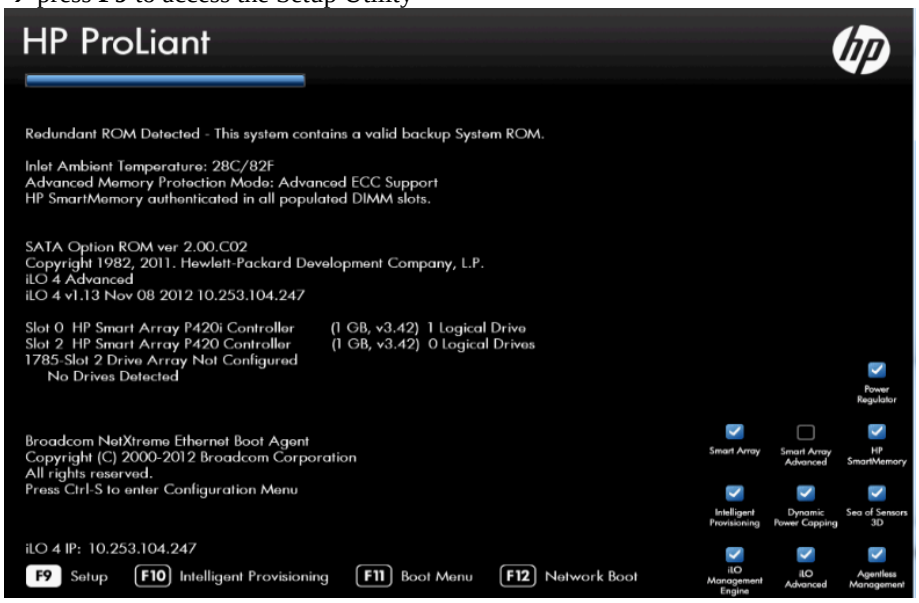
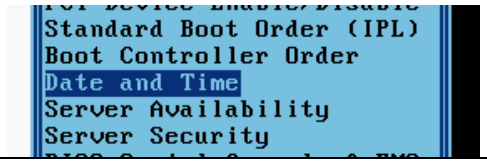
		 → Quickly press **F8** to access the iLO configuration menu
4. ☐	**Server's Console:** Access DHCP setting form	Select **DNS/DHCP** from the Network tab pull-down. 
5. ☐	**Server's Console:** Configure DHCP Off Press F10 to save	Disable DHCP and press **F10** to save. 
6. ☐	**Server's Console:** Access IP address form	Select **NIC and TCP/IP** from the Network tab pull-down. 

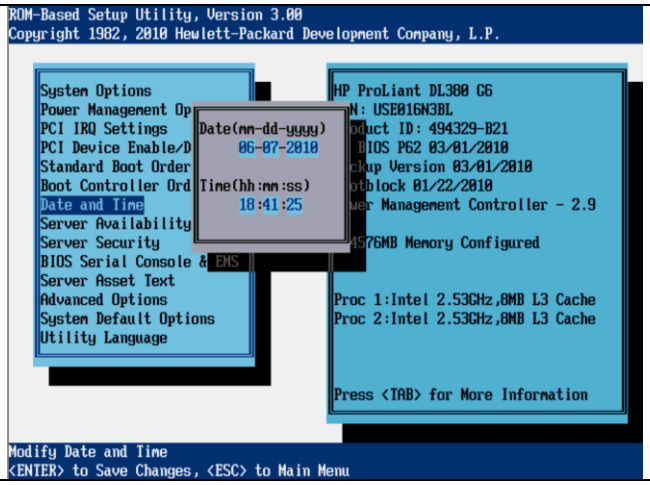
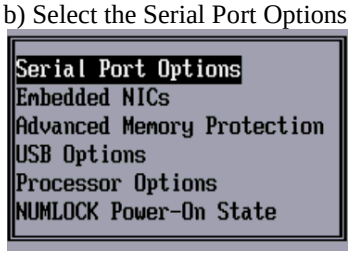
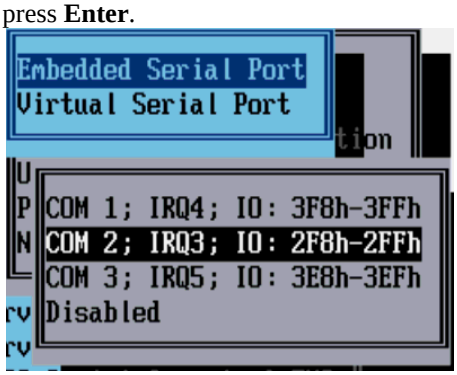
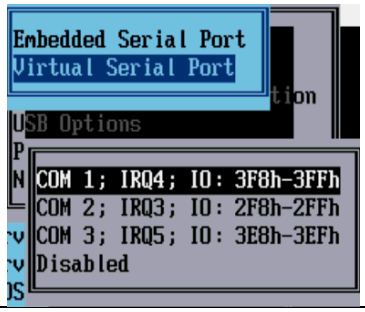
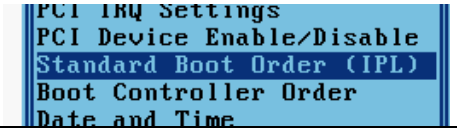
7. ☐	**Server's Console:** Configure IP address for iLo port, Press F10 to save	Configure the **IP address**, **netmask**, and **gateway**, and press **F10** to save. 
8. ☐	**Server's Console:** Access User Edit form	Select **Edit** from the User tab pull-down. 
9. ☐	**Server's Console:** Configure Administrator password, press F10 to save	Configure a Password as provided by an appropriate authority for the default Administrator account and press **F10** to save. 
10. ☐	**Server's Console:** Add additional user, and password if required.	Select **Add** from the User tab pull-down menu and create an additional user, with all privileges set to yes and an appropriate password Press **F10** to save.
11. ☐	**Server's Console:** Exit the configuration	Exit the configuration utility. Server will proceed with OS boot.

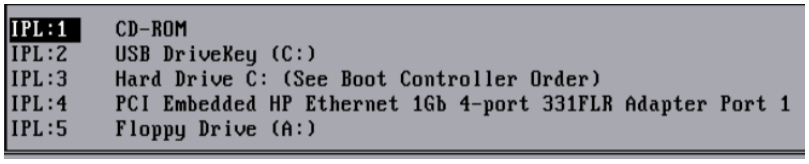
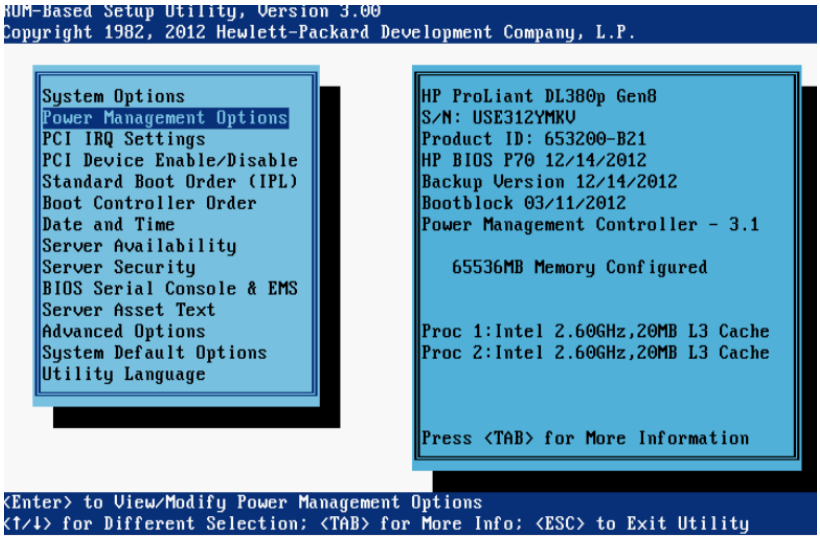
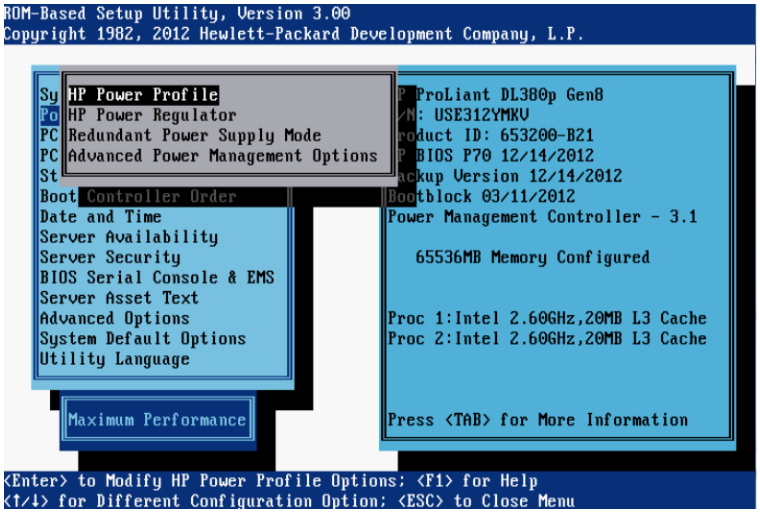
THIS PROCEDURE HAS BEEN COMPLETED

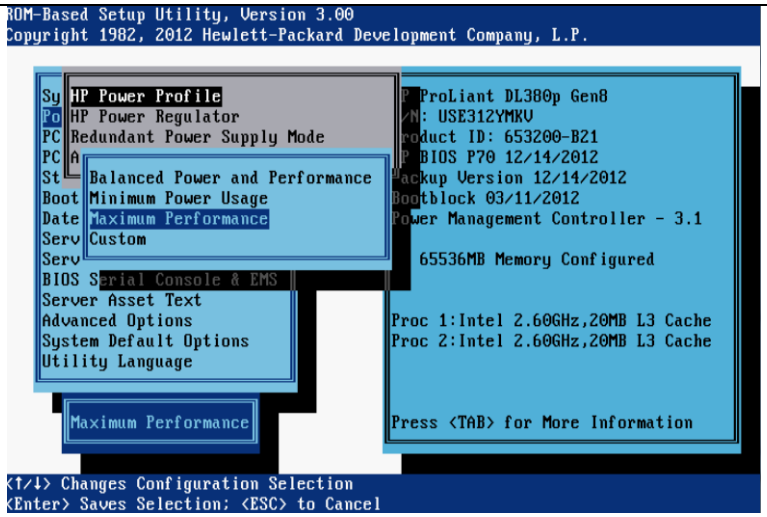
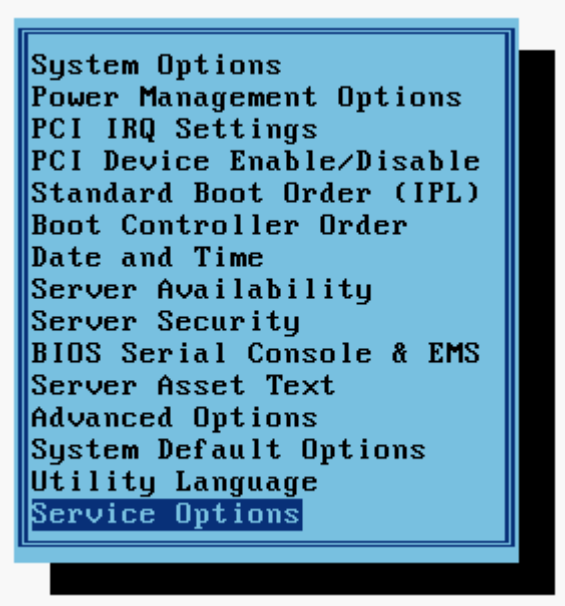
Procedure 3: Configure BIOS

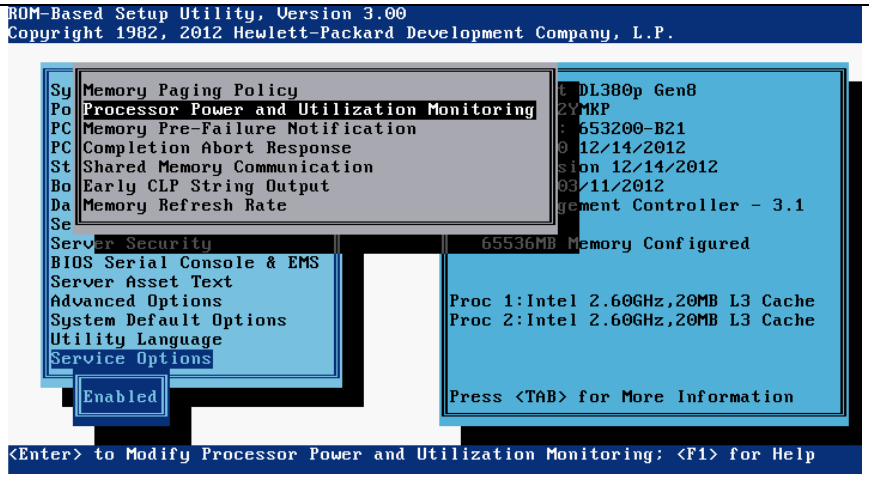
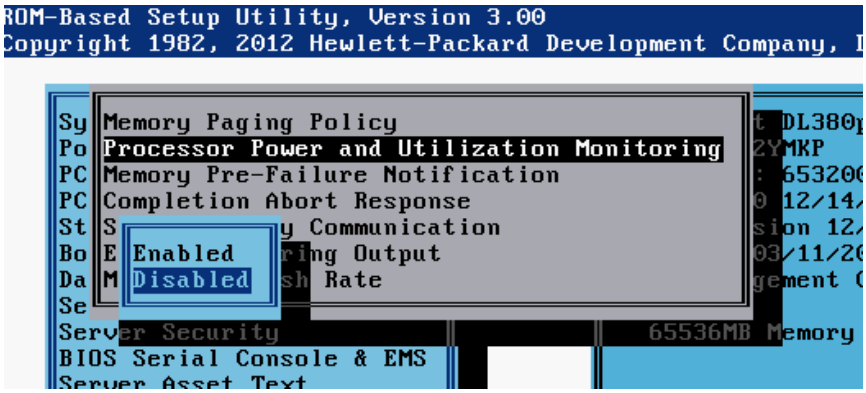
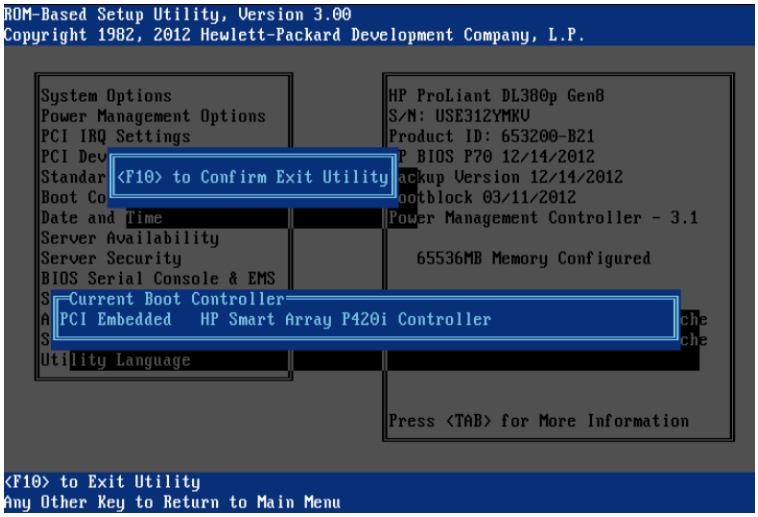
Procedure 3: Configure BIOS

S T E P #	This procedure will configure the RMS SERVERS' BIOS. BIOS configuration may have been preconfigured by Tekelec/Oracle but should be confirmed using this procedure Note: It is known that step 10 of this procedure "Set the Power Profile to Maximum Performance " will not yet have been configured in advance by Tekelec./Oracle and will have to be configured as part of this confirmation check.	
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 Remote Console) Reference the procedures at the end of this document (Appendix B or C) based on the hardware used to start the remote console of the server via iLO web interface page
2. ☐	**Server's Console:** reboot server	reboot the server: either through remote console's reset button, or use this command form the cli/remote console: # **shutdown -r now**
3. ☐	**Server's Console:** Enter Setup configuration menu (F9)	As the server is completing its POST startup, you will see the message: Press F9 to access BIOS settings. → press **F9** to access the Setup Utility 
4. ☐	**Server's Console:** Select Date and Time	Scroll down until you see Date and Time, and press **Enter**. 
5. ☐	**Server's Console:** Set Date and Time	Set the date and time, according to UTC, and press **Enter**. For example:

		
6. ☐	**Server's 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**. 
7. ☐	**Server's Console:** Select Standard Boot Order menu	Return to the main menu, select **Standard Boot Order**, and press **Enter** . 

8. ☐	**Server's Console:** Set Standard Boot Order	Validate the boot order and modify as needed. • CD-ROM should be 1st in case the ISO image would be on a CD-ROM . • In servers that do not have CD-ROM drive , USB that has ISO image can be used instead so USB should be 1st in this case in the boot order list • If mounting the ISO image via iLO remote console is used in installation then this step should be skipped.  Press **Esc** to return to the main menu.
9. ☐	**Server's Console:** Select Power Management Options menu	Select Power Management Options and press **Enter**.  Select HP Power Profile and press **Enter**. 
10. ☐	**Server's 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 return to the Main Menu.
11. ☐	**Server's Console: Set** "Processor Power and Utilization Monitoring." to disable	From the Main Menu **Press "Control+A".** This will reveal an additional menu option: "Service Options". 
12. ☐	**Server's Console: Set** "Processor Power and Utilization Monitoring." to disable	Select "Service Options" and scroll down to "Processor Power and Utilization Monitoring." The default setting is "Enabled".

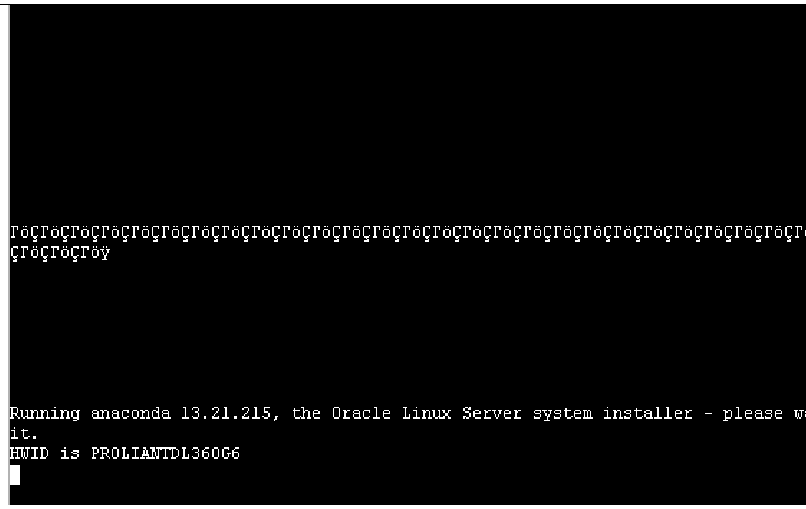
<table>
<tr><td></td><td></td><td> 
</td></tr>
<tr><td>13.
☐</td><td>Server’s Console: Set "Processor Power and Utilization Monitoring." to disable</td><td>Select "Processor Power and Utilization Monitoring." and change the default option of “enabled” to “disabled”.
 
</td></tr>
<tr><td>14.
☐</td><td>Server’s Console: Exit the Setup Utility</td><td>Press Esc until you are prompted to Confirm Exit Utility.
<F10> to confirm Exit of Utility and save configuration changes and reboot
 
</td></tr>
<tr><td colspan="3">THIS PROCEDURE HAS BEEN COMPLETED</td></tr>
</table>

3.2 TPD Installation

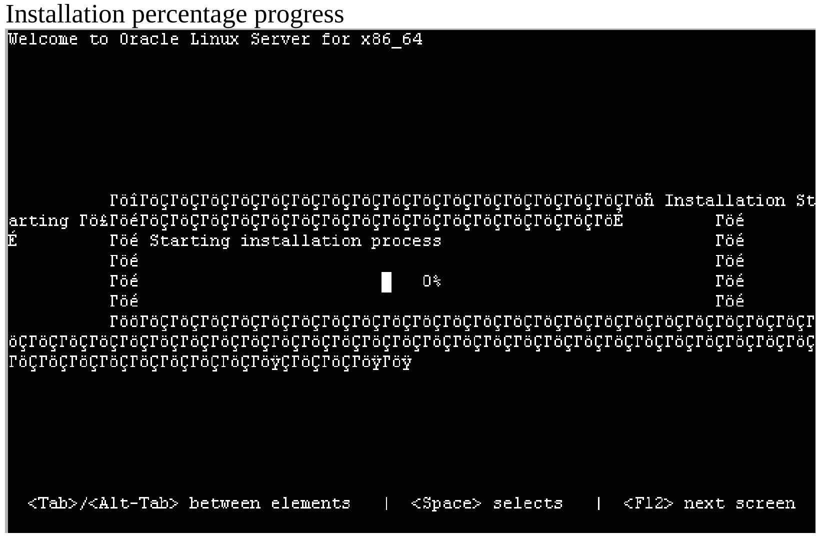
Procedure 4: Install OS of RMS Server

Procedure 4: Install OS of RMS Server

S T E P #	Policy Application 11.5 uses TPD 6.7. TPD 6.7 requires a fresh install as documented in this procedure. This will reformat the hard drive after which the 11.5 Policy Applications will be installed. This procedure will install the TPD platform and 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) - TPD iso image file.	
1. ☐	**Server's iLO Manager Remote Console:** Launch the remote console	Reference the procedures at the end of this document (Appendix B or C) based on the hardware used to start the remote console of the server via iLO web interface page and mount the TPD ISO image
2. ☐	**Console:** Boot server, wait for TPD boot:	Once the iso image file has been mounted using the remote console of the iLO, reboot the server with <shutdown –r now> from the cli. Upon reboot to the mounted image file to install the TPD platform the following window is displayed: Release: 6.7.0.0.1_84.17.0 Arch: x86_64 For a detailed description of all the supported commands and their options, please refer to the Initial Platform Manufacture document for this release. In addition to **linux** & **rescue** TPD provides the following kickstart profiles: [TPD ¦ TPDnoraid ¦ TPDblade ¦ TPDcompact ¦ HDD] Commonly used options are: [console=<console_option>[,<console_option>]] [primaryConsole=<console_option>] [rdate=<server_ip>] [scrub] [reserved=<size1>[,<sizeN>]] [diskconfig=HWRAID[,force]] [drives=<device>[,device]] [guestArchive]
3. ☐	**Console:** Enter TPD boot: command with correct options TPD install takes 20 - 30 minutes to complete	Install the TPD platform using the following command at the "boot:" prompt. For HP RMS H/W: boot: **TPDnoraid diskconfig=HPHW,force console=tty0** For Sun Netra H/W: boot: **TPDnoraid console=tty0** The TPD installation takes 20 - 30 minutes to complete, during which, you will view several messages and screens in the process like the following samples:

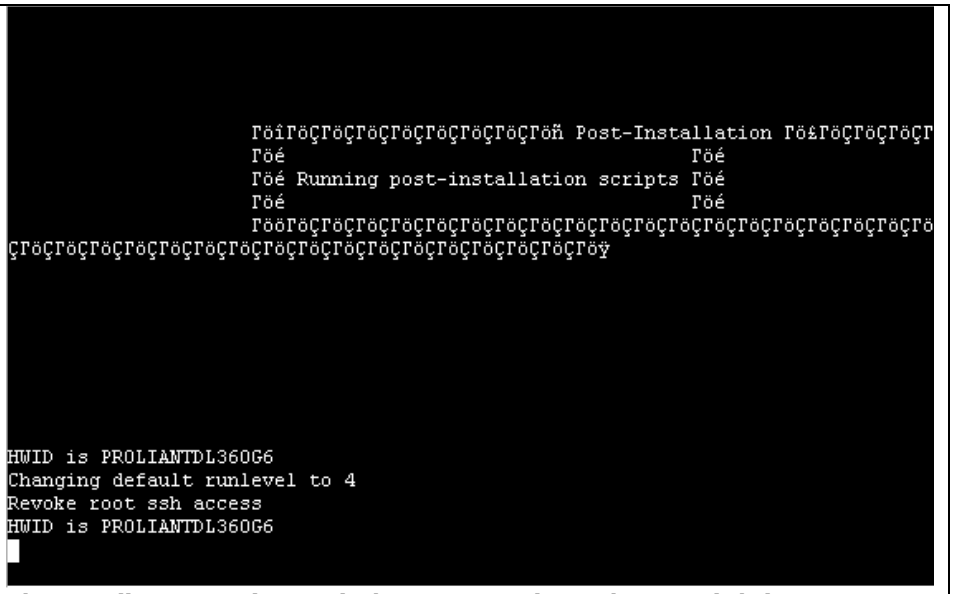


Installation percentage progress



Packages installation:

Post installation scripts:

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


Then installation completes and reboot is required as in the example below :

</td>
</tr>
<tr>
<td>4.
☐</td>
<td>Console: Press Enter to reboot</td>
<td>
Unmount the iso image from the iLO remote console and press Enter to reboot the server. .

