Oracle® Communications Policy and Charging Rules Function

PCRF 9.4 to 11.5 Cable Policy Upgrade Procedure

Release 11.5

E61662-01

February 2015

ORACLE®

Oracle® Communications Policy and Charging Rules Function, 9.4 to 11.5 Cable Policy Upgrade Procedure, Release 11.5

CAUTION: Use only the Upgrade procedure included in the Upgrade Kit.
Before upgrading any system, please access Oracle's Customer Support site and review any Technical Service Bulletins (TSBs) that relate to this upgrade.
Refer to G for instructions on accessing this site.

Contact MOS and inform them of your upgrade plans prior to beginning this or any upgrade procedure.

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**

1.1 PURPOSE AND SCOPE 4
1.2 SUPPORTING DOCUMENTATION 4
1.3 9.4 UPGRADE CONSIDERATIONS 4
1.4 UPGRADE INFRASTRUCTURE 5
1.5 REQUIRED MATERIALS 5
1.6 ACRONYMS 5

2. CMP CLUSTER(S) UPGRADE **6**

2.1 CMP PRE-UPGRADE CHECKS 6
Procedure 1: CMP pre-Upgrade checks 6
Procedure 2: Exchange SSH Keys 8
2.2 PREPARE ISO IMAGE 9
Procedure 3: Prepare ISO image 9
2.3 STAGE UPGRADE SCRIPTS 11
Procedure 4: Copy over upgrade scripts from 11.5 ISO image 11
2.4 UPGRADE CMP SERVERS 14
Procedure 5: Upgrade CMP Servers 14
2.5 UPGRADED CMP CLUSTER VALIDATION 22
Procedure 6: Post Upgrade Validation 22
2.6 BACK OUT THE UPGRADE 24
Procedure 7: Backing out the upgrade 24
2.7 ACCEPT THE UPGRADE 26
Procedure 8: Accept the upgrade 26

3. MA/MPE-R/MPE-S/BOD CLUSTER UPGRADES **28**

3.1 MA CLUSTER UPGRADE 28
Procedure 9: MA Cluster Upgrade 28
3.2 MPE-R/MPE-S CLUSTER UPGRADE 34
Procedure 10: MPE-R/MPE-S Cluster Upgrade 34
3.3 BOD CLUSTER UPGRADE 43
Procedure 11: BOD Cluster Upgrade 43

1. Introduction

1.1 Purpose and Scope

Due to the recent transition OF Cable Policy solution to TPD platform, software upgrade to release 11.5 will only be supportable from TPD based Releases 9.3 and 9.4.
This document describes the procedures to upgrade Cable Policy solution from release 9.4 to release 11.5. The upgrade includes the TPD upgrade.

Cable Policy software 9.4 can be installed on any of the following supported HP RMS hardware types:

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

Hence the upgrade to 11.5 is also supported on any of these Hardware types.

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

Note: During the upgrade period the Cable Policy system may have configuration where some of CMPs, MAs, MPEs, and BoD-AMs are running Release 9.4 software and some are running Release 11.5 software. This could result in some alarms which will be suppressed after the full solution is upgraded and reaches one coherent release.

1.2 Supporting Documentation

[1] *PD001866 Formal Peer Review Process*
[2] *FE007452 Cable Reference Architecture*
[3] *FD008005 Release 11.5 Upgrade*
[4] *TR007406 Upgrade guide to 11.5 from releases 9.3/9.4*
[5] *FD008102 Policy platform multiple modes*

1.3 9.4 upgrade considerations

- The upgrade path from 9.4 to 11.5 requires that policy solution is on 9.4.1 release to be upgraded to 11.5, accordingly all 9.4 customers will need to upgrade to 9.4.1 if they are on earlier 9.4 revision before going to 11.5 release.

- Back Plane link should be available and configured before upgrade since it is a mandatory setup to complete the upgrade process to 11.5 successfully.

Cable Policy solution is upgraded in the following order:

- CMP (Primary Site, then Geo-Redundant Site if present)
- MA
- MPE-R
- MPE-S
- BoD-AM

1.4 Upgrade infrastructure

Upgrade is supported from Release 9.4 on all supported HP rack mount server configurations (Gen6, Gen7 and Gen8).

Source	Destination	Hardware	Direct-Link before upgrade	Direct-Link after upgrade
9.4	11.5/Cable	DL360G6	Enable	Enable
		DL360G7	Enable	Enable
		DL360G8	Enable	Enable
		DL380G8	Enable	Enable

1.5 Required Materials

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

1.6 Acronyms

Acronym	Definition
BOD	Bandwidth on Demand
GUI	Graphical User Interface
HA	High Availability
MA	Management Agent
MPE-R	Multimedia Policy Engine (Routing) also known as tier 1 Policy Server
MPE-S	Multimedia Policy Engine (Serving) also known as tier 2 Policy Server
CMP	Camiant Management Platform
OAM	Operation, Administration and Management
SIG	Signaling Network
CD	Compact Disk
iLO	Integrated Lights Out manager
IE	Internet Explorer
IPM	Initial Product Manufacture – the process of installing TPD on a hardware platform
OS	Operating System (e.g. TPD)
RMS	Rack Mount Server
SFTP	SFTP Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
TPD	Tekelec Platform Distribution

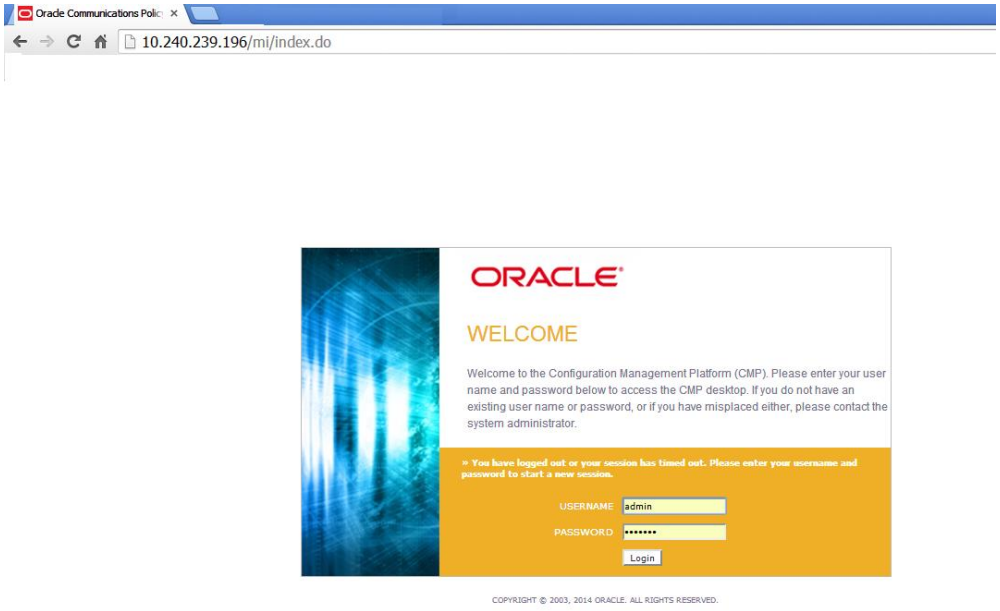
Table 1 Acronyms

2. CMP Cluster(s) Upgrade

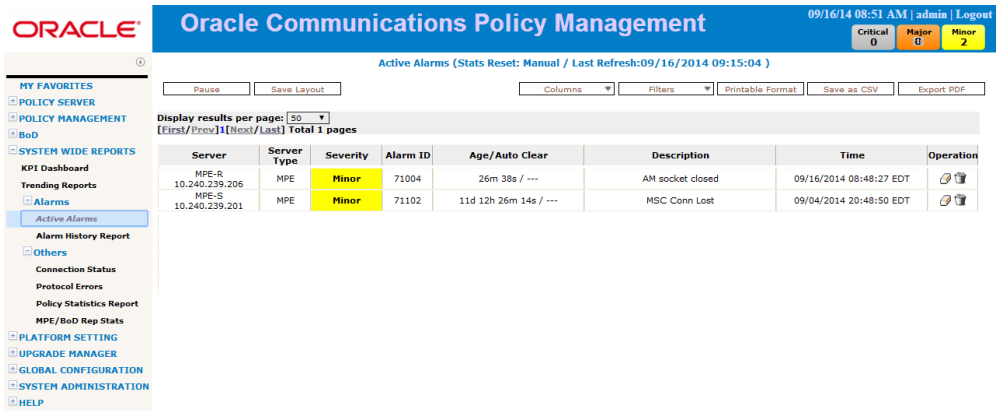
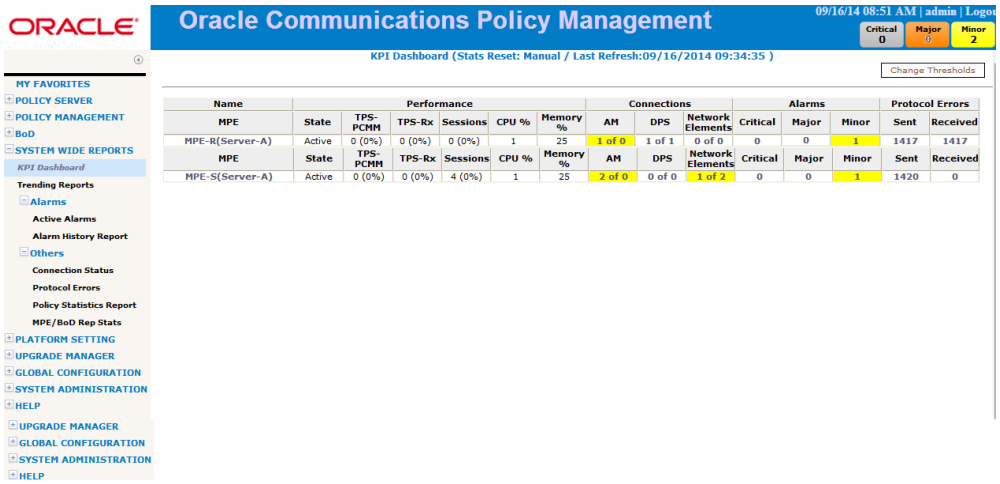
2.1 CMP Pre-Upgrade checks

Procedure 1: CMP pre-Upgrade checks

Procedure 1. CMP Pre-Upgrade checks

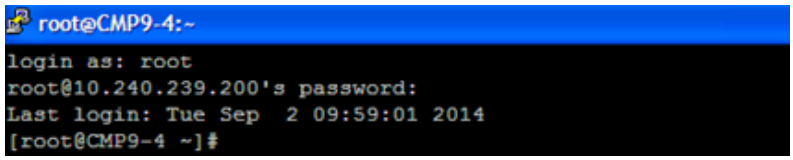
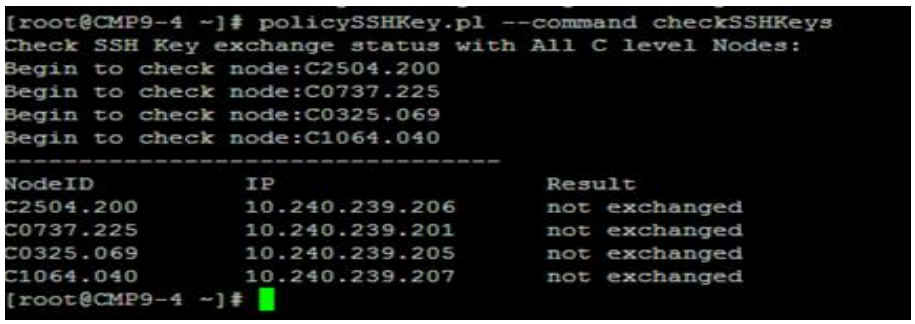
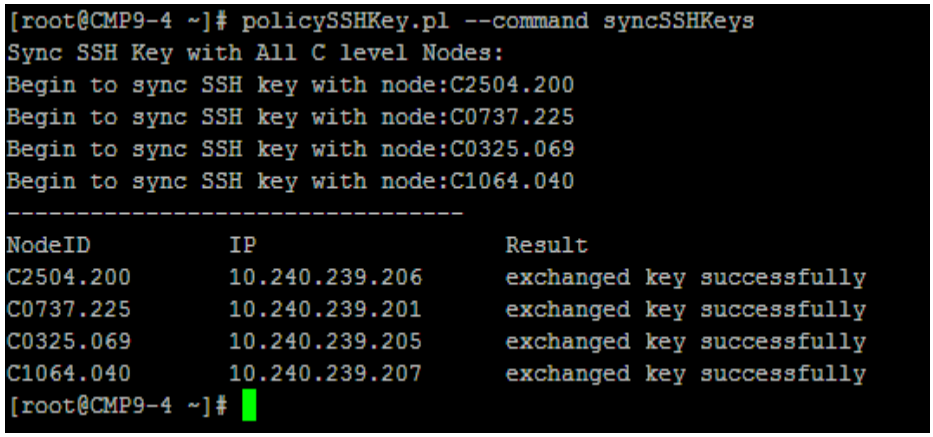
S T E P #	This procedure will check the health and state of every component of the Cable Policy solution to ensure the readiness before the upgrade. **Needed material:** - Access to customer's network to access the Cable Policy solution - CMP OAM VIP - Admin login to CMP	
1. ☐	**Computer on solutions' network or remote access to solutions' network:** Login to CMP	Open a browser and enter CMP's OAM VIP to Navigate to CMP GUI:  Enter the password for the admin account and push "Login": 

Procedure 1. CMP Pre-Upgrade checks

2. ☐	**CMP GUI:** Check active alarms	Navigate to System Wide Reports → Alarms → Active Alarms  Inspect the displayed MAJOR alarms and analyze them to confirm they will not impact the upgrade process.
3. ☐	**CMP GUI:** Check KPI Dashboard	Navigate to System Wide Reports → KPI Dashboard  Ensure system is not overloaded and running in an adequate metrics from CPU / Memory / transactions perspective

Procedure 2: Exchange SSH Keys

Procedure 2: Exchange SSH keys from Active CMP

S T E P #		
	This procedure will make sure SSH keys are exchanged from Active CMP to the different servers of the Cable Policy solution servers. **Needed material:** - Root access to CMP active CLI	
1. ☐	**9.4 Active CMP CLI:** Connect to CLI	SSH to 9.4 Active CMP CLI as root: 
2. ☐	**9.4 Active CMP CLI:** Validate if keys are exchanged	Run the following command to check if SSH keys status: 
3. ☐	**9.4 Active CMP CLI:** Exchange the SSH keys	In case the results of the previous step include "not exchanged", run the following command to perform the SSH keys exchange: 

