ORACLE

Oracle® Communications

Policy Management
Bare Metal Installation Guide

Release 9.4

E85553-01
March 2017

TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 Purpose

This document describes the procedures to configure the hardware and platform components of a hardware environment to run Policy Management Software 9.4.

Policy Management 9.4 runs on HP ProLiant hardware. Including:

- HP ProLiant DL360G6
- HP ProLiant DL360G7
- HP ProLiant DL360pGen8
- HP ProLiant DL380pGen8

The purpose of this document is to describe the Installation Procedures for servers running Policy Management 9.4.

Policy Management 9.4 is based on Tekelec Platform 6.0 Software.

- Carrier Grade Operating System TPD 6.0.1
- High Performance In-memory DB COMCOL 6.1
- Policy Management Applications 9.4: MPE, MA, BOD and CMP

This document is intended for engineering, integration, documentation, technical services, and test groups. This document may be used in discussions with the customer to determine if this product satisfies their expectations. The reader is assumed to be familiar with Policy Management Products.

The scope of this document is to describe the Procedures for Policy Management 9.4 Installation.

Other procedures required for Policy Management 9.4 include Aquiring Firmware, [TODO]. For information on these procedures please refer to *Platform 5.x HP G6/G7 Configuration Procedure Reference*.

1.2 Product Summary

Ensure that all equipment has been physically installed and is under power. If this has not been already performed, do so now before continuing with this document (refer to the appropriate hardware installation guide).

Some of the procedures used in this guide require direct console access. Ensure that you have a keyboard and monitor available, as well as all the required adapters for working with HP equipment.

It is required that IP network layout, addressing, and cabling be determined prior to performing the procedures in this guide. This includes:

- Knowledge of which networks will be used for Management, iLO/RMM, OAM, Signaling-A, and Signaling-B interfaces (refer to Policy Management on HP Rack Mount System Networking Interconnect TR007293).
- All IP addresses and gateways to be configured on the Policy Management systems and support equipment (aggregation switches, PM&C server, etc.). Refer to the IP Network Site Survey.
- NTP and DNS information.

1.3 References

- *Disaster Recovery Process for HP c-Class*, 909-1638-001
- *HP Solutions Firmware Upgrade Pack Release Notes*, 795-000-2xx
- *HP Solutions Firmware Upgrade Pack Release Notes*, 909-1927-001.
- *Platform 5.x HP G6/G7 Configuration Procedure Reference*, 909-1620-001
- *SNMP User's Guide*, 910-6288-001
- *Platform 5.x HP G6/G7 Configuration Procedure Reference*, 909-1620-001
- *Initial Product Manufacture*, 909-2130-001
- *Oracle Communication Policy Management Disaster Recovery Procedures*, E85223-01

1.4 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

1.5 My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with My Oracle Support registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the following sequence on the Support telephone menu:

1. Select **2** for New Service Request
2. Select **3** for Hardware, Networking and Solaris Operating System Support
3. Select one of the following options:
    a. For Technical issues such as creating a new Service Request (SR), select **1**
    b. For Non-technical issues such as registration or assistance with My Oracle Support, Select **2**

You will be connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket. *My Oracle Support* is available 24 hours a day, 7 days a week, 365 days a year.

2.0 INSTALLATION PROCEDURES

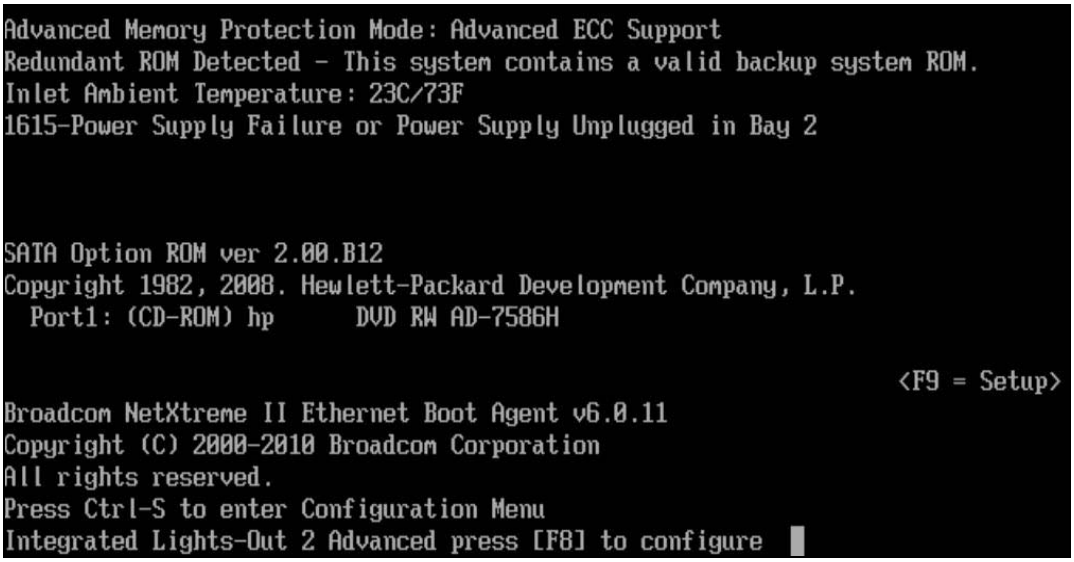
2.1 Updating and Configuring the HP blade

2.1.1 Procedure 1: Updating the HP Firmware and Configuring the BIOS

To perform this procedure perform the steps described in Ch. 3.10.1 Upgrade DL360 or DL380 Server Firmware in *Platform 5.x HP G6/G7 Configuration Procedure Reference*, 909-1620-001.

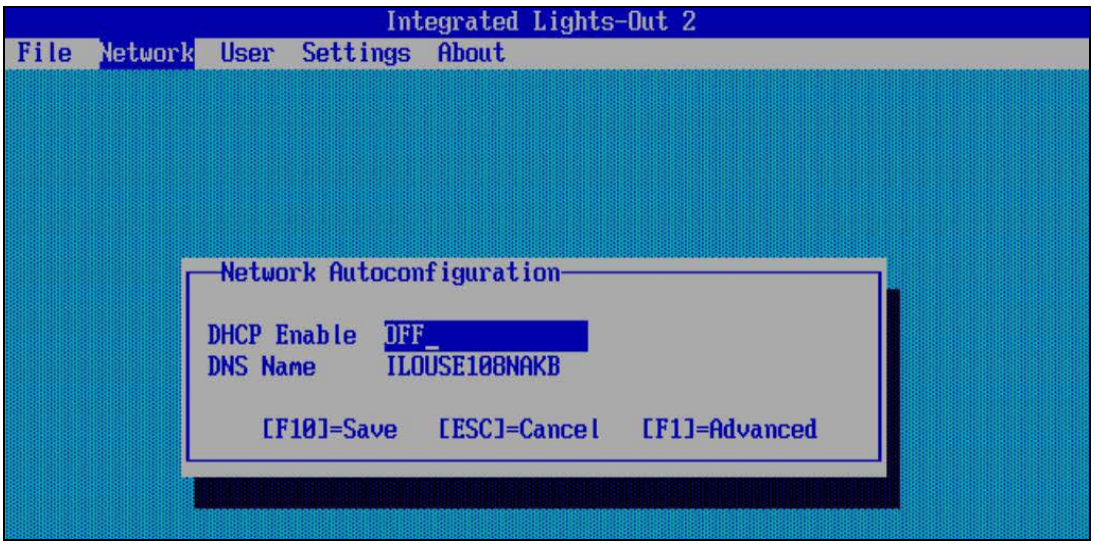
2.1.2 Procedure 2: Configuring the DL360 iLO Port

1. Connect to the console and reboot the DL360 server.
2. After the server has rebooted, press **F8** to access the iLO configuration menu, as soon as you see `Integrated Lights-Out 2 Advanced press [F8] to configure` at the bottom of the screen

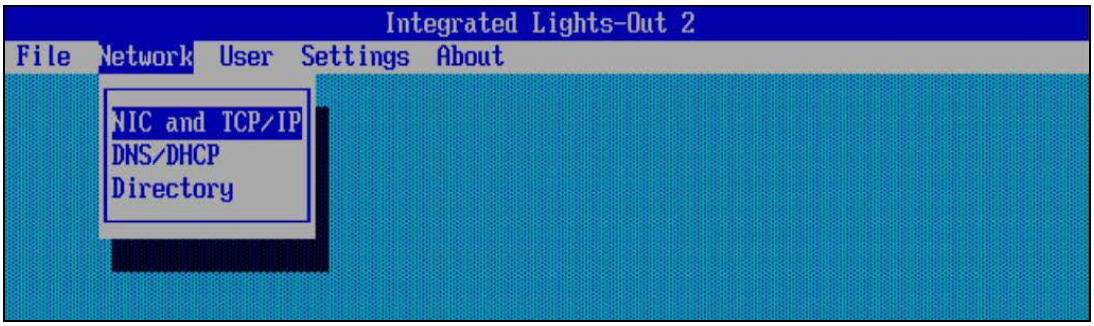


3. Select **DNS/DHCP** from the Network tab pull-down.

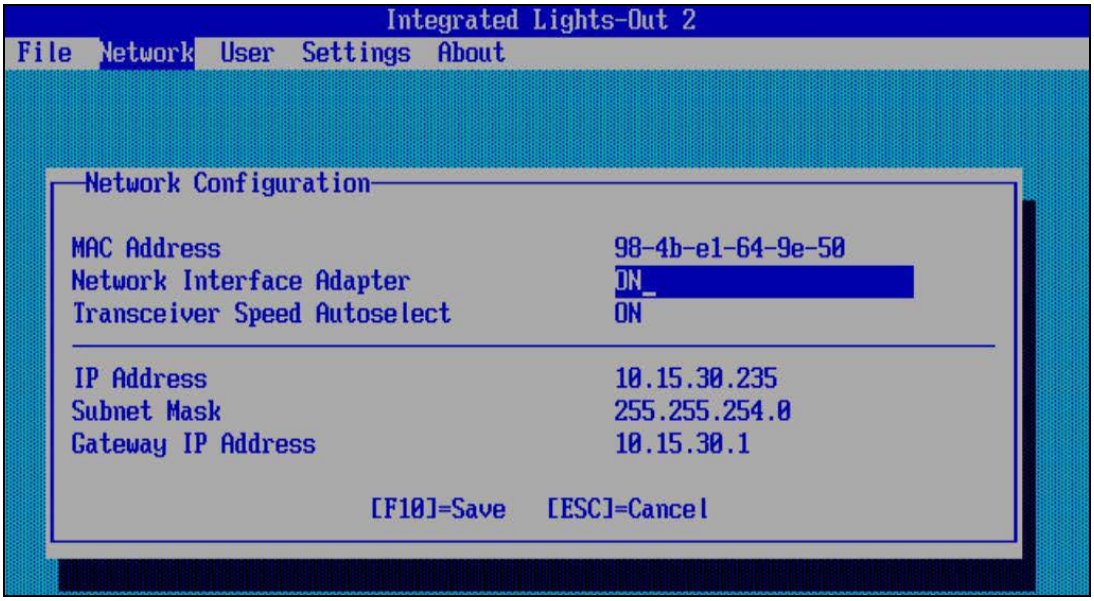
4. Disable DHCP and press **F10** to save.



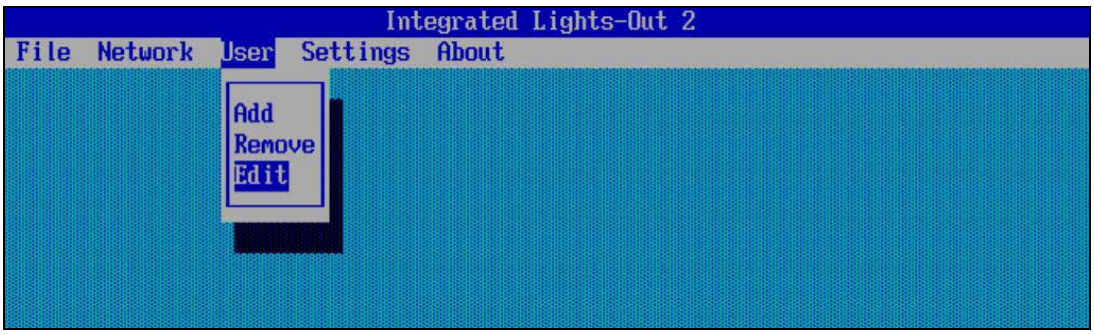
5. Select **NIC and TCP/IP** from the Network tab pull-down.