Note: In the case the iso image was not unmounted before this reboot was performed, you will be prompted as if the TPD image is to be installed as in the initial screen of this procedure. Rather than reinstall TPD a second time, make sure the iso image has been unmounted this time and reboot again.

Following sample shows server boot from the installed TPD:
</td>
</tr>
</table>

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

```
   GNU GRUB  version 0.97  (637K lower / 3658876K upper memory)

 +-------------------------------------------------------------------------+
 | TPD (2.6.32-431.11.2.el6prerel6.7.0.0.1_84.15.0.x86_64)                 |
 |                                                                         |
 |                                                                         |
 |                                                                         |
 |                                                                         |
 |                                                                         |
 |                                                                         |
 |                                                                         |
 |                                                                         |
 |                                                                         |
 |                                                                         |
 |                                                                         |
 +-------------------------------------------------------------------------+
      Use the ^ and v keys to select which entry is highlighted.
      Press enter to boot the selected OS or 'p' to enter a
      password to unlock the next set of features.


  The highlighted entry will be booted automatically in 5 seconds.
```

</td>
</tr>
<tr>
<td>5.
☐</td>
<td>Console: Login as root</td>
<td>

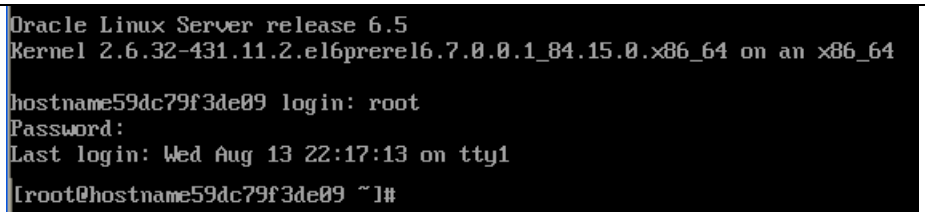
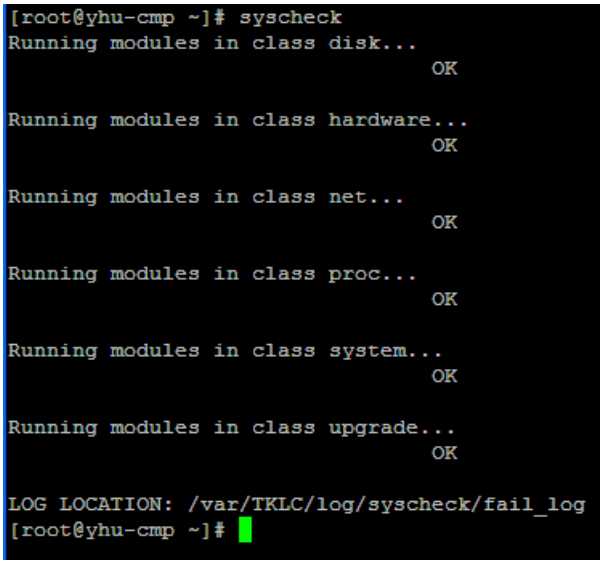
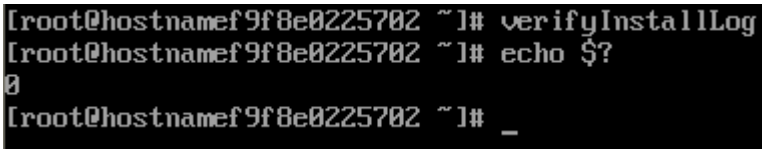
After the server boots from the installed TPD, some steps will be performed during which server will reboot couple of times :

```
######################
1407461721: Upstart Job killall: starting
1407461721: Upstart Job killall: started
######################



######################
1407461721: Upstart Job reboot: starting
Sending all processes the TERM signal... [  OK  ]
Sending all processes the KILL signal... [  OK  ]
Saving random seed:  [  OK  ]
Syncing hardware clock to system time [  OK  ]
Turning off quotas:  [  OK  ]
Unmounting file systems:  [  OK  ]
init: Re-executing /sbin/init
Please stand by while rebooting the system...
e1000e 0000:07:00.1: PCI INT A disabled
e1000e 0000:07:00.0: PCI INT B disabled
e1000e 0000:06:00.1: PCI INT A disabled
e1000e 0000:06:00.0: PCI INT B disabled
Restarting system.
machine restart
```

```
sending termination signals...done
sending kill signals...done
disabling swap...
unmounting filesystems...
        /mnt/runtime done
        disabling /dev/loop0
        /dev/pts done
        /selinux done
        /mnt/sysimage/boot done
        /mnt/sysimage/dev/pts done
        /mnt/sysimage/dev/shm done
        /mnt/sysimage/dev done
        /mnt/sysimage/proc/bus/usb done
        /mnt/sysimage/proc done
        /mnt/sysimage/sys done
        /mnt/sysimage/tmp done
        /mnt/sysimage/usr done
        /mnt/sysimage/var/TKLC done
        /mnt/sysimage/var done
        /mnt/sysimage/selinux done
        /mnt/sysimage done
waiting for mdraid sets to become clean...
rebooting system
```

Then the installation would be complete and a login prompt occurs

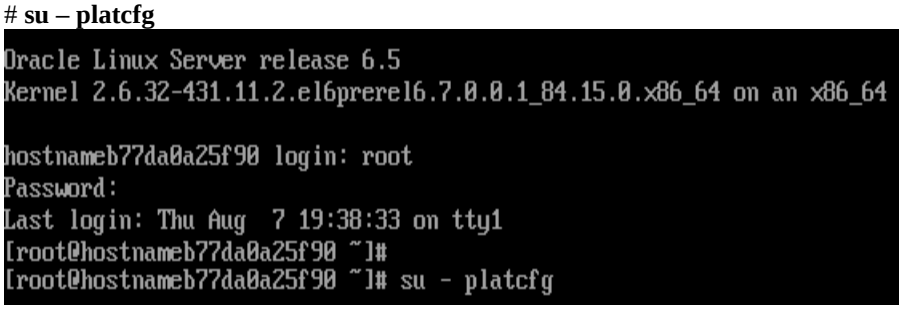
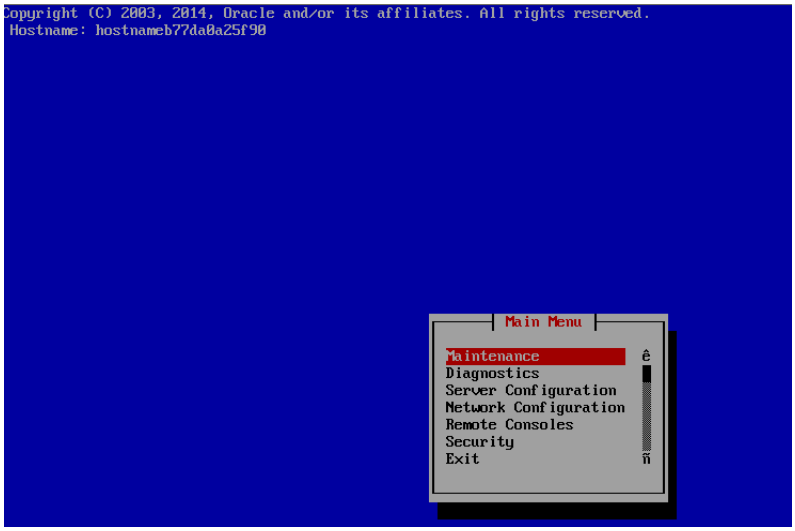
</td>
</tr>
</table>

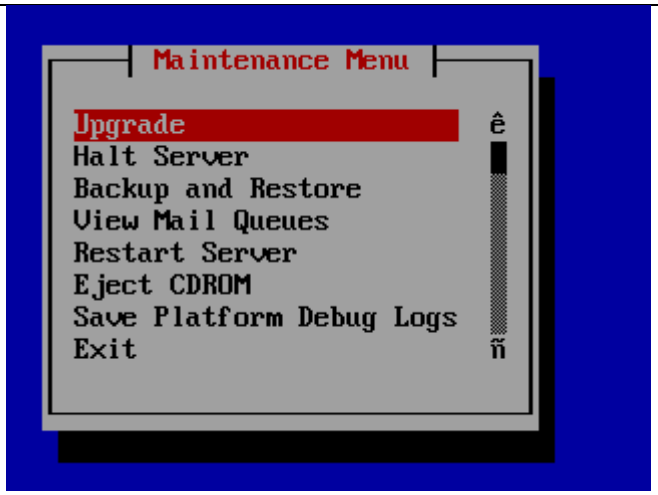
		 Login as root.
6. ☐	**Console:** Run syscheck	At the login prompt, log in as user "root" and execute <syscheck> from the cli prompt. The system health check begins automatically. This checks the health of each of the major subcomponents of the system, and displays an "OK" if all passed, or a descriptive 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.  As NTP has not yet been configured you may get an "ntp" failure error. This can be ignored as NTP will be configured later. If any of the modules returns an error other than NTP, wait a minimum of 5 minutes and re-execute a system check a second time.. If syscheck error persists, do not continue; contact Customer Support and report the error condition.
7. ☐	**Console:** Verify Install success	Verify that the TPD installation completed successfully by checking the install logs for errors. To do this, log in as **root** and then run the following commands: # **verifyInstallLog** # **echo $?**  **This should return "0".** If no errors are present, the TPD installation process is completed. If errors are found, contact Customer Support.
8. ☐	**Console:** Verify Install success	Verify the TPD platform version by executing <getPlatRev> from the cli. For example:

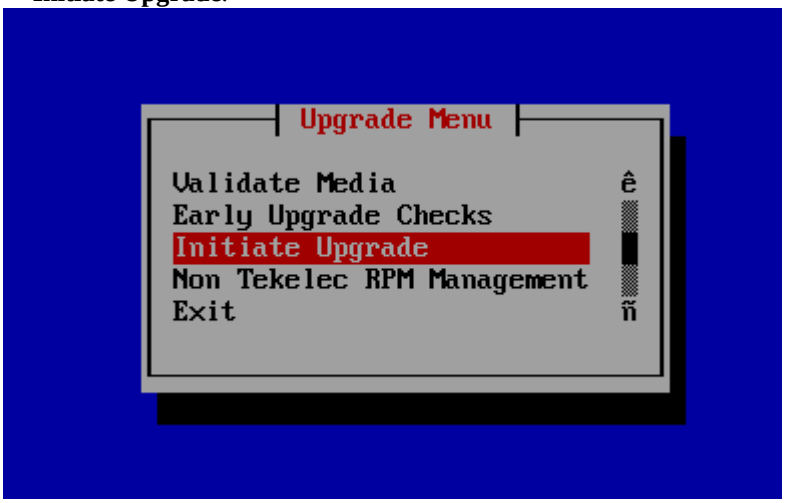
		[root@hostnamef9f8e0225702 ~]# getPlatRev 6.7.0.0.1-84.17.0 [root@hostnamef9f8e0225702 ~]# _
THIS PROCEDURE HAS BEEN COMPLETED		

Procedure 5: Install Application Software (RMS)

Procedure 5: RMS Application Software Installation

S T E P #	This procedure will install the 11.5 PCRF Cable Application components. **Needed material:** GA Policy software iso images (CMP, MPE, BOD, MA).	
1. ☐	**Server's iLO Manager Remote Console:** Prepare the policy component's ISO image for the upgrade	Mount the Policy Software iso image according to the steps outlined in Appendix B or C based on the hardware used. Alternatively you may copy over the ISO image to the upgrade path locally on the server as outlined in Appendix D ***Note***: The installation from within the local upgrade path as outlined in Appendix D is recommended for the latency of the process in case remote mounting method is used.
2. ☐	**Console:** run platcfg	Start the Platcfg utility by issuing the following command: # **su – platcfg**  From within the platcfg utility, navigate to **Maintenance**  ➤ **Upgrade**

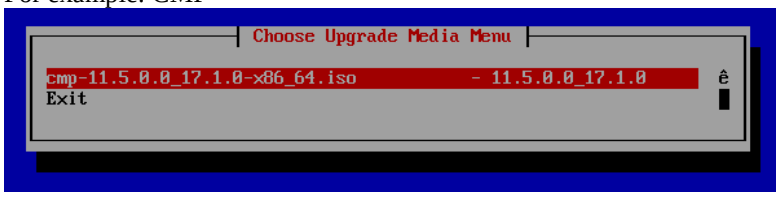
<table>
<tr>
<td></td>
<td></td>
<td>


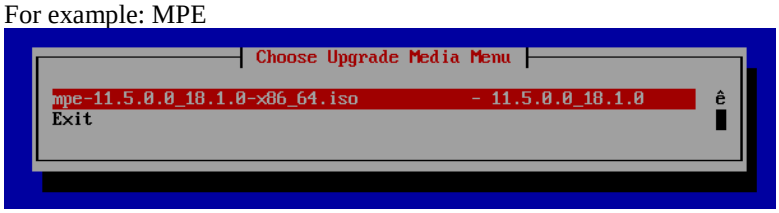
➤ Initiate Upgrade.


</td>
</tr>
<tr>
<td>3.
☐</td>
<td>Console: Select ISO to install, and confirm

Application install may take 20 Minutes</td>
<td>
Select the iso image from the Media Menu, and select OK.
Software Install may take 20 Minutes.

Note: There are separate image files for the CMP / MPE / BOD / MA. Make sure the correct image is present.

For example: CMP


For example: MPE


Note: The cmp (or mpe/ma/bod) servers will reboot during the installation process, As you are logged into the iLO you will see several screens as well as the reboot like in the following samples:
</td>
</tr>
</table>

The start of the installation will begin with some upgrade checks :

```
Running earlyUpgradeChecks() for Upgrade::EarlyPolicy::TPDEarlyChecks upgrade policy...
Verified server is not pending accept of previous upgrade
Hardware architectures match
Install products match.
No Application installed yet.. Skip alarm check!
Early Upgrade Checks Have Passed!
Initializing upgrade information...
The runlevel transition complete RC file was created as /etc/rc3.d/S99smartd_runlevel_transition_complete.
Changing to run-level 3...
```

Platform revision that being installed and back-out information details:

```
Changing platform revision so must upgrade
Determining the appropriate upgrade command...
Variable "$ugwrap" will not stay shared at /mnt/upgrade/upgrade/lib/UGWrap/QPSchemaUpgrade.pm line 429.
Subroutine new redefined at /mnt/upgrade/upgrade/lib/UGWrap/QPSchemaUpgrade.pm line 498.
Subroutine DESTROY redefined at /mnt/upgrade/upgrade/lib/UGWrap/QPSchemaUpgrade.pm line 512.
Using /mnt/upgrade/upgrade/ugwrap as the upgrade command

    Current platform version:  6.7.0.0.1-84.17.0
 No backout release boundary:  5.0.0-0.0.0
/mnt/upgrade/upgrade/lib/upgrade.sh: line 519: cmpVersions: command not found

Backout will be supported...

Running prepareUpgrade() for Upgrade::Policy::Platform upgrade policy...
Preserving files so verifyUpgrade can run.
preserveVerifyUpgradeFiles(): File does not exist!
FILE: /mnt/upgrade/upgrade/etc/multiRpmsAllowed.sed Skipping...
Adding /usr/TKLC/plat/etc/alarms/alarms.xml to BCS...
Adding /usr/TKLC/plat/etc/alarms/alarms.dtd to BCS...
Adding /usr/TKLC/plat/lib/Syscheck/modules/proc/ntp/config to BCS...
Running prepareUpgrade() for Upgrade::Policy::HP upgrade policy...
Running prepareUpgrade() for Upgrade::Policy::MBL upgrade policy...
Running prepareUpgrade() for Upgrade::Policy::QPBondConfig upgrade policy...
Running prepareUpgrade() for Upgrade::Policy::QPFirewallFixes upgrade policy...
Running prepareUpgrade() for Upgrade::Policy::QPIPv6Fixes upgrade policy...
Running prepareUpgrade() for Upgrade::Policy::QPJDKPolicy upgrade policy...
Running prepareUpgrade() for Upgrade::Policy::QPMySQLPolicy upgrade policy...
Running prepareUpgrade() for Upgrade::Policy::QPNTPFixes upgrade policy...
Running prepareUpgrade() for Upgrade::Policy::QPRunPostRPMActionsPolicy upgrade policy...
Running prepareUpgrade() for Upgrade::Policy::PlatformLast upgrade policy...
Initializing upgrade...
Verify BCS repository and checkin files...
```

RPMs installation:

```
Loading Backout::BackoutType::RPM
Setting up for backout.
Cleaning backout directory.
Copying locale archive template to backout directory.
Generating dependency whiteout partlet...
Rebuilding /etc/rpm/macros...
Adding /usr/TKLC/plat/etc/rpm.d/plat.begin to /etc/rpm/macros...

Adding /usr/TKLC/plat/etc/rpm.d/plat.alarmMgr.macro to /etc/rpm/macros...
                                                          [  OK  ]
Adding /usr/TKLC/plat/etc/rpm.d/plat.core-complex.macro to /etc/rpm/macros...
                                                          [  OK  ]
Adding /usr/TKLC/plat/etc/rpm.d/plat.core.macro to /etc/rpm/macros...
                                                          [  OK  ]
Adding /usr/TKLC/plat/etc/rpm.d/plat.dep_whiteout.macro to /etc/rpm/macros...
                                                          [  OK  ]
Adding /usr/TKLC/plat/etc/rpm.d/plat.genMethods.macro to /etc/rpm/macros...
                                                          [  OK  ]
Adding /usr/TKLC/plat/etc/rpm.d/plat.perl-TKLCplat.macro to /etc/rpm/macros...
                                                          [  OK  ]
Adding /usr/TKLC/plat/etc/rpm.d/plat.platcfg.macro to /etc/rpm/macros...
                                                          [  OK  ]
Adding /usr/TKLC/plat/etc/rpm.d/plat.SELinux-policy.macro to /etc/rpm/macros...
                                                          [  OK  ]
Adding /usr/TKLC/plat/etc/rpm.d/plat.service_conf.macro to /etc/rpm/macros...
                                                          [  OK  ]
Adding /usr/TKLC/plat/etc/rpm.d/plat.syscheck.macro to /etc/rpm/macros...
                                                          [  OK  ]
Adding /usr/TKLC/plat/etc/rpm.d/plat.TKLCalarms.macro to /etc/rpm/macros...
                                                          [  OK  ]
Adding /usr/TKLC/plat/etc/rpm.d/plat.TKLCbackuptk.macro to /etc/rpm/macros...
                                                          [  OK  ]
Adding /usr/TKLC/plat/etc/rpm.d/plat.TKLCplat.macro to /etc/rpm/macros...
                                                          [  OK  ]
Adding /usr/TKLC/plat/etc/rpm.d/plat.TPD-provd.macro to /etc/rpm/macros...
                                                          [  OK  ]
```

TPD ISO image validation:

```
Updating /etc/rpm/macros...

Now dispatching /mnt/upgrade/upgrade/ugwrap                [  OK  ]
Variable "$ugwrap" will not stay shared at /mnt/upgrade/upgrade/lib/UGWrap/QPSchemaUpgrade.pm line 429.
Subroutine new redefined at /mnt/upgrade/upgrade/lib/UGWrap/QPSchemaUpgrade.pm line 498.
Subroutine DESTROY redefined at /mnt/upgrade/upgrade/lib/UGWrap/QPSchemaUpgrade.pm line 512.
Initializing Upgrade Wrapper...
Validating Distribution...
Validating cdrom...
########
```

