Policy Management

Platform Configuration User's Guide

Release 15.0

F83835-04

February 2026

Policy Management Platform Configuration User's Guide, Release 15.0

F83835-04

Contents

About This Guide

1 Introduction

2 Performing Initial Server Configuration

3 Managing Certificates

4 Synchronizing Files

5 Editing Network Interface Ethernet Parameters

6 Backing Up and Restoring the System and Server

About This Guide

This chapter describes the organization of the document and provides other information that could be useful to the reader.

How This Guide is Organized

The information in this guide is presented in the following order:

- About This Guide contains general information about this guide, the organization of this guide, and how to get technical assistance.
- Introduction describes how to access the platcfg utility, how to use the utility interface in a Policy Management environment, and troubleshooting.
- Performing Initial Server Configuration describes how to access the platcfg utility and configure your application's initial configuration, and then how to verify the configuration.
- Managing Certificates describes how to access the platcfg utility to manage SSL security certificates, which allow two systems to interact with a high level of security.
- Synchronizing Files describes how and when to synchronize files in clusters.
- Editing Network Interface Ethernet Parameters describes how to manually configure Ethtool options.
- Backing Up and Restoring the System and Server describes how to perform system and server backups and restores.
- Glossary

Intended Audience

This guide is intended for service personnel who are responsible for operating Policy Management systems.

Related Publications

For information about additional publications related to this document, refer to the Oracle Help Center site. See Locate Product Documentation on the Oracle Help Center Site for more information on related product publications.

Locate Product Documentation on the Oracle Help Center Site

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

1. Access the Oracle Help Center site at http://docs.oracle.com.

2. Click `Industries`.
3. Under the Oracle Communications subheading, click the `Oracle Communications documentation` link.

   The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
4. Click on your Product and then the Release Number.

   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the `PDF` link, select `Save target as` (or similar command based on your browser), and save to a local folder.

Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training:

http://education.oracle.com/communication

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site:

www.oracle.com/education/contacts

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 can assist you with My Oracle Support registration.

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

- For Technical issues such as creating a new Service Request (SR), select **1**.
- For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.
- For Hardware, Networking and Solaris Operating System Support, select **3**.

You are 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.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support main number at 1-800-223-1711 (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system’s ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

List of Figures

List of Tables

1 Introduction

This chapter describes how to use the **Oracle Communications Policy Management Platform Configuration** utility (**platcfg**) to configure **Oracle Communications Policy Management** (**Policy Management**) on Policy Management Configuration Management Platform (**CMP**) servers and Policy Management servers.

The reference to Policy Management servers will be used throughout this document to mean the **Policy Management Multimedia Policy Engine** (**MPE**) device, **Policy Management Multi-Protocol Routing Agent** (**MRA**) device, **Policy Management Bandwidth on Demand** (**BoD**) server, **Policy Management Message Distribution Function** (**MDF**) server, and **Policy Management Management Agent