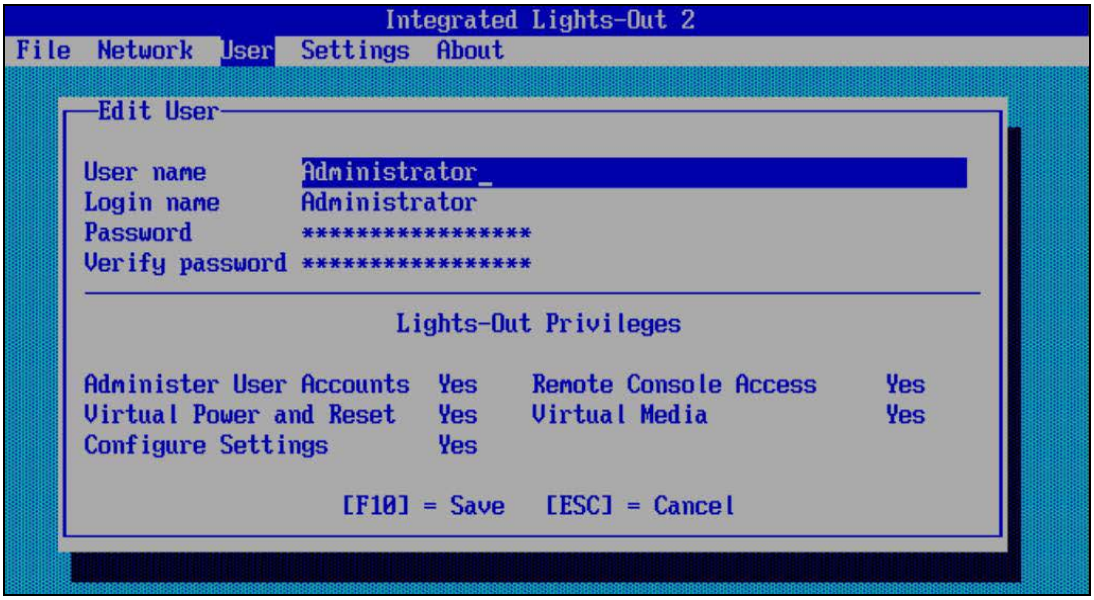
6. Configure the **IP address, Subnet netmask**, and Gateway IP Address, and press F10 to save.



7. Select **Edit** from the User tab pull-down.



8. Configure a password for the default administrator account and press **F10** to save.



9. Select **Add** from the User tab pull-down menu.
10. Create a root user with all privileges set to **Yes**. Press **F10** to save.
11. Exit the configuration utility.

2.2 Software Installation

2.2.1 Procedure 3: TPD Installation

To perform this procedure perform the steps described in section 3.10.2 of the *Platform 5.x HP G6/G7 Configuration Procedure Reference*, 909-1620-001

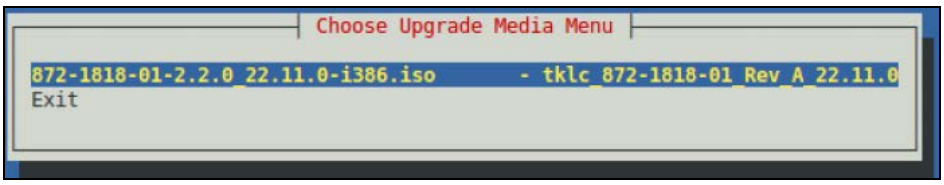
2.2.2 Procedure 4: Application Software Installation

1. Insert the Policy Management application media into the optical drive. For DL380pGen8 where optical drive does not exist, we can mount the ISO using iLO virtual media manager, or follow the steps in section 1.4 of PG005024 to copy the ISO from a USB stick to /var/TKLC/upgrade of the server.
2. Connect to the server console and log in as **root**.
3. Start the Platcfg utility by issuing the following command:

```
#   su-platcfg
```

4. From the platcfg utility, navigate to **Maintenance → Upgrade → Initiate Upgrade**.

5. Select the ISO image from the Upgrade Media Menu. For example:



NOTE: The server will reboot twice during the installation process, Do Not Remove the media at this time.

6. Once the login prompt is displayed, installation is complete. Remove the DVD from the DVD drive. It's also safe to delete the iso file in /var/TKLC/upgrade.

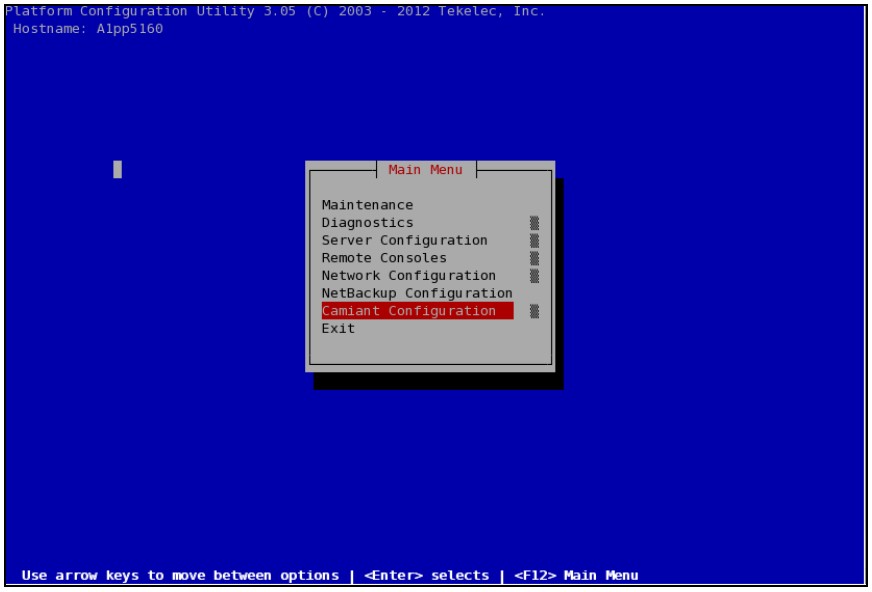
2.2.3 Procedure 5: Initial platcfg Configuration

Clustered Policy Management products perform replication using an external interface. This interface is defined as the OAM Real IP address. This interface is always active on the server and is used in later procedures, as part of the cluster definition. This procedure requires a single IP address on the OAM network for each server.

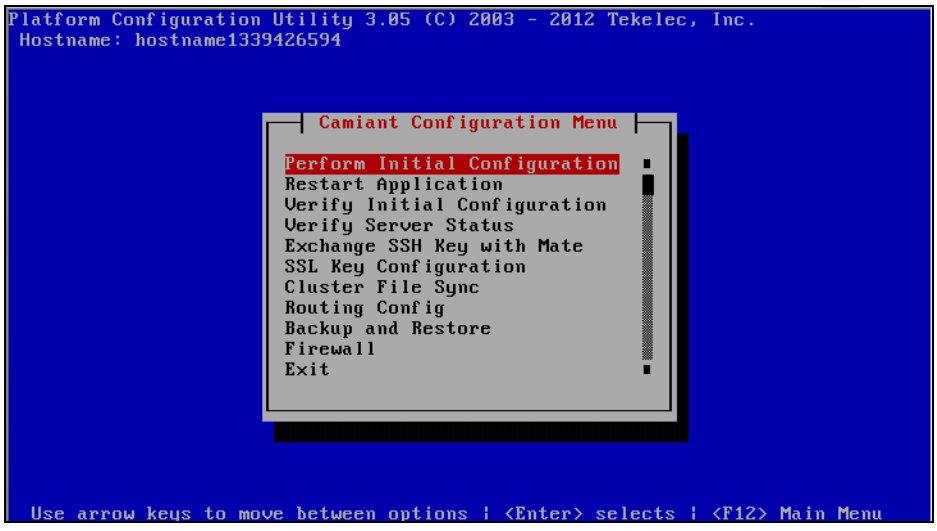
1. Log in as **root** and then open the platcfg utility, using the following command:

```
#   su–platcfg
```

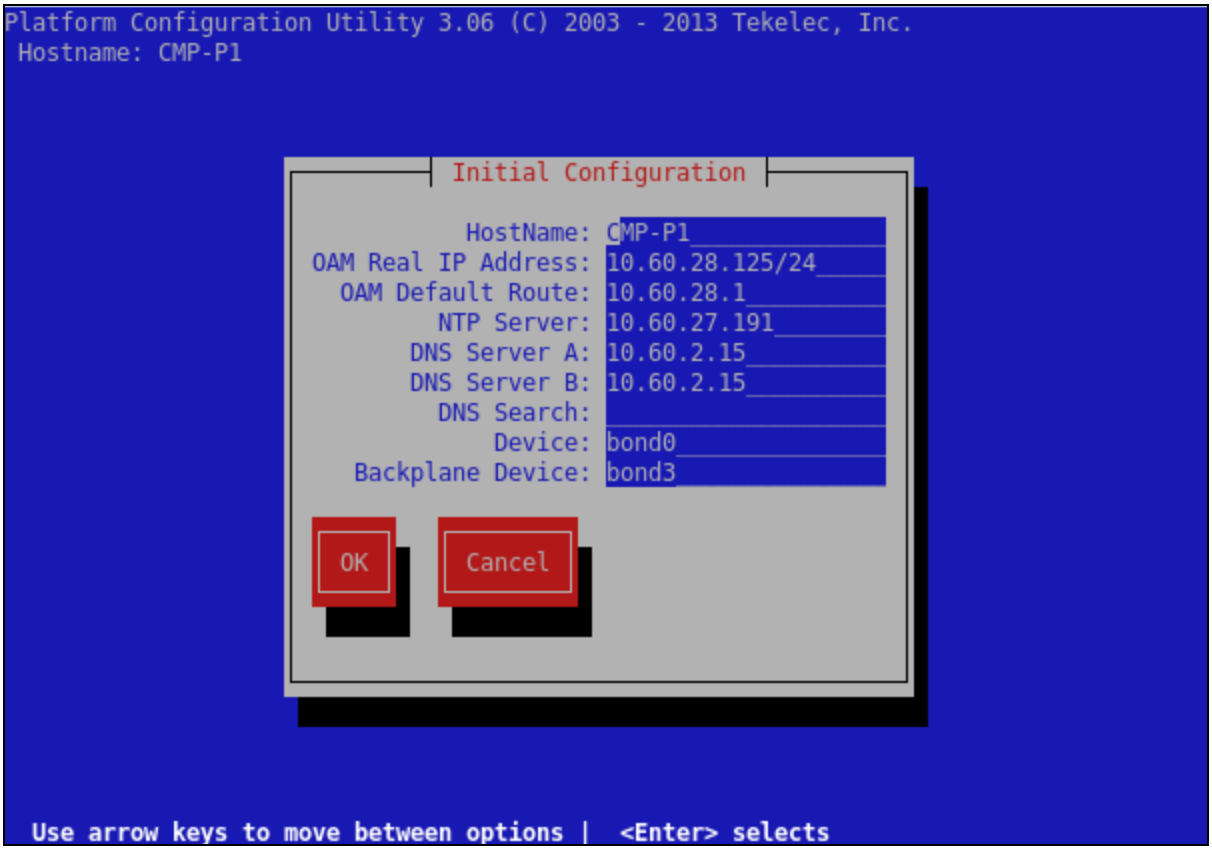
2. From the platcfg utility, select **Camiant Server Configuration** from the Main Menu.