Adding Policy related operations to the Platform Management menu:

```
Set the following menus: PolicyFirewall to visible=1
qp_platcfg-1.3.0-11.5.0.0_17.1.0: Running qp_platcfg pre-install script...
qp_platcfg                  ##################################################
qp_platcfg-1.3.0-11.5.0.0_17.1.0: Running qp_platcfg post-install script...
Added QP configuration.
Set the following menus: QP to visible=1
Added PolicyCheckConfig configuration.
Set the following menus: PolicyCheckConfig to visible=1
Added PolicyCheckServer configuration.
Set the following menus: PolicyCheckServer to visible=1
Added PolicyInitialConfig configuration.
Set the following menus: PolicyInitialConfig to visible=1
Added PolicyExchangeKey configuration.
Set the following menus: PolicyExchangeKey to visible=1
Added PolicyRestartMgr configuration.
Set the following menus: PolicyRestartMgr to visible=1
Added PolicyBackupRestore configuration.
Set the following menus: PolicyBackupRestore to visible=1
Added PolicyRestore configuration.
Set the following menus: PolicyRestore to visible=1
Added PolicyBackup configuration.
Set the following menus: PolicyBackup to visible=1
Added PolicyBackupSchedules configuration.
Set the following menus: PolicyBackupSchedules to visible=1
Added PolicyBackupSettings configuration.
Set the following menus: PolicyBackupSettings to visible=1
Added PolicyBackupList configuration.
Set the following menus: PolicyBackupList to visible=1
Added PolicyServerBackup configuration.
Set the following menus: PolicyServerBackup to visible=1
Added PolicyServerRestore configuration.
Set the following menus: PolicyServerRestore to visible=1
Added PolicyBackupRemote configuration.
Set the following menus: PolicyBackupRemote to visible=1
Added PolicyClusterFileSync configuration.
Set the following menus: PolicyClusterFileSync to visible=1
Added PolicyConfigRoute configuration.
Set the following menus: PolicyConfigRoute to visible=1
Added PolicySaveLogs configuration.
Set the following menus: PolicySaveLogs to visible=1
Added PolicyDSCP configuration.
Set the following menus: PolicyDSCP to visible=1
```

Password account creation and removing anonymous user for MySql database:

```
A RANDOM PASSWORD HAS BEEN SET FOR THE MySQL root USER !
You will find that password in '/home/platcfg/.mysql_secret'.

You must change that password on your first connect,
no other statement but 'SET PASSWORD' will be accepted.
See the manual for the semantics of the 'password expired' flag.

Also, the account for the anonymous user has been removed.

In addition, you can run:

  /usr/bin/mysql_secure_installation

which will also give you the option of removing the test database.
This is strongly recommended for production servers.

See the manual for more instructions.

Please report any problems at http://bugs.mysql.com/

The latest information about MySQL is available on the web at

  http://www.mysql.com

Support MySQL by buying support/licenses at http://shop.mysql.com

New default config file was created as /usr/my.cnf and
will be used by default by the server when you start it.
You may edit this file to change server settings

WARNING: Default config file /etc/my.cnf exists on the system
This file will be read by default by the MySQL server
If you do not want to use this, either remove it, or use the
--defaults-file argument to mysqld_safe when starting the server
```

Upgrade completion message:

```
Updating modules.dep and map files for kernel: 2.6.32-431.3.1.el6prerel6.7.0.0.0_84.9.0.x86_64.
Enabling crashkernel boot parameter...
Looking for boot entries...
Searching boot entry 'TPD (2.6.32-431.11.2.el6prerel6.7.0.0.1_84.15.0.x86_64)' for 'crashkernel' parameter...
Boot entry 'TPD (2.6.32-431.11.2.el6prerel6.7.0.0.1_84.15.0.x86_64)' already contains 'crashkernel=128M'. Doi
Running postTransactions() for Upgrade::Policy::HP upgrade policy...
Running postTransactions() for Upgrade::Policy::MBL upgrade policy...
Running postTransactions() for Upgrade::Policy::QPBondConfig upgrade policy...
Running postTransactions() for Upgrade::Policy::QPFirewallFixes upgrade policy...
Running postTransactions() for Upgrade::Policy::QPIPv6Fixes upgrade policy...
Running postTransactions() for Upgrade::Policy::QPJDKPolicy upgrade policy...
Running postTransactions() for Upgrade::Policy::QPMySQLPolicy upgrade policy...
Running postTransactions() for Upgrade::Policy::QPNTPFixes upgrade policy...
Running postTransactions() for Upgrade::Policy::QPRunPostRPMActionsPolicy upgrade policy...
Running postTransactions() for Upgrade::Policy::PlatformLast upgrade policy...
Executing ldconfig
Updating RPM manifest file.
FILE: /usr/TKLC/plat/etc/upgrade/rpm_manifest.
Enabling applications on the server
Running prelink
Enabling applications on the server...
File cleanup.  MODE is --upgrade
FILE is /mnt/upgrade/upgrade/etc/upg_delete_these_files
Applications Enabled.
Running /usr/TKLC/plat/bin/service_conf reconfig

UPGRADE IS COMPLETE

/mnt/upgrade/upgrade/ugwrap  returned success!
Running postUpgrade() for Upgrade::Policy::Platform upgrade policy...
Restarting alarmMgr.
Setting Upgrade Accept/Reject alarm.
Updating MOTD.
/var/log/sun-ssm exists. No need to restore.
Running postUpgrade() for Upgrade::Policy::HP upgrade policy...
Running postUpgrade() for Upgrade::Policy::MBL upgrade policy...
Running postUpgrade() for Upgrade::Policy::QPBondConfig upgrade policy...
```

Rebooting:

```
IRC: hostnameb77da0a25f90 - HP iLO 2 Integrated Remote Console - Windows Internet Explorer
https://10.253.103.138/HRemCons.htm?fullscreen=0&restart=0
Restarting system.
```

After rebooting operations:

```
######################
1407620552: Upstart Job ntpd: starting
Starting ntpd: [  OK  ]
1407620552: Upstart Job ntpd: started
######################



######################
1407620552: Upstart Job regenMethods: starting
Generating perl methods: [  OK  ]
1407620553: Upstart Job regenMethods: started
######################



######################
1407620553: Upstart Job TPDsec: starting
Starting TPDsec:
Creating SSH User Keys: [  OK  ]
Creating SSL Certificate:
[  OK  ]
[  OK  ]
1407620554: Upstart Job TPDsec: started
######################



######################
1407620554: Upstart Job upgrade: starting
1407620554:: Running mountCDROM to mount upgrade media.
1407620554:: Trying to mount /dev/sr1, on /mnt/upgrade
mount: you must specify the filesystem type
1407620569:: No media found on device /dev/sr1. Trying next device..
1407620569:: Trying to mount /dev/sr0, on /mnt/upgrade
mount: block device /dev/sr0 is write-protected, mounting read-only
1407620572:: We found a UUID match on /dev/sr0!
1407620572:: Running upgrade_dispatcher...
```

Continue upgrade:

```
1407620554: Upstart Job upgrade: starting
1407620554:: Running mountCDROM to mount upgrade media.
1407620554:: Trying to mount /dev/sr1, on /mnt/upgrade
mount: you must specify the filesystem type
1407620569:: No media found on device /dev/sr1. Trying next device..
1407620569:: Trying to mount /dev/sr0, on /mnt/upgrade
mount: block device /dev/sr0 is write-protected, mounting read-only
1407620572:: We found a UUID match on /dev/sr0!
1407620572:: Running upgrade_dispatcher...
Chroot execing /mnt/upgrade/upgrade/upgrade_dispatcher --continueUpgrade
```

After completion another reboot occurs then login screen occurs with a hint that upgrade need to be either accepted or rejected message:

		hostname0c87275c01fb login: root Password: Last login: Fri Aug 8 22:15:46 on tty1 |==========| | This system has been upgraded but the upgrade has not yet | | been accepted or rejected. Please accept or reject the | | upgrade soon. | |==========| [root@hostname0c87275c01fb ~]# _
4. ☐	**Console:** Verify Policy install version	Login with root using the remote console and run the following commands to check the installed policy component and its revision: **# appRev** (cmp) [root@hostnamef17a42059171 ~]# appRev Install Time: Thu Aug 14 18:37:41 2014 Product Name: cmp Product Release: 11.5.0.0_17.1.0 Base Distro Product: TPD Base Distro Release: 6.7.0.0.1_84.17.0 Base Distro ISO: TPD.install-6.7.0.0.1_84.17.0-OracleLinux6.5-x86_64.iso OS: OracleLinux 6.5 **# appRev** (mpe) [admusr@MPE-R11-5 ~]$ appRev Install Time: Wed Aug 13 20:49:25 2014 Product Name: mpe Product Release: 11.5.0.0_18.1.0 Base Distro Product: TPD Base Distro Release: 6.7.0.0.1_84.17.0 Base Distro ISO: TPD.install-6.7.0.0.1_84.17.0-OracleLinux6.5-x86_64.iso OS: OracleLinux 6.5 **# appRev** (ma) [root@hostname59dc79f3de09 ~]# appRev Install Time: Wed Aug 13 22:16:11 2014 Product Name: ma Product Release: 11.5.0.0_17.1.0 Base Distro Product: TPD Base Distro Release: 6.7.0.0.1_84.17.0 Base Distro ISO: TPD.install-6.7.0.0.1_84.17.0-OracleLinux6.5-x86_64.iso OS: OracleLinux 6.5 **# appRev** (bod) [root@BOD-11-5 ~]# appRev Install Time: Wed Aug 13 13:10:06 2014 Product Name: bod Product Release: 11.5.0.0_18.1.0 Base Distro Product: TPD Base Distro Release: 6.7.0.0.1_84.17.0 Base Distro ISO: TPD.install-6.7.0.0.1_84.17.0-OracleLinux6.5-x86_64.iso OS: OracleLinux 6.5
5. ☐	**Console:** Verify Install success	**# tail /var/TKLC/log/upgrade/upgrade.log** The following indicates SUCCESS of Install. You can now proceed with the next section to perform the “Initial IP Configuration” for the newly installed server.

		[root@hostname1378910153 upgrade]# pwd /var/TKLC/log/upgrade [root@hostname1378910153 upgrade]# tail upgrade.log 1378948659:: Running postUpgrade() for Upgrade::Policy::PlatformLast upgrade pol icy... 1378948659:: Waiting for reboot 1378948659:: Updating platform revision file... 1378948659:: Upgrade returned success! 1378948659:: 1378948659:: 1378948659:: A reboot of the server is required. 1378948659:: The server will be rebooted in 10 seconds 1378948950:: Chroot execing /var/TKLC/backout/upgrade_dispatcher --continueUpgr ade 1378948952:: Now dispatching /var/TKLC/backout/ugwrap --session [root@hostname1378910153 upgrade]# IF UPGRADE_STATUS is not equal to SUCCESS, then search log for errors.
THIS PROCEDURE HAS BEEN COMPLETED		

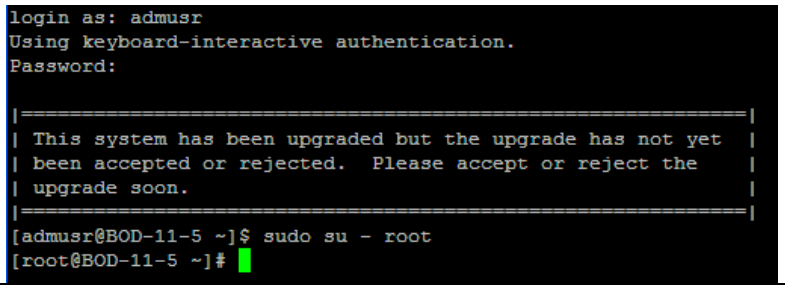
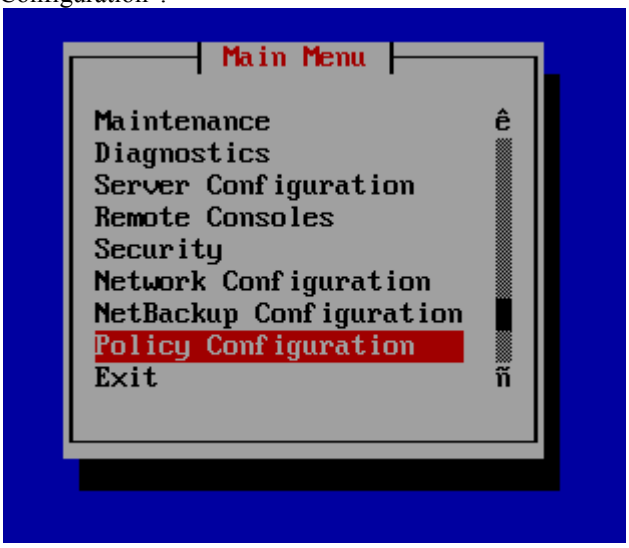
4. Configure Policy Application Servers

4.2 Configure Policy Mode

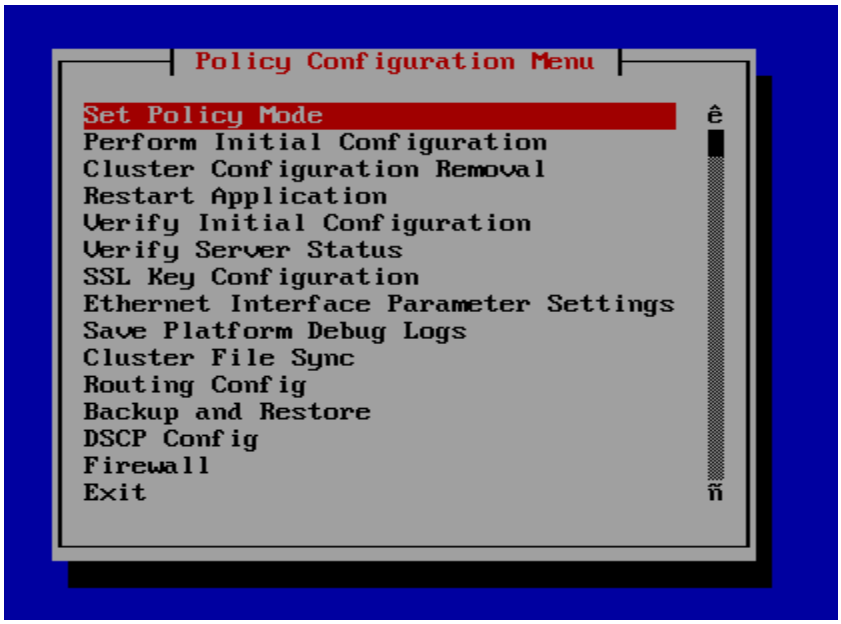
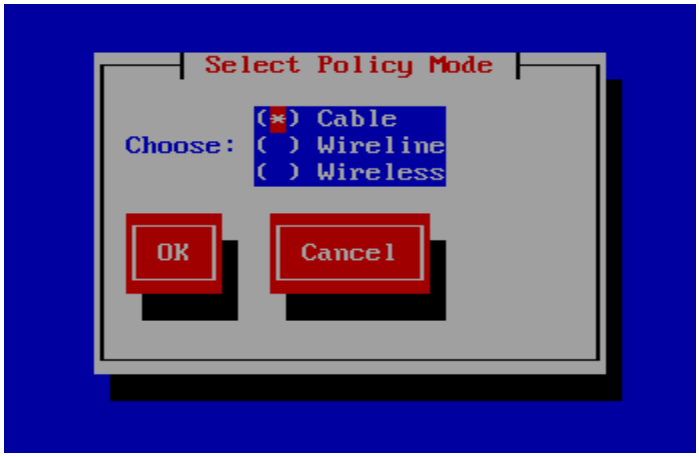
Procedure 6: Perform Policy Mode for Policy Servers

This sets the policy mode for the servers. This process need to be performed on each server of the policy solution.

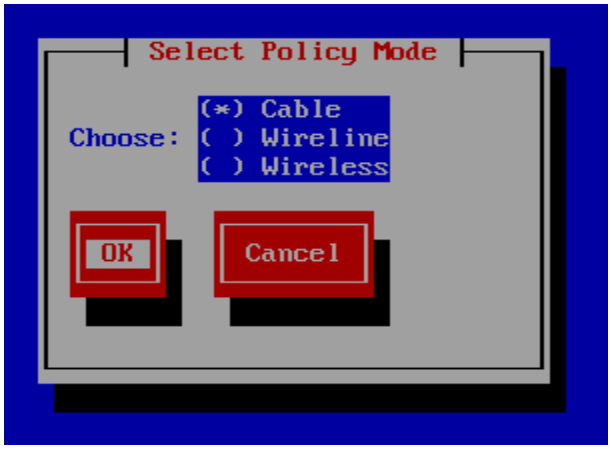
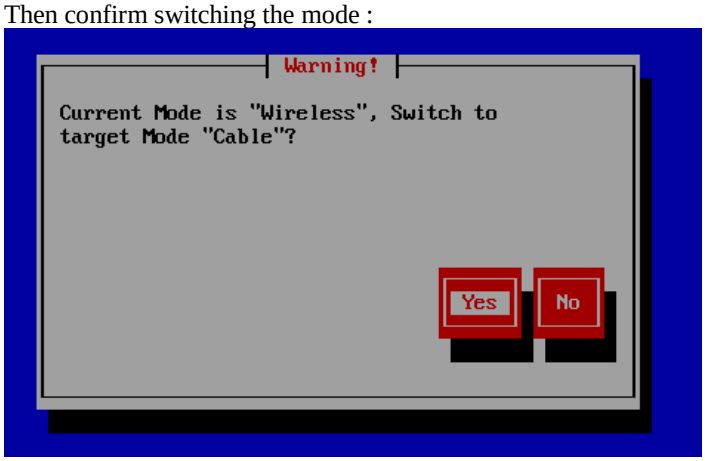
Procedure 6. Set Policy mode for the Policy Servers

S T E P #	This procedure will set the policy mode on each server of the policy solution components. After completing this procedure for PCRF components (CMP / MPE / BOD / MA) will have the "cable" policy mode set. This step is a new step that was introduced in PCRF release 11.5 as PCRF release is common for all markets (Wireless, Wireline, Cable)	
1. ☐	**Server's iLO Manager Remote Console:** Launch the remote console	Login to the server as "***admusr***" then switch to the "***root***" user 
2. ☐	Run platcfg tool	# su - platcfg When presented with following screen choose "Policy Configuration". 

Procedure 6. Set Policy mode for the Policy Servers

3. ☐	Select Set Policy Mode menu item	
4. ☐	**Check the "Cable" item**	

Procedure 6. Set Policy mode for the Policy Servers

5. ☐	**Confirm the mode choice**	Click **OK**
		 
		
		Then confirm switching the mode :
		 
		
		System will automatically work on setting off old mode features and setting on the Cable mode features:
		`in mode:Wireless, no feature need to be set off`
		`succeed to set off features of mode Wireless`
		`begin to deploy mode Cable`
		`to deploy feature: CableMaDistributor`
		`succeed to deploy CableMaDistributor`
		`to deploy feature: directLink`
		When process completes, display will return to the platform configuration. Exit from the platform configuration to the prompt and issue the following command to validate the current mode is set to “Cable” successfully
		`[root@hostname0c87275c01fb ~]# cat /etc/camiant/qpfeature.history`
		`previousMode=Wireless`
		`currentMode=Cable`
		`[root@hostname0c87275c01fb ~]#`

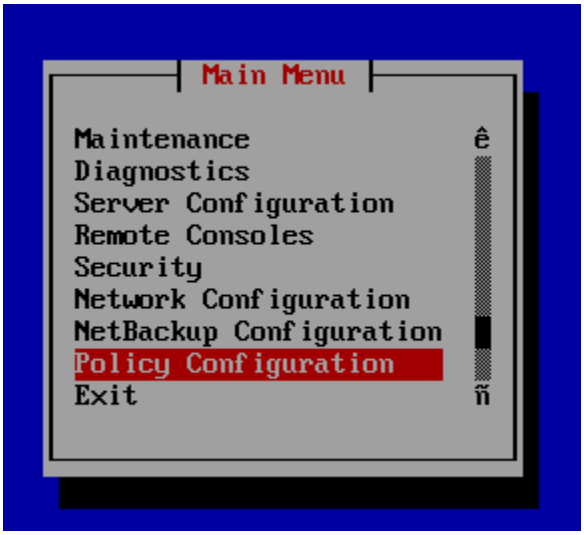
THIS PROCEDURE HAS BEEN COMPLETED		

4.3 Configure Network Topology

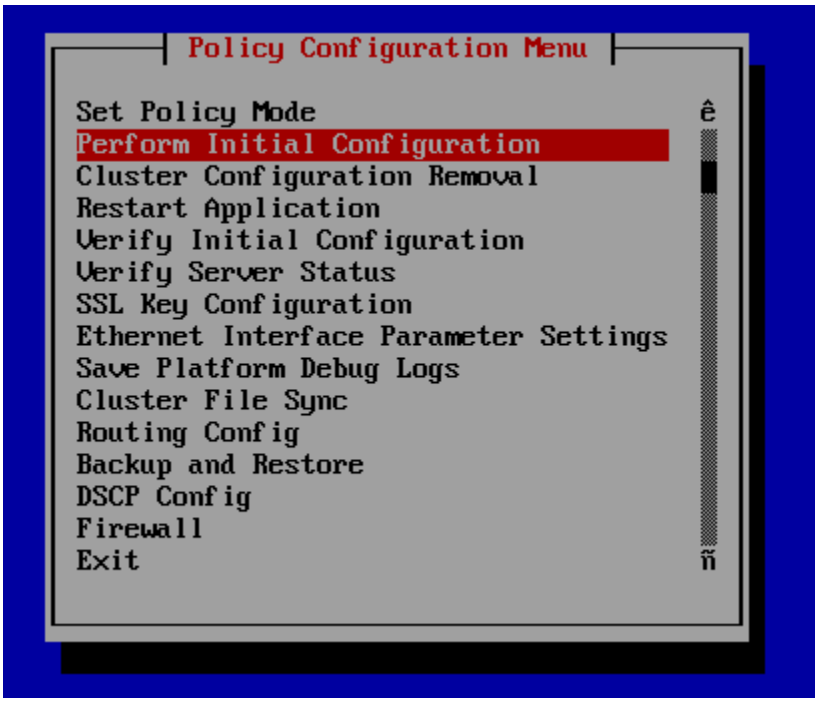
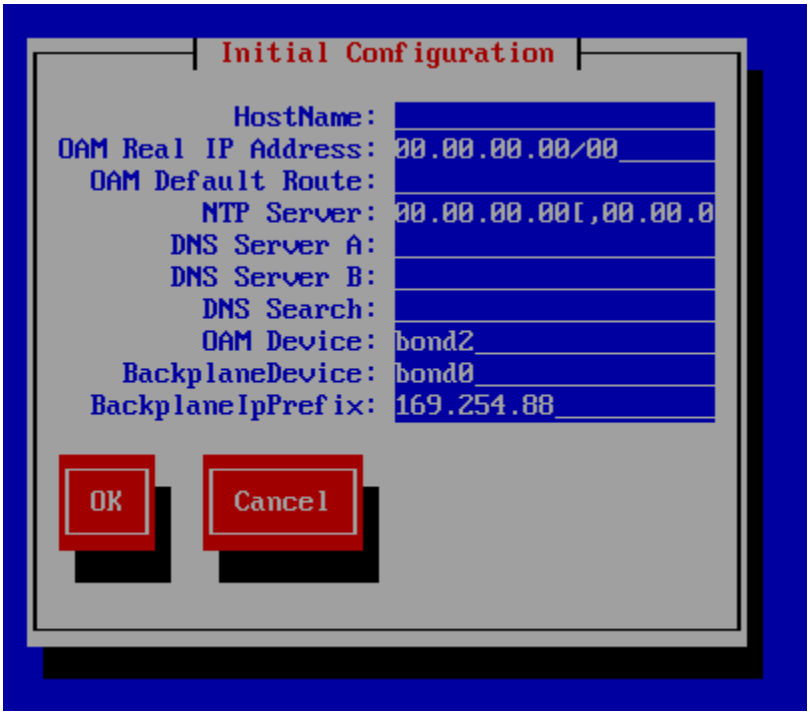
Procedure 7: Perform Initial IP Configuration of Policy Servers

This sets the initial IP network assignments for the servers.