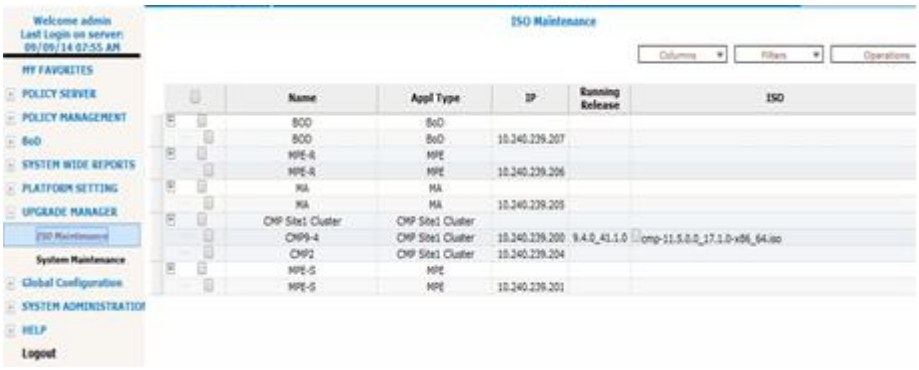
2.2 Prepare ISO image

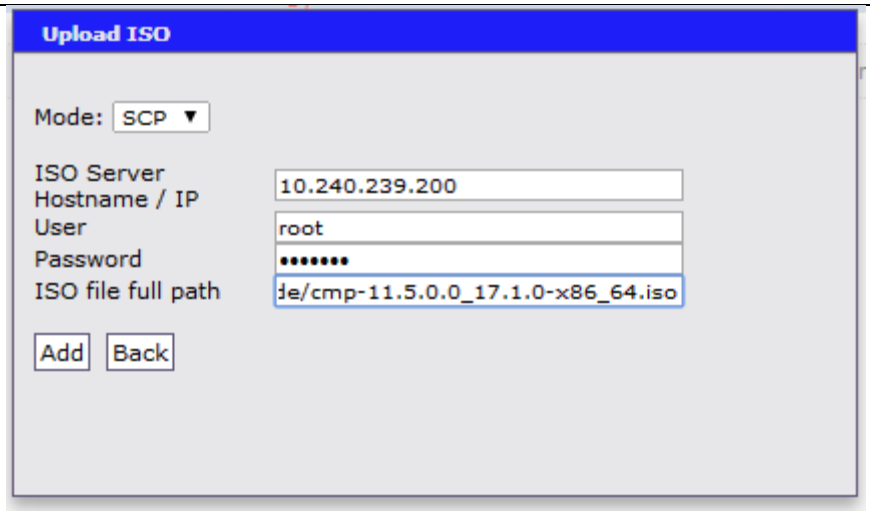
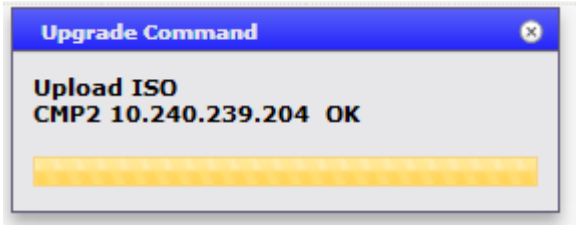
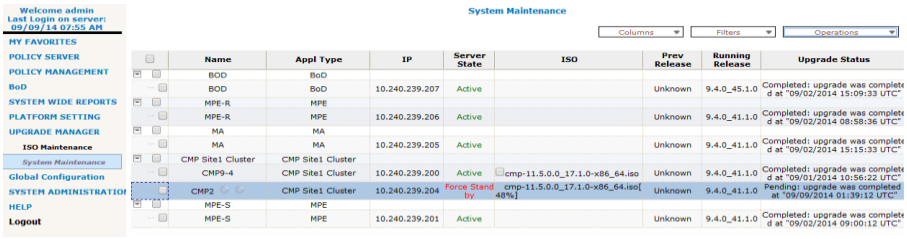
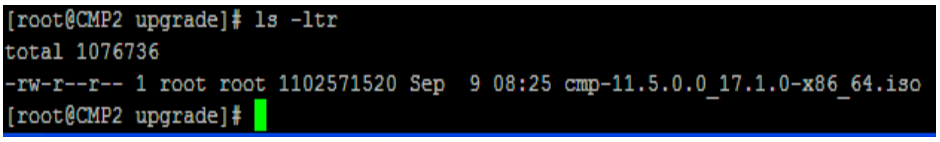
Procedure 3: Prepare ISO image

Procedure 3: Prepare ISO image

S T E P #	This procedure will transfer the ISO image of 11.5 CMP into the upgrade path in preparation for the upgrade. **Needed material:** - 11.5 CMP iso image file.	

1. ☐	**9.4 Active CMP server:** Transfer 11.5 ISO image file to the upgrade path	Transfer the 11.5 ISO image file into the upgrade path (/var/TKLC/upgrade/) of the 9.4 active CMP server:
		
		`[root@CMP9-4 upgrade]# pwd`
		`/var/TKLC/upgrade`
		`[root@CMP9-4 upgrade]# ls -ltr`
		`total 1076736`
		`-rw-r--r-- 1 root root 1102571520 Aug 8 13:01 cmp-11.5.0.0_17.1.0-x86_64.iso`
		`[root@CMP9-4 upgrade]#`

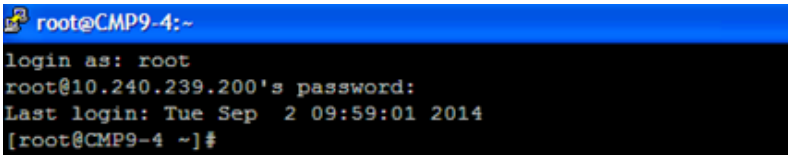
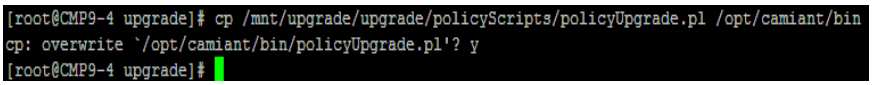
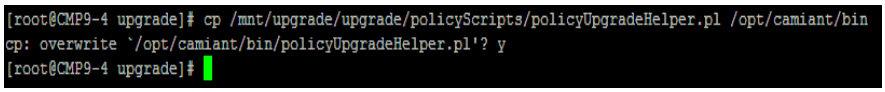
2. ☐	**9.4 CMP GUI:** Upload 11.5 CMP ISO image via CMP GUI	11.5 ISO image file can be copied over to upgrade path via CMP GUI as shown in the below steps: Login to CMP GUI as administrator then navigate to Upgrade Manager → ISO Maintenance:  Check the active CMP server then expand “Operations” menu and select “Upload ISO” :  Fill in the upload ISO window with the details to transfer the ISO image :

		 Confirm the process completed successfully : 
3. ☐	**9.4 CMP GUI:** Confirm ISO image transfer completion	Navigate to Upgrade Manager → System Maintenance to confirm the 11.5 CMP ISO image appear under ISO column for the CMP cluster 
4. ☐	**9.4 CMP CLI:** Confirm ISO image exists under upgrade path	Login to 9.4 CMP servers as root then validate ISO image file exists under upgrade path (/var/TKLC/upgrade): 

2.3 Stage upgrade scripts

Procedure 4: Copy over upgrade scripts from 11.5 ISO image

Procedure 4. Copy upgrade scripts from 11.5 ISO image

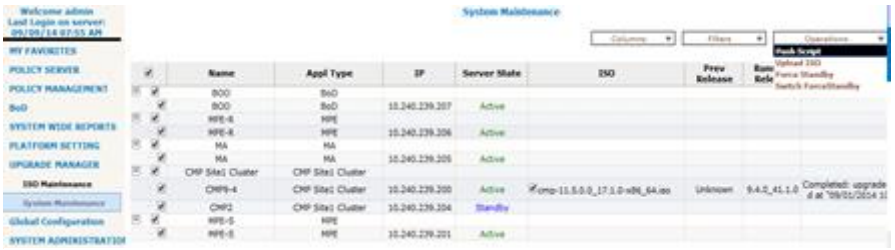
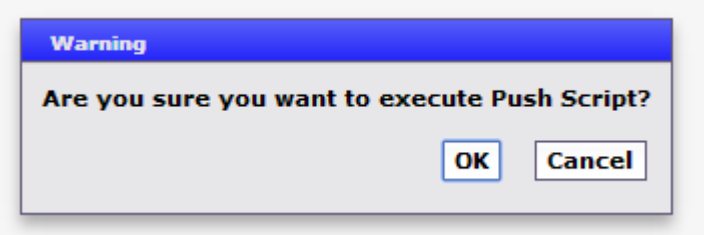
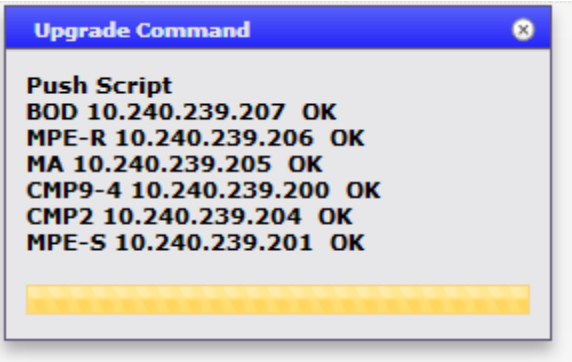
STEP #		
	This procedure will copy necessary upgrade scripts from 11.5 CMP ISO image overwriting the existing scripts. **Needed material:** - 9.4 Active CMP CLI access	
1. ☐	**9.4 Active CMP CLI:** SSH to the server's CLI	Login to the 9.4 active CMP CLI as root: 
2. ☐	**9.4 Active CMP CLI:** mount ISO image	Run the following command to mount the 11.5 CMP ISO image file: ***mount -o loop /var/TKLC/upgrade/cmp-11.5.0.0_17.1.0-x86_64.iso /mnt/upgrade*** 
3. ☐	**9.4 Active CMP CLI:** Extract needed upgrade scripts	Run the following commands to extract the upgrade scripts overwriting the old scripts: • cp /mnt/upgrade/upgrade/policyScripts/policyUpgrade.pl /opt/camiant/bin  • cp /mnt/upgrade/upgrade/policyScripts/policyUpgradeHelper.pl /opt/camiant/bin •  • cp /mnt/upgrade/upgrade/policyScripts/qpSSHKeyProv.pl /opt/camiant/bin 

Procedure 4. Copy upgrade scripts from 11.5 ISO image

4. ☐	**9.4 Active CMP CLI:** Unmount ISO image	Run the following command to unmount the 11.5 CMP ISO image file:
		
		umount /mnt/upgrade
		
		`[root@CMP9-4 upgrade]# umount /mnt/upgrade`
		`[root@CMP9-4 upgrade]#`

5.	**9.4 Active CMP CLI: E**xchange SSH keys to all servers configured in the topology	Run the following command to exchange SSH keys to all servers configured in the topology :
		
		qpSSHKeyProv.pl –prov –user=root
		
		`[root@CMP9-4 ~]# qpSSHKeyProv.pl --prov --user=root`
		
		`The password of root in topology:`
		`Connecting to root@CMP9-4 (10.240.239.200) ...`
		`Connecting to root@MPE-R (10.240.239.206) ...`
		`Connecting to root@CMP2 (10.240.239.204) ...`
		`Connecting to root@MPE-S (10.240.239.201) ...`
		`Connecting to root@MA (10.240.239.205) ...`
		`Connecting to root@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 CMP2 (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.`
		
		`[root@CMP9-4 ~]#`
		
		Note that root password needs to be supplied for script to run successfully.

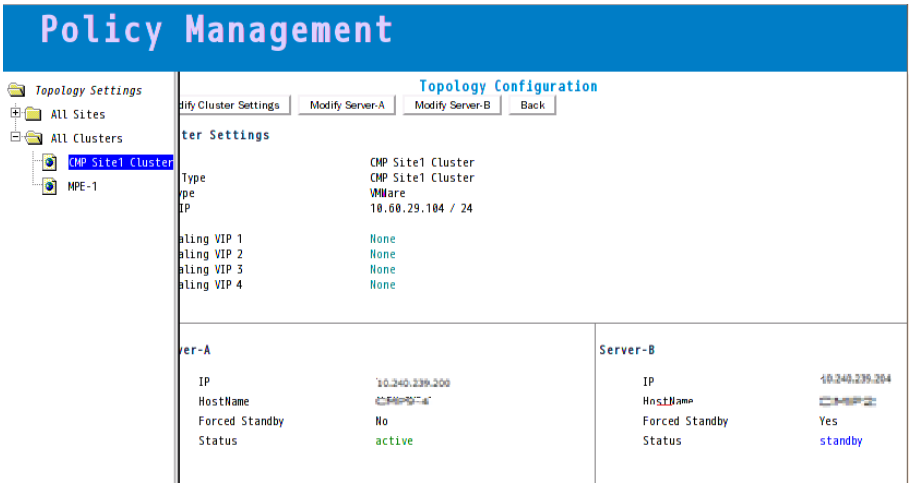
Procedure 4. Copy upgrade scripts from 11.5 ISO image

6.	**9.4 Active CMP** **CLI:** Push scripts to all servers in the topology	From CMP GUI, navigate to Upgrade Manager → System Maintenance then select "Push Script" from the operations menu:  Confirm the action in the dialog box:  Validate that action completed and script is pushed to all servers in the topology: 

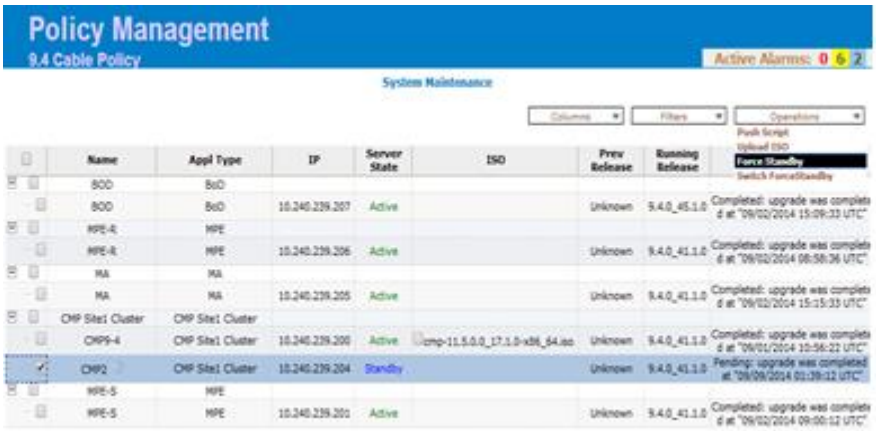
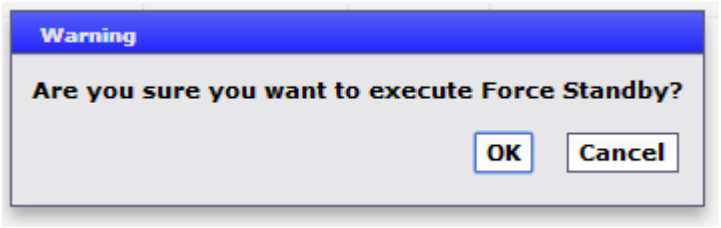
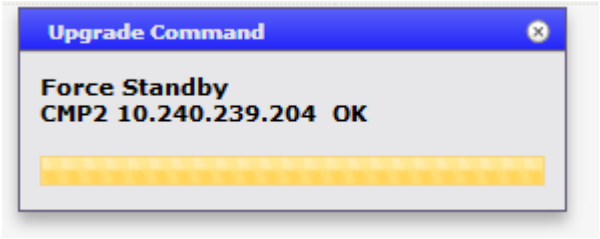
2.4 Upgrade CMP servers