3. Select **Perform Initial Configuration**.



4. Once selected, the following screen is displayed:



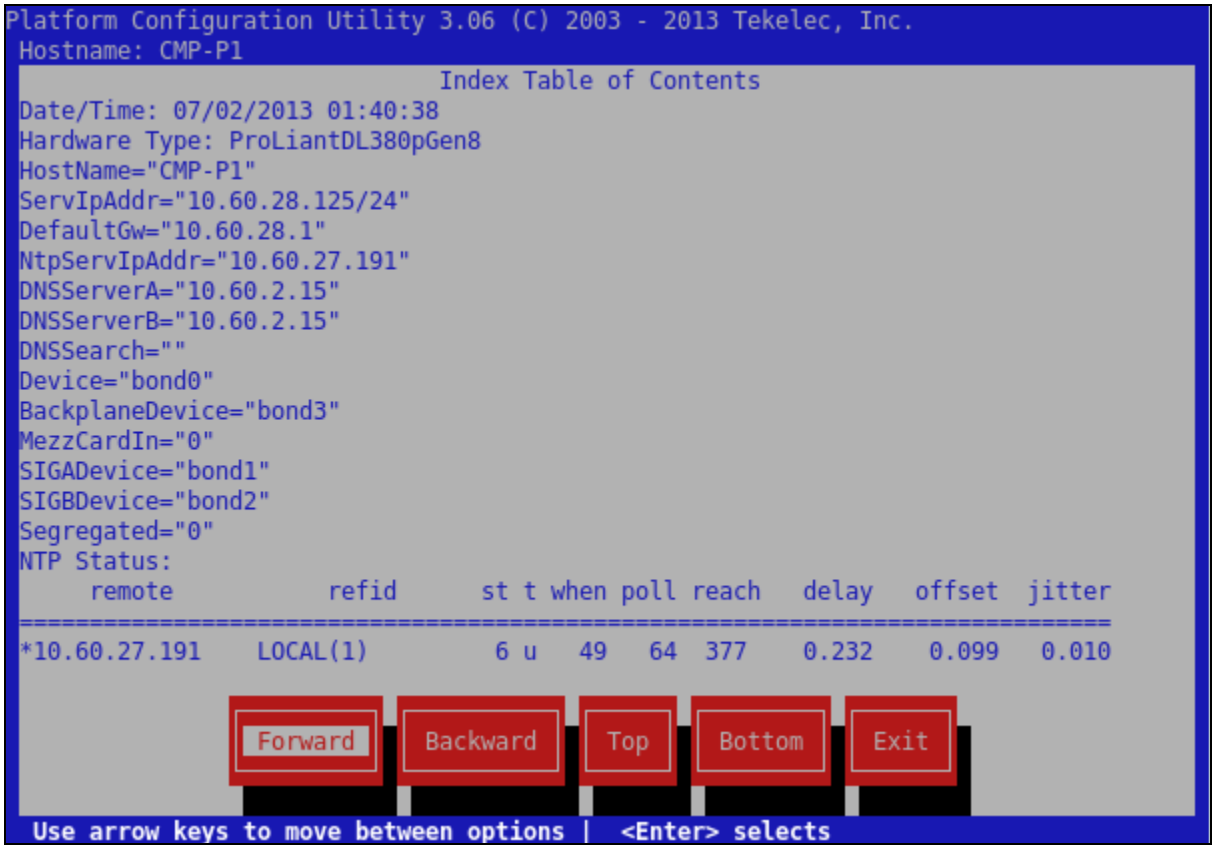
Where:

- **Hostname**—the unique hostname for the device being configured.
- **OAM Real IP Address**—the IP address that is permanently assigned to this device.
- **OAM Default Route**—the default route of the OAM network.
- **NTP Server**—a reachable NTP server.
- **DNS Server A**— a reachable DNS server. This is optional but recommended.
- **DNS Server B**— a second reachable DNS server. This is optional but recommended.
- **DNS Search**—is a directive to a DNS resolver (client) to append the specified domain name (suffix) before sending out a DNS query.
- **Device**—the bond interface of the OAM device. Note that the default value should be used, as changing this value is not supported.
- **Backplane Device** – the bond interface of the Backplane device. Note that the default value should be used, as changing this value is not supported.

5. Enter the configuration and then click **OK**.
6. When prompted to save and apply, click **Yes**.

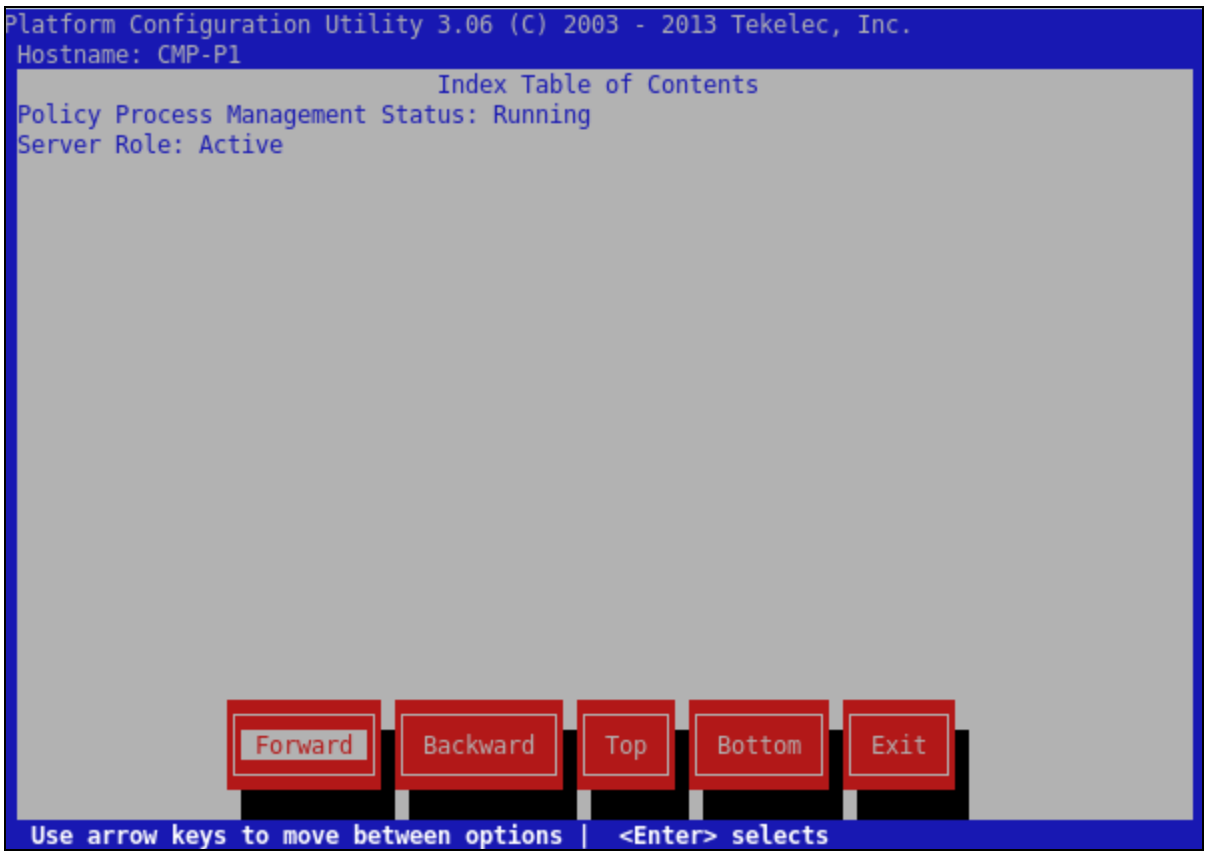
   At this point the screen pauses for approximately one minute. This is normal behavior and occurs while the configuration updates.

7. Verify the configuration by selecting **Camiant Server Configuration→Verify Initial Configuration** from the platcfg utility. A display similar to the following is shown.



NOTE: The NTP status may not have updated yet. This is normal behavior.

8. Exit from this screen and select **Verify Server Status**. The server should be in a running state. For example:



9. Exit the platcfg utility and ping the default gateway to validate network connectivity.
10. Repeat this procedure on all servers.

Once all servers are configured you are now ready to begin the topology and clustering configuration.

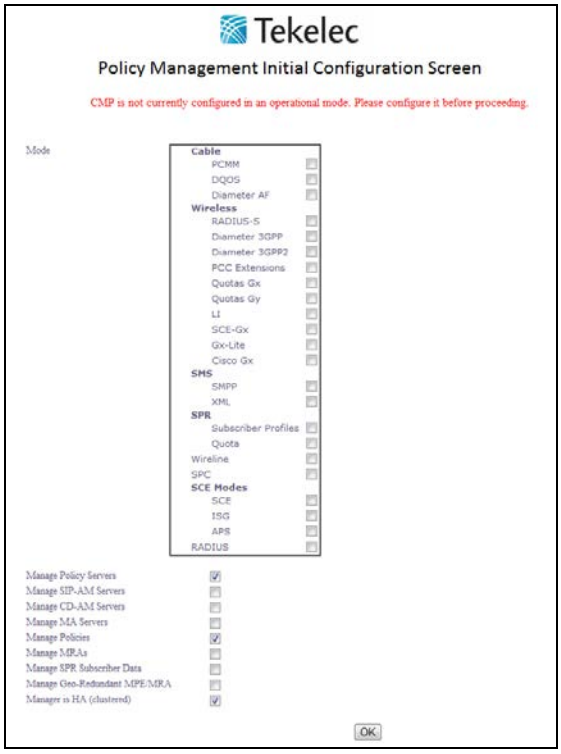
2.3 Configuring the Policy Management Application

2.3.1 Procedure 6: CMP Topology Configuration

Once the product software has been installed and the initial configuration has been performed, you must now use the CMP GUI to configure topology to provide a clustered environment, ensuring high system availability. The CMP has a different procedure than the MPE/MA/BoD, and must be configured first.

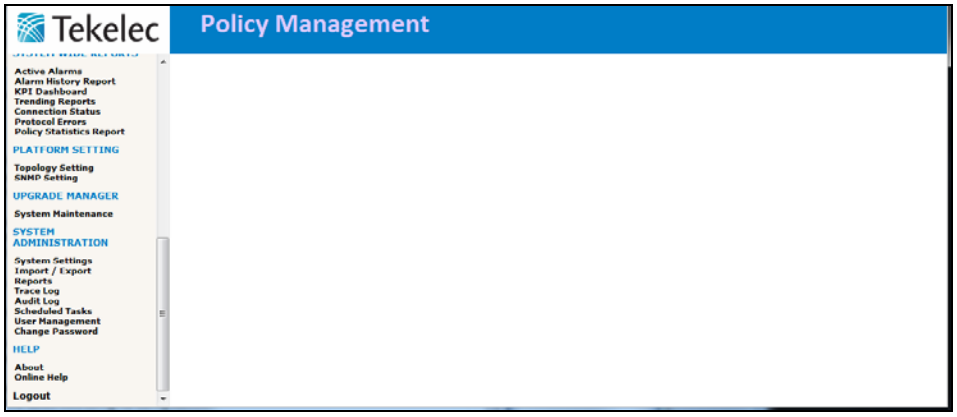
This procedure requires a single IP address on the OAM network to be used as the OAM VIP for the CMP cluster. The OAM Real IP address configured in the initial configuration procedure cannot be used for this purpose.

1. Open a WEB browser and enter the OAM Real IP address of the first CMP blade (in this example CMP-a).
2. Enter the mode of operation and when finished, click **OK**. For example:

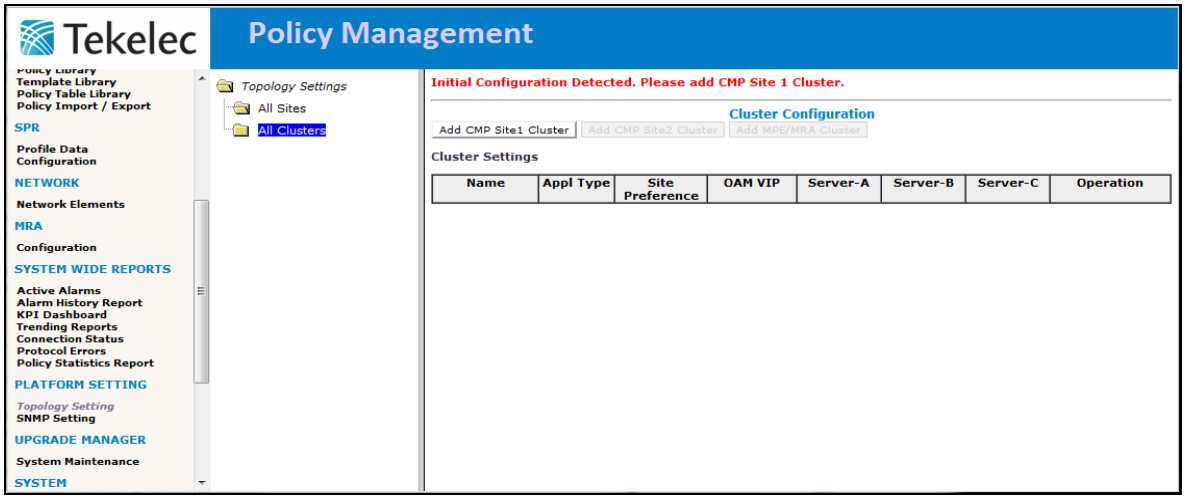


NOTE: Check the item "Manage Geo-Redundant MPE/MRA" if you are building geo-redundant solution.