Procedure 7. Perform Initial Configuration of the Policy Servers

S T E P #	This procedure will configure the OAM Network Address of the server, and related networking. After completing this procedure for PCRF 10.4, a physical (or "real") ip address will been assigned to the Bond0 (OAM network) for each server in each cluster (CMP and MPE). IP addresses assigned here are required for the communication to setup management relationships between the CMP and the MPE when completing further procedures in this document. . **Needed material:** - IP Addresses from the Network IP Planning document (or other customer provided document)	
1. ☐	Start the platcfg (refer to steps 1 and 2 in the previous procedure)	Navigate to "Policy Configuration". 

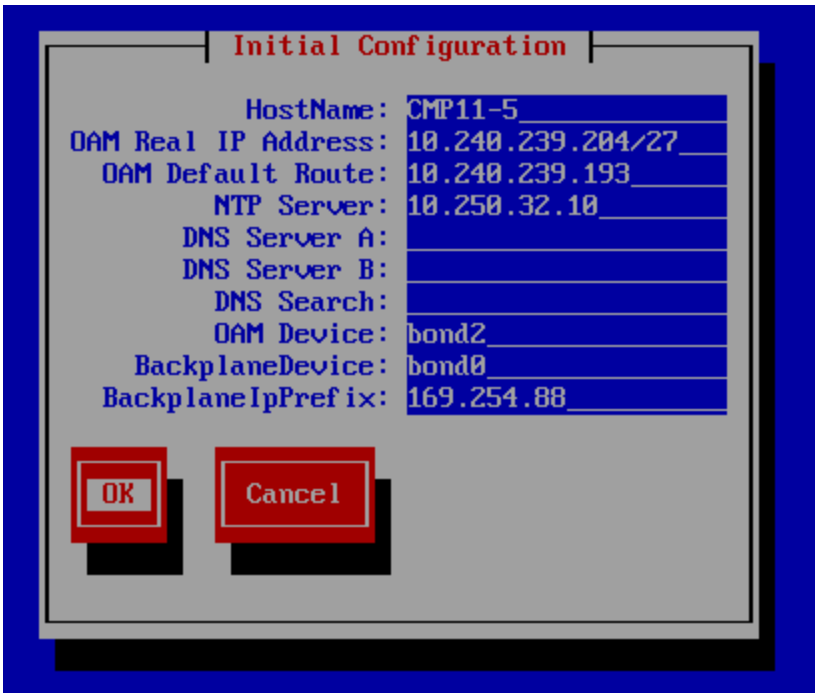
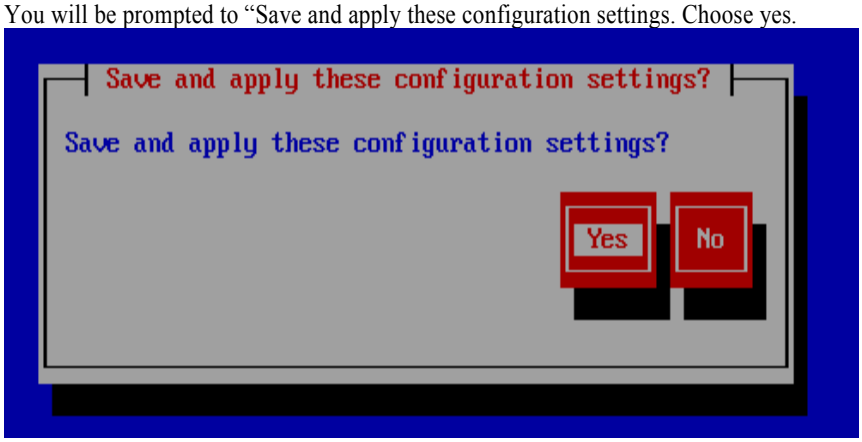
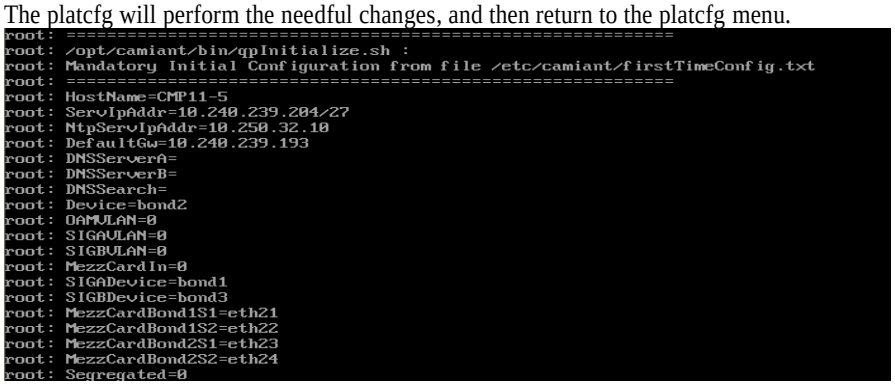
Procedure 7. Perform Initial Configuration of the Policy Servers

2. ☐	Select Perform Initial Configuration	
3. ☐	**Complete Initial Configuration form**	

Procedure 7. Perform Initial Configuration of the Policy Servers

4. ☐	**Complete Initial Configuration form**	• Hostname - the unique hostname for the device being configured. • OAM Real IP Address - the IP address that is permanently assigned to this device. (sometimes called “Physical IP” or “Real IP). • OAM Default Route - the default route of the OAM network. • NTP Server - a reachable NTP (required-this must be data filled even if the NTP server is not yet reachable) • DNS Server A - a reachable DNS server (optional-not used by Verizon) • DNS Server B - a reachable DNS server (optional-not used by Verizon) • DNS Search - is 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 <u>changing this value is not supported.</u> • Backplane Device – the bond interface of the backplane device Note that the default value should be used, as <u>changing this value is not supported.</u> • Backplane IP Prefix – The Ip address prefix assigned for the Backplane direct link

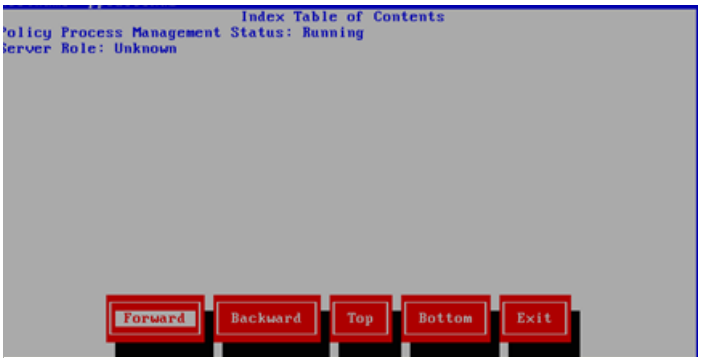
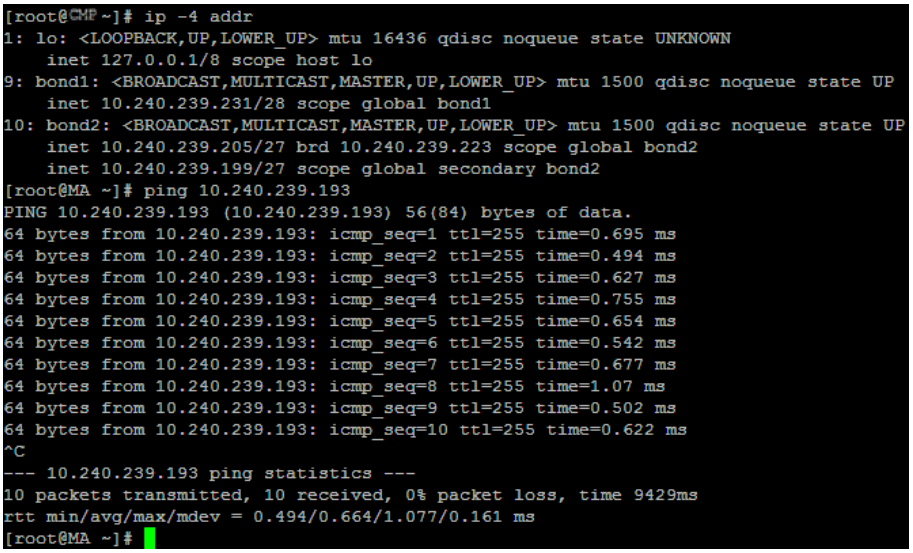
Procedure 7. Perform Initial Configuration of the Policy Servers

5. ☐	**Save configuration**	Enter the configuration (example datafill below) and then select **OK**  You will be prompted to "Save and apply these configuration settings. Choose yes.  The platcfg will perform the needful changes, and then return to the platcfg menu. 

Procedure 7. Perform Initial Configuration of the Policy Servers

6.	**Verify Config**	Verify the configuration by selecting **Policy Configuration** -> **Verify Initial Configuration** from within the platcfg utility.
7. ☐	**Verify Config**	Confirm the configured "Hostname, ServIpAddr, DefaultGw and NtpServIpAddr" previously configured are present. A display similar to the following is shown. Other fields will be configured with their default values and can be left as they are. Copyright (C) 2003, 2014, Oracle and/or its affiliates. All rights reserved. Hostname: CMP11-5 Index Table of Contents Date/Time: 08/20/2014 16:06:14 Hardware Type: ProLiantDL360G6 BackplaneDevice="bond0" BackplaneEnable="1" BackplaneIpPrefix="169.254.88" DNSSearch="" DNSServerA="" DNSServerB="" DefaultGw="10.240.239.193" Device="bond2" HostName="CMP11-5" LayoutProfile="directlink" NtpServIpAddr="10.250.32.10" OAMDevice="bond2" SIGADevice="bond1" SIGBDevice="bond3" ServIpAddr="10.240.239.205/27" NTP Status: remote refid st t when poll reach delay offset jitter ========== *10.250.32.10 192.5.41.40 2 u 16 64 1 0.289 0.315 0.142

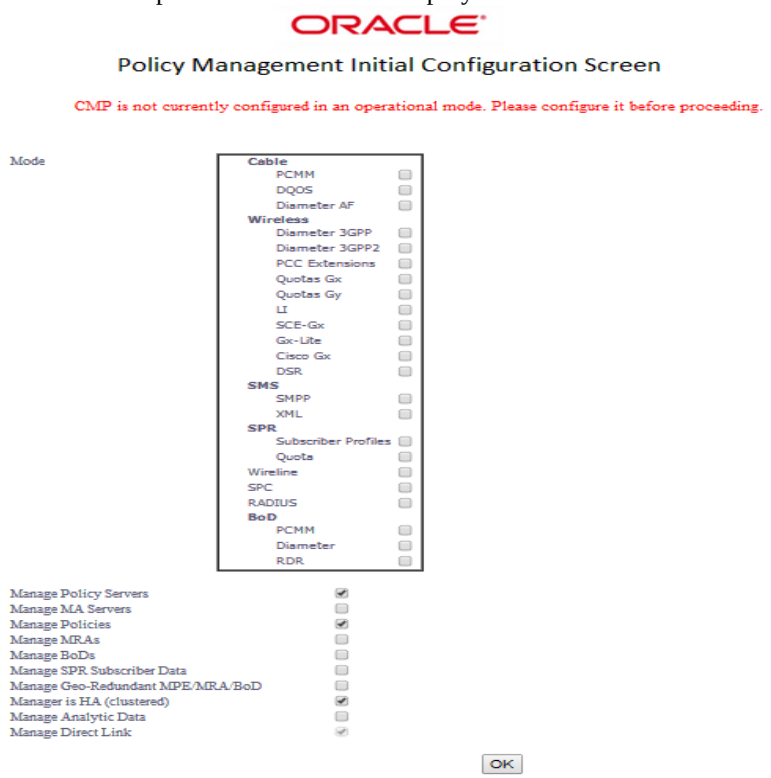
Procedure 7. Perform Initial Configuration of the Policy Servers

8. ☐	**Verify Server Status**	From the Policy Configuration menu in platcfg, navigate to Verify Server Status and enter. The server should be in a running state. For example:  Exit platcfg
9. ☐	**Ping the OAM default gateway to verify server is available on the network**	Ping the default gateway from the cli to validate network connectivity that was configured above. You can also execute "ip -4 addr" from the cli to confirm the configured IP address 
10. ☐	**Optional: ssh to server assigned OAM address**	If networking is in place, it will be possible to login (ssh) to the server via the server's assigned IP address in case remote access has not been disabled.
11. ☐	**Repeat on additional servers**	Repeat this procedure on all Policy servers that are planned for service for all the components CMP, BOD, MPE, MA.
	THIS PROCEDURE HAS BEEN COMPLETED	

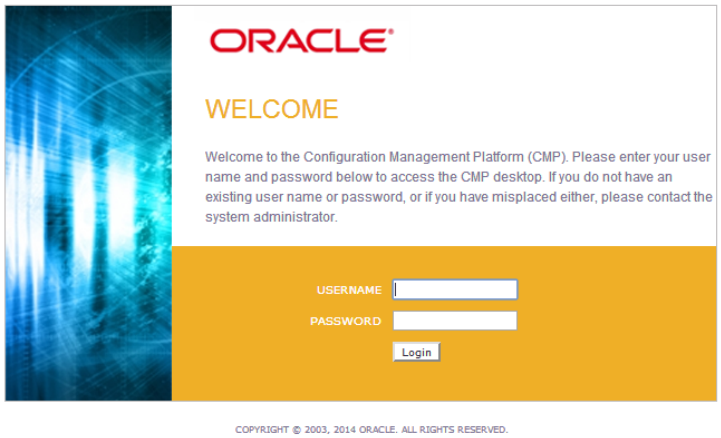
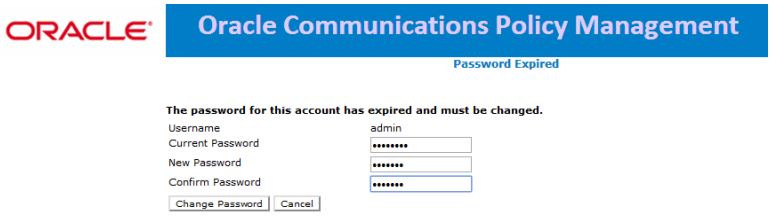
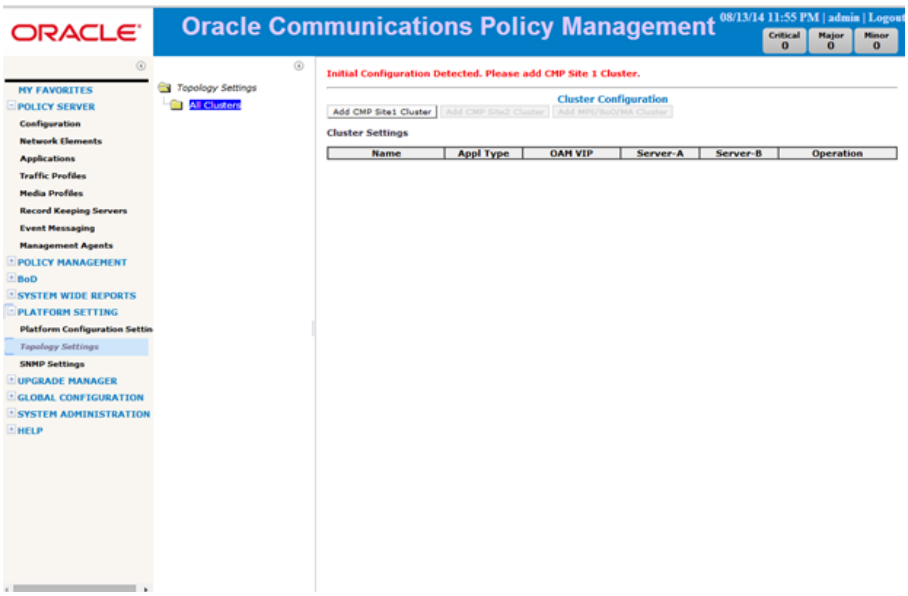
Procedure 8: CMP GUI Initial Configuration

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

Procedure 8. CMP GUI Initial Configuration

S T E P #	This procedure will configure the CMP at the Active site. This procedure will configure the Cable Mode options on the CMP required for the Cable PCRF Solution. VIP addresses for the OAM and SIG-A interfaces on the CMP are also assigned. **Pre-requisite:** Network access to the CMP OAM IP address, to bring up a web Browser GUI (http)	
1. ☐	Set Policy Server Modes on initial browser connection over http to the CMP	For this step, network access is needed to the CMP OAM IP address via a http session (Firefox/IE Browser). i.e. open a Browser and enter the CMP OAM ip address in the navigation bar. This IP address was assigned to the CMP during the initial IP configuration as the OAM Real IP address (refer to step 4 of previous procedure). The initial screen presented prompts the user to select the "modes" for the system. The mode selection depends on the customer deployment  The options selected depends widely on the modes of operations and deployment architecture that customer decides to use. Following some items to consider in order to decide which options to set in the CMP mode setting: • The protocols used in the deployment (PCMM/Diameter or both) • BoD implementation as the application manager used for the solution • MA implementation • Support of geo-redundancy for BOD and MPE-S • Using BackPlane direct link for HA and replication traffic between mates in a cluster (For this to work cabling between the mate servers should be in place in the correct eth ports as outlined in figures 2 in this document based on the hardware used) After checking the proper options click on "OK"

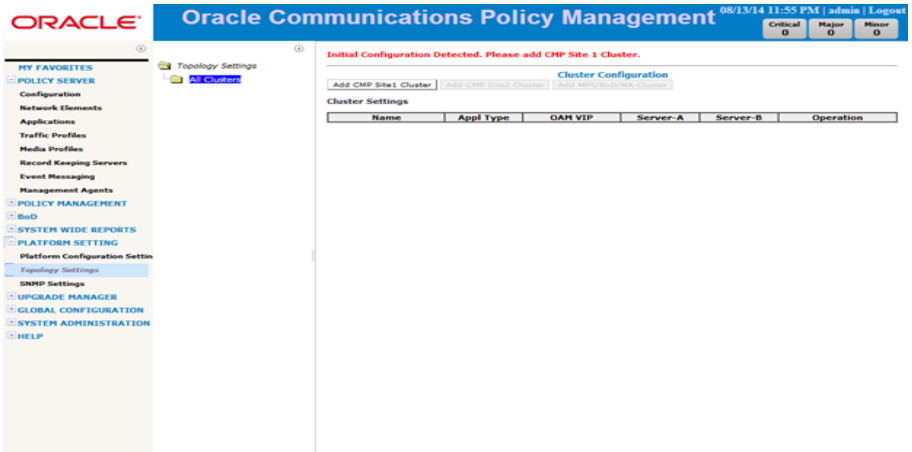
Procedure 8. CMP GUI Initial Configuration

2. ☐	GUI Login with Admin	The next screen requires a login. Initial login is admin/policies 
3.	Set admin password	After logging in for the first time, the system will prompt the user to change the initial admin password.  After change the admin password successfully, CMP will log off then user will log in again using the new set password.
4. ☐	**Verify that the CMP GUI is displayed, with expected menus.**	A message indicates that initial configuration of CMP is detected and the CMP site 1 server need to be configured in CMP's topology: 