Procedure 5: Upgrade CMP Servers

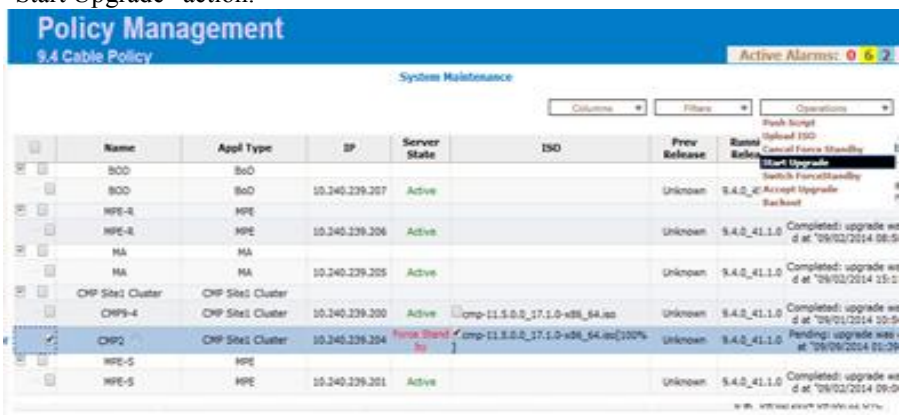
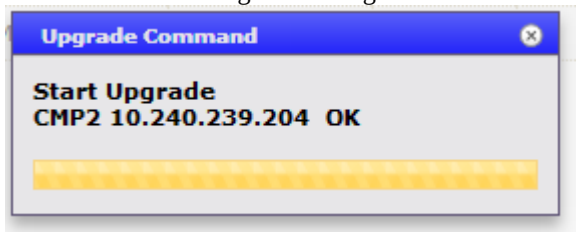
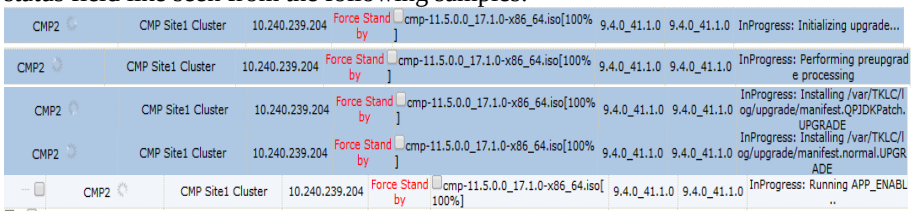
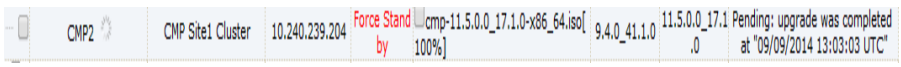
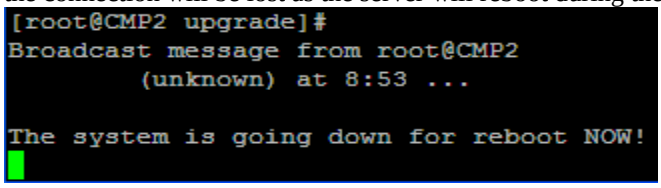
Procedure 5. Upgrade CMP Servers

STEP #		
	This procedure will perform the actual upgrade of the CMP cluster(s) servers. **Needed material:** - Admin access to CMP GUI to perform the upgrade	
1. ☐	**9.4 CMP GUI:** Validate CMP servers status	Login to CMP GUI as admin and navigate to Platform Settings → Topology Setting and choose the CMP cluster  Validate the status of the CMP servers to ensure none of the servers is in OOS (Out Of Service) state.

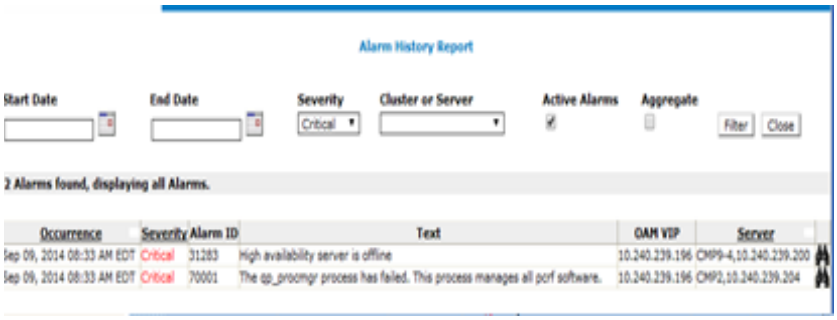
Procedure 5. Upgrade CMP Servers

2. ☐	**9.4 CMP GUI:** Enable Force Stand By on the stand By CMP server	Navigate to Upgrade Manager → System Maintenance, check the CMP stand By server checkbox then from the operations menu click "Force Standby":  Confirm the dialog box to perform the action:  Validate action completed :  Now CMP server should have the "Force Standby" state: 

Procedure 5. Upgrade CMP Servers

3. ☐	**9.4 CMP GUI:** Start the upgrade	With the Force Stand By server checked, open the operations menu and choose "Start Upgrade" action:  Confirm the action on the next dialog box:  An information message indicating the successful start of the upgrade displays:  The upgrade will go through multiple phases that would be displayed in the upgrade status field like seen from the following samples:  Then when upgrade completes, the upgrade status will reflect that as below:  Note that in case an SSH session is opened to the server while it is being upgraded, the connection will be lost as the server will reboot during the upgrade process: 

Procedure 5. Upgrade CMP Servers

4. ☐	**9.4 CMP GUI:** Expected alarms	During the upgrade some alarms may raise like the following:  These alarms are expected and would be automatically cleared after the upgrade concludes successfully

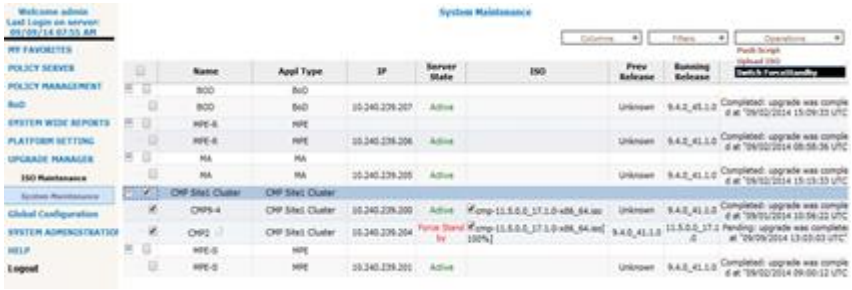
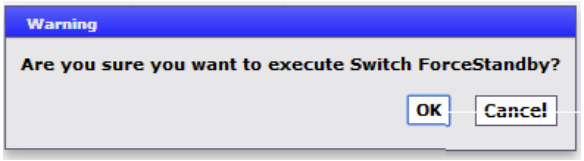
5.	**11.5 upgraded CMP server CLI:** Validate upgrade log file	SSH to upgraded CMP server and login then tail the upgrade log file as follows :
		`| This system has been upgraded but the upgrade has not yet |`
		`| been accepted or rejected. Please accept or reject the |`
		`| upgrade soon. |`
		`[admusr@CMP2 ~]$ tail /var/TKLC/log/upgrade/upgrade.log`
		`1410267783:: Running postUpgradeBoot() for Upgrade::Policy::QPBondConfig upgrade policy...`
		`1410267783:: Running postUpgradeBoot() for Upgrade::Policy::QPFirewallFixes upgrade policy...`
		`1410267783:: Running postUpgradeBoot() for Upgrade::Policy::QPIPv6Fixes upgrade policy...`
		`1410267783:: Running postUpgradeBoot() for Upgrade::Policy::QPJDKPolicy upgrade policy...`
		`1410267783:: Running postUpgradeBoot() for Upgrade::Policy::QPMySQLPolicy upgrade policy...`
		`1410267783:: Running postUpgradeBoot() for Upgrade::Policy::QPNTPFixes upgrade policy...`
		`1410267783:: Running postUpgradeBoot() for Upgrade::Policy::QPRunPostRPMActionsPolicy upgrade policy...`
		`1410267783:: Running postUpgradeBoot() for Upgrade::Policy::PlatformLast upgrade policy...`
		`1410267783:: Updating platform revision file...`
		`1410267783:: Upgrade returned success!`
		`[admusr@CMP2 ~]$`
		Validate upgrade returned success.

6.	**11.5 Upgraded CMP server CLI:** Validate policy revision	Run the following command to check running policy version:
		`[admusr@CMP2 ~]$ getPolicyRev -f cmp_11.5.0.0_17.1.0`
		`[admusr@CMP2 ~]$`
		Make sure the version is the upgraded version "11.5"

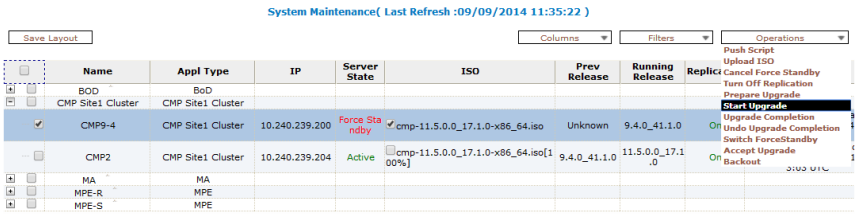
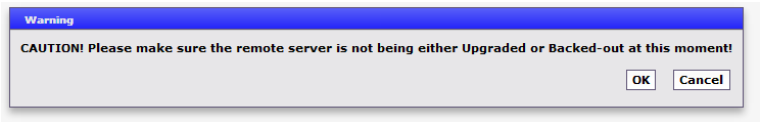
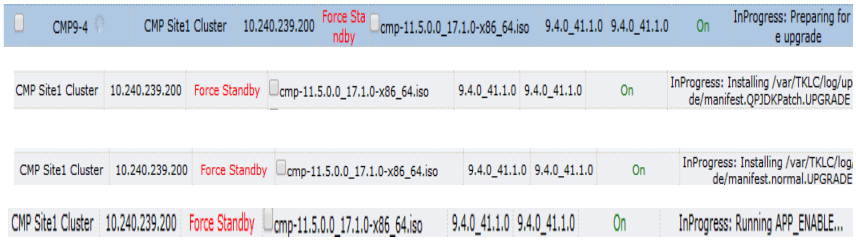
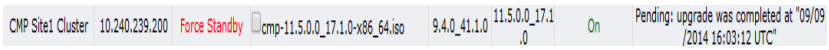
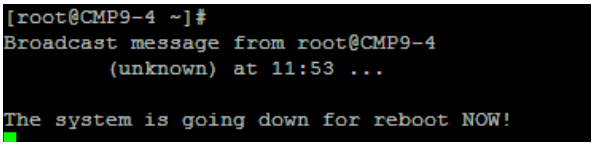
7.	**11.5 Upgraded CMP server CLI as root:** Verify the server's HA role	Run the command "ha.mystate" to verify the server has the stand By role:
		`resourceId role node subResources lastUpdate`
		`DbReplication Stby A2527.223 0 0909:122539.810`
		`VIP Stby A2527.223 0 0909:122539.812`
		`QP Stby A2527.223 0 0909:122552.834`
		`DbReplication_old OOS A2527.223 0 0909:122534.044`

8.	**11.5 Upgraded CMP server CLI as root:** Verify NTP sync	Run the command "ntpq -pn" to verify the server is in sync with the NTP server:
		`remote refid st t when poll reach delay offset jitter`
		`==========`
		`*10.250.32.10 192.5.41.40 2 u 657 1024 377 1.488 -1.334 0.765`

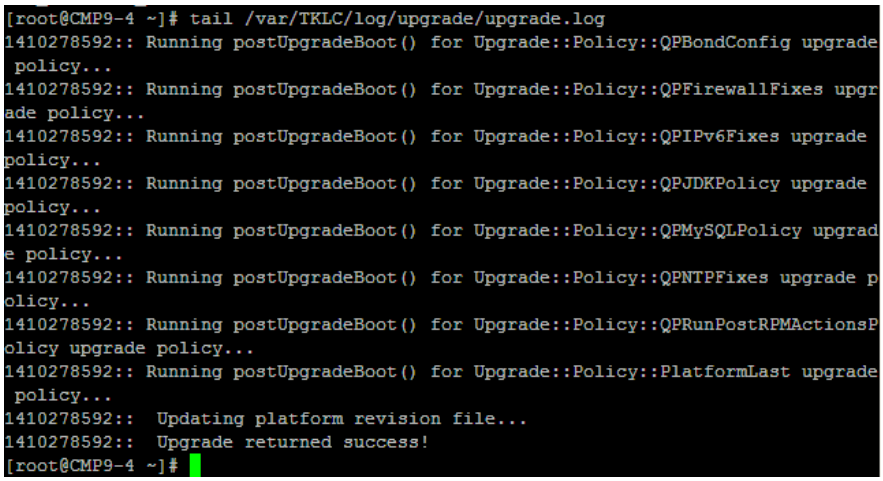
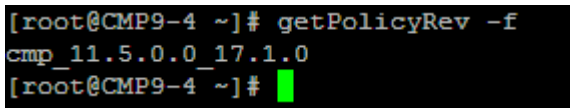
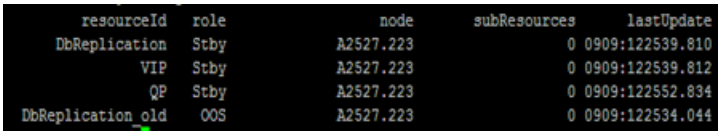
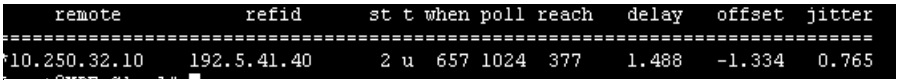
Procedure 5. Upgrade CMP Servers

9.	**9.4 CMP GUI:** Switch Stand By CMP servers	From the System Maintenance screen, check the CMP cluster and choose "Switch Force StandBy" from the operations menu:  Confirm the action on the following dialog box:  Connection to CMP GUI will be lost due to the switch of the CMP servers' state, you will need to re-login to CMP GUI again which will be on 11.5 release. Navigate to System Maintenance again to confirm the upgraded server assumed the Active state while the other CMP server is in Force Stand By state: 