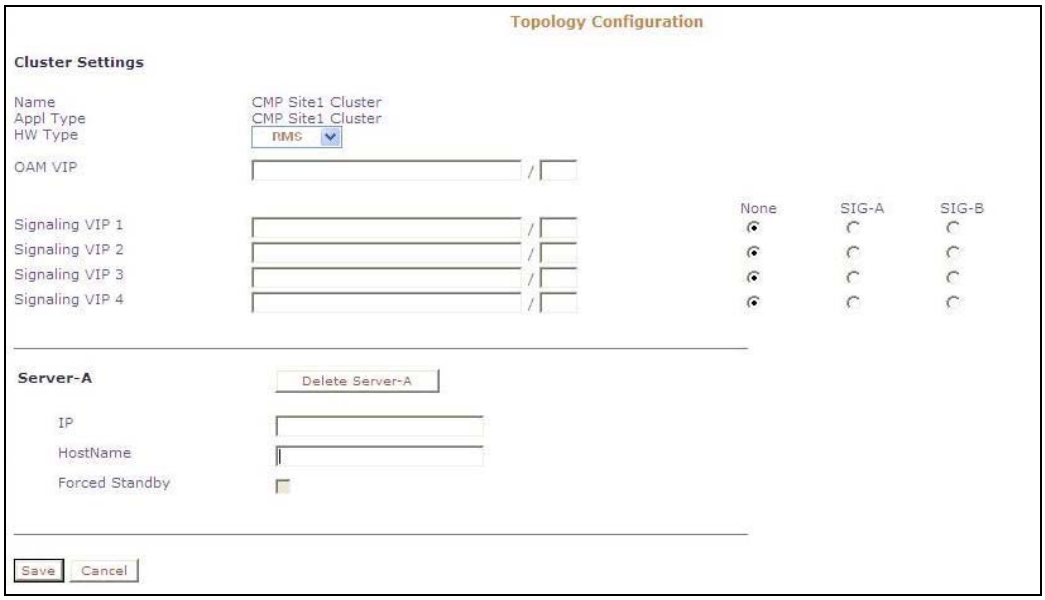
3. Log in as `admin`, with a password of `policies`.
4. You are prompted to change your password. Enter your new password and then click **Change Password**. The main CMP page is displayed.



5. Configure the CMP topology by selecting **Topology Setting**, located in the Platform Setting section of the navigation pane.



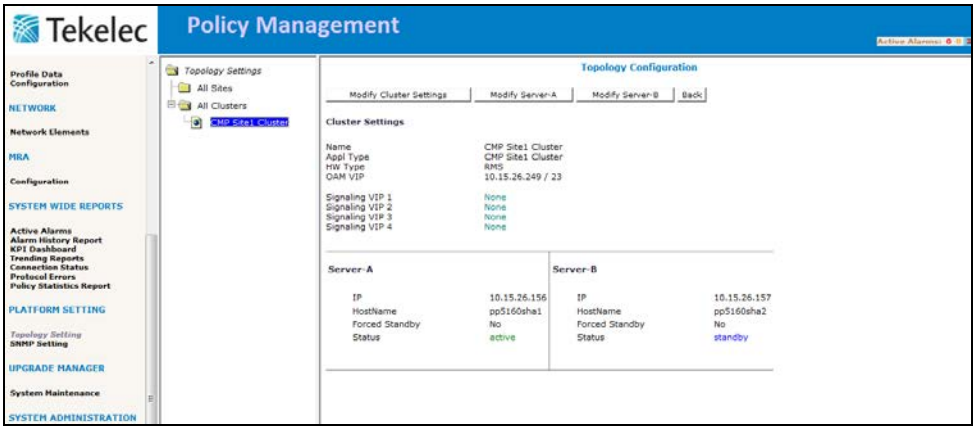
6. Click **Add CMP Site 1 Cluster**. The Cluster Setting page is displayed.



7. Configure the following items; click **Save** when finished.
   - **HW Type**—If you are using DL360G6 or G7, please select **DG360G6/G7**. If you are using anything else, select **RMS**.
   - **OAM VIP**—IP address and netmask for the cluster VIP on the OAM network.
   - **Signaling VIP**—(optional) VIP and netmask for the cluster on the signaling network. Note that you must select SIG-A or SIG-B interface.
   - **Server-A IP**—OAM Real IP address for the first server (predefined, no input necessary).
   - **Server-A Hostname**—hostname for the first server (predefined, no input necessary).
8. SSH to the CMP-a blade (hostname Cfg1-CMP-a in this example) and log in as `root`.
9. On CMP-a, use the `ha.mystate` command to verify that the blade becomes active by noting the role switching to Active. The following example illustrates this:

```
[root@CMP-P1 ~]# ha.mystate
          resourceId   role         node       subResources      lastUpdate
       DbReplication Active    A0509.253                  0 0624:031437.275
                 VIP Active    A0509.253                  0 0624:031437.298
                  QP Active    A0509.253                  0 0625:032503.679
   DbReplication_old    OOS    A0509.253                  0 0624:031433.975
```

10. Log in to the CMP GUI using the OAM VIP configured in this procedure.
11. Select the topology link and click **View** for the CMP site-1 cluster.
12. Click **Modify Server-B** and configure the following:
    - **Server-B IP**—OAM Real IP address for the second server.
    - **Server-B Hostname**—hostname for the second server. This hostname must exactly match the hostname configured in platcfg (same as `uname -n`).
13. Click **Save** when finished. The following is an example of a completed configuration.



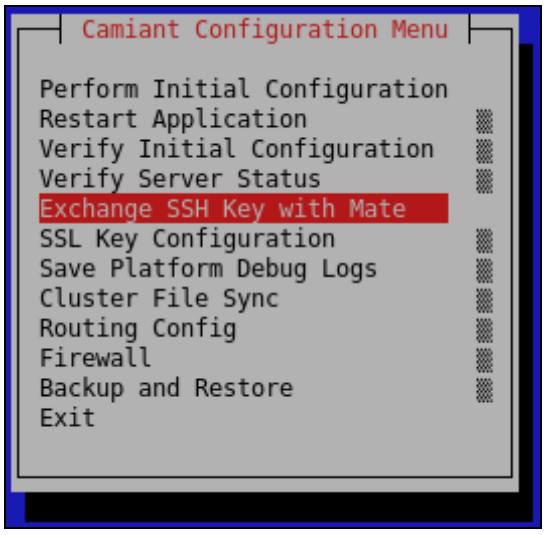
14. Log into the CMP GUI and select **Topology**.
15. Click **View** for the CMP site-1 cluster.
16. Click **Modify** for Server-B and select **Force Standby.**
17. Click **Save** when finished.
18. Log in as `root` on both blades and enter:

```
ha.mystate.
```

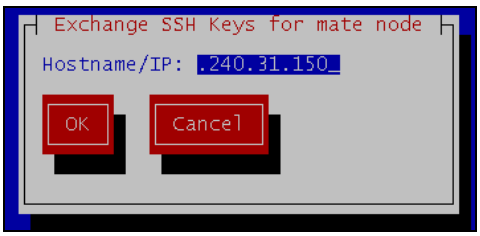
19. Wait for one blade to be in Stby and the other Active.
20. On the active blade, enter the following command to access the platcfg utility:

```
#   su–platcfg
```

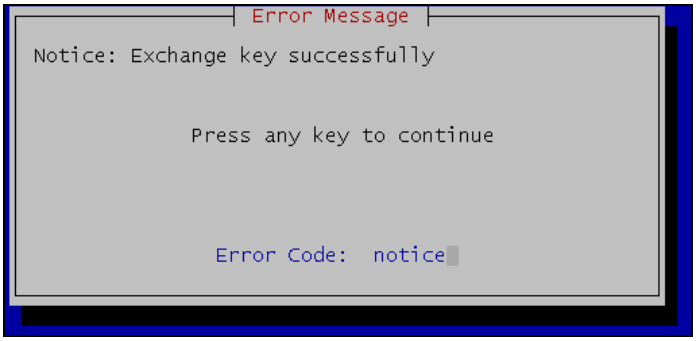
21. In the platcfg utility Main Menu, select **Camiant Server Configuration**.
22. Select **Exchange SSH Key with Mate**.



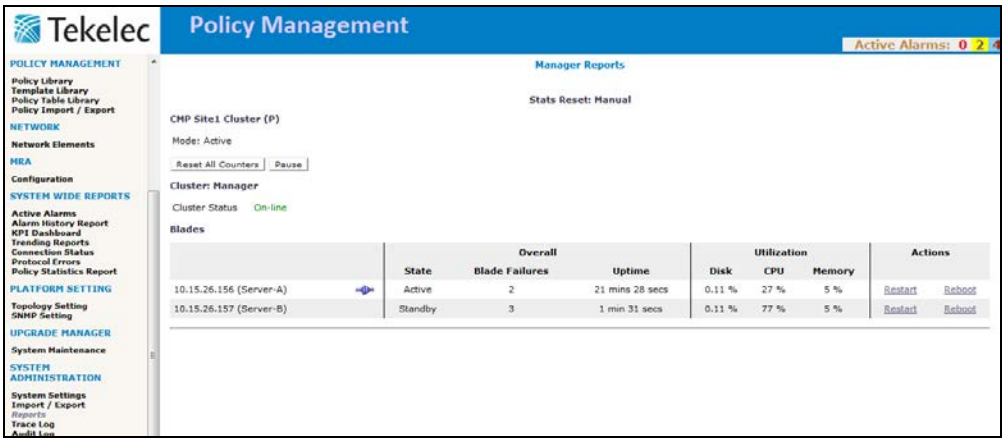
23. The hostname or IP address of the mate is displayed for verification purposes. For example:



24. If the hostname or IP address is correct, click **OK**. Some activity may be noticed while the key exchange occurs, and after a few seconds a message is displayed:



25. Press **Enter**.
26. Exit the platcfg utility.
27. Log in to the CMP GUI and select **Reports**, located in System Administration on the navigation bar. Both CMP blades should be displayed with `Topology OK`. For example:



You are now ready to configure your MPE, MA or BOD servers topology.

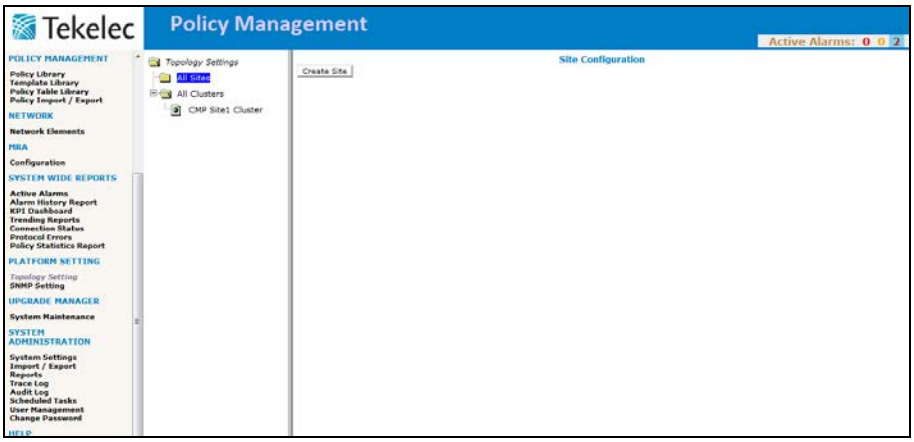
2.3.2 Procedure 7: MPE-R/MPE-S/MA/BOD Topology and Clustering Configuration

Once the MPE/MA/BOD software has been installed and the initial configuration has been performed, you can configure your topology to provide a clustered environment, ensuring high system availability. Note that the CMP topology must be configured prior to configuring the MPE-R/MPE-S/MA/BOD.