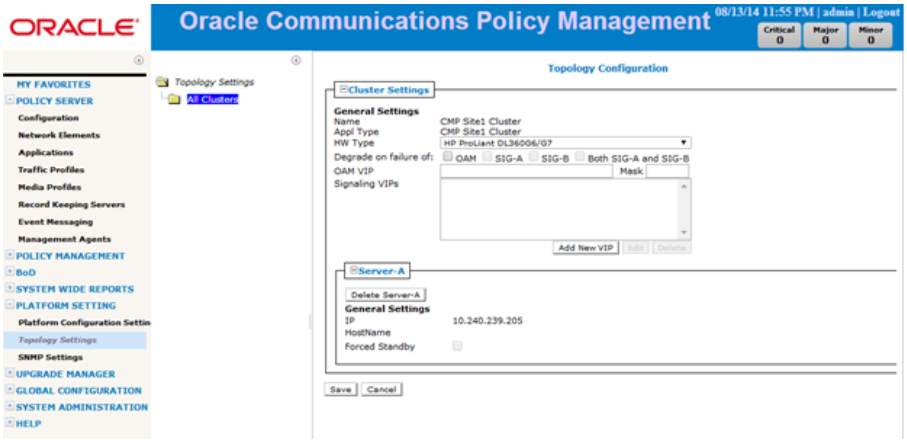
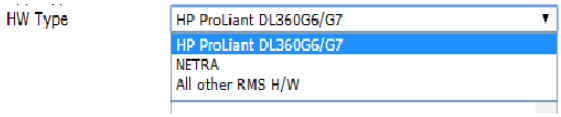
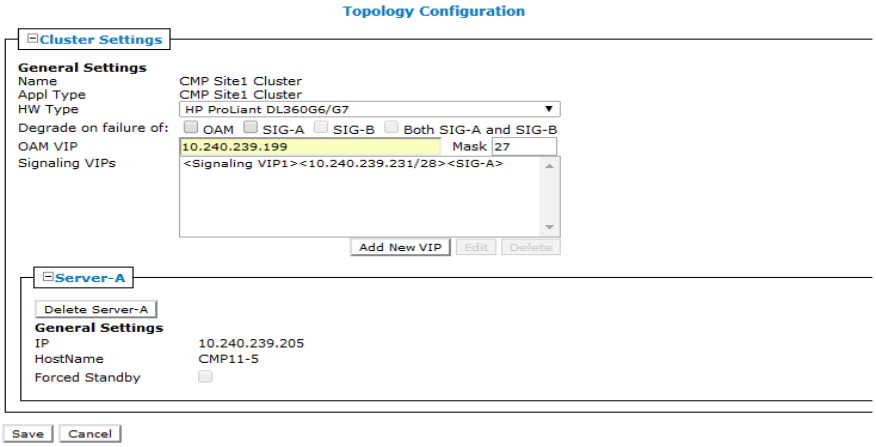
Procedure 9: Add Topology Configuration for CMP Cluster

This procedure will perform topology configuration of the CMP Site1 cluster. **This procedure only needs to be performed on one of the two servers that will make up the CMP HA cluster.**

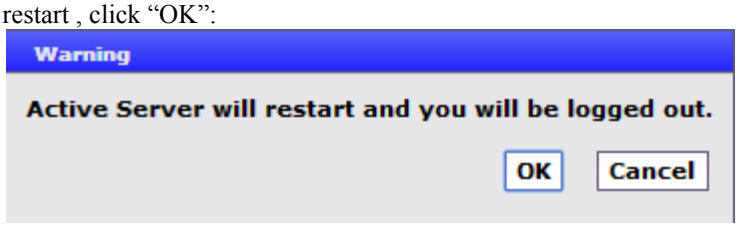
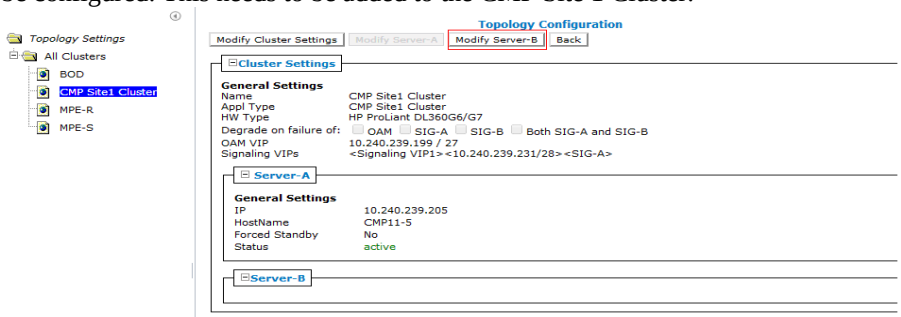
Procedure 9. CMP GUI CMP Cluster Configuration

1. ☐	**View Topology Settings**	Select: Menu -> Topology Settings The initial form will open, and display a message that a CMP Site 1 Cluster must be added. 

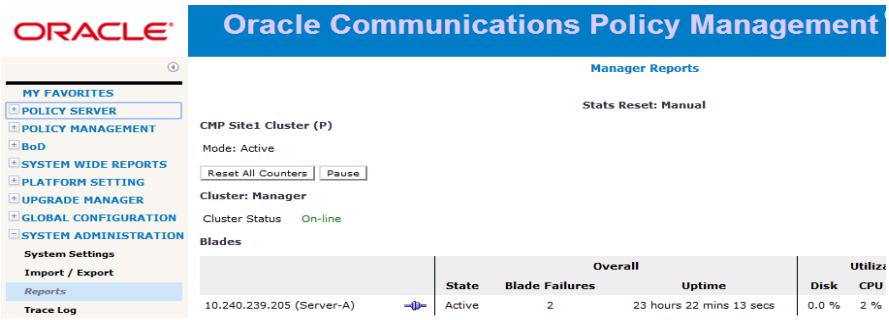
Procedure 9. CMP GUI CMP Cluster Configuration

2.	**Add CMP Site 1 Cluster – Server A**	Select the button to "Add CMP Site 1 Cluster". Following form will appear to set the settings of the CMP cluster:  HW Type — Lists all available RMS & Sun Netra H/W supported for this release.  The H/W used for PCRF deployment needs to be selected Degrade on failure of — define server degrade criteria based on connection problems of which network interfaces OAM VIP — IP address and netmask for the cluster on the OAM network. Signaling VIPs — IP address and netmask for the cluster on the SIG-A, SIG-B networks Server-A IP — OAM Real IP address for the first server (predefined, no input necessary). Server-A Hostname — hostname for the first server (has to match what is used in the platform initial configuration as in step 4 of procedure 8 above)  When done, save the form.

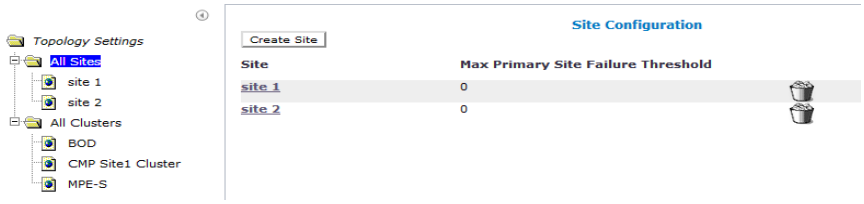
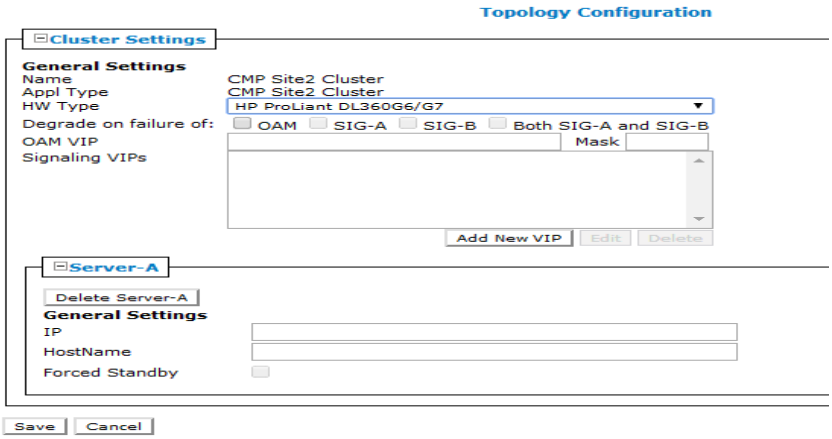
Procedure 9. CMP GUI CMP Cluster Configuration

3. ☐	**Login using the CMP cluster VIP.**	After the Topology Configuration is saved, a message indicating that server will restart , click "OK":  The CMP VIP address will be taken by the Active CMP server of the cluster.. This server will be referred to as Server A of ther CMP cluster. CMP will disconnect , login back in CMP GUI (Server-A) using the newly assigned VIP address.
4. ☐	**IF the CMP VIP is not available…**	SSH to the CMP server phyiscal IP address and issue the "ha.mystate" command as **root** to verify that the blade has become active by noting the role as shown below: # ha.mystate [admusr@CMP11-5 ~]$ sudo su - root [root@CMP11-5 ~]# ha.mystate resourceId role node subResources lastUpdate DbReplication Active A2780.220 0 0820:161936.441 VIP Active A2780.220 0 0820:161936.443 QP Active A2780.220 0 0820:161939.684 DbReplication_old OOS A2780.220 0 0820:161926.152 [root@CMP11-5 ~]# NOTE: OOS role for DbReplication_old is OK If the role is not active contact support. If it is "active" proceed to the next step.
5.	**Modify CMP Site 1 Cluster – add Server B**	**Log back into the CMP GUI using the newly assigned CMP HA Cluster VIP (Virtual IP) address**. Now a second CMP server "Server-B" (for redundancy) can be configured. This needs to be added to the CMP Site 1 Cluster.  Same steps 2 and 3 above used for CMP Server-A can be followed for Server-B
6.	**Verify Server B is added**	You will be returned to a screen showing the CMP cluster Server-B as "out-of-service". **You will need to refresh this screen** and Server-B should now have standby status with forced standby enabled.
7. ☐	**GUI: Remove Force Standby on Server B**	Return to the CMP GUI menu Platform Setting/Topology/CMP-Site1-Cluster Click Modify for Server-B and uncheck "Force Standby", then click Save when finished.

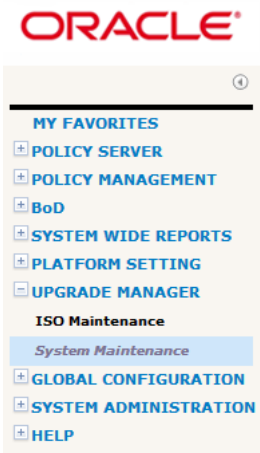
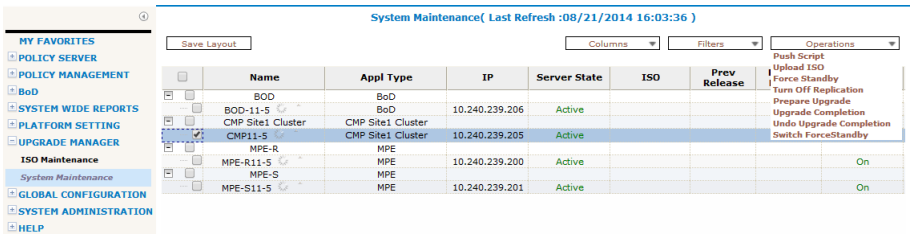
Procedure 9. CMP GUI CMP Cluster Configuration

8. ☐	**GUI: Check the CMP cluster state**	In the CMP GUI menu navigate to System Administration>Reports and display the CMP cluster status. The cluster status should show a state of "**on-line**".  Allow several minutes for alarms to clear.

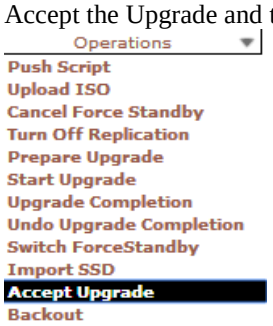
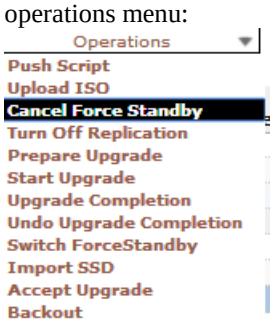
Procedure 9. CMP GUI CMP Cluster Configuration

9.	**Topology setting in geo-redundant deployment**	In case Cable policy solution is geo-redundant, geo-redundancy function should have been already enabled in CMP mode settings (refer to step 1 in procedure 9): Also, the 2 sites need to be created under the "All sites" tree item in Topology settings: After creation of the sites:  Then from the "Topology Settings", under "All Clusters" in the navigation tree, click "Add CMP Site2 Cluster": Configure the second CMP cluster in the same fashion as done for the site1 CMP cluster in this procedure: 

Procedure 9. CMP GUI CMP Cluster Configuration

10. ☐	**Clear "Accept Upgrade" alarm for CMP cluster (Server-A)**	After the CMP topolgy configuration has been completed you may note the following alarm from each CMP server. Aug 20, 2014 04:06 PM EDT | Minor | 32532 | Server Upgrade Pending Accept/Reject | 10.240.239.199 | CMP11-5 10.240.239.205 To clear these alarms follow the below steps to accept the upgrade. In the CMP GUI Navigate to Upgrade Manager → System Maintenance  Check the checkboxes for the CMP server and expand the "Operations" menu:  Select "Forece StandBy" for the standby CMP server.

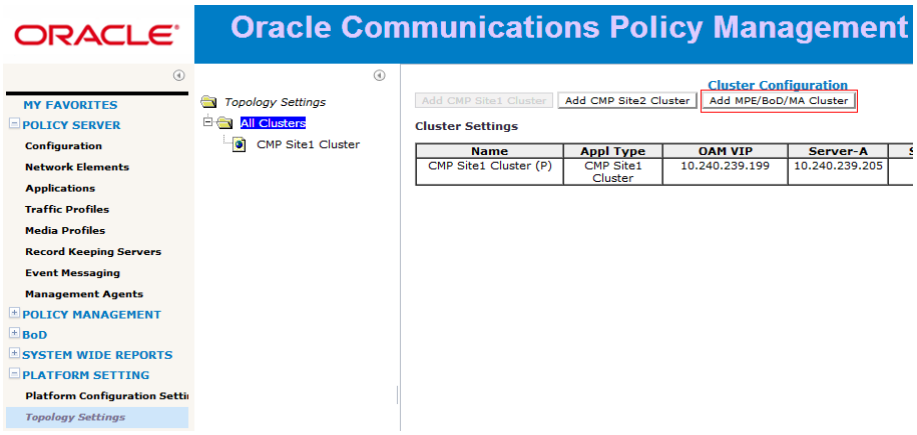
Procedure 9. CMP GUI CMP Cluster Configuration

11. ☐	**Clear "Accept Upgrade" alarm for CMP Cluster (Server-B)**	Accept the Upgrade and the alarm for this server will clear.  When operation completes , cancel the force stanby for the CMP server from the operations menu:  Now follow same steps for the second CMP server to accept the upgrade. **Note you will be logged out of the CMP GUI when setting the active server of the CMP as Force Standby** as the cluster will failover and you will need to login again to proceed with this procedure. The final step is to recheck the boxes for the server that just accepted the upgrade to take that server out of "forcedStandby". Same steps need to be followed for CMP site2 server(s) to accept the upgrade on them and clear the corresponding alarms

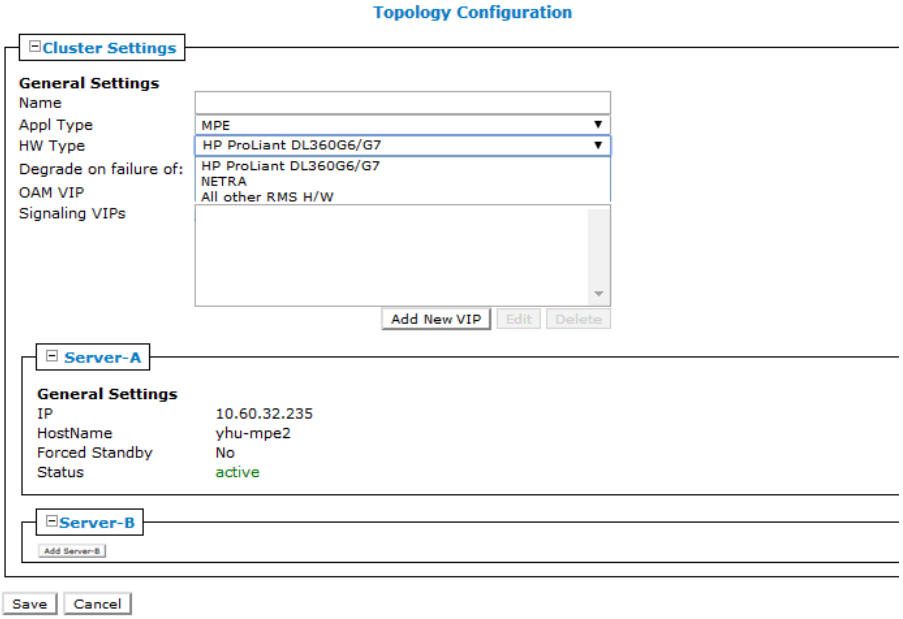
Procedure 10: Add MPE/BOD/MA Clusters to the Topology Configuration

This procedure will perform initial configuration of the MPE/BOD/MA clusters.

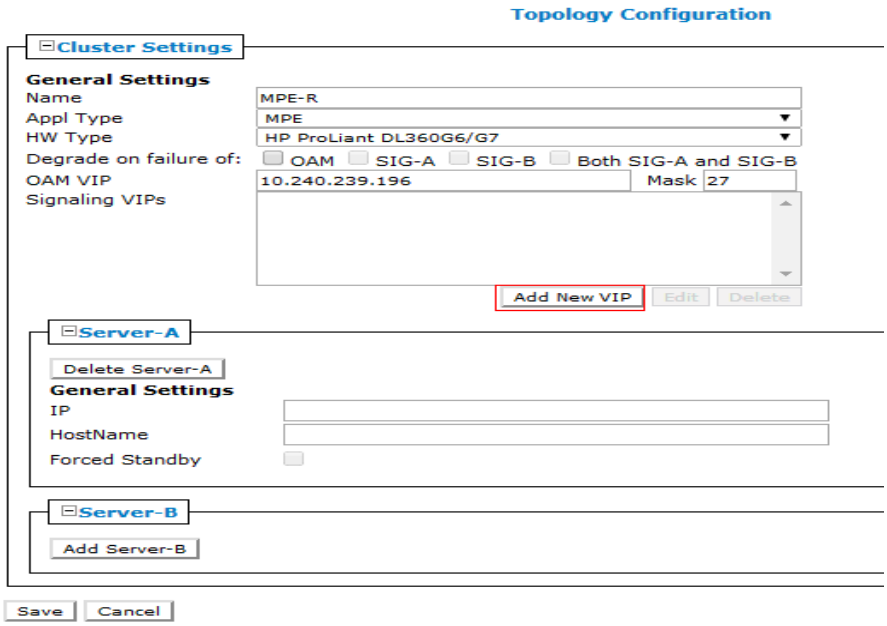
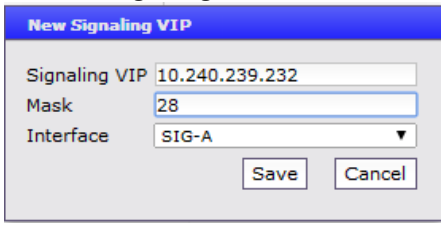
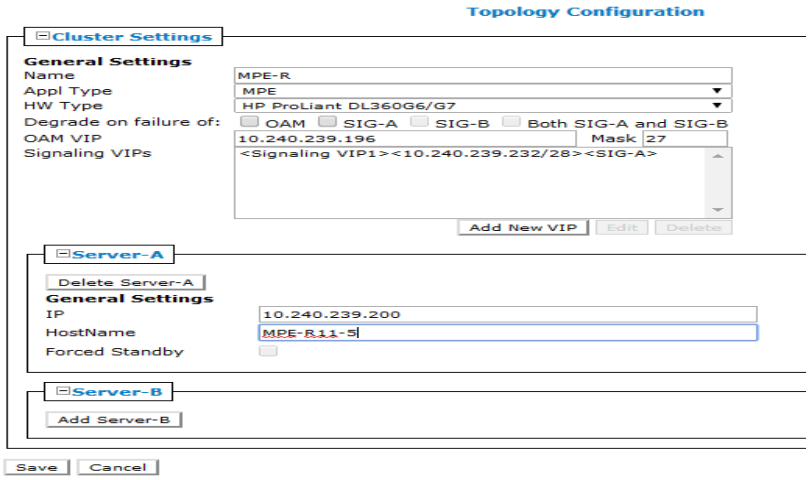
Procedure 10. Topology Configuration of MPE/BOD/MA clusters

S T E P #	This procedure will configure the management relationships between the CMPs and the PCRF components (MPE/BOD/MA clusters). After this, the status of the MPE, BOD, MA servers will be available from the CMP GUI. **IMPORTANT:** **Certain IP network services must be allowed between the CMP** and the other components 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. **Note that connectivity between the CMP and the PCRF components (MPE, BOD, and MA) must be confirmed before this procedure can be performed. This procedure will configure the MPE VIP addresses for the (OAM), (SIG-A) & (Sig-B) interfaces** **Pre-requisite:** - Network access to the CMP OAM IP address, to bring up a web Browser GUI (http) **Note:** We shall include here the steps for configuring the topology of MPE cluster as an example, same steps would be followed for BOD and MA clusters	
1. ☐	Login to CMP Server GUI (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 Alarm may affect configuration activities.
3.	**View Topology Settings**	Select: Menu -> Topology Settings The initial form will open, and display the existing configured Clusters. Select "Add MPE/BOD/MA Cluster" 

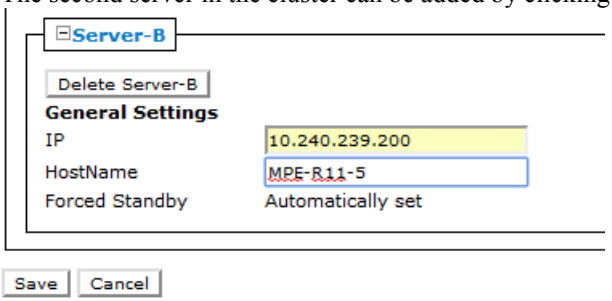
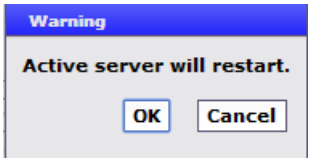
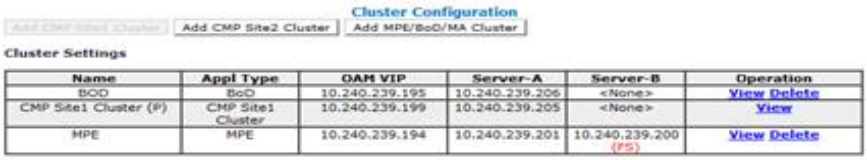
Procedure 10. Topology Configuration of MPE/BOD/MA clusters

4. ☐	**Add MPE Cluster**	The Topology Cluster configuration screen will be displayed.  It is allowed to add both Server A and Server B in this form at the same time in one step.