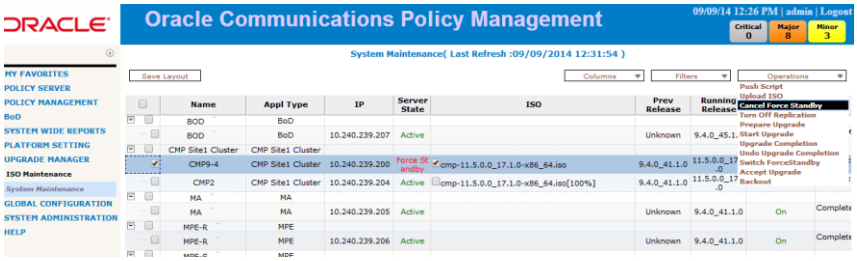
Procedure 5. Upgrade CMP Servers

10.	**11.5 CMP GUI:** Upgrade the second server in the CMP cluster	Having the second server checked, click the operations menu and choose start upgrade:  Confirm the action on the following dialog box:  Upgrade will start and goes through several stages which will be reflected in the upgrade status column of the server. Following a sample of those stages:  Then when upgrade completes, the upgrade status will reflect that as below:  Within the upgrade steps, the server will reboot so any opened ssh sessions shall disconnect: 

Procedure 5. Upgrade CMP Servers

11.	**11.5 secondly upgraded CMP server CLI:** Validate upgrade log file	SSH to latest Upgraded CMP server and login then tail the upgrade log file as follows : 
12.	**11.5 secondly upgraded CMP server CLI:** Validate policy revision	Run the following command to check running policy version:  Make sure the version is the upgraded version “11.5”
13.	**11.5 secondly upgraded CMP server CLI as root:** Verify the server’s HA role	Run the command “ha.mystate” to verify the server has the stand By role: 
14.	**11.5 secondly upgraded CMP server CLI as root:** Verify NTP sync	Run the command “ntpq -pn” to verify the server is in sync with the NTP server: 

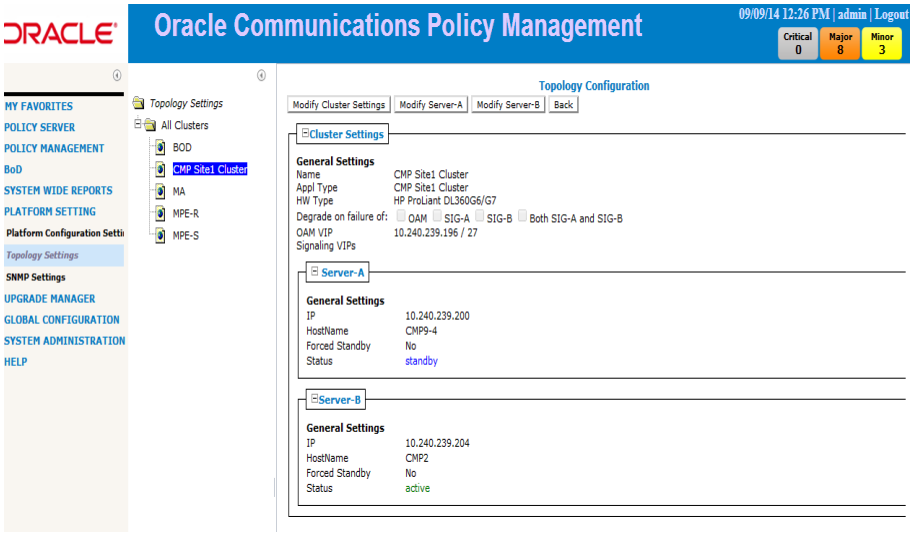
Procedure 5. Upgrade CMP Servers

15.	**11.5 CMP GUI:** Cancel the force stand By state	From the system maintenance screen of CMP GUI, check the latest upgraded server then from operations menu choose cancel force standby action:  Now the server state should be changed to “StandBy”: 
16.	**11.5 secondary site CMP cluster**	In case solution is geo-redundant , follow the same current procedure to upgrade CMP cluster in secondary site

2.5 Upgraded CMP cluster validation

Procedure 6: Post Upgrade Validation

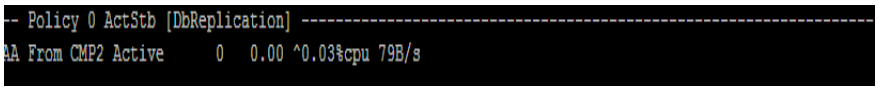
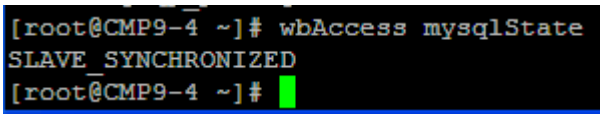
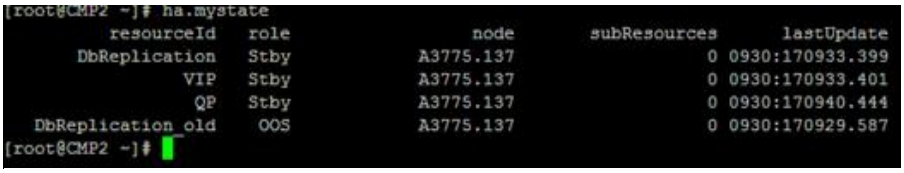
Procedure 6. Post CMP cluster Upgrade Validation

S T E P #		
	This procedure will validate the CMP cluster was upgraded successfully. **Needed material:** - Admin access to CMP GUI - Access to SSH to server's CLI	
1. ☐	**11.5 CMP GUI:** Validate CMP servers status in Topology	Login to CMP GUI as admin and navigate to Platform Settings → Topology Setting and choose the CMP cluster  Validate the status of the CMP servers is correct: one in Active state and the other in StandBy state

2.	**11.5 Active CMP server CLI:** Validate MySql database state	Run the following command to check running MySql configuration database state of the server:
		
		`[root@CMP2 ~]# wbAccess mysqlState`
		`MASTER`
		`[root@CMP2 ~]#`
		
		Note: This command can only be used for CMP and MA components.

3.	**11.5 Active CMP server CLI:** Verify the server's HA role	Run the following command to verify the server has the Active HA role:
		
		`[root@CMP9-4 ~]# ha.mystate`
		`resourceId role node subResources lastUpdate`
		`DbReplication Active A2527.223 0 0909:130054.744`
		`VIP Active A2527.223 0 0909:130054.746`
		`QP Active A2527.223 0 0909:130057.669`
		`DbReplication_old OOS A2527.223 0 0909:125923.153`
		`[root@CMP9-4 ~]#`

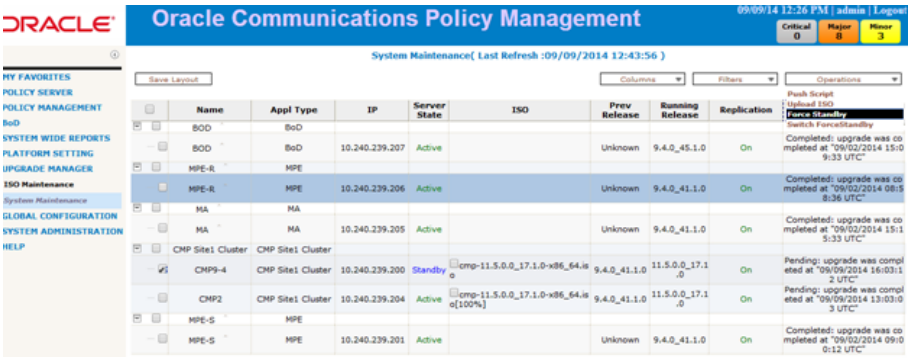
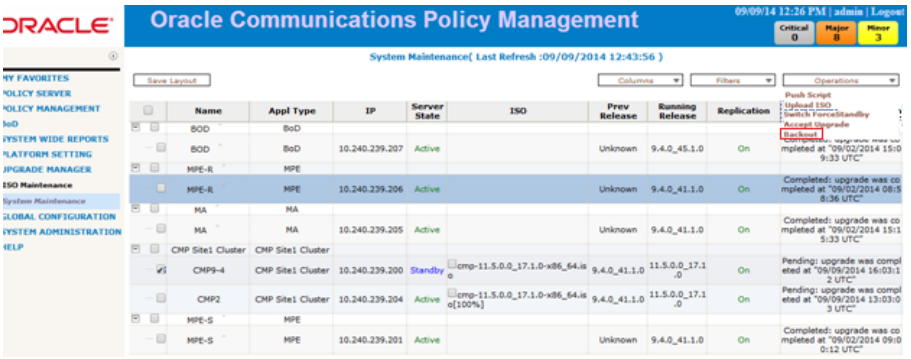
Procedure 6. Post CMP cluster Upgrade Validation

4.	**11.5 Active CMP server CLI:** Verify the server's replication role	Run the command ***"# irepstat"*** to verify the server has the Active replication role: 
5.	**11.5 StandBy CMP server CLI:** Validate MySql database state	Run the following command to verify the server has the Active HA role: 
6.	**11.5 StandBy CMP server CLI:** Verify the server's HA role	Run the following command to verify the server has the stand By role: 
7.	**Validation results**	In case of failure of one or more of the upgrade validation steps in this procedure without a plan for recovery, back out should be performed as in the following procedure. However in case all validation steps passed skip the following procedure (Back out the upgrade) and go directly to accept upgrade procedure in section 2.7.

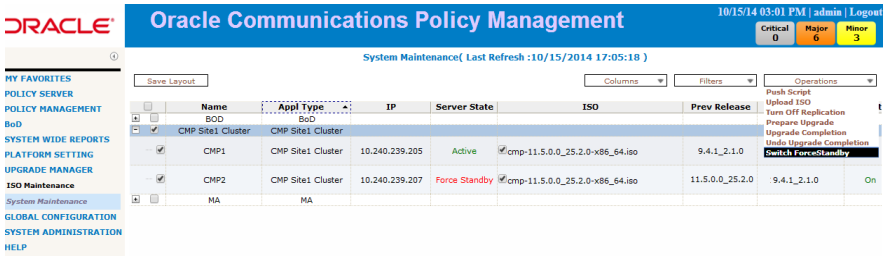
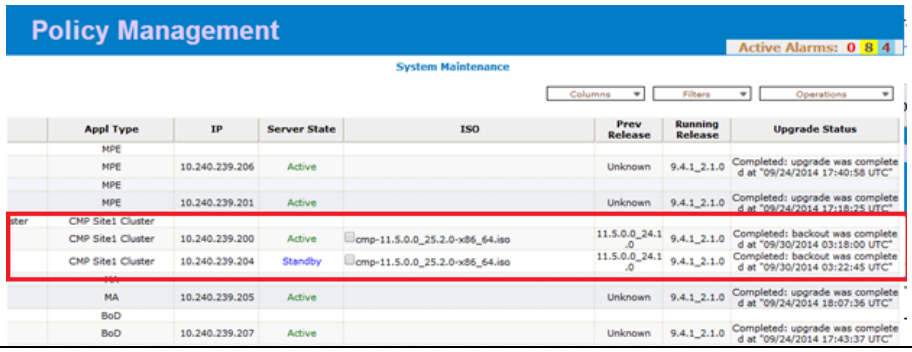
2.6 Back out the upgrade

Procedure 7: Backing out the upgrade

Procedure 7. Back out the upgrade

S T E P #		
	This procedure is only needed if the upgrade verification fails and back out is decided. This Back out procedures can only be followed successfully if: 1. Upgrade was not accepted 2. No configuration or new features have been set up 3. CMP can be backed out only when all other policy components were backed out successfully **Needed material:** - Admin access to CMP GUI	
1.	**11.5 CMP GUI:** Undo upgrade completion for the CMP servers	Navigate to Upgrade Manager →System Maintenance, check the CM cluster check box then from the operations menu choose "Undo upgrade completion" : 
2. ☐	**11.5 CMP GUI:** Force Stand By the upgraded Stand By server	Navigate to Upgrade Manager →System Maintenance, set the upgraded server that has the StandBy status to Force StandBy from the operations menu 
3. ☐	**11.5 CMP GUI:** Back out the upgraded Stand By server	With the server set to Force StandBy checked, choose "Backout" from the operations menu: 

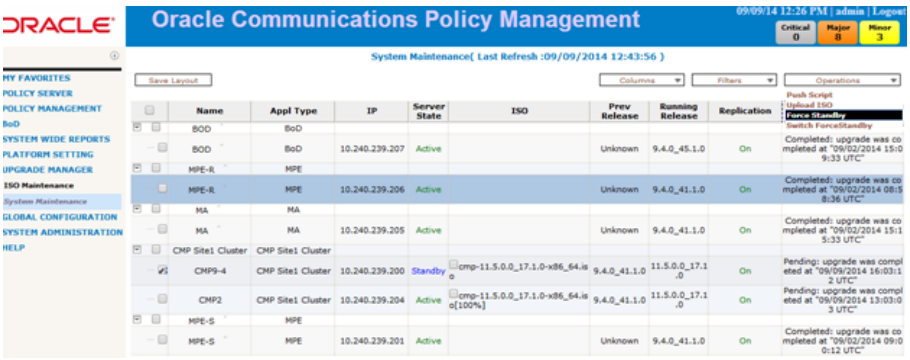
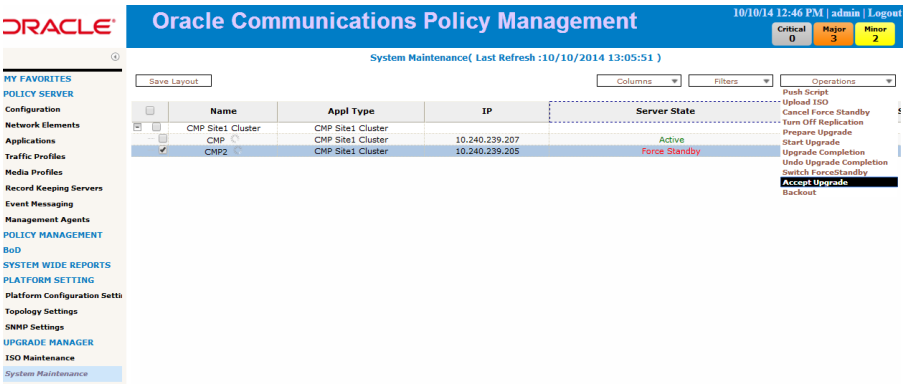
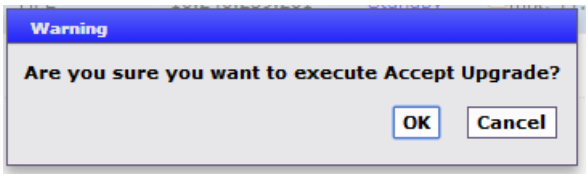
Procedure 7. Back out the upgrade

4.	**11.5 CMP GUI:** Switch Force Stand By	With the cluster checked, choose switch Force standby from the operations menu  Session to CMP GUI will be lost, re-login to backed out 9.4 CMP GUI then back out the force stand by server as shown in the previous step
5.	**9.4 CMP GUI:** CMP cluster back out completed	Validate that release running is back to 9.4 release and upgrade status for both servers in the CMP cluster indicates “backout was complete” then from the “Operations” menu, cancel force standby of the latest backed out server : 
6.	**9.4 Active CMP CLI:** Clean up upgrade files	Login to Active CMP CLI as root run the following command: ***policyUpgrade.pl –cleanupUpgrade***