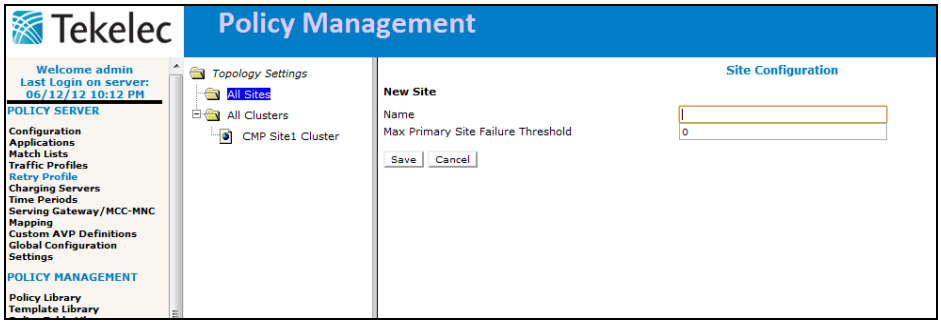
The OAM Real IP address configured in the initial configuration procedure is used for configuring the MPE/MA/BoD servers. Also, this procedure requires a minimum of 1 IP address on either the Signaling-A or Signaling-B network to be used as the signaling VIP for the MPE cluster.

1. Open a web browser and enter the OAM VIP of the CMP.
2. Click **Manager** within the window and log in as `admin`.

3. Configure the Site Topology. Note this requires that you selected **Manage Geo-Redundant MPE/MRA** on the mode page, as described in section 2.3.1, Procedure 6: CMP Topology Configuration.

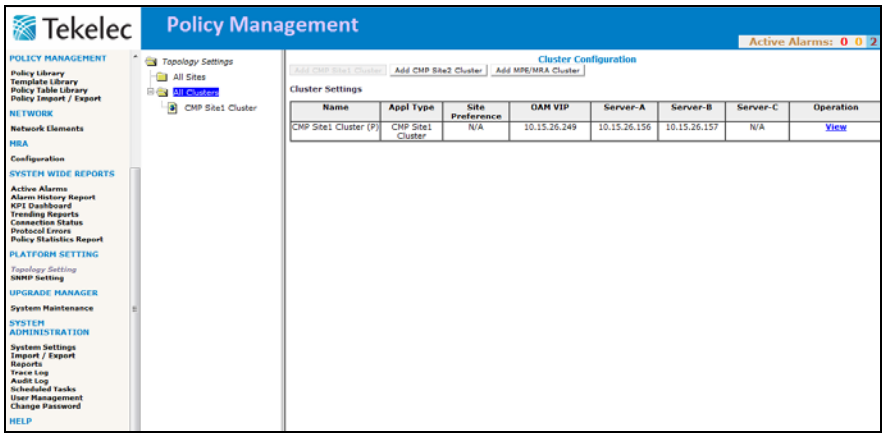


4. Click **Create Site**. The Site Configuration opens.

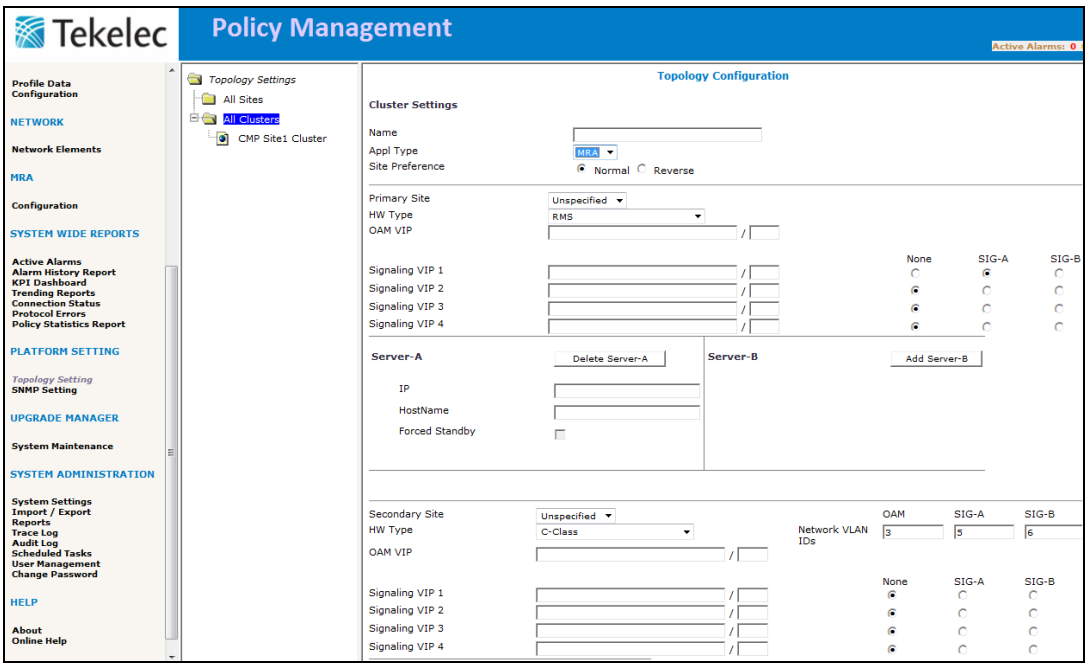


- **Name**—used to provide an identifying name for the Site within the CMP GUI and within the topology.
- **Max Primary Site Failure Threshold**—Fill in the number of Primary Site MPEs that must fail before an Alarm is raised.

5. Configure the MPE/MA/BOD topology by selecting **Topology Setting**, located within the Platform Setting section of the navigation pane.



6. Click **Add MPE/Bod/MA Cluster**. The Cluster Setting page is displayed.

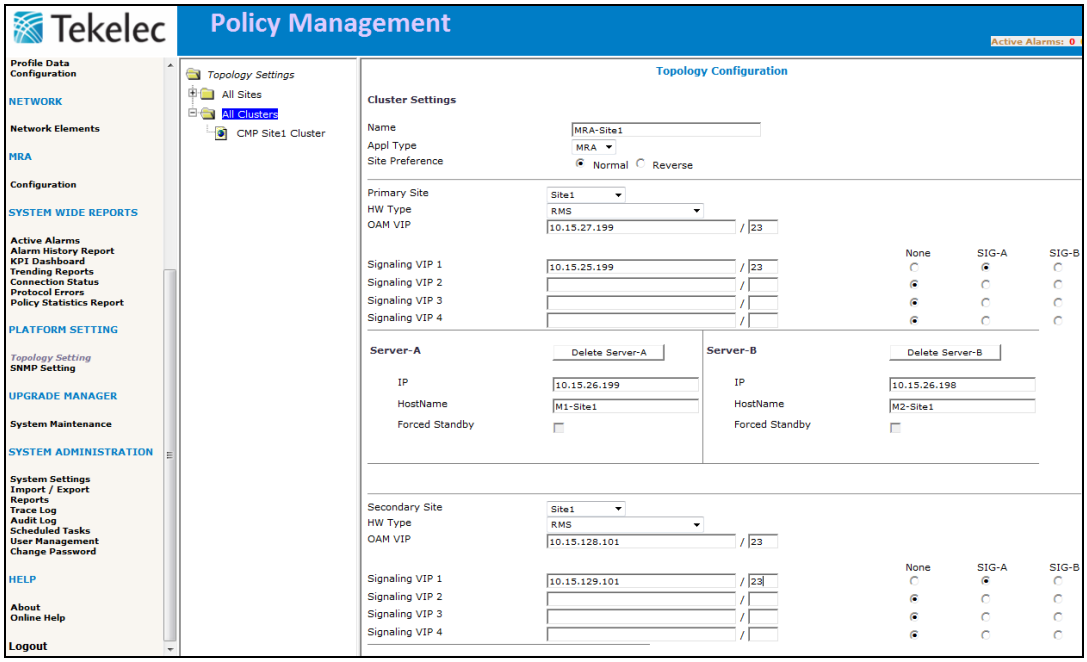


7. Configure the following items, click **Save** when finished:

   NOTE: OAM VIP and Server IP addresses require IPv4. Only SIG-A/B VIP may be IPv6 or IPv4

   - **Name**—used to provide an identifying name for the cluster within the CMP GUI.
   - **Application Type**—the application type.
   - **Primary Site/Secondary Site**—used to identify which site this cluster is in. If keep this input as default, The other servers in topology may raise alarm 31209. This alarm should also raise if servers in different clusters but configured with same site name.
   - **HW Type**—select RMS or DL360G6/G7. Depending on your hardware type.
   - **OAM VIP**—VIP and netmask for the cluster on the OAM network.
   - **Signaling VIP1**—VIP and netmask for the cluster on the signaling network. Note that you must select SIG-A or SIG-B interface. Each interface can have more than one VIP. Note that one cluster might require you to configure 2 VIPs for the two different sites.
   - **Server-A IP**—OAM Real IP address for the first server.
   - **Server-A Hostname**—hostname for the first server.
   - **Server-B IP**—OAM Real IP address of the second server (click **Add Server B**, if needed).
   - **Server-B Hostname**—hostname for the second server.
   - **Server-B Forced Standby**—Click this checkbox to prevent server from Providing Service (Forced Standby automatically checked when server is first added).
   - **Server-C IP**—OAM Real IP address for the first server. NOTE: Server-C Configuration is only required for the PCRF Geo-Redundancy Feature.
   - **Server-C Hostname**—hostname for the spare server.
   - **Server-C Forced Standby**— Click this checkbox to prevent server from Providing Service (Forced Standby automatically checked when server is first added).

The following is an example of a configured MPE Cluster Setting pages.



8. Log in as `root` on both blades and type

```
ha.states
```

Wait for one blade to report Active and one to report Stby. For example:

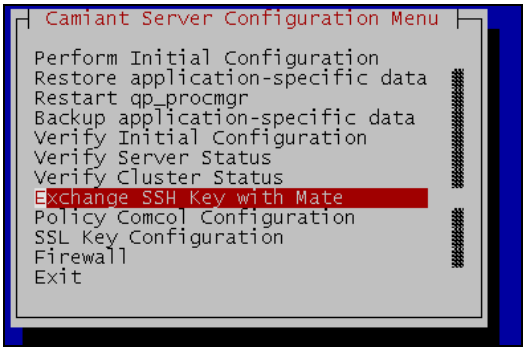
```
          resourceId   role         node      subResources       lastUpdate
       DbReplication   Stby    C1126.004                 0 0511:161808.551
       DbReplication Active    C1126.151                 0 0511:161507.429
                 VIP   Stby    C1126.004                 0 0511:161808.563
                 VIP Active    C1126.151                 0 0511:161507.453
                  QP   Stby    C1126.004                 0 0511:161837.544
                  QP Active    C1126.151                 0 0511:161551.230
   DbReplication_old    OOS    C1126.004                 0 0511:161808.138
   DbReplication_old    OOS    C1126.151                 0 0511:161851.073
```

If a display similar to the above is not displayed, contact My Oracle Support.

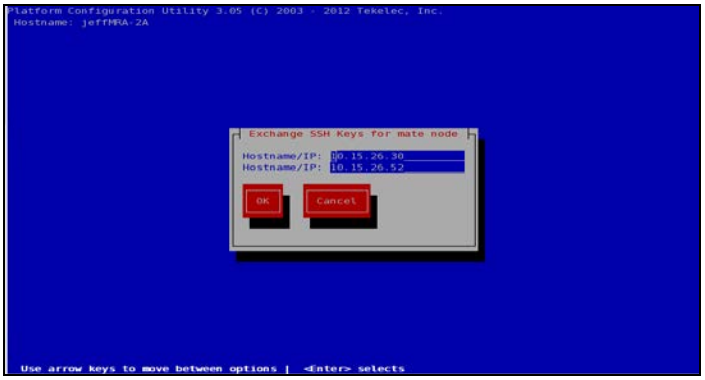
9. Press **Ctrl-C** to exit from the `ha.states` command.
10. On the active blade (the blade with a role of Active), log in as `root` and enter the following command to access the platcfg utility:

```
#   su-platcfg
```

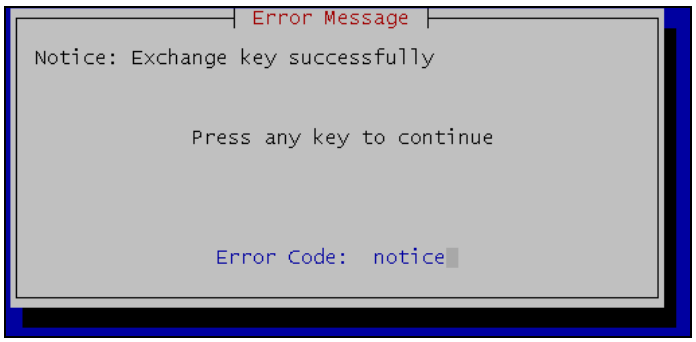
11. In the platcfg utility Main Menu, select **Camiant Server Configuration**.
12. Select **Exchange SSH Key with Mate**.