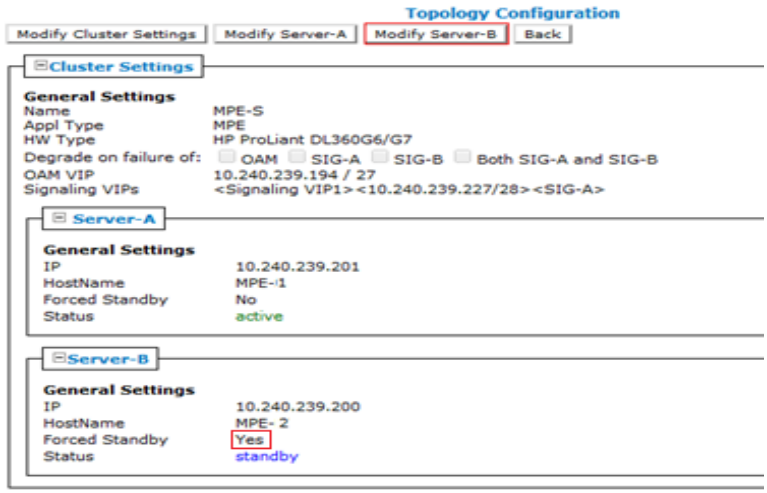
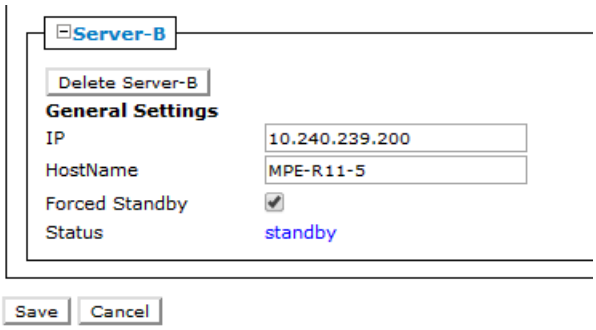
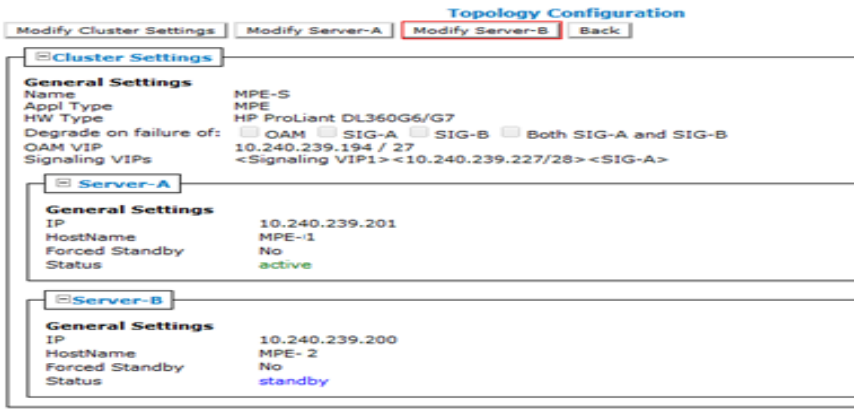
Procedure 10. Topology Configuration of MPE/BOD/MA clusters

5. ☐	**Add MPE Cluster**	In the Topology Configuration form, enter the cluster details including the H/W type, OAM VIP + netmask. Then click the "Add New VIP" to configure the SIG-A + netamsk, in the same way add Sig-B + netmask if SIG-B is used.  Fill in the signaling VIP details:  Fill in the Server-A details: 

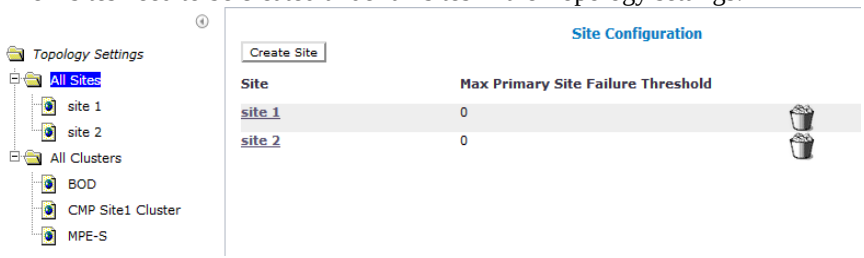
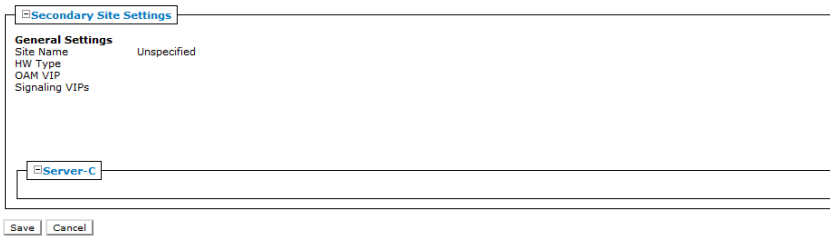
Procedure 10. Topology Configuration of MPE/BOD/MA clusters

6.	**Add MPE Cluster (continued)**	The second server in the cluster can be added by clicking "Add Server-B" button :  Server A and Server B physical IP addresses and Hostnames (as assigned during initial configuration of the MPEs) will need to be provided. Make sure the hostnames matches the hostnames assigned to the corresponding MPE servers. Save the configuration at the bottom of the screen, a warning message to confirm the active server will restart will be displayed, click "OK":  You should now be presented with a "Toplogy Settings" screen confirming both the MPE clusters have been added into the Topology.  Name | Appl Type | OAM VIP | Server-A | Server-B | Operation BOD | BoD | 10.240.239.195 | 10.240.239.206 | <None> | View Delete CMP Site1 Cluster (P) | CMP Site1 Cluster | 10.240.239.199 | 10.240.239.205 | <None> | View MPE | MPE | 10.240.239.194 | 10.240.239.201 | 10.240.239.200 (PS) | View Delete

Procedure 10. Topology Configuration of MPE/BOD/MA clusters

7. ☐	**Remove Force standby of Server B**	**If Server-A and Server-B were added to the Topology at the same time this step will not be needed.** If Server-A was added first and then server-B was added at a later time, Server-B will be on Force Standby.  Click "**Modify Server-B"**, uncheck **Force Standby**, then **Save** 
8. ☐	**Verify Topology**	Select: Menu -> Topology Settings → View Cluster  Validate the status of each the servers that should be Active/Standby and none is Forced Standby. Wait several minutes for all alarms to clear. You should be left with accept/reject upgrade alarms that will be cleared in the next step.

Procedure 10. Topology Configuration of MPE/BOD/MA clusters

9.	**Topology setting in geo-redundant deployment**	In case Cable policy solution is geo-redundant, geo-redundancy function should have been already enabled in CMP mode settings (refer to step 1 in procedure 9): Manage Geo-Redundant MPE/MRA/BoD ☑ The 2 sites need to be created under all sites in the Topology settings:  Also, CMP site2 cluster should have been configured prior to adding secondary site for MPE or BOD clusters. For MPE and BOD clusters, secondary site cluster configuration and a third server "Server-C" will exist in the topology settings page to configure the geo-redundant server in the secondary site:  Click "modify secondary site" button then configure the secondary site settings and Server-C in the same fashion as primary site and servers A or B. Validate that Server-C will have "spare" status after it is configured correctly.

Procedure 10. Topology Configuration of MPE/BOD/MA clusters

10.	**Active CMP Server CLI: Exchange SSH Keys**	From the Active CMP server CLI as root user, change directory to "/opt/camiant/bin" then run the command in the screen shot below to exchange the SSH keys for all cluster's configured in the topology:
		
		`# cd /opt/camiant/bin`
		`# qpSSHKeyProv.pl --prov`
		
		`The password of admusr in topology:`
		
		Enter the admusr password and hit enter, the SSH keys will be exchanged, validate that process returns OK in the end:
		
		`Connecting to admusr@CMP9-4 (10.240.239.200) ...`
		`Connecting to admusr@MPE-R (10.240.239.206) ...`
		`Connecting to admusr@MPE-S1 (10.240.239.204) ...`
		`Connecting to admusr@MPE-S (10.240.239.201) ...`
		`Connecting to admusr@MA (10.240.239.205) ...`
		`Connecting to admusr@BOD (10.240.239.207) ...`
		
		`[1/6] Provsioning SSH keys on MPE-R (10.240.239.206) ...`
		
		`[2/6] Provsioning SSH keys on CMP9-4 (10.240.239.200) ...`
		
		`[3/6] Provsioning SSH keys on MPE-S1 (10.240.239.204) ...`
		
		`[4/6] Provsioning SSH keys on MPE-S (10.240.239.201) ...`
		
		`[5/6] Provsioning SSH keys on MA (10.240.239.205) ...`
		
		`[6/6] Provsioning SSH keys on BOD (10.240.239.207) ...`
		
		`SSH keys are OK.`

Procedure 10. Topology Configuration of MPE/BOD/MA clusters

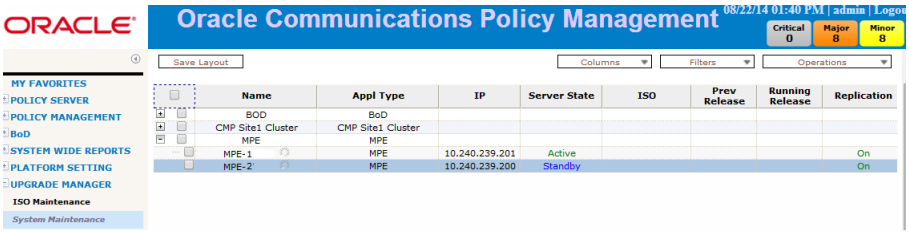
11. ☐ **Clear "Accept Upgrade" alarm for MPE**

After the MPE topolgy configuration has been completed you may note the following alarm from each MPE server.

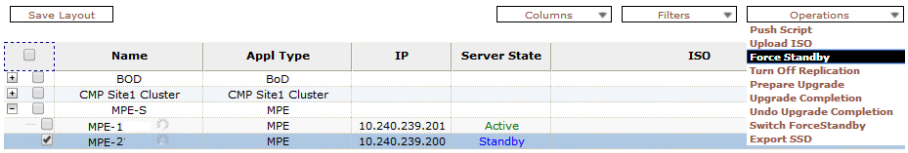
Aug 20, 2014 10:56 AM EDT	Minor	32532	Server Upgrade Pending Accept/Reject	10.240.239.194	MPE-1 10.240.239.201	
Aug 18, 2014 06:14 PM EDT	Minor	32532	Server Upgrade Pending Accept/Reject	10.240.239.194	MPE-2 10.240.239.200	

To clear these alarms follow the following steps.

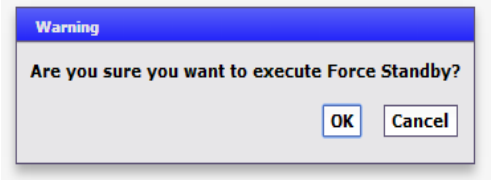
In the CMP GUI Navigate to Upgrade Manager → System Maintenance



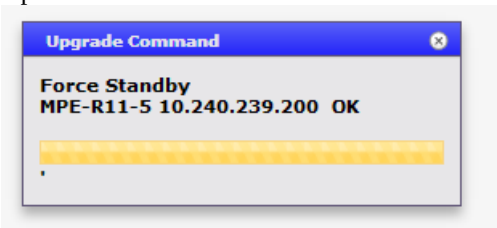
Check the checkboxes for the MPE server which is in "Standby" mode and put that server in "Forced Standby" under the "operations" tab as in this snapshot



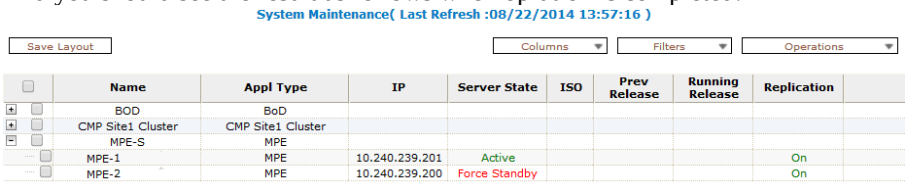
Confirm the operation in the next warning message:



Operation will start:



And you should see the result as follows when opration is completed:



Procedure 10. Topology Configuration of MPE/BOD/MA clusters

12. ☐	**Clear "Accept Upgrade" alarm for MPE**	Choose the Standby server then click on the "operations tab" again and choose the "Accept Upgrade" operation.

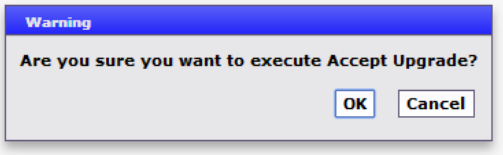
System Maintenance(Last Refresh :08/22/2014 13:58:05)

Save Layout | Columns | Filters | Operations

Name	Appl Type	IP	Server State	ISO	Prev Release	Running Release
BOD	BoD					
CMP Site1 Cluster	CMP Site1 Cluster					
MPE-S	MPE					
MPE-1	MPE	10.240.239.201	Active			
MPE-2	MPE	10.240.239.200	Force Standby			

Operations: Push Script, Upload ISO, Cancel Force Standby, Turn Off Replication, Prepare Upgrade, Start Upgrade, Upgrade Completion, Undo Upgrade Completion, Switch ForceStandby, Import SSD, **Accept Upgrade**, Backout

Confirm the operation in the next warning message.



Now the force standby can be cleared from the server:

System Maintenance(Last Refresh :08/22/2014 14:05:45)

Save Layout | Columns | Filters | Operations

Name	Appl Type	IP	Server State	ISO
BOD	BoD			
BOD-11-5	BoD	10.240.239.206	Active	
CMP Site1 Cluster	CMP Site1 Cluster			
CMP11-5	CMP Site1 Cluster	10.240.239.205	Active	
MPE-S	MPE			
MPE-1	MPE	10.240.239.201	Active	
MPE-2	MPE	10.240.239.200	Force Standby	

Operations: Push Script, Upload ISO, **Cancel Force Standby**, Turn Off Replication, Prepare Upgrade, Start Upgrade, Upgrade Completion, Undo Upgrade Completion, Switch ForceStandby, Import SSD, Accept Upgrade, Backout

After operation completes with a short while refresh the screen and you should notice that server status is back to "standby":

Name	Appl Type	IP	Server State
BOD	BoD		
BOD-11-5	BoD	10.240.239.206	Active
CMP Site1 Cluster	CMP Site1 Cluster		
CMP11-5	CMP Site1 Cluster	10.240.239.205	Active
MPE-S	MPE		
MPE-S11-5	MPE	10.240.239.201	Active
MPE-R11-5	MPE	10.240.239.200	Standby

Now follow the exact same steps with the other MPE server in the cluster to accept the upgrade. Force standby the server:

System Maintenance(Last Refresh :08/22/2014 14:07:45)

Save Layout | Columns | Filters | Operations

Name	Appl Type	IP	Server State	ISO
BOD	BoD			
BOD-11-5	BoD	10.240.239.206	Active	
CMP Site1 Cluster	CMP Site1 Cluster			
CMP11-5	CMP Site1 Cluster	10.240.239.205	Active	
MPE-S	MPE			
MPE-1	MPE	10.240.239.201	Active	
MPE-2	MPE	10.240.239.200	Standby	

Operations: Push Script, Upload ISO, **Force Standby**, Turn Off Replication, Prepare Upgrade, Upgrade Completion, Undo Upgrade Completion, Switch ForceStandby, Export SSD

Then accept the upgrade:

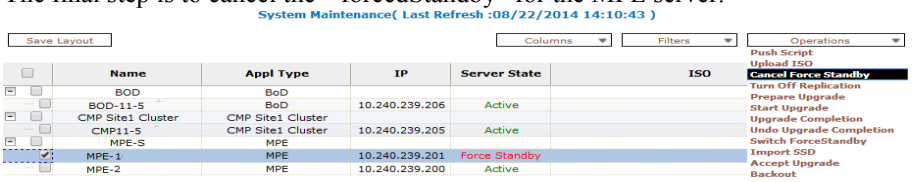
System Maintenance(Last Refresh :08/22/2014 14:09:23)

Save Layout | Columns | Filters | Operations

Name	Appl Type	IP	Server State	ISO
BOD	BoD			
BOD-11-5	BoD	10.240.239.206	Active	
CMP Site1 Cluster	CMP Site1 Cluster			
CMP11-5	CMP Site1 Cluster	10.240.239.205	Active	
MPE-S	MPE			
MPE-1	MPE	10.240.239.201	Force Standby	
MPE-2	MPE	10.240.239.200	Standby	

Operations: Push Script, Upload ISO, Cancel Force Standby, Turn Off Replication, Prepare Upgrade, Start Upgrade, Upgrade Completion, Undo Upgrade Completion, Switch ForceStandby, Import SSD, **Accept Upgrade**, Backout

Procedure 10. Topology Configuration of MPE/BOD/MA clusters

<table>
<tr><td>13.
☐</td><td>Clear “Accept Upgrade” alarm for MPE</td><td>The final step is to cancel the “forcedStandby” for the MPE server.
 

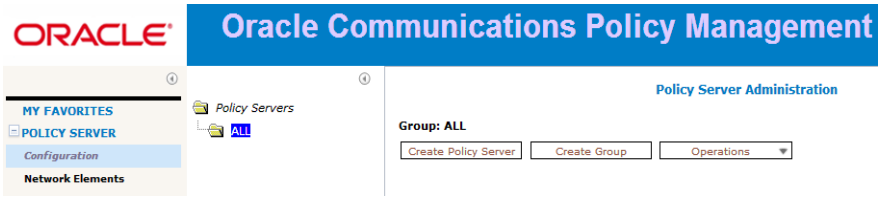
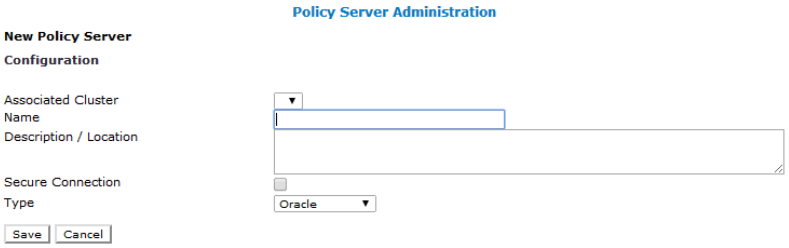
And the topology should now show an “active” and a “standby” server in the MPE cluster.
<table>
<tr><th></th><th>Name</th><th>Appl Type</th><th>IP</th><th>Server State</th></tr>
<tr><td></td><td>BOD</td><td>BoD</td><td></td><td></td></tr>
<tr><td></td><td>BOD-11-5</td><td>BoD</td><td>10.240.239.206</td><td>Active</td></tr>
<tr><td></td><td>CMP Site1 Cluster</td><td>CMP Site1 Cluster</td><td></td><td></td></tr>
<tr><td></td><td>CMP11-5</td><td>CMP Site1 Cluster</td><td>10.240.239.205</td><td>Active</td></tr>
<tr><td></td><td>MPE-S</td><td>MPE</td><td></td><td></td></tr>
<tr><td></td><td>MPE-1</td><td>MPE</td><td>10.240.239.201</td><td>Standby</td></tr>
<tr><td></td><td>MPE-2</td><td>MPE</td><td>10.240.239.200</td><td>Active</td></tr>
</table>

Same steps would need to be followed for Server-C in case of geo-redundant clusters and a secondary site is configured for MPE.</td></tr>
<tr><td>14.</td><td>Topology Settings for BOD and/or MA clusters</td><td>The same steps in this procedure would be followed for BOD and/or MA clusters’ topology settings if those components are part of the planned deployement of the Cable Policy solution.</td></tr>
</table>

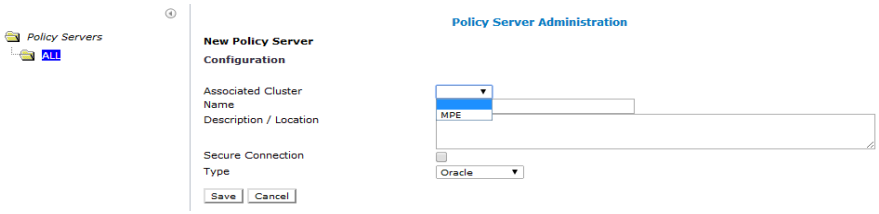
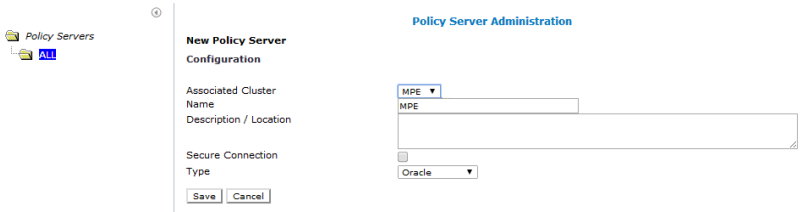
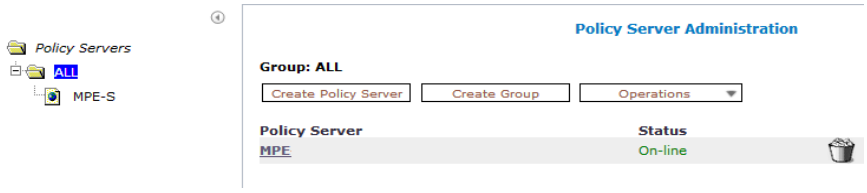
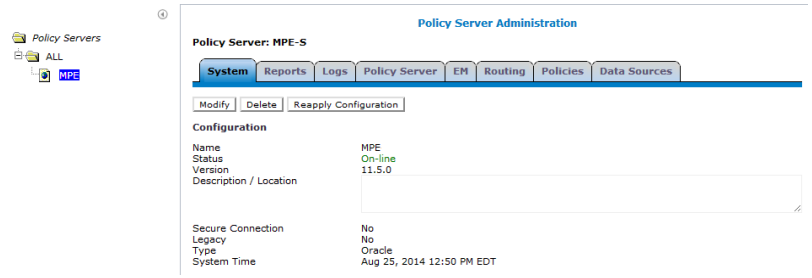
Procedure 11: Add Policy Servers (MPEs) to CMP Menu

This procedure will add the MPE Clusters to the Policy Server/Configuration tab of the CMP GUI.