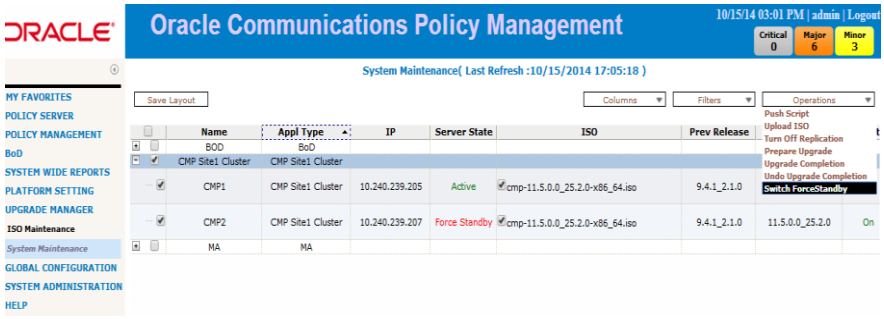
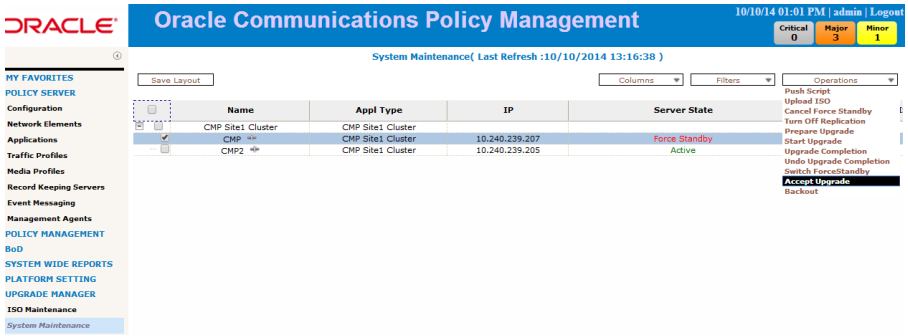
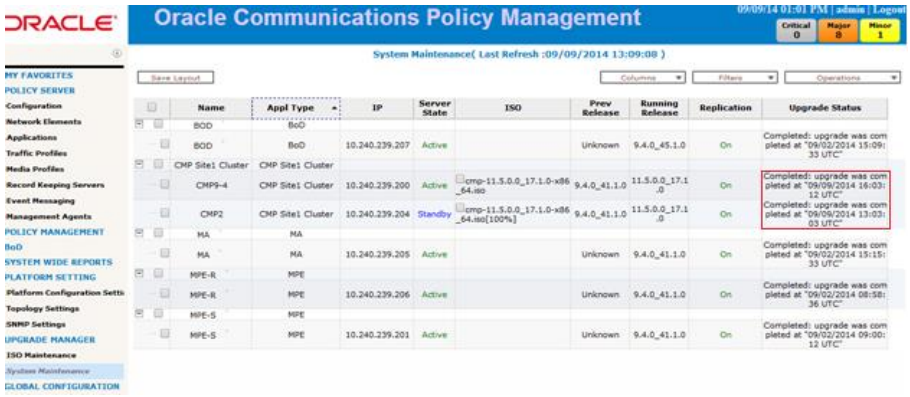
2.7 Accept the upgrade

Procedure 8: Accept the upgrade

Procedure 8. Accept the upgrade

S T E P #		
	This procedure will accept the upgrade. **Needed material:** - Admin access to CMP GUI	
7. ☐	**11.5 CMP GUI:** Force Stand By the upgraded Stand By server	Navigate to Upgrade Manager →System Maintenance, set the upgraded server that has the StandBy status to Force StandBy from the operations menu 
8. ☐	**11.5 CMP GUI:** Accept the upgrade for Stand By server	With the server set to Force StandBy checked, choose "Accept Upgrade" from the operations menu:  Then confirm the action on the next dialog message: 

Procedure 8. Accept the upgrade

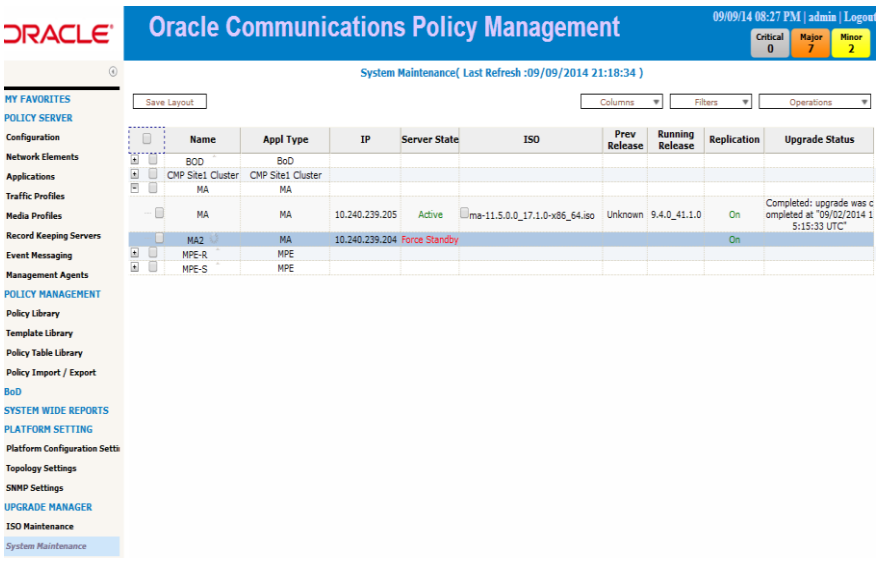
9.	**11.5 CMP GUI:** Switch Force Stand By	With the cluster checked, choose switch Force standby from the operations menu  Session to CMP GUI will be lost, re-login to CMP GUI then accept the upgrade for the second server 
10.	**11.5 CMP GUI:** upgrade completion validation	Validate that upgrade pending alarms are cleared out for the cluster. Also validate that both servers in the cluster are showing completed upgrade status: 
11.	**11.5 secondary site CMP cluster**	In case solution is geo-redundant , follow the same current procedure to accept the upgrade of the CMP cluster in secondary site

3. MA/MPE-R/MPE-S/BOD Cluster Upgrades

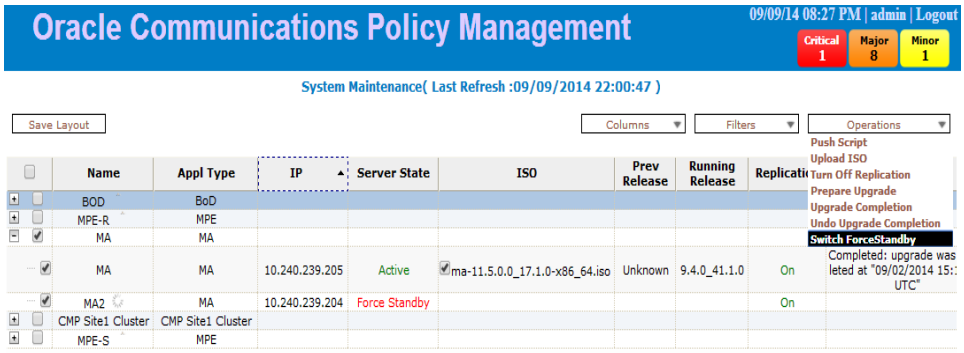
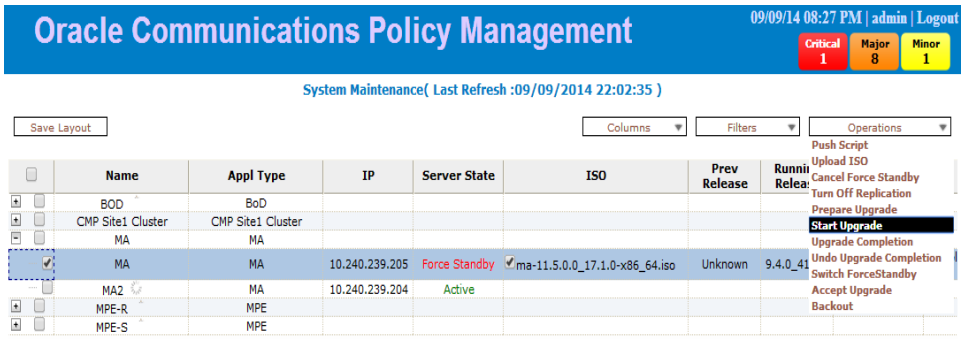
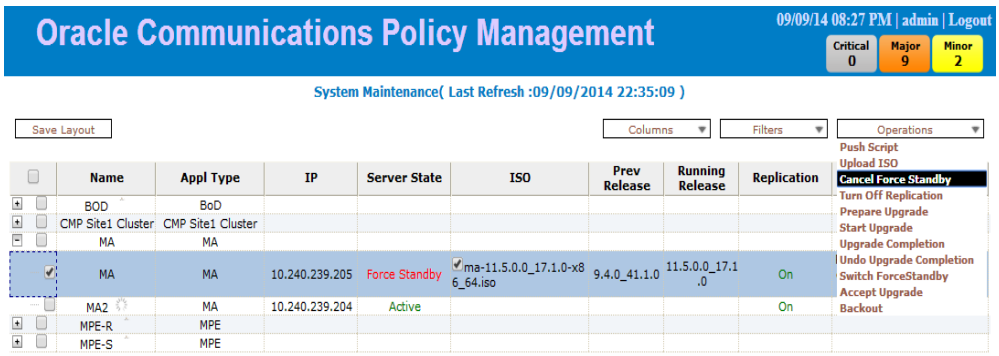
3.1 MA cluster upgrade

Procedure 9: MA Cluster Upgrade

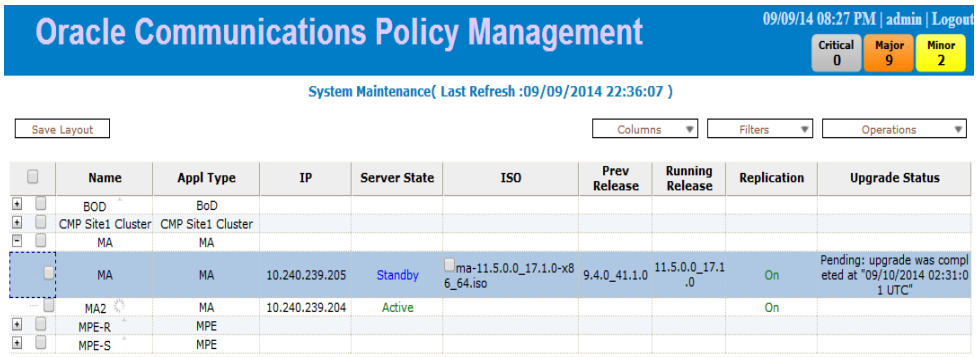
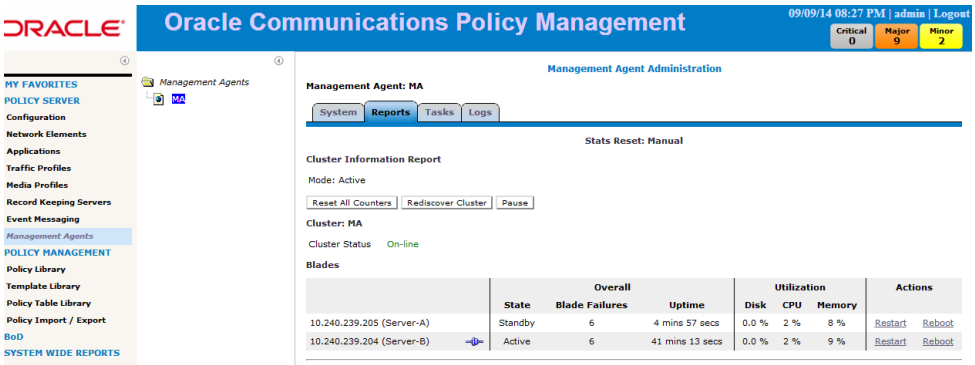
Procedure 9. MA Upgrade

S T E P #		
	This procedure will perform the upgrade for the MA cluster if exists in the Policy Solution to be Upgraded **Needed material:** - Access to customer's network to access the Cable Policy solution - CMP OAM VIP - Admin login to CMP - 11.5 MA ISO image	
1. ☐	**Computer on solutions' network or remote access to solutions' network:** Transfer MA ISO Image	Follow the same procedures outlined in section 2.2 of this document to transfer the 11.5 MA ISO Image into the servers to be upgraded from 9.4 release
2. ☐	**CMP GUI:** Force StandBy the standby server	Navigate to Upgrade Manager → System Maintenance then check the standBy MA server and from the operations menu choose "Force StandBy":  Then with the server checked from the operations menu, choose "Start Upgrade". The upgrade will go through multiple steps including rebooting the server; those steps are reflected in the MA's "Upgrade Status" field of the System Maintenance screen. Wait till the upgrade status indicates upgrade was completed. For more details you can refer to steps followed for CMP upgrade in section 2.4 of this document which applies also for MA upgrade

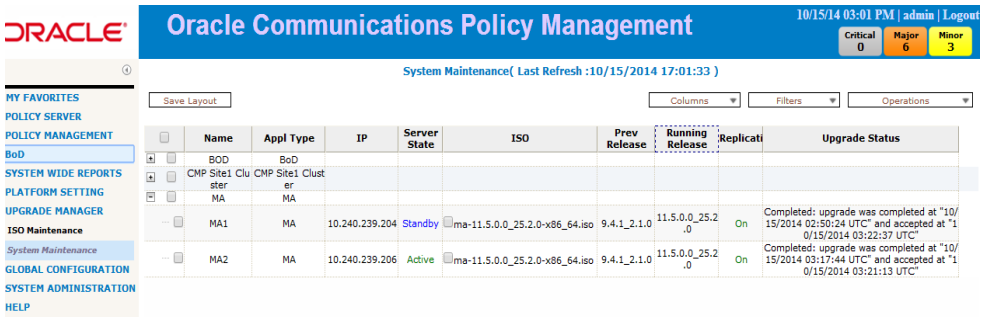
Procedure 9. MA Upgrade

3.	**CMP GUI:** Switch Force StandBy	Navigate to Upgrade Manager → System Maintenance then check the MA cluster and from the operations menu choose "Switch Force StandBy":  Then with the second server checked (the force StandBy server) , open the operations menu and choose the "Start Upgarde"  After upgrade completes, cancel Force Standby from the operations menu : 