13. If the hostname or IP address is correct, click **OK**.



Some activity may be noticed while the key exchange occurs and after a few seconds a message is displayed:



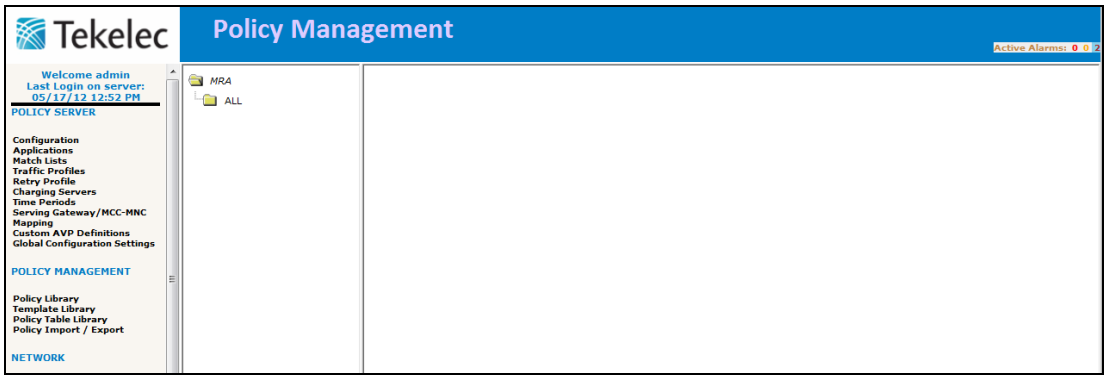
14. **Enter** to continue.
15. Exit the platcfg utility.

You are now ready to add your MPE, MA or BOD cluster to the CMP.

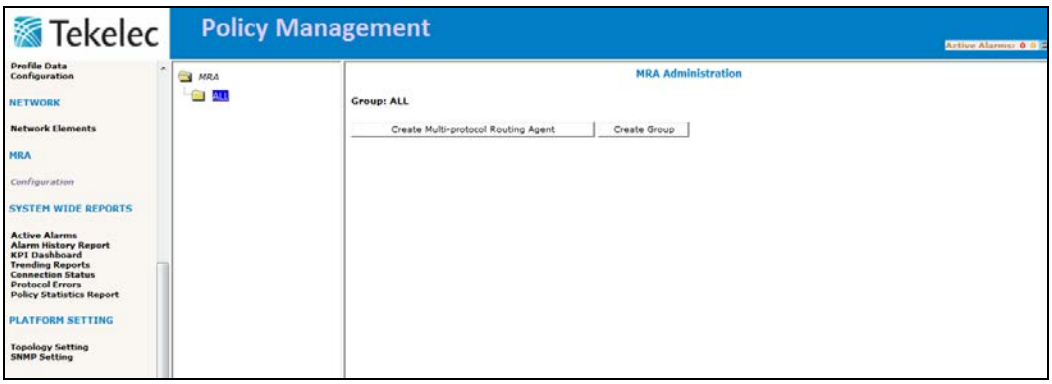
2.3.3 Procedure 8: Adding MPE, MA or BOD cluster to the CMP

Once the MPE/MA/BoD software has been installed, is running correctly, and the servers have their topology/clustering established between the two servers, the servers need to be added to the master CMP and have the cluster procedure completed within the CMP.

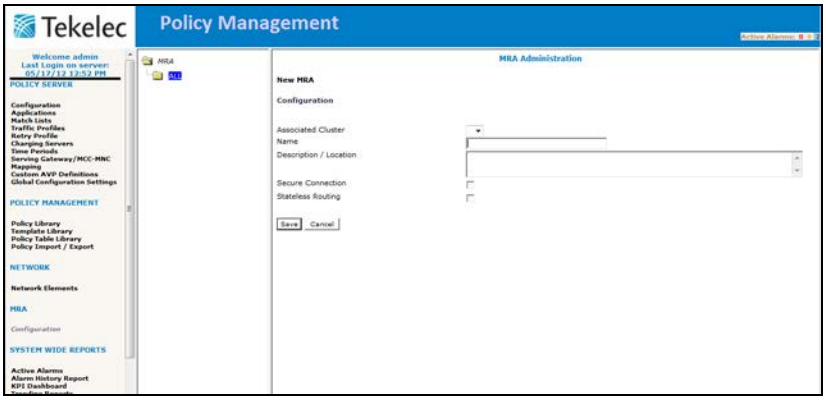
1. From within the CMP:
   - Under Policy Server, select **Configuration** to add an MPE
   - Select **Management Agents** to add an MA.
   - Under BoD, select **Configuration** to add a BoD.



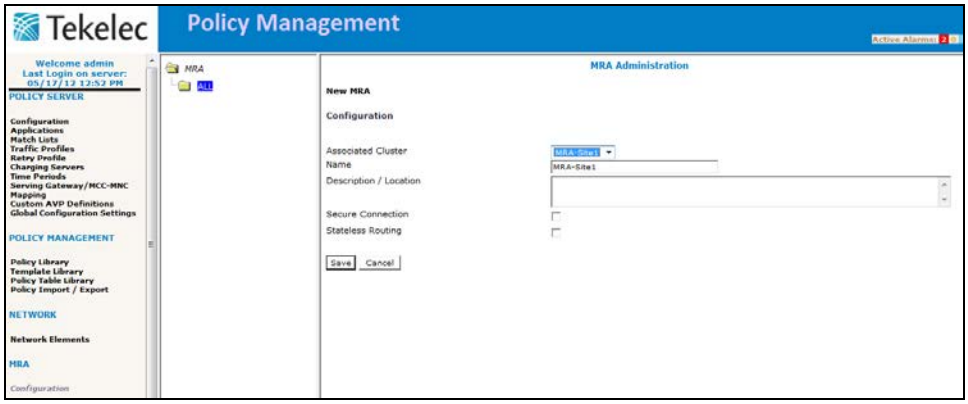
2. Click **ALL**.



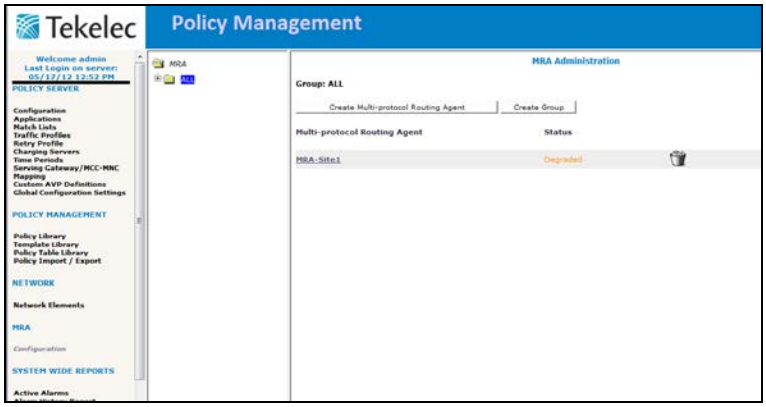
3. Click **Create Policy Server** or **Create Management Agent** or **Create Bandwidth on Demand Server.**



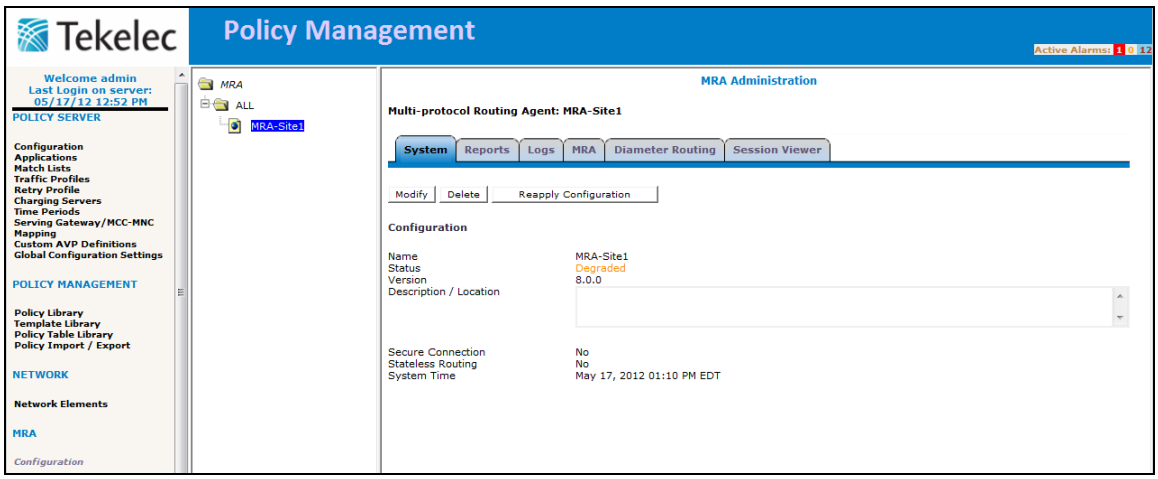
4. In the Associated Cluster field, select the cluster from the pull down menu. The name and description automatically populates. For example:



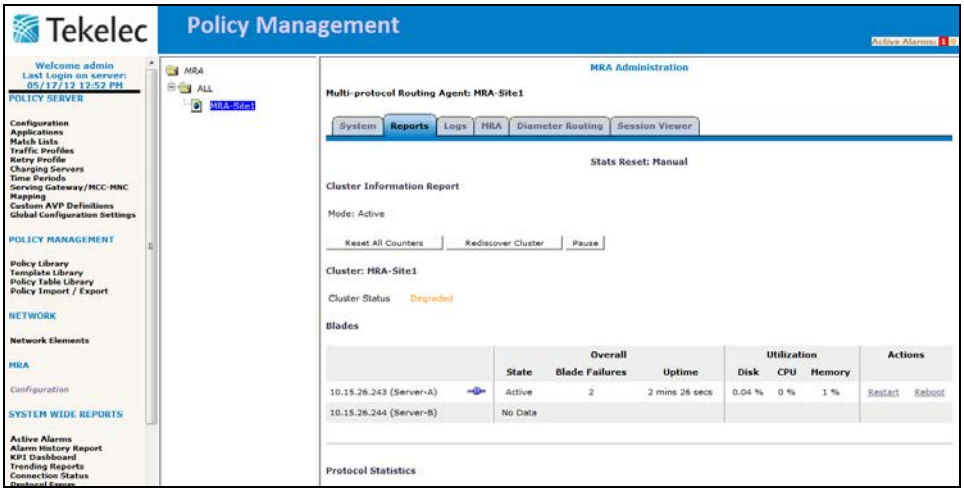
5. Click **Save**. The new device is listed within the Policy Server page. For example:



6. Select the device, located under Policy Server or MA/BoD Server to view the administrative tabs. For example:



7. Click **Reports** and verify that all blades for the cluster are listed. For example:



8. Repeat this procedure for the remaining MPE, MA or BoD clusters.

2.4 Configuring CMP Geo-Redundancy

2.4.1 Procedure 9: Configuring CMP Georedundancy

This chapter describes how to configure and maintain redundancy between two CMP Manager systems that are located locally and in geographically different locations. The Georedundancy feature allows you to replicate the databases between two CMP systems, and manage the active relationship between them.

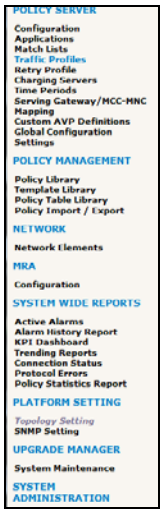
MPE and MA/BoD Clusters located at the Georedundant site are added to the (Primary) CMP GUI following the same procedure used in this guide to add MPE/MA/BoD Clusters located at the primary site.

NOTE: The following procedure assumes that you performed the initial procedures on both CMPs at the second site.