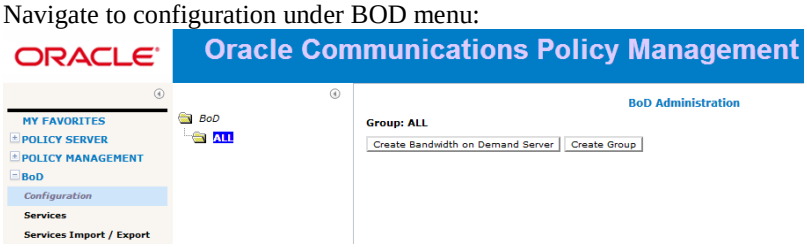
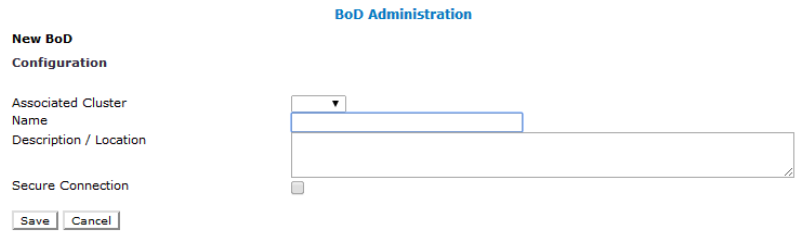
Procedure 11. Add Policy Servers (MPEs) to CMP Menu

S T E P #	The MPE clusters must be added to the CMP system as Policy Servers. This is done from the CMP GUI by choosing Policy Server: Configuration → Policy Server : All : Create Policy Server. When creating a Policy Server, the user will be provided with a list of MPE clusters to choose from. I.e. a Policy Server is a configuration of a MPE cluster. **Pre-requisite:** - CMP and MPE/BOD/MA clusters topology configuration are completed	
1. ☐	**Login to CMP GUI (using CMP cluster's VIP)**	From Browser, login to CMP GUI as admin (or a user with admin privileges)
2. ☐	**Create Policy Server**	Navigate to Configuration under Policy Server and click on "ALL" . You will be presnted with the option to Create Policy Server" 
3.	**Create Policy Server**	Click on "Create Policy Server" and the following screen presents. 

Procedure 11. Add Policy Servers (MPEs) to CMP Menu

4. ☐	**Create Policy Server**	Click on the "Associated Cluster" drop down tab. You should see all MPE cluster(s) by name that have been added previously to the CMP GUI in the Topology Settings:  Chosse the Policy Server (MPE cluster) to be created from the dropdown tab. Add a description if appropriate. Type will be "Oracle". 
5.	**Confirm Policy Server Creation**	Save the configuration. You should see that the selected MPE is now present and is in an "on-line" state"  Open up the newly created Policy Server(MPE) by clicking on the appropriate Policy Server now available in the navigation tree or on the MPE name link in the workspace area.  All Policy Server details will be displayed in the workspace area within multiple tabs .

Procedure 11. Add Policy Servers (MPEs) to CMP Menu

6.	**Confirm Policy Server Creation**	Click on the "Reports" Tab and confirm that both Server A and Server B are reported with their corresponding IP address. One blade (Server-A or Server-B) should be active and the other blade should be standby.
7. ☐	**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 serious problems that affect the system.
8.	**Adding BOD cluster to CMP GUI**	In case BOD is part of the Oracle's policy server deployment, BOD cluster(s) will need to be added to CMP GUI in the same manner done with MPE(s) in this procedure as follows: Navigate to configuration under BOD menu:  Then click on "Create Bandwidth on Demand Server" button:  Fill in the details and save then validate BOD cluster and servers appear online like done with MPEs

Procedure 11. Add Policy Servers (MPEs) to CMP Menu

9.	**Adding MA cluster to CMP GUI**	In case MA clusters are configured in topology settings, they can be added to CMP GUI also as MPE and BOD clusters from “Management Agents” under “Policy Server” menu item:

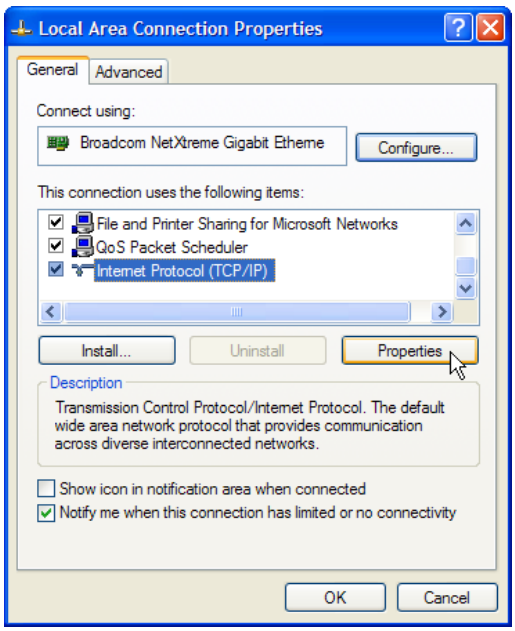
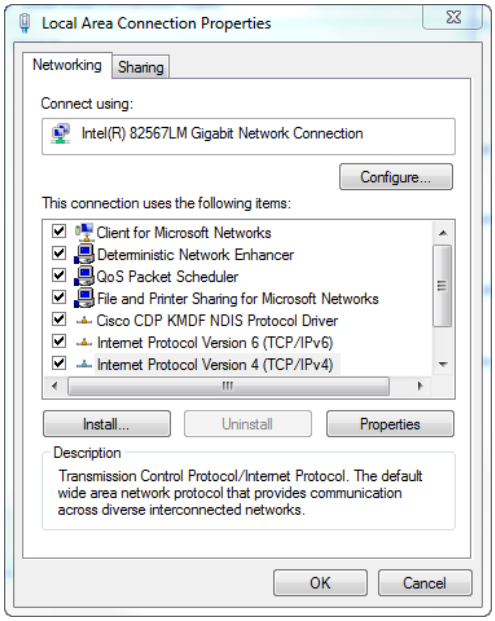
5. Supporting Procedures

Appendix A: Connecting to the HP DL360/380 G8 iLO Manager from a laptop

This procedure contains the steps to connect a laptop to the HPDL360/380 G8 iLO via an Ethernet connection.

If this is a newly shipped server and the iLO is being connected to for the first time there will be small pullout tab on the front of the server with the assigned ip address and the currently configured username/password for iLO access.

Appendix A Connecting to the HP DL360/380 G6/8 iLO Manager from a laptop

Step	Procedure	Result	
		Windows XP	**Windows 7**
1. ☐	Access the laptop network interface card's TCP/IP "Properties" screen. **NOTE:** *For this step follow the instruction specific to the laptop's OS*	• Go to Control Panel • Double-click on Network Connections • Right-click the wired Ethernet Interface icon and select "Properties" • Select "Internet Protocol (TCP/IP)" and select "Properties"  	• Go to Control Panel. • Double-click on Network and Sharing Center • Select 'Local Area Connection'. • Select the 'Properties' button. • Select "Internet Protocol Version 4 (TCP/IPv4)" and hten select the 'Properties' button. 

Appendix A Connecting to the HP DL360/380 G6/8 iLO Manager from a laptop

2. ☐

1) Click "**use the following IP address**",

set the **IP address**:

for example: 192.168.101.19

Subnet mask:

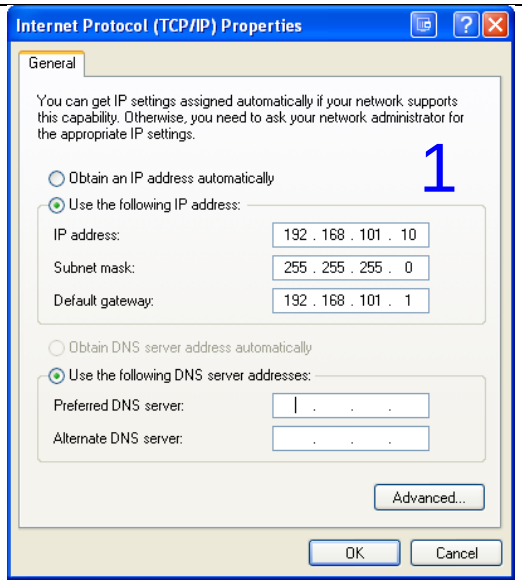
255.255.255.0

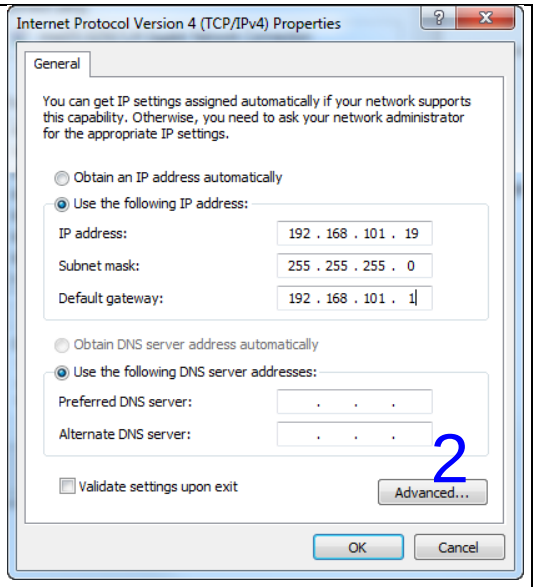
Default gateway:

192.168.101.1

click **"OK"**.

2) Click **"Close"** from the network interface card's main "Properties" screen.

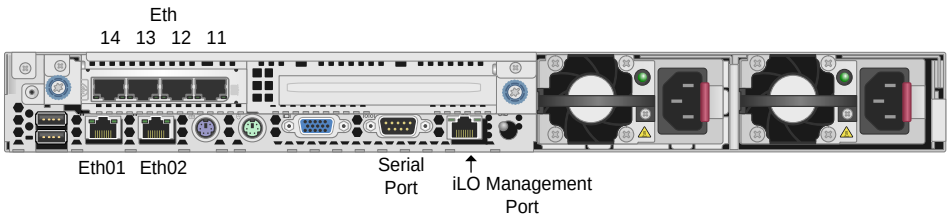




3. ☐

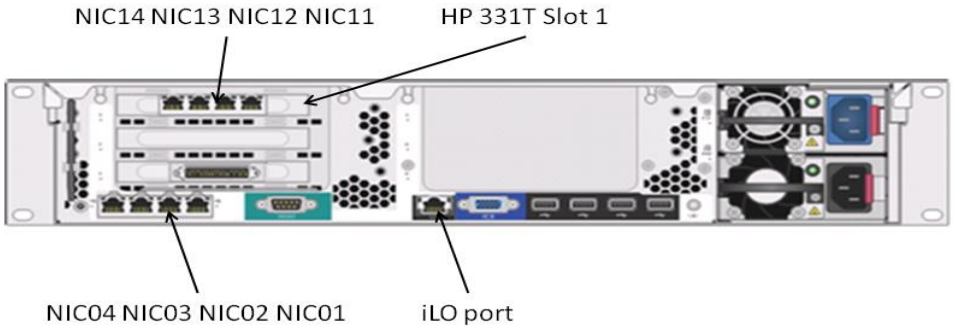
Connect the laptop's Ethernet port directly to the iLO port using a standard Cat-5 cable.

DL360G6 rear view :



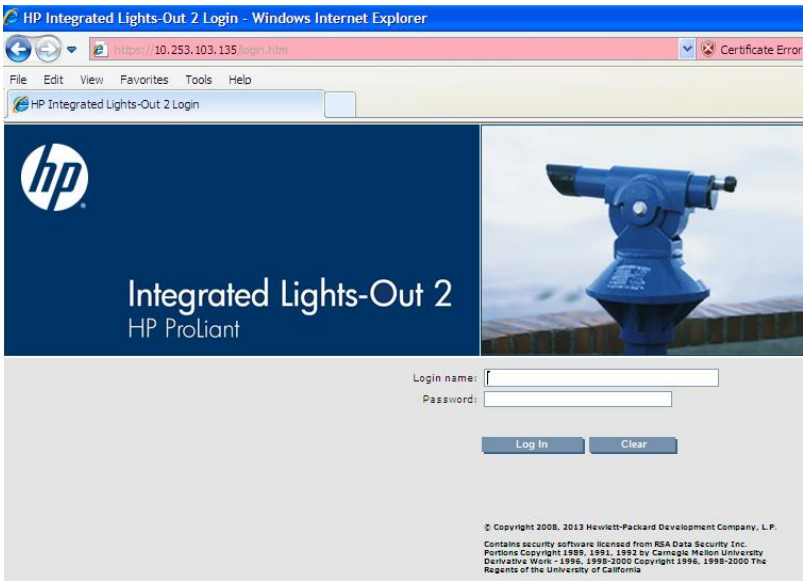
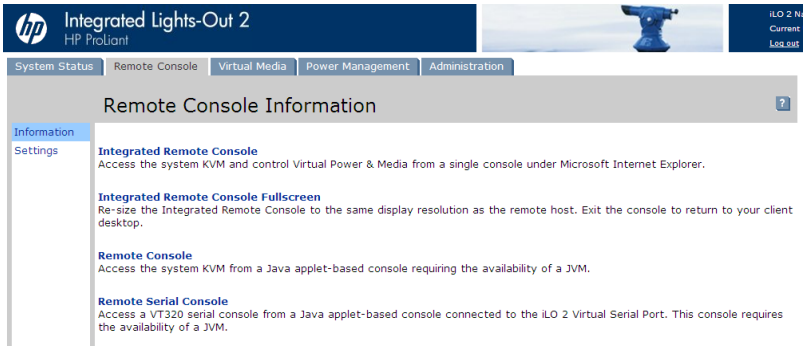
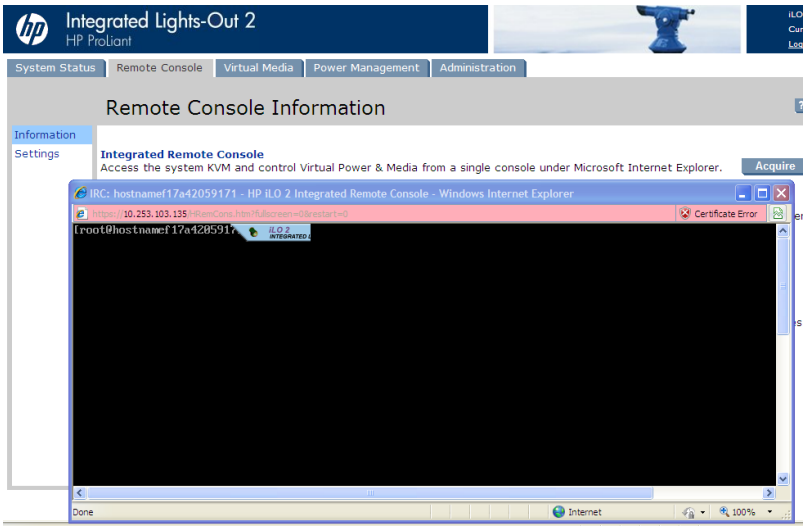
DL360pGen8 rear view:

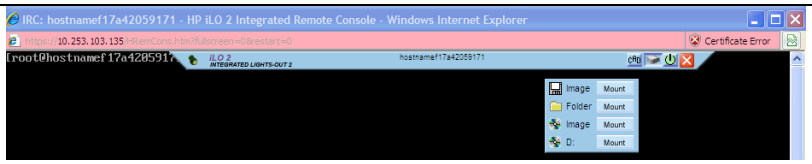
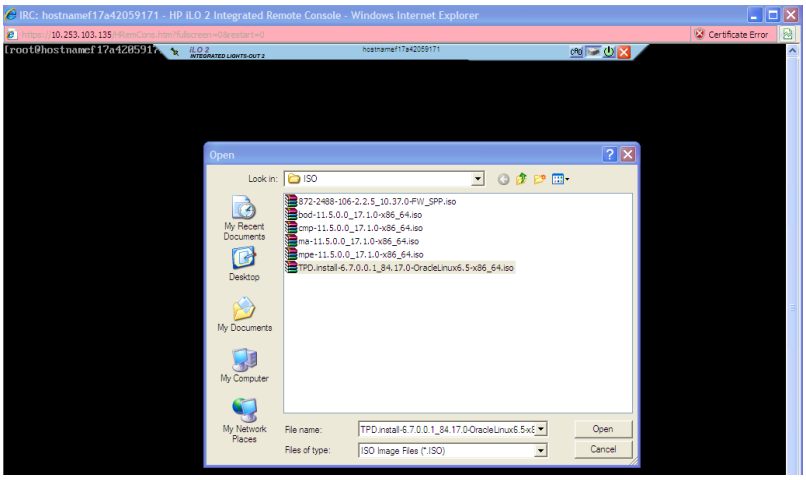
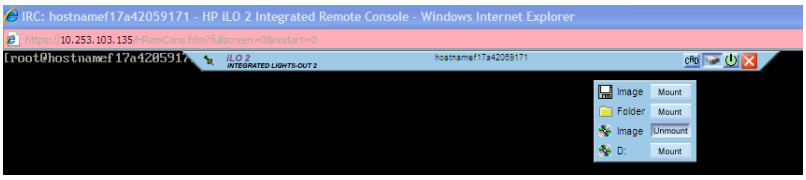
DL380pGen8 rear view:

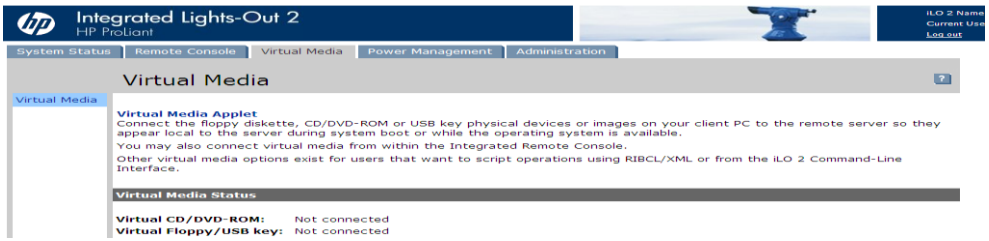
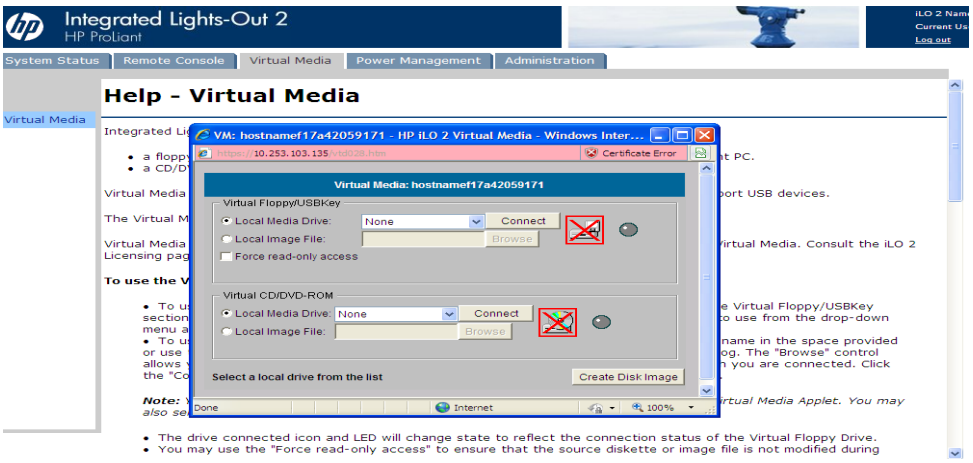
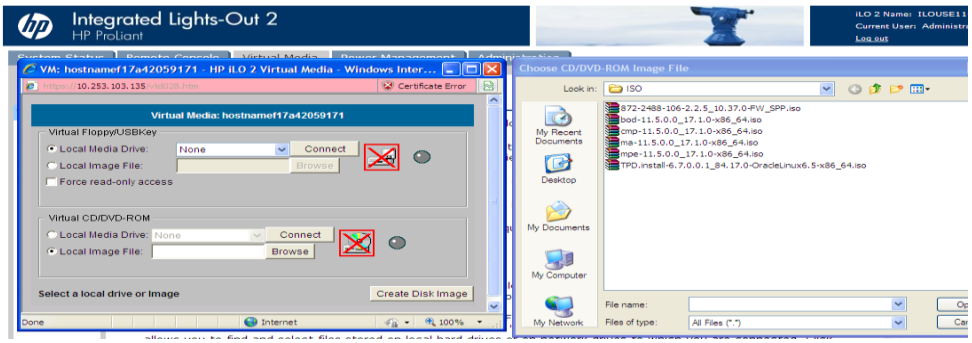
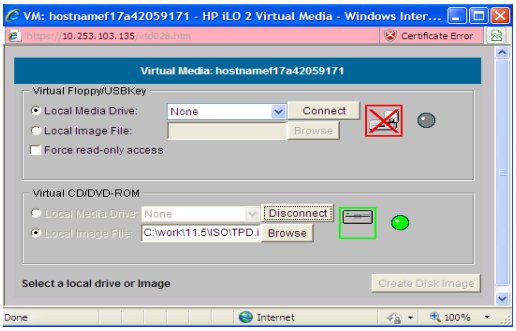


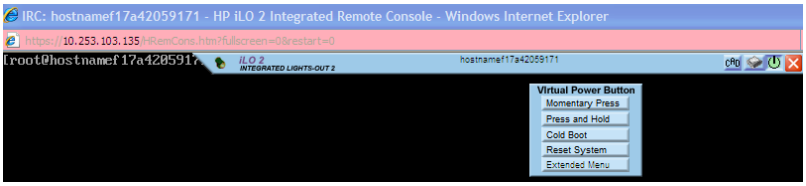
THIS PROCEDURE HAS BEEN COMPLETED

Appendix B: Use Remote Console of the iLO Manager to virtually mount an iso image file (HL DL360)