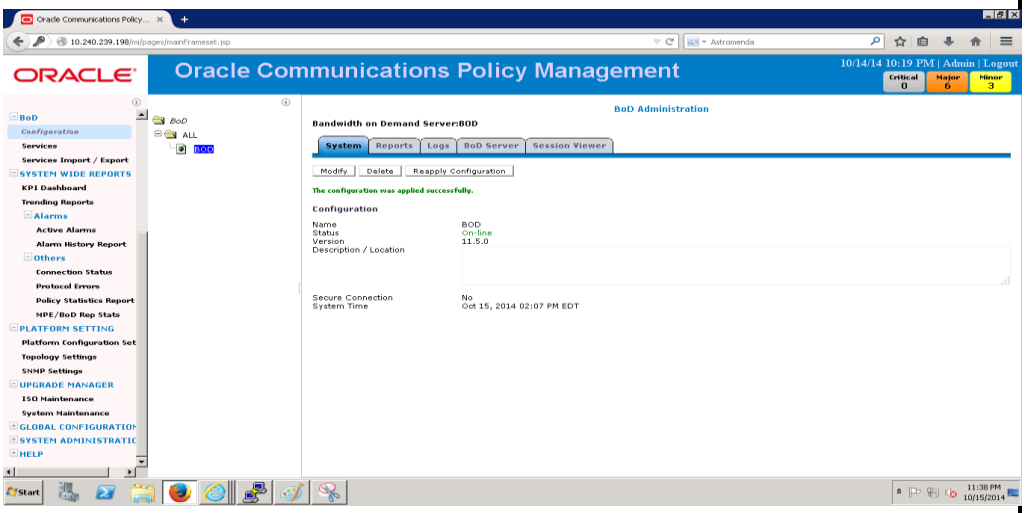
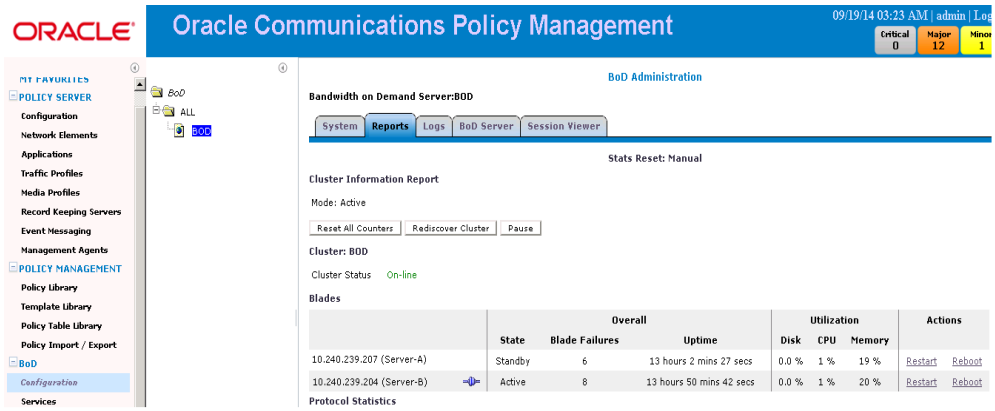
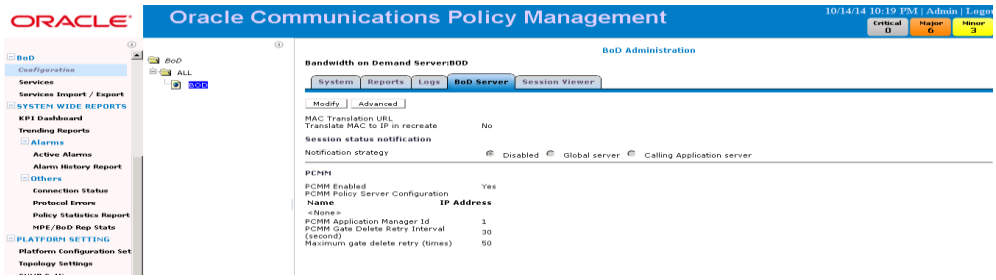
Procedure 9. MA Upgrade

4.	**CMP GUI:** MA servers status check	Validate that now one of the MA servers is in "Active" State and the other is in "StandBy" state: 
5.	**CMP GUI:** MA cluster configuration	Navigate to Policy Server → Management Agents  Validate the state of the MA cluster is "On-line" and that the version reflects the upgraded release. Then switch to the "Reports" tab in the MA administartion :  Validate both servers of the cluster are displayed and with correct "Active" and "StandBy" state.
6.	**Post upgrade checks**	Follow the same procedures outlined in section 2.5 of this document to validate the upgrade completed successfully

Procedure 9. MA Upgrade

7.	**Accept the upgrade**	Follow the same procedures outlined in section 2.7 of this document to accept the upgrade 

Procedure 9. MA Upgrade

	CMP GUI: BOD cluster configuration	Navigate to BoD → Configuration  Validate the state of the BOD cluster is "On-line" and that the version reflects the upgraded release. Then switch to the "Reports" tab in the BOD administartion :  Validate both servers of the cluster are displayed and with correct "Active" and "StandBy" state. Then Switch to "BoD Server" tab in BOD Administration.  Validate that the association with policy server MPE-R is maintained after the upgarde

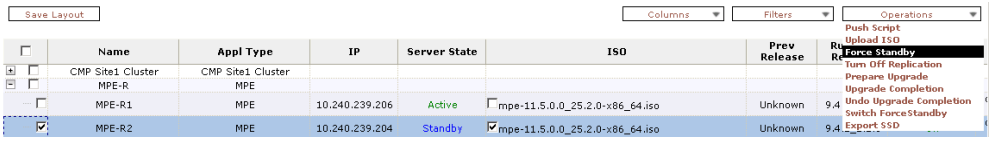
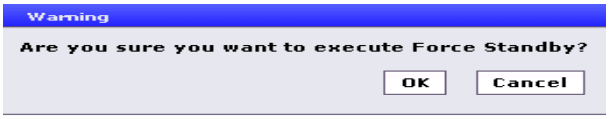
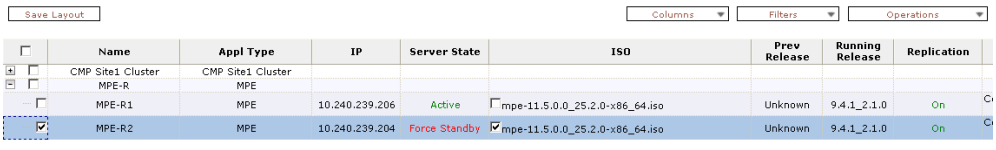
Procedure 9. MA Upgrade

9.	**Post upgrade checks**	Follow the same procedures outlined in section 2.5 of this document to validate the upgrade completed successfully
10.	**Back out the upgrade**	In case post upgrade checks failed and back out is decided, follow the same procedures outlined in section 2.6 of this document to back out the MA cluster
11.	**Accept the upgrade**	Follow the same procedures outlined in section 2.7 of this document to accept the upgrade

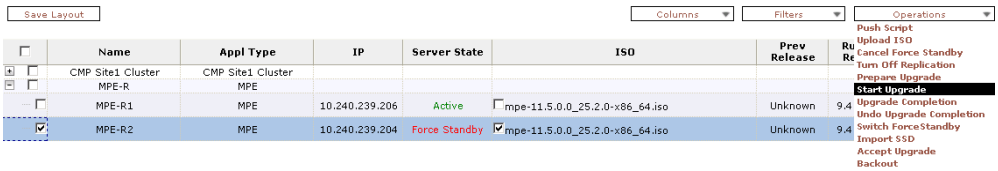
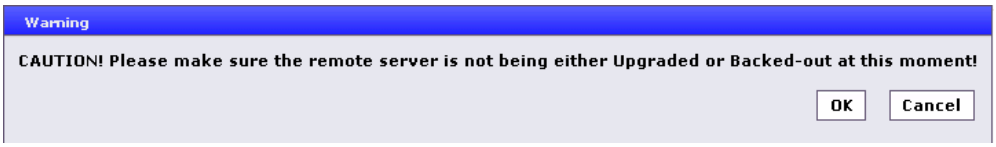
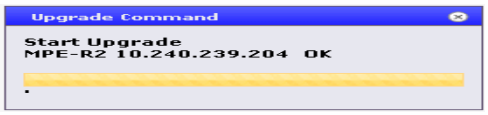
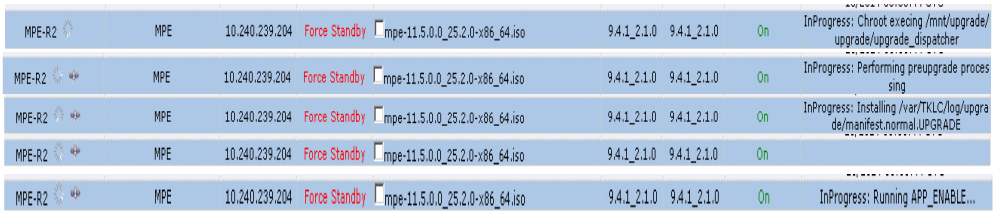
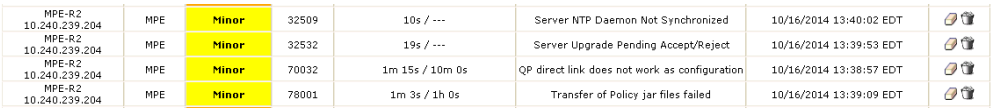
3.2 MPE-R/MPE-S cluster upgrade

Procedure 10: MPE-R/MPE-S Cluster Upgrade

Procedure 10. MPE-R/MPE-S Upgrade

S T E P #		
	This procedure will perform the upgrade for the MPE-R/MPE-S cluster if exists in the Policy Solution to be upgraded. **Needed material:** - Access to customer's network to access the Cable Policy solution - CMP OAM VIP, MPE-R/MPE-S iLO IP & OAM Real IP - Admin login to CMP, iLO Admin & CLI root login to MPE-R/MPE-S - 11.5 MPE-R/MPE-S ISO image	
1. ☐	**Computer on solutions' network or remote access to solutions' network:** Transfer MPE-R/MPE-S ISO Image	Follow the same procedures outlined in section 2.2 of this document to transfer the 11.5 MPE-R/MPE-S ISO Image into the servers to be upgraded from 9.4 release
2. ☐	**CMP GUI:** Force StandBy the standby server	Navigate to Upgrade Manager → System Maintenance then check the standBy MPE-R/MPE-S server and from the operations menu choose "Force StandBy":  Confirm the action on the next dialog box  An information message indicating the successful execution of Force standby appears. 

Procedure 10. MPE-R/MPE-S Upgrade

3.	**CMP GUI:** Start the upgrade	Then with the server checked from the operations menu, choose "Start Upgrade".  Confirm the action on the next dialog box:  An information message indicating the successful start of the upgrade displays:  The upgrade will go through multiple steps including rebooting the server; those steps are reflected in the MPE-R/MPE-S "Upgrade Status" field of the System Maintenance screen.  Wait till the upgrade status indicates upgrade was completed. 
4.	**CMP GUI:** Expected alarms	During the upgrade some alarms may raise like the following:  These alarms are expected and would be automatically cleared after the upgrade concludes successfully

Procedure 10. MPE-R/MPE-S Upgrade

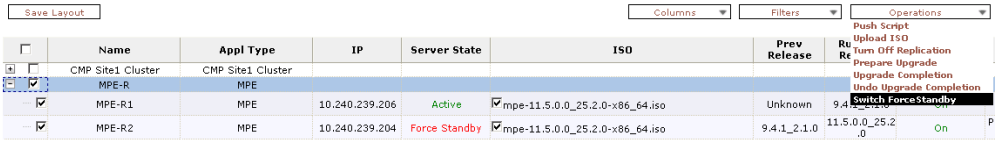
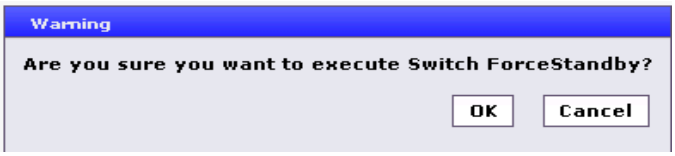
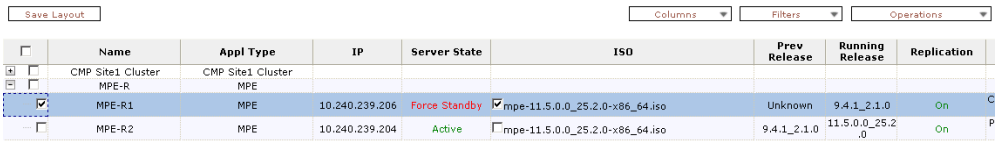
5.	**11.5 upgraded MPE server CLI:** Validate upgrade log file	SSH to upgraded MPE-R/MPE-S server and login then tail the upgrade log file as follows :
		
		Validate upgrade returned success.
		
		`[root@MPE-R2 ~]# tail /var/TKLC/log/upgrade/upgrade.log`
		`1413481118:: Running postUpgradeBoot() for Upgrade::Policy::HP upgrade policy...`
		`1413481118:: Running postUpgradeBoot() for Upgrade::Policy::MBL upgrade policy...`
		`1413481118:: Running postUpgradeBoot() for Upgrade::Policy::QPFirewallFixes upgrade policy...`
		`1413481118:: Running postUpgradeBoot() for Upgrade::Policy::QPIPv6Fixes upgrade policy...`
		`1413481118:: Running postUpgradeBoot() for Upgrade::Policy::QPJDKPolicy upgrade policy...`
		`1413481118:: Running postUpgradeBoot() for Upgrade::Policy::QPNTPFixes upgrade policy...`
		`1413481118:: Running postUpgradeBoot() for Upgrade::Policy::QPRunPostRPMActionsPolicy upgrade policy...`
		`1413481118:: Running postUpgradeBoot() for Upgrade::Policy::PlatformLast upgrade policy...`
		`1413481118:: Updating platform revision file...`
		`1413481119:: Upgrade returned success!`

6.	**11.5 upgraded MPE server CLI:** Validate policy revision	Run the following command to check running policy version:
		
		`[root@MPE-R2 ~]# getPolicyRev -f`
		`mpe_11.5.0.0_25.2.0`
		
		Make sure the version is the upgraded version "11.5"

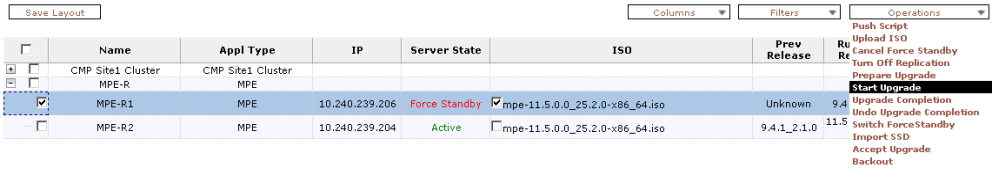
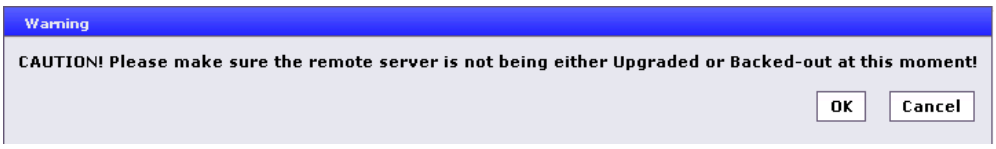
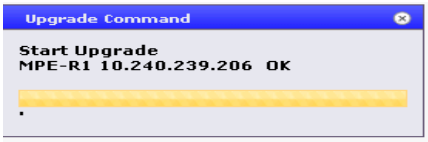
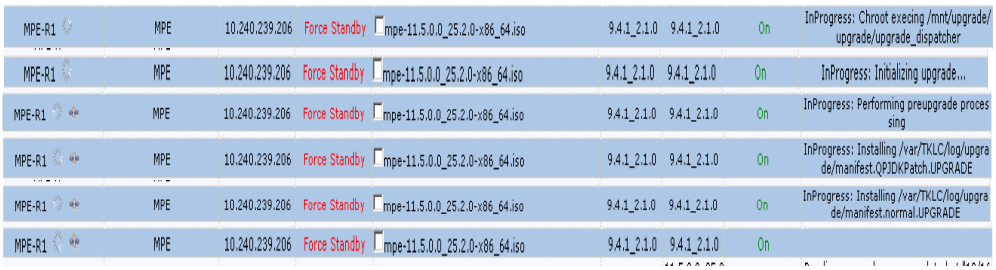
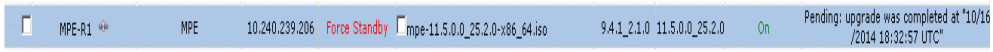
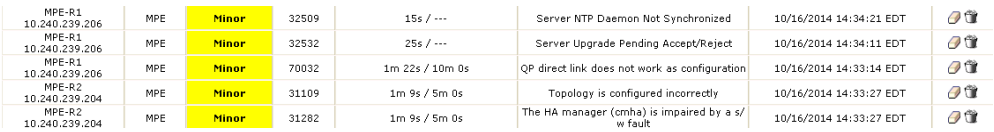
7.	**11.5 upgraded MPE server CLI:** Verify the server's HA role	Run the command "ha.mystate" to verify the server has the stand By role:
		
		`[root@MPE-R2 ~]# ha.mystate`
		`resourceId role node subResources lastUpdate`
		`DbReplication Stby C0093.217 0 1016:133848.348`
		`VIP Stby C0093.217 0 1016:133848.350`
		`QP Stby C0093.217 0 1016:133853.894`
		`DbReplication_old OOS C0093.217 0 1016:133843.189`

8.	**11.5 upgraded MPE server CLI:** Verify NTP sync	Run the command "ntpq -pn" to verify the server is in sync with the NTP server:
		
		`[root@MPE-R2 ~]# ntpq -pn`
		`remote refid st t when poll reach delay offset jitter`
		`==========`
		`*10.250.32.10 192.5.41.40 2 u 35 64 7 0.316 7.918 3.595`

Procedure 10. MPE-R/MPE-S Upgrade

9.	**CMP GUI:** Switch Force StandBy	Navigate to Upgrade Manager → System Maintenance then check the MPE-R/MPE-S cluster and from the operations menu choose "Switch Force StandBy":  Confirm the action on the next dialog box  An information message indicating the successful execution of Switch Force standby appears.  

Procedure 10. MPE-R/MPE-S Upgrade

10.	**CMP GUI:** Start the upgrade	Then with the server checked from the operations menu, choose "Start Upgrade".  Confirm the action on the next dialog box:  An information message indicating the successful start of the upgrade displays:  The upgrade will go through multiple steps including rebooting the server; those steps are reflected in the MPE-R/MPE-S "Upgrade Status" field of the System Maintenance screen.  Wait till the upgrade status indicates upgrade was completed. 
11.	**CMP GUI:** Expected alarms	During the upgrade some alarms may raise like the following:  These alarms are expected and would be automatically cleared after the upgrade concludes successfully

Procedure 10. MPE-R/MPE-S Upgrade

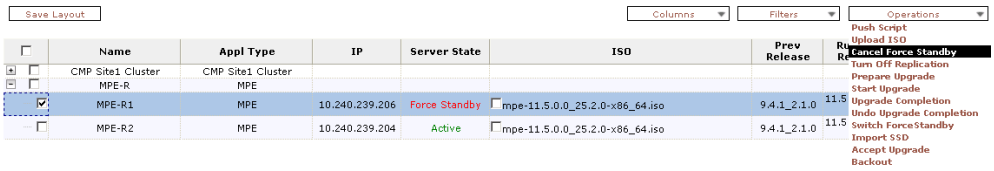
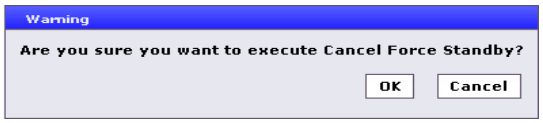
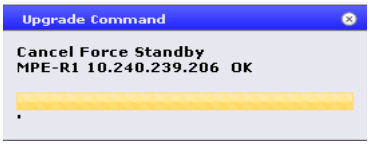
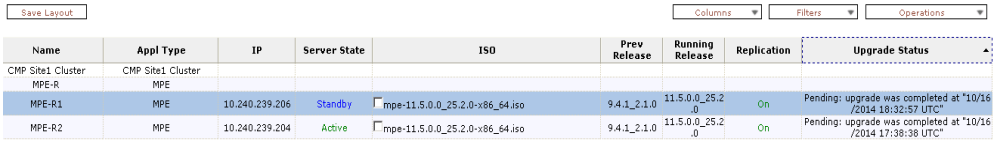
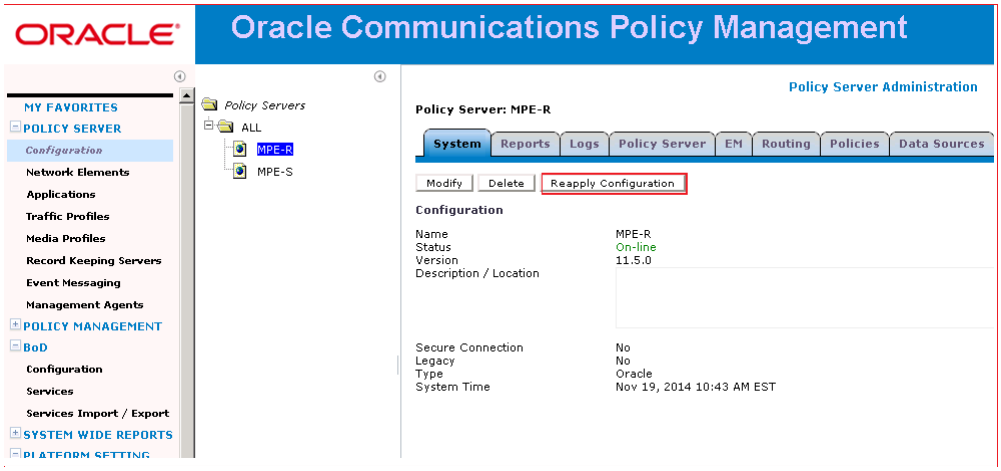
12.	**11.5 upgraded MPE server CLI:** Validate upgrade log file	SSH to upgraded MPE-R/MPE-S server and login then tail the upgrade log file as follows :
		
		Validate upgrade returned success.
		
		`[root@MPE-R1 ~]# tail /var/TKLC/log/upgrade/upgrade.log`
		`1413484376:: Running postUpgradeBoot() for Upgrade::Policy::HP upgrade policy...`
		`1413484376:: Running postUpgradeBoot() for Upgrade::Policy::MBL upgrade policy...`
		`1413484376:: Running postUpgradeBoot() for Upgrade::Policy::QPFirewallFixes upgrade policy...`
		`1413484376:: Running postUpgradeBoot() for Upgrade::Policy::QPIPv6Fixes upgrade policy...`
		`1413484376:: Running postUpgradeBoot() for Upgrade::Policy::QPJDKPolicy upgrade policy...`
		`1413484376:: Running postUpgradeBoot() for Upgrade::Policy::QPNTPFixes upgrade policy...`
		`1413484376:: Running postUpgradeBoot() for Upgrade::Policy::QPRunPostRPMActionsPolicy upgrade policy...`
		`1413484376:: Running postUpgradeBoot() for Upgrade::Policy::PlatformLast upgrade policy...`
		`1413484377::  Updating platform revision file...`
		`1413484377::  Upgrade returned success!`

13.	**11.5 upgraded MPE server CLI:** Validate policy revision	Run the following command to check running policy version:
		
		`[root@MPE-R1 ~]# getPolicyRev -f`
		`mpe_11.5.0.0_25.2.0`
		
		Make sure the version is the upgraded version “11.5”

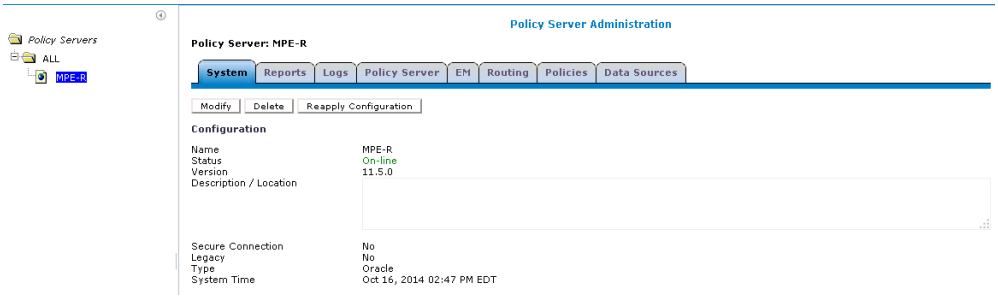
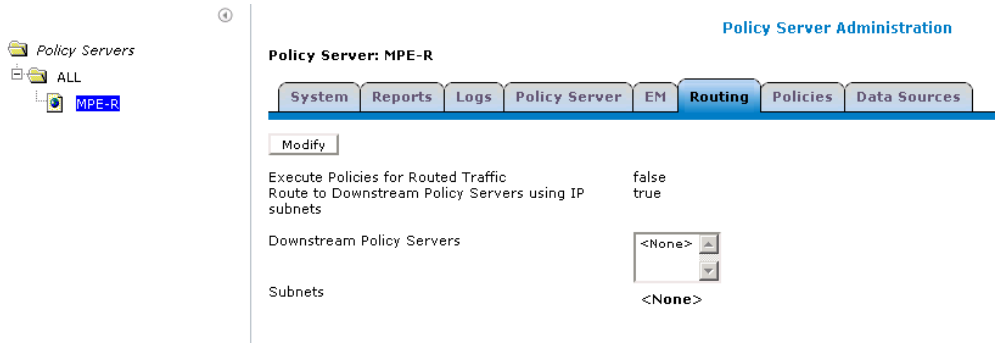
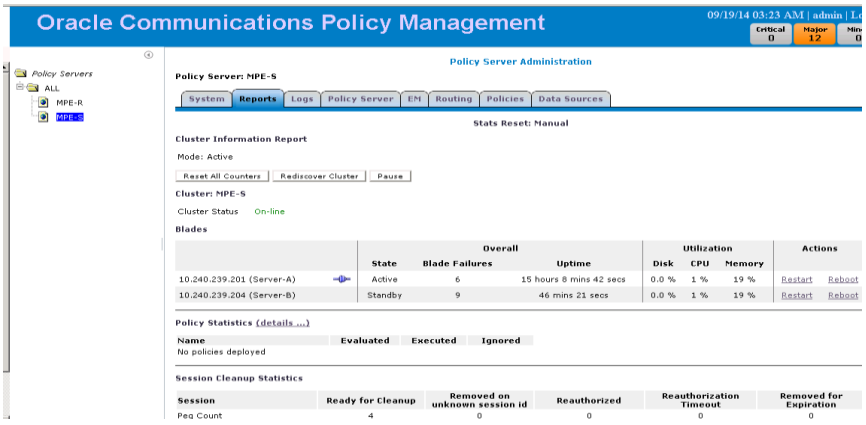
14.	**11.5 upgraded MPE server CLI:**
	
	Verify the server’s HA role
		Run the command “ha.mystate” to verify the server has the stand By role:
		
		`[root@MPE-R1 ~]# ha.mystate`
		`resourceId role node subResources lastUpdate`
		`DbReplication Stby C0093.093 0 1016:143357.380`
		`VIP Stby C0093.093 0 1016:143357.383`
		`QP Stby C0093.093 0 1016:143357.384`
		`DbReplication_old OOS C0093.093 0 1016:143300.861`

15.	**11.5 upgraded MPE server CLI:**
	
	Verify NTP sync
		Run the command “ntpq -pn” to verify the server is in sync with the NTP server:
		
		`[root@MPE-R1 ~]# ntpq -pn`
		`remote refid st t when poll reach delay offset jitter`
		`==========`
		`*10.250.32.10 192.5.41.40 2 u 52 64 17 0.347 2.022 0.988`

Procedure 10. MPE-R/MPE-S Upgrade

16.	**CMP GUI:** Cancel force standby	After upgrade completes, cancel Force Standby from the operations menu :  Confirm the action on the next dialog box  An information message indicating the successful cancellation of Force standby 
17.	**CMP GUI:** MPE servers status check	Validate that now one of the MPE-R/MPE-S servers is in "Active" State and the other is in "StandBy" state: 
18.	**11.5 secondary site MPE-S spare server**	In case solution is geo-redundant , follow the same current procedure to upgrade the MPE-S spare server in secondary site
19.	**CMP GUI:** MPE-R/MPE-S cluster configuration	Navigate to Policy Server →Configuration and Reapply Configuration to clear configuration mismatch in 

Procedure 10. MPE-R/MPE-S Upgrade

20.	**CMP GUI:** MPE-R/MPE-S cluster configuration	Navigate to Policy Server → Configuration  Validate the state of the MPE-R/MPE-S cluster is "On-line" and that the version reflects the upgraded release. Then switch to the "Routing" tab in the MPE-R/MPE-S administration:  Validate configurations are maintained for MPE-R/MPE-S after the upgarde. Then switch to the "Policy Server" tab in the MPE-R/MPE-S administration:, validate that associations of MPE-S with CMTS are intact after the upgarde. Then switch to the "Reports" tab in the MPE-R/MPE-S administartion :  Validate both servers of the cluster are displayed and with correct "Active" and "StandBy" state.
21.	**Post upgrade checks**	Follow the same procedures outlined in section 2.5 of this document to validate the upgrade completed successfully.

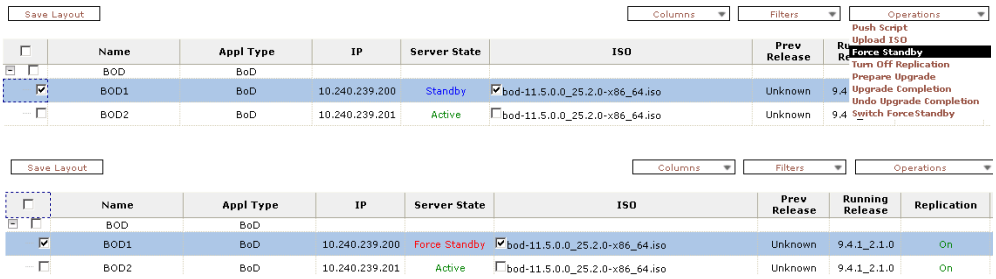
Procedure 10. MPE-R/MPE-S Upgrade

22.	**Back out the upgrade**	In case post upgrade checks failed and back out is decided, follow the same procedures outlined in section 2.6 of this document to back out the MPE clusters
23.	**Accept the upgrade**	Follow the same procedures outlined in section 2.7 of this document to accept the upgrade.

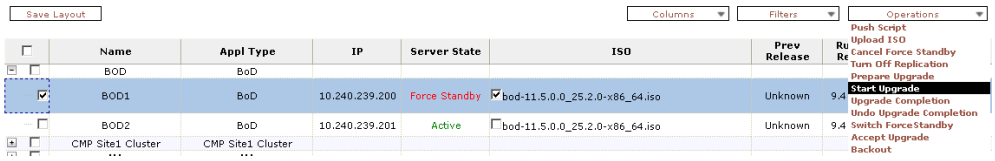
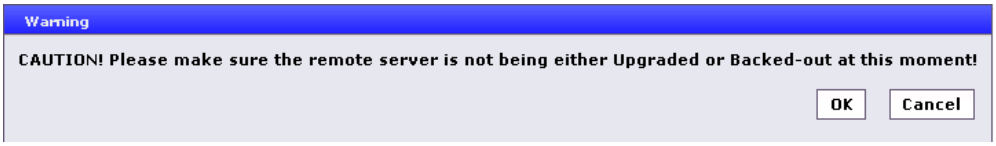
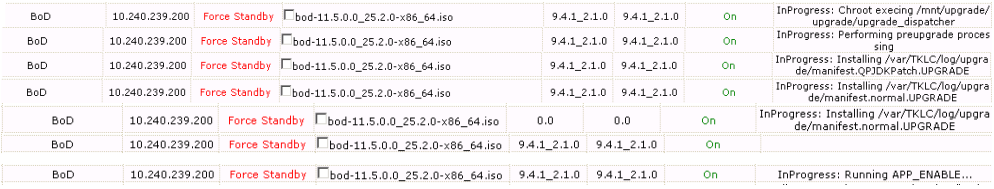
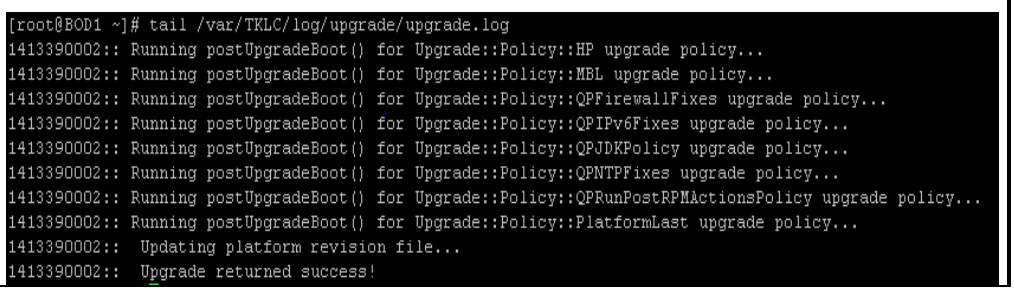
3.3 BOD cluster upgrade

Procedure 11: BOD Cluster Upgrade

Procedure 11. BOD Upgrade

S T E P #		
	This procedure will perform the upgrade for the BOD cluster if exists in the Policy Solution to be upgraded. **Needed material:** - Access to customer's network to access the Cable Policy solution - CMP OAM VIP, BOD iLO IP & OAM Real IP - Admin login to CMP, iLO Admin & CLI root login to BOD - 11.5 BOD ISO image	
1. ☐	**Computer on solutions' network or remote access to solutions' network:** Transfer BOD ISO Image	Follow the same procedures outlined in section 2.2 of this document to transfer the 11.5 BOD ISO Image into the servers to be upgraded from 9.4 release
2. ☐	**CMP GUI:** Force StandBy the standby server	Navigate to Upgrade Manager → System Maintenance then check the standBy BOD server and from the operations menu choose "Force StandBy": 

Procedure 11. BOD Upgrade

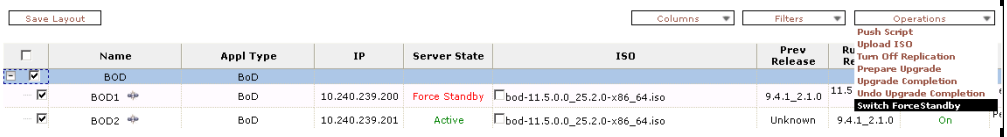
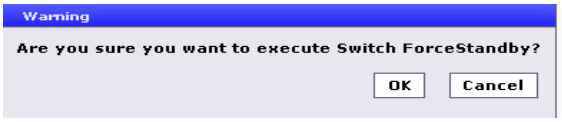
3.	**CMP GUI:** Start the upgrade	Then with the server checked from the operations menu, choose "Start Upgrade".  Confirm the action on the next dialog box:  An information message indicating the successful start of the upgrade displays: The upgrade will go through multiple steps including rebooting the server; those steps are reflected in the BOD's "Upgrade Status" field of the System Maintenance screen.  Wait till the upgrade status indicates upgrade was completed. 
4.	**CMP GUI:** Expected alarms	During the upgrade some alarms may raise like the following:  These alarms are expected and would be automatically cleared after the upgrade concludes successfully
5.	**11.5 upgraded BOD server CLI:** Validate upgrade log file	SSH to upgraded BOD server and login then tail the upgrade log file as follows : Validate upgrade returned success. 

Procedure 11. BOD Upgrade

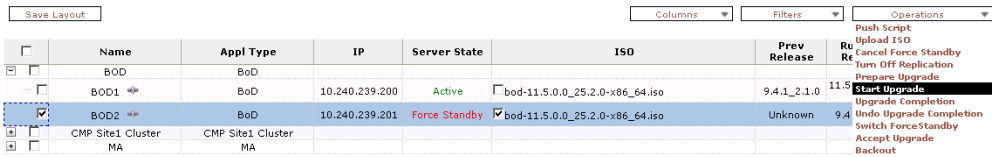
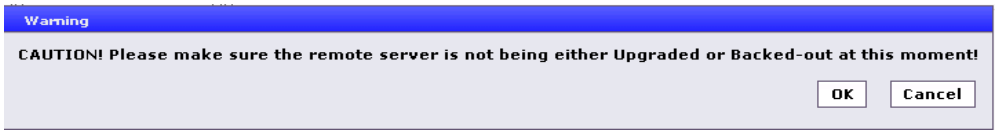
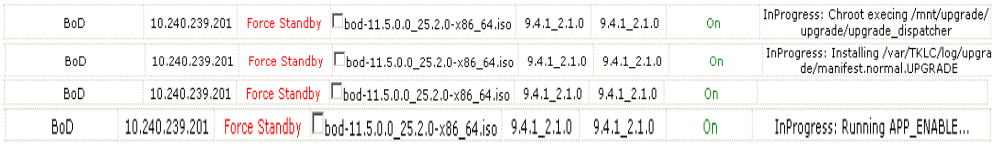
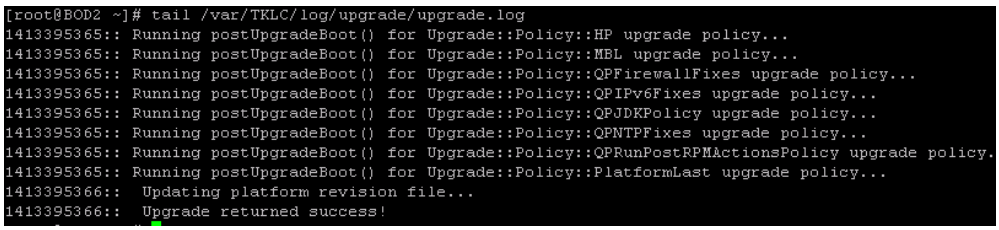
6.	**11.5 Upgraded BOD server CLI:** Validate policy revision	Run the following command to check running policy version: `[root@BOD1 ~]# getPolicyRev -f bod_11.5.0.0_25.2.0` Make sure the version is the upgraded version "11.5"

7.	**11.5 Upgraded BOD server CLI as root:** Verify the server's HA role	Run the command "ha.mystate" to verify the server has the stand By role:
		
		`[root@BOD1 ~]# ha.mystate`
		`resourceId role node subResources lastUpdate`
		`DbReplication Stby C1729.018 0 1015:122011.283`
		`VIP Stby C1729.018 0 1015:122011.285`
		`QP Stby C1729.018 0 1015:122016.448`
		`DbReplication_old OOS C1729.018 0 1015:122005.910`

8.	**11.5 Upgraded BOD server CLI as root:** Verify NTP sync	Run the command "ntpq -pn" to verify the server is in sync with the NTP server:
		
		`[root@BOD1 ~]# ntpq -pn`
		`remote refid st t when poll reach delay offset jitter`
		`*10.250.32.10 192.5.41.209 2 u 115 128 377 0.291 -0.441 0.037`

12.	**CMP GUI:** Switch Force StandBy to upgrade the second sever in BOD cluster	Navigate to Upgrade Manager → System Maintenance then check the BOD cluster and from the operations menu choose "Switch Force StandBy":  Confirm the action on the next dialog box  An information message indicating the successful switch force standby is displayed: 

Procedure 11. BOD Upgrade

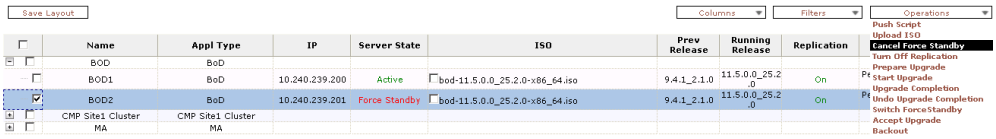
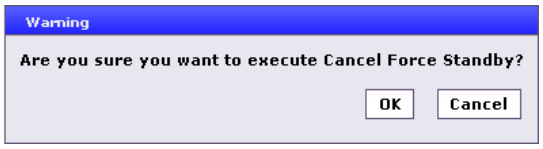
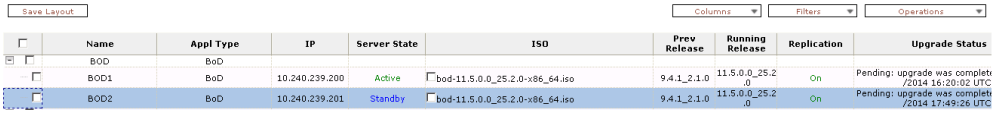
13.	**CMP GUI:** Start upgrade	Then with the second server checked (the force StandBy server) , open the operations menu and choose the "Start Upgarde"  Confirm the action on the next dialog box  An information message indicating the successful start of the upgrade displays and upgrade starts. The upgrade will go through multiple steps including rebooting the server; those steps are reflected in the BOD's "Upgrade Status" field of the System Maintenance screen.  Wait till the upgrade status indicates upgrade was completed. 
14.	**CMP GUI:** Expected alarms	During the upgrade some alarms may raise like the following:  These alarms are expected and would be automatically cleared after the upgrade concludes successfully
15.	**11.5 upgraded BOD server CLI:** Validate upgrade log file	SSH to upgraded BOD server and login then tail the upgrade log file as follows :  Validate upgrade returned success.

Procedure 11. BOD Upgrade

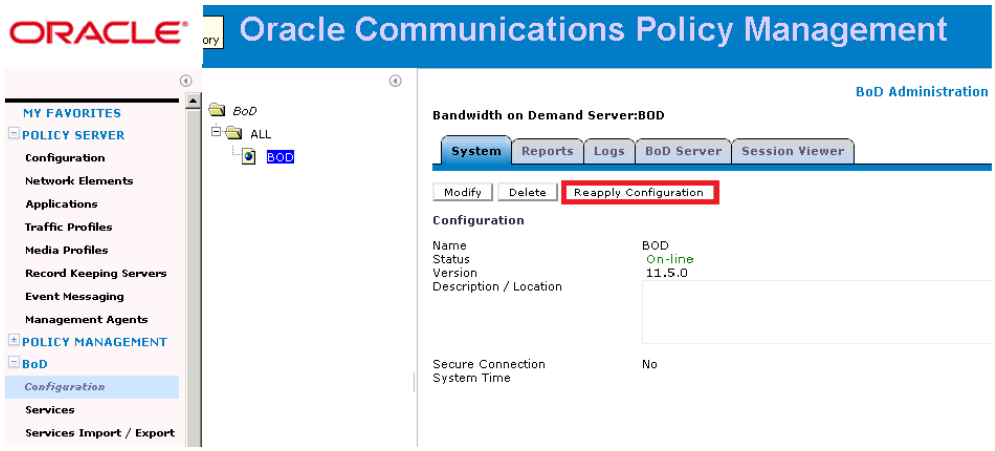
16.	**11.5 upgraded BOD server CLI:** Validate policy revision	Run the following command to check running policy version: `[root@BOD2 ~]# getPolicyRev -f bod_11.5.0.0_25.2.0` Make sure the version is the upgraded version "11.5"

17.	**11.5 upgraded BOD server CLI:** Verify the server's HA role	Run the command "ha.mystate" to verify the server has the stand By role:
		`[root@BOD2 ~]# ha.mystate`
		`resourceId role node subResources lastUpdate`
		`DbReplication Stby C1729.168 0 1015:135016.099`
		`VIP Stby C1729.168 0 1015:135016.100`
		`QP Stby C1729.168 0 1015:135016.139`
		`DbReplication_old OOS C1729.168 0 1015:134929.756`

18.	**11.5 upgraded BOD server CLI:** Verify NTP sync	Run the command "ntpq -pn" to verify the server is in sync with the NTP server:
		`[root@BOD2 ~]# ntpq -pn`
		`remote refid st t when poll reach delay offset jitter`
		`*10.250.32.10 192.5.41.209 2 u 21 64 177 0.260 4.834 2.056`

19.	**CMP GUI:** Cancel force standby	After upgrade completes, cancel Force Standby from the operations menu :  Confirm the action on the next dialog box  An information message indicating the successful cancellation of Force standby
20.	**CMP GUI:** BOD servers status check	Validate that now one of the BOD servers is in "Active" State and the other is in "StandBy" state: 
21.	**11.5 secondary site BOD spare server**	In case solution is geo-redundant , follow the same current procedure to upgrade the BOD spare server in secondary site

Procedure 11. BOD Upgrade

22.	**CMP GUI:** BOD Configuration	Navigate to BOD →Configuration and Reapply Configuration to clear configuraion mismatch 
23.	**Post upgrade checks**	Follow the same procedures outlined in section 2.5 of this document to validate the upgrade completed successfully.
24.	**Back out the upgrade**	In case post upgrade checks failed and back out is decided, follow the same procedures outlined in section 2.6 of this document to back out the BOD cluster
25.	**Accept the upgrade**	Follow the same procedures outlined in section 2.7 of this document to accept the upgrade.