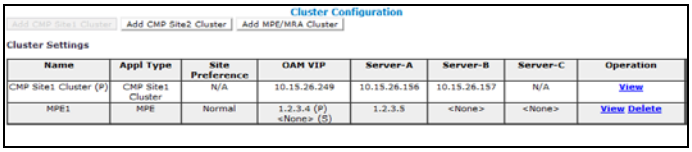
2.4.1.1 Procedure 38: Configuring CMP Georedundancy

To configure CMP Georedundancy, complete the following:

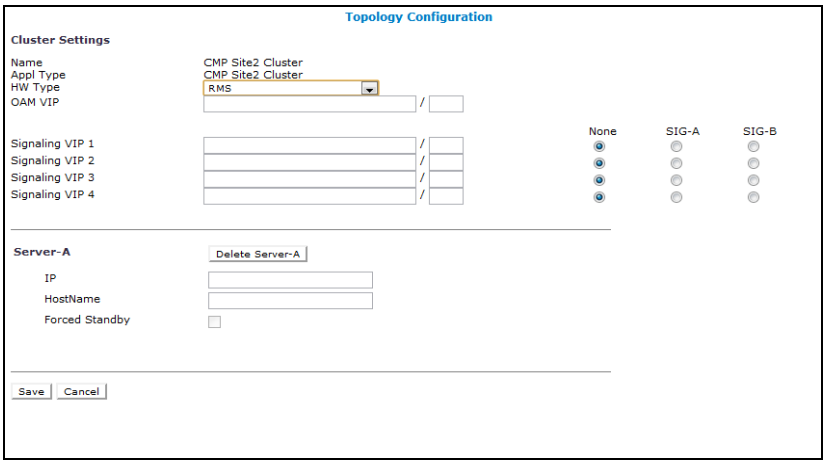
1. Log in to the CMP and click **Topology Setting**, located under the **Platform Setting** menu item.



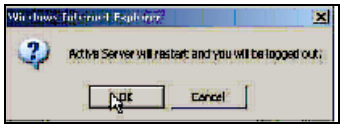
2. Click **Add CMP Site2 Cluster**.



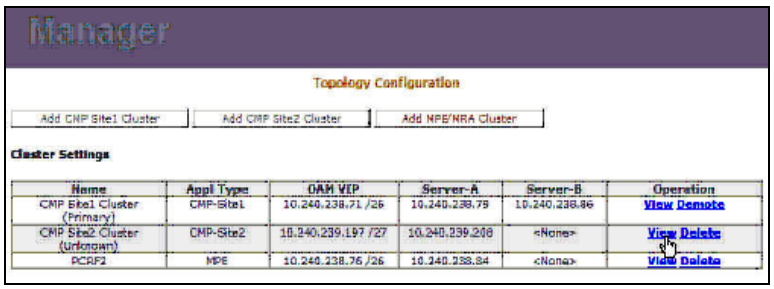
3. Complete the form. For example:
   - Select the appropriate HW Type (C-Class or RMS).
   - Enter the correct Network VLAN IDs (C-Class only).
   - Enter the OAM VIP address for the second CMP cluster.
   - Enter the Server-A IP address (must match value entered during Initial configuration).
   - Enter the Server-A Hostname (must match value entered during Initial configuration).
   - Click **Save** when finished.



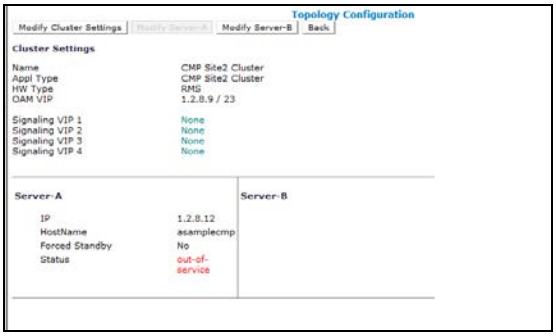
4. Confirm the popup to acknowledge the server restart.



5. A screen similar to the following displaying the Topology Configuration is displayed. For example:

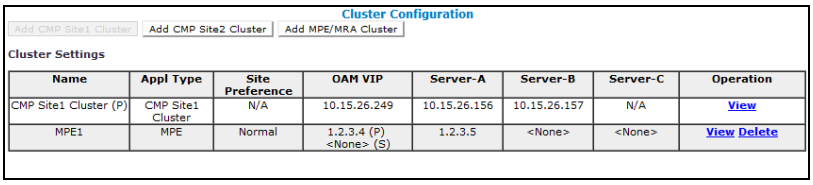


6. Click **View**, located next to the new CMP Site2 Cluster. For example:

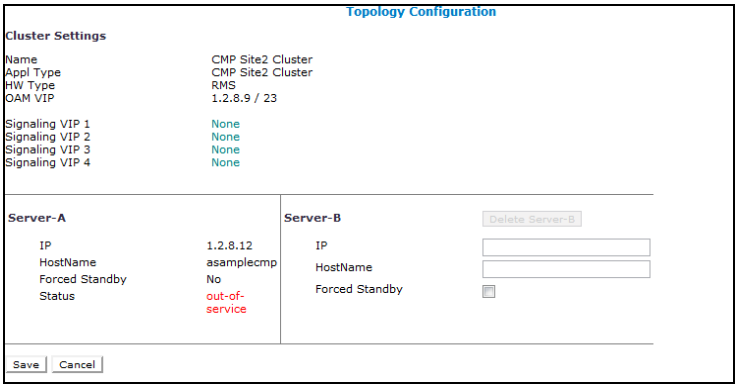


NOTE: The Server-A Status may be one of Active, Standby or Forced-Standby

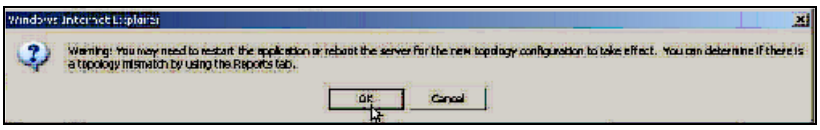
7. Select Modify Server-B.
8. Complete the form and click **Save**. For example:
   - Enter the Server-B IP address (must match value entered during Initial configuration).
   - Enter the Server-B Hostname (must match value entered during Initial configuration).
9. Confirm the popup to acknowledge the server restart.
10. You are returned to the list of Cluster Settings. Verify that both servers of the second CMP cluster are displayed. For example:



11. Click **View** beside the new CMP Site2 Cluster.
12. Select **Modify Server**.
13. Uncheck the **Forced Standby** checkbox, and then click **Save**.



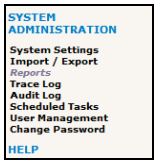
14. You are prompted to acknowledge the information. Click **OK**.



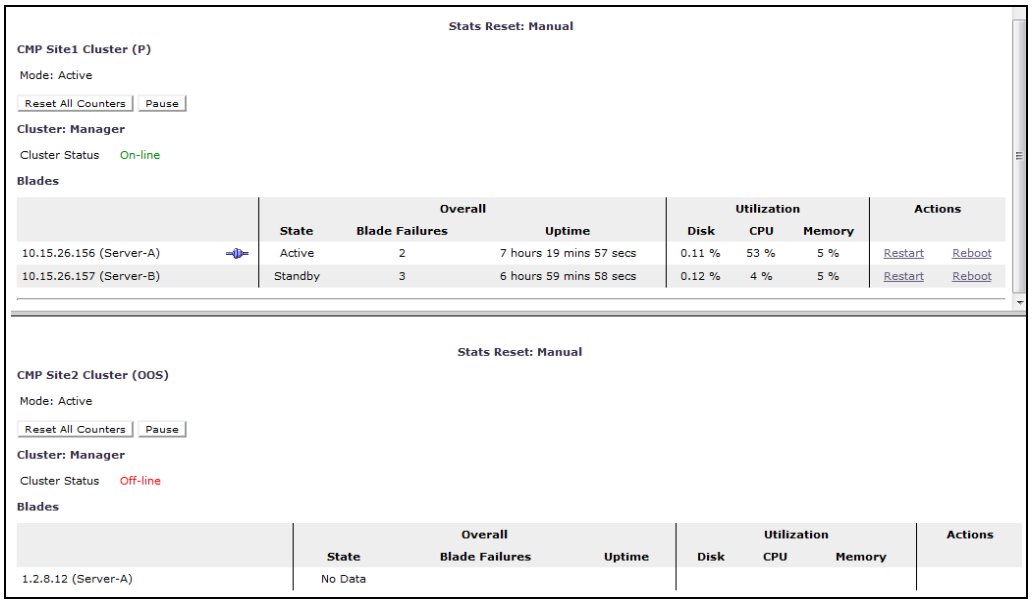
15. Log in to one or both of the new CMP clusters as root, and at the root prompt enter the `ha.states` command and monitor the output for one of one blade to report Active, the other blade to report Stby.:

```
          resourceId   role         node      subResources      lastUpdate
       DbReplication   Stby    A1126.004                 0 0511:161808.551
       DbReplication Active    A1126.151                 0 0511:161507.429
                 VIP   Stby    A1126.004                 0 0511:161808.563
                 VIP Active    A1126.151                 0 0511:161507.453
                  QP   Stby    A1126.004                 0 0511:161837.544
                  QP Active    A1126.151                 0 0511:161551.230
  DbReplication_old    OOS    A1126.004                 0 0511:161808.138
  DbReplication_old    OOS    A1126.151                 0 0511:161851.073
```

16. Once the servers have their respective roles, return to the GUI for the primary and secondary servers and select **Reports** item from the nave pane.



17. Verify that the Topology is reported as `OK`. If a mismatch is reported, click **Restart** next to the mismatched server.

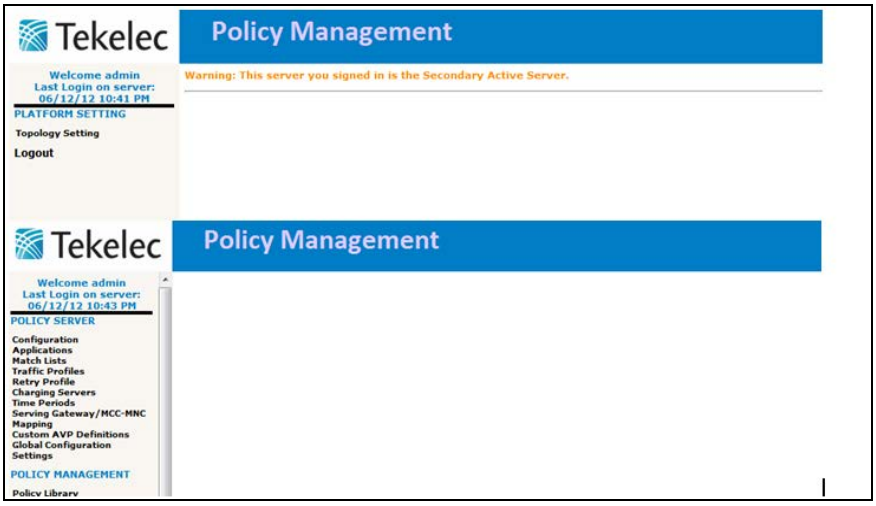


NOTE: The Server State will be one of Active, Standby, Forced-Standby or No Data.

18. Log in to the GUI of both CMP clusters, using the OAM VIP addresses, and complete the following:
    - Verify that the Secondary CMP GUI displays the following warning:

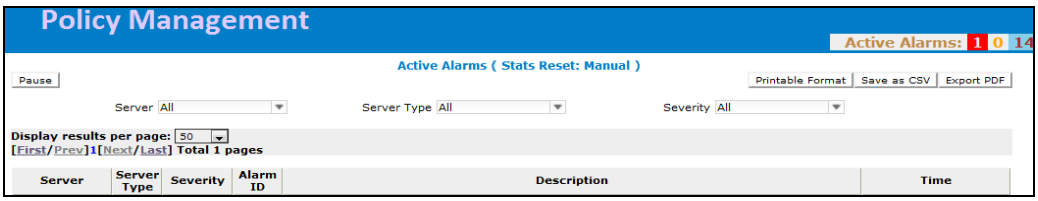
```
Warning: This server you signed in is the Secondary Active Server"
```

- Verify that the Primary CMP Cluster does not display the previous message.