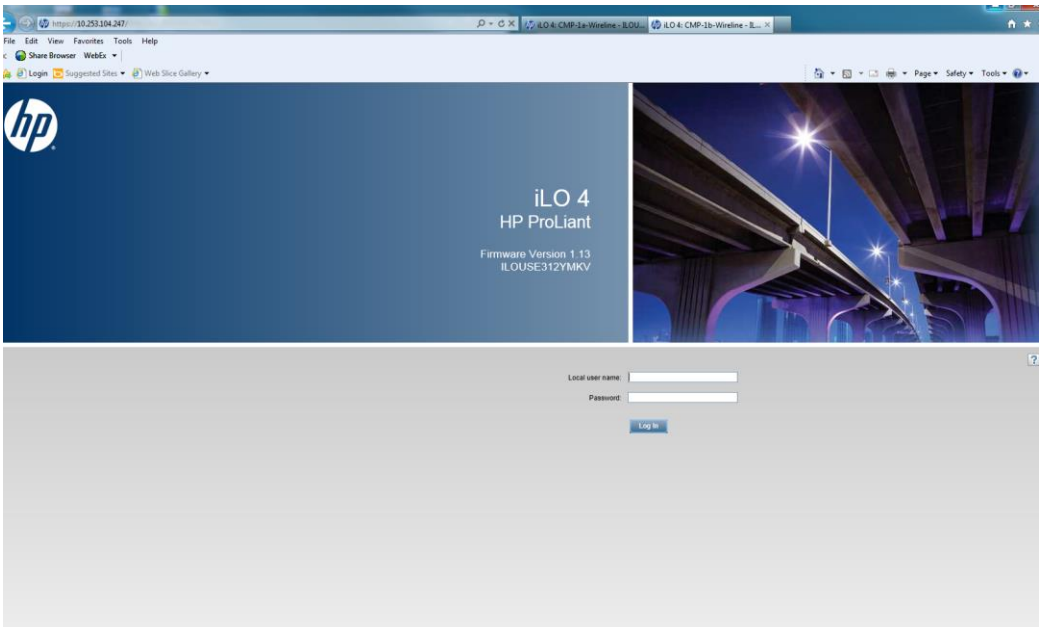
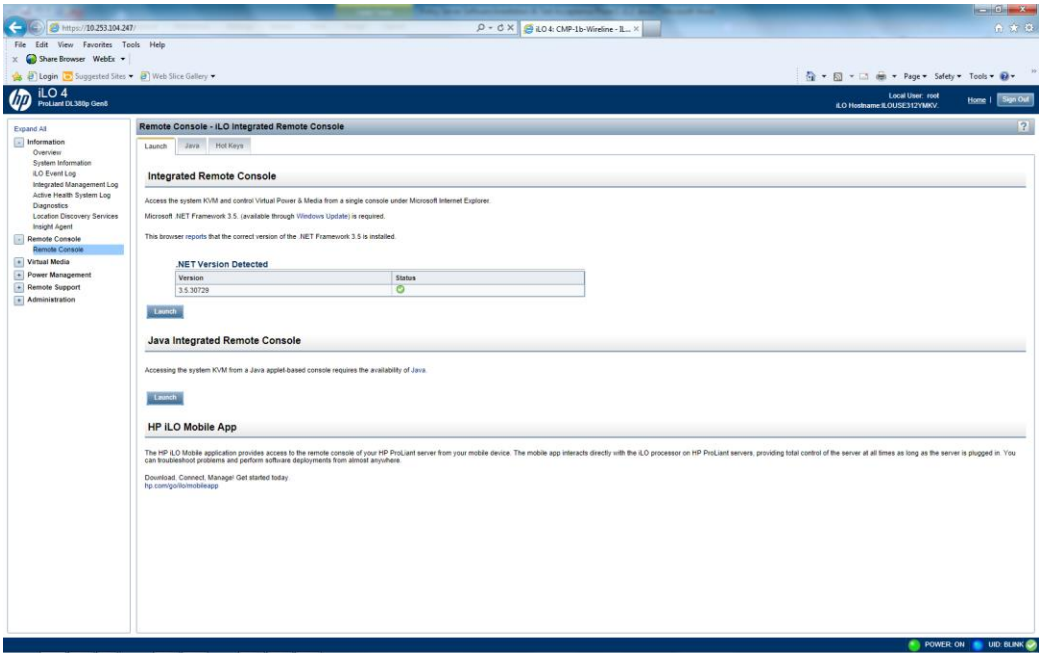
Step	Procedure	Result
1. ☐	Log into the iLO Manager with a browser pointed at the iLO IP address	
2. ☐	Navigate to *Remote Console.* .	
3. ☐	Launch the Remote Console by clicking on Integrated Remote Console or the legacy remote Console	

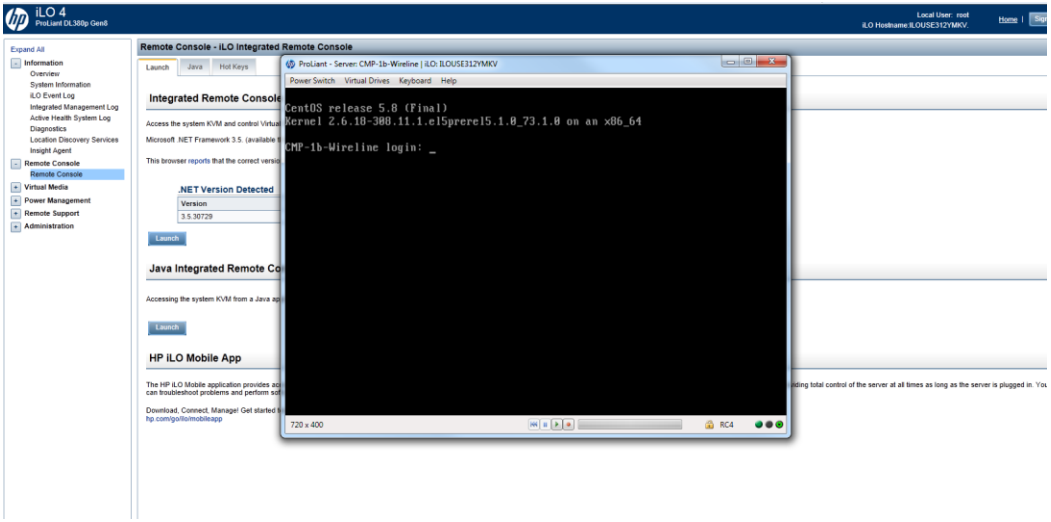
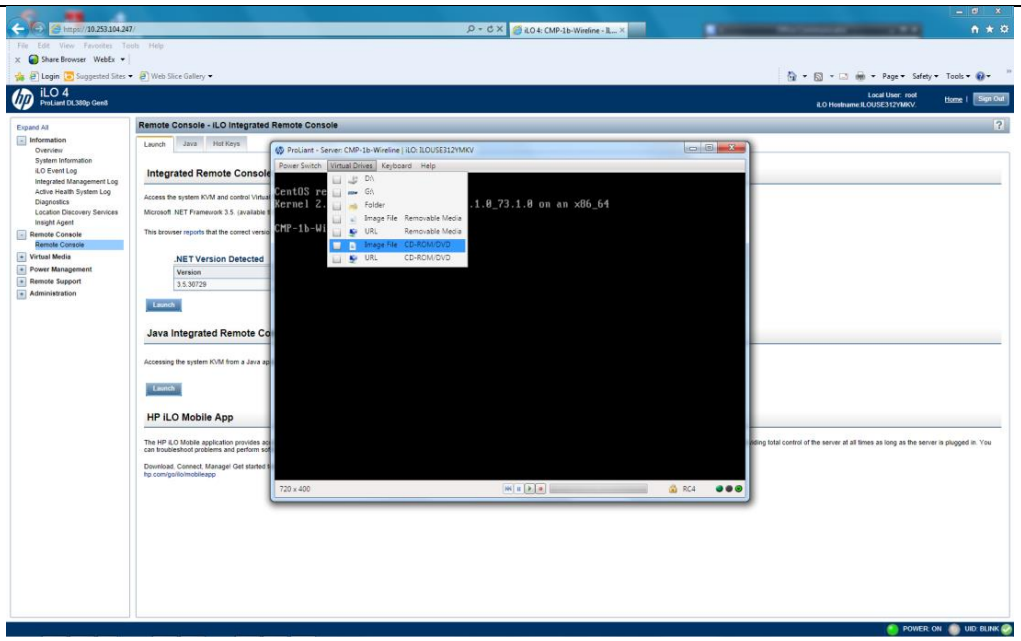
4. ☐	Open up the drop down menu of the remote console and click on the "mount" button besides image	
5. ☐	Browse to the iso image location on your local drive, highlight it and click "open" on the browse dialog box to mount the ISO image.	
6. ☐	To "unmount" an image file, return to the drop down menu in the remote console and click "unmount" button	

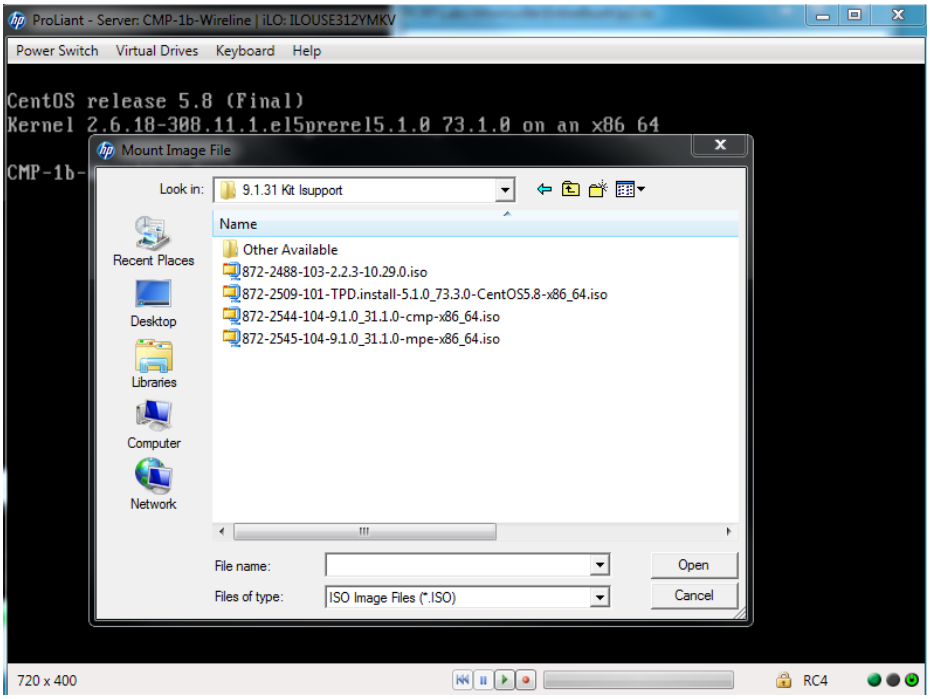
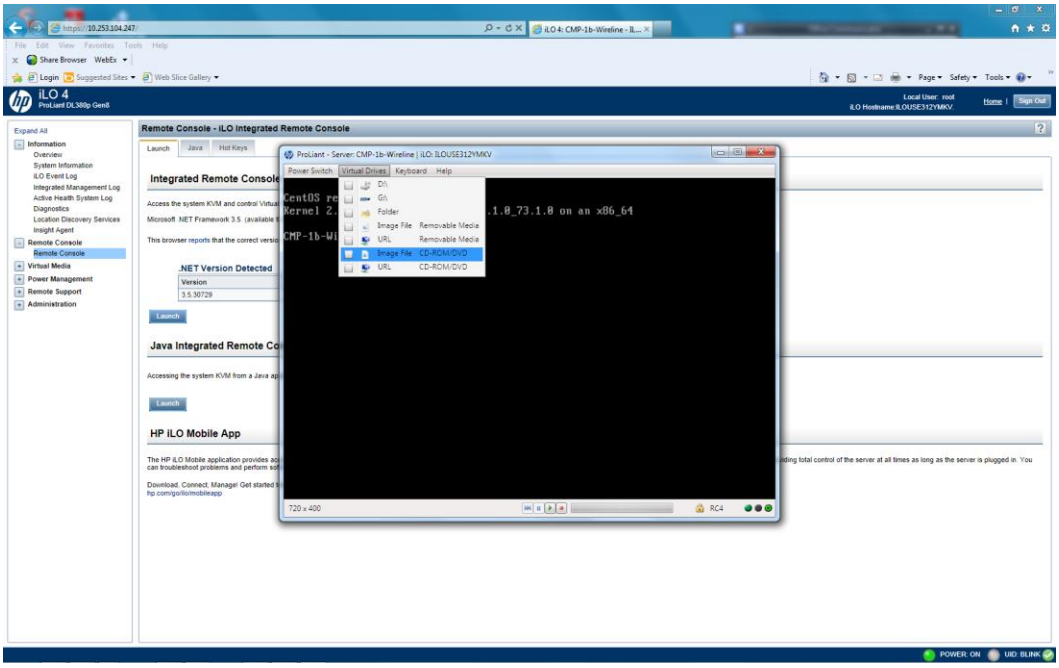
7.	Alternatively ISO image could be mounted via virtual media applet	Click on the "Virtual media" tab in the iLO main screen:  Click on the "Virtual media applet" hyperlink:  Check the checkbox besides the "Local image file" option under virtual CD/DVD-ROM and click "Browse"  Locate the file on the local drive and click "open" in the browse dialog box then click connect on the virtual media applet to mount the iso image:  To unmount the ISO image, just click "disconnect" button.

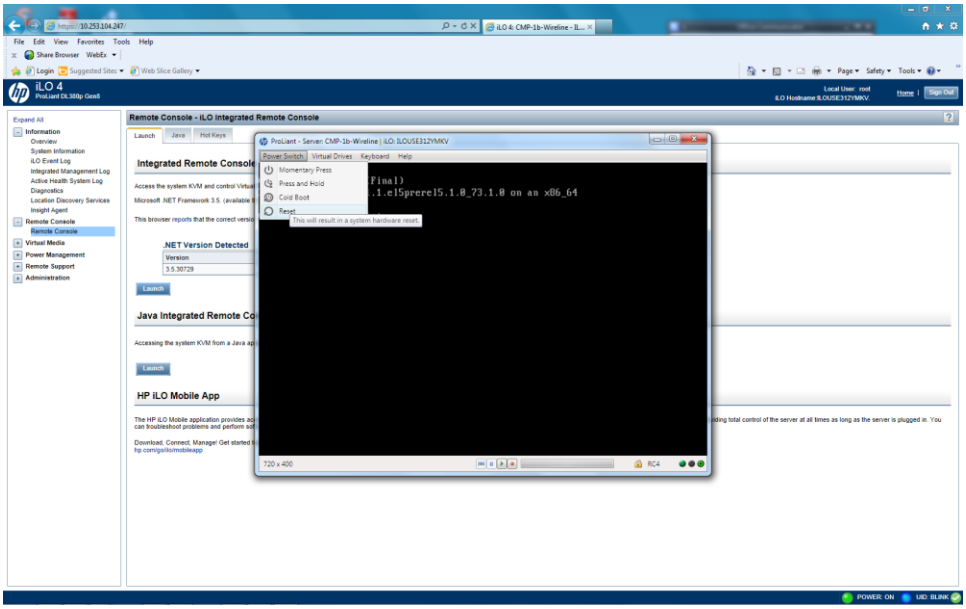
8. ☐	A reboot can be executed from within the remote console by clicking on the <Power Options> tab of the remote console and choosing <Reset> . Alternately the “shutdown –r now” can be issued form the command line prompt	 You have now mounted and “unmounted” an image file using the remote console of the iLO interface. You may be requested to either “mount” or “unmount” an image file prior to rebooting the server as part of a specific procedure
THIS PROCEDURE HAS BEEN COMPLETED		

Appendix C: Use Remote Console of the iLO Manager to virtually mount an iso image file (HP DL380)

Step	Procedure	Result
1. ☐	Log into the iLO Manager with a browser pointed at the iLO IP address	
2. ☐	Navigate to *Remote Console.* .	

3. ☐	Launch the Remote Console using by clicking on <Launch> of the .NET version of the remote Console	
4. ☐	Open up the drop down menu of the remote console under <Virtual Drives> and choose <Image file CD-ROM DVD>	

5. ☐	You will be presented with a <Mount Image File> dialog. Choose and "open" the image file required, which should be accessible locally. The <Mount Image File> window will close and the "iso image file" selected has now been "mounted".	
6. ☐	To "unmount" an image file, return to the <Virtual Drive> drop down tab in the remote and <u>uncheck</u> the "check box" for *<Image file CD-ROM DVD>*.	

7. ☐	A reboot can be executed from within the remote console by clicking on the <Power Options> tab of the remote console and choosing <Reset> . Alternately the “shutdown –r now” can be issued form the command line prompt	 You have now mounted and “unmounted” an image file using the remote console of the iLO interface. You may be requested to either “mount” or “unmount” an image file prior to rebooting the server as part of a specific procedure
THIS PROCEDURE HAS BEEN COMPLETED		

Appendix D: Configure SNMP

SNMP configuration architecture is based on using traps to notify a network management system of events and alarms that are generated by any policy component (MPE, MA, BOD)
Alarms and telemetry data are continuously collected from the entire Policy Application Network and stored on the CMP servers. Alarms will then cause a trap to be sent as a notification of an event.

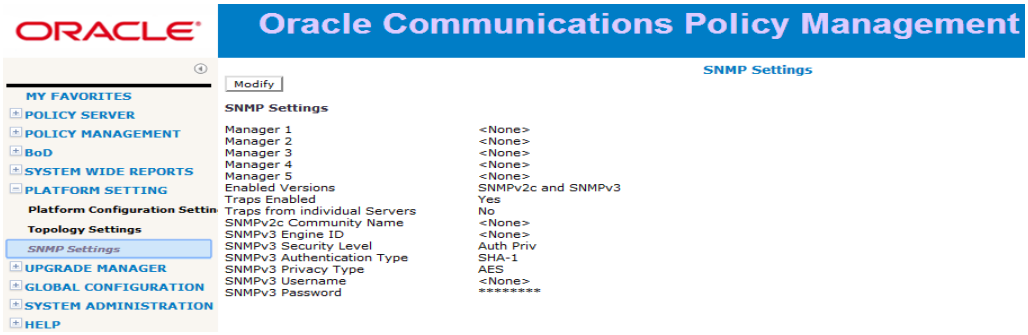
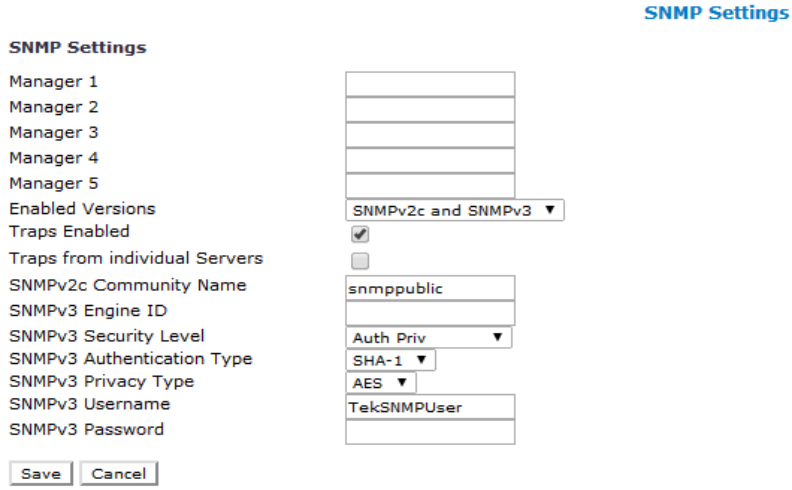
SNMP can be configured in either of 2 ways:

- The Policy system can be configured so that the CMP is the source of all traps.
- The Policy systems can be configured to allow each server to generate its own traps and deliver them to the SNMP management server(s).

Policy support multiple SNMP Versions:

- SNMP version 2c (SNMPv2c) and SNMP version 3 (SNMPv3) are supported.
- SNMP version 1 (SNMPv1) is not supported. On the SNMP Setting Edit screen
- When you configure SNMPv2c, you must use a community that is not "public" or "private".
- When you configure SNMPv3, you must enter an "Engine ID", and a "username" and "password" for the SNMPv3 user.

Note: SNMP settings configuration must be done on a server that is the Active Blade in the Primary Cluster. A banner warning appears if the login is not on the primary/active CMP. SNMP cannot be configured from servers other than the active/primary CMP.

Step	Procedure	Result
1. ☐	Log into CMP GUI as admin or with user that has proper privilege then navigate to SNMP settings under Platform Configuration	
2. ☐	Click modify button to configure the SNMP then “Save” when done	

The SNMP settings are described as follows:

Field Name	Description
Manager 1-5	SNMP Manager to receive traps and send SNMP requests. Each Manager field can be filled as either a valid host name or an IP address. A hostname should include only alphanumeric characters. Maximum length is 20 characters, and it is not case-sensitive. This field can also be an IP address. An IP address should be in a standard dot-formatted IP address string. The field is required to allow the Manager to receive traps. By default, these fields are empty.
Enabled Versions	Supported SNMP versions: • SNMPv2c • SNMPv3 • SNMPv2c and SNMPv3 (default)
Traps Enabled	Enable sending SNMPv2 traps (box checked ; default) Disable sending SNMPv2 traps (box not checked)
Traps from Individual Servers	Enable sending traps from an individual server (box checked). Sending traps from the active CMP (box not checked; default)
SNMPv2c Community Name	The SNMP read-write community string. The field is required if SNMPv2c is enabled. The name can contain alphanumeric characters and cannot exceed 31 characters in length. The name cannot be either “private” or “public.” The default value is “snmppublic”.
SNMPv3 Engine ID	The length can be from 10 to 64 digits. The default is no value (empty).
SNMPv3 User Name	The SNMPv3 User Name. The field is required if SNMPv3 is enabled. The name must contain alphanumeric characters and cannot not exceed 32 characters in length. The default value is “TekSNMPUser”.
SNMPv3 Security Level	SNMPv3 Authentication and Privacy options. **1.** “No Auth No Priv” - Authenticate using the Username. No Privacy. **2.** “Auth No Priv” - Authentication using MD5 or SHA1 protocol. **3.** “Auth Priv” - Authenticate using MD5 or SHA1 protocol. Encrypt using the AES and DES protocol. The default value is “Auth Priv”.
SNMPv3 Authentication Type	Authentication protocol for SNMPv3. Options are: **1.** SHA-1” - Use Secure Hash Algorithm authentication. **2.** “MD5” - Use Message Digest authentication. The default value is “SHA-1”.
SNMPv3 Privacy Type	Privacy Protocol for SNMPv3. Options are: **1.** “AES”: Use Advanced Encryption Standard privacy. **2.** “DES”: Use Data Encryption Standard privacy. The default value is “AES”.

SNMPv3 Password	Authentication password for SNMPv3. This value is also used for msgPrivacyParameters. SNMPv3 Password The field is required If SNMPv3 is enabled. The length of the password must be between 8 and 64 characters; it can include any character. The default value is “snmpv3password.”