19. Select the **Active Alarms** item.

20. Verify that no alarms are reporting Georedundancy or new CMP server issues.



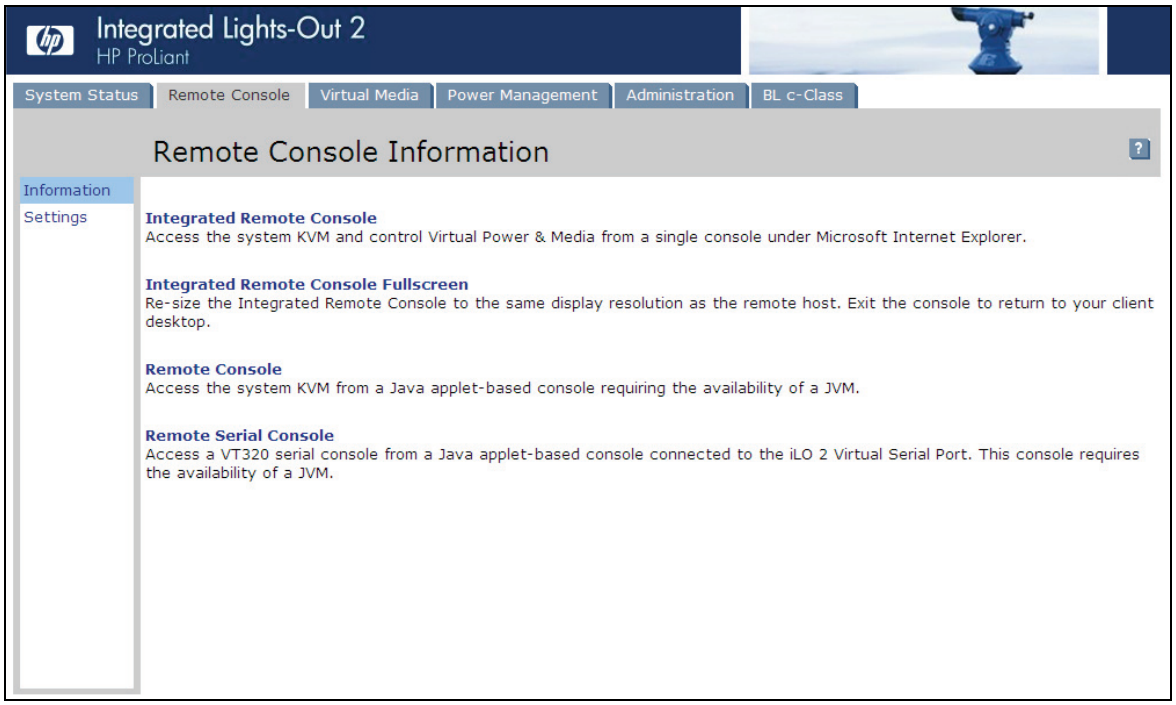
2.5 Accessing the Server Console

2.5.1 Visiting HP Console iLO

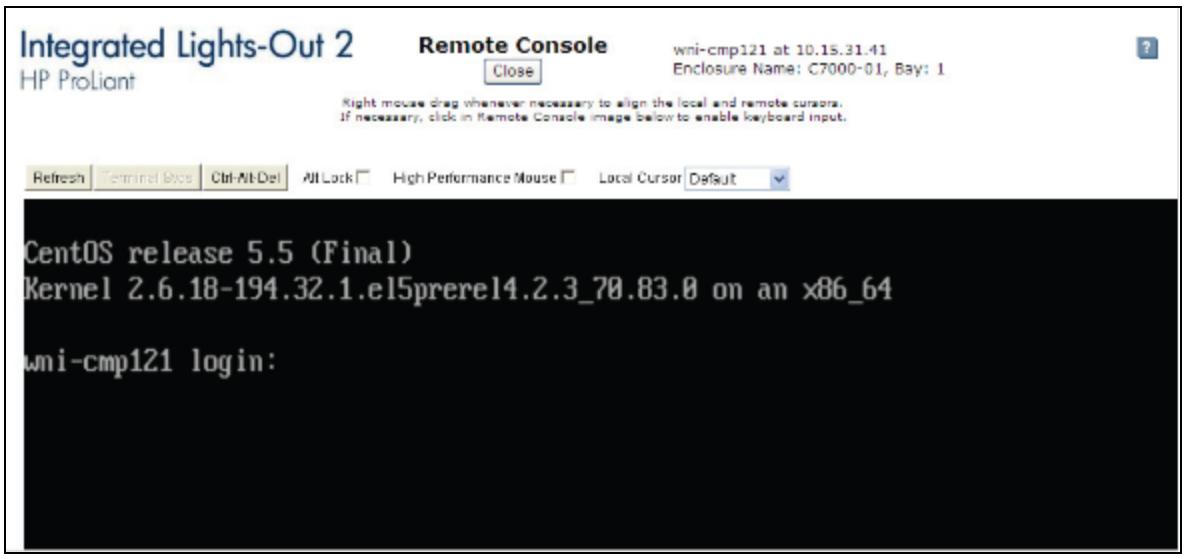
1. Enter the iLo IP address into a web browser. Note that you will be prompted with a warning for security certificates; this occurs because the certificate is self-signed.

2. Log in as Administrator.

3. Click **Remote Console** tab and then the Remote Console link.



4. Server Console displays the following:



2.6 Configuring SNMP

2.6.1 Policy Management Application

NOTE: The following comes from 910-6288-001

SNMP configuration architecture is based on using traps to notify a network management system of events and alarms that are generated by the MPE, MA and BoD software.

Alarms and telemetry data are continuously collected from the entire Policy Management Application Network and stored on the CMP servers. Alarms will then cause a trap to be sent as a notification of an event.

Because the underlying platform can deliver the alarms from the MPE/MA/BoD to the CMP, SNMP can be configured in either of 2 ways:

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

NOTE on SNMP Versions

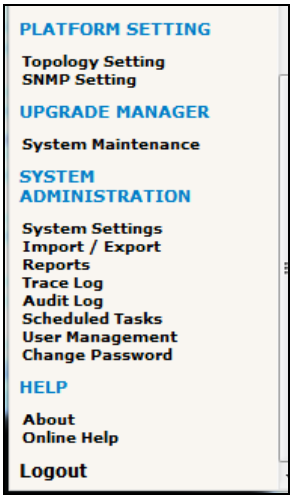
- SNMP version 2c (SNMPv2c) and SNMP version 3 (SNMPv3) are supported.
- SNMP version 1 (SNMPv1) is not supported. On the SNMP Setting Edit screen
- When you configure SNMPv2c, you must use a community that is not "public" or "private".
- When you configure SNMPv3, you must enter an Engine ID, and a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

The CMP system provides a screen for configuring SNMP settings for the CMP system and all MPE, MA and BoD servers in the topology network. For more details on using the CMP system, refer to the *CMP Wireless User's Guide*.

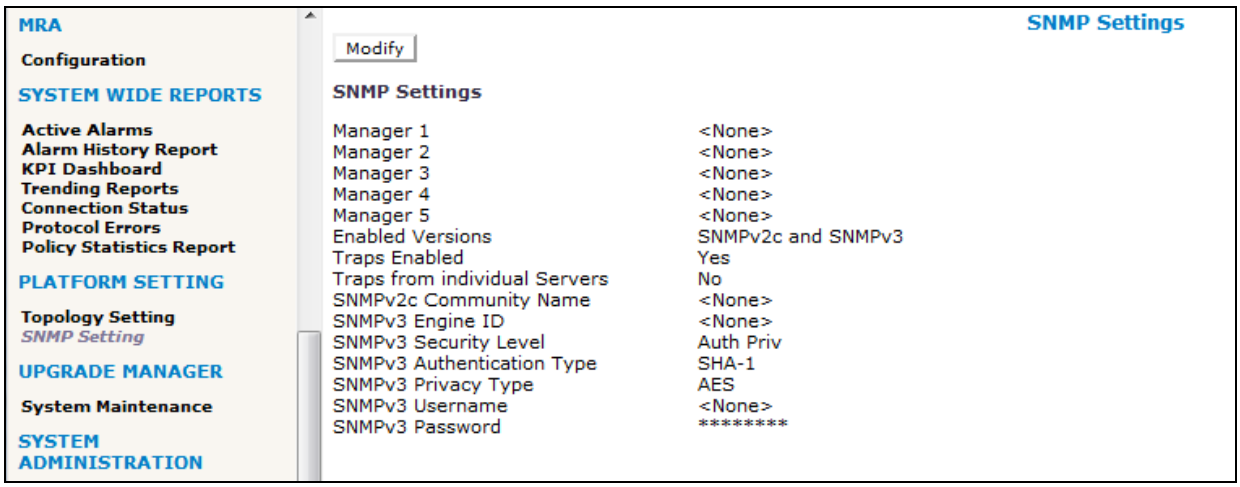
NOTE: SNMP settings configuration must be done on a server that is the Active Blade in the Primary Cluster. A banner warning appears if the login is not on the primary/active CMP. SNMP cannot be configured from servers other than the active/primary CMP.

To configure SNMP settings:

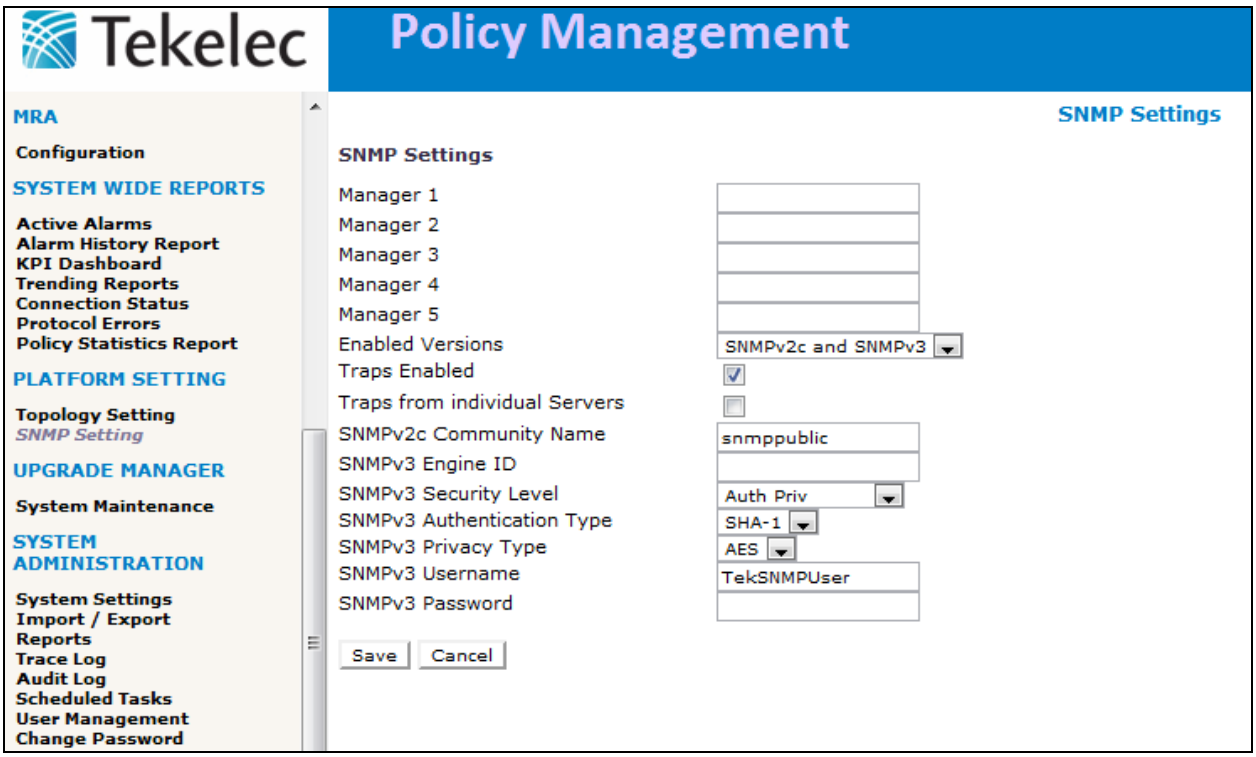
1. Log into the CMP system from its server address as the Administration user. The CMP **Navigation Pane** is displayed.



2. Click **SNMP Setting** link under **Platform Setting**. The SNMP Settings Attributes are displayed.



3. Click **Modify** Button



4. Edit the SNMP Settings attributes that need to be entered or changed. The settings are described below.

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 is the 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 is the 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.

Field Name	Description
SNMPv3 Security Level	SNMPv3 Authentication and Privacy options. • **No Auth No Priv**—Authenticate using the Username. No Privacy. • **Auth No Priv**—Authentication using MD5 or SHA1 protocol. • **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: • **SHA-1**—Use Secure Hash Algorithm authentication. • **MD5**—Use Message Digest authentication. The default value is **SHA-1**.
SNMPv3 Privacy Type	Privacy Protocol for SNMPv3. Options are: • **AES**—Use Advanced Encryption Standard privacy. • **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.”

5. Click **Save** to save the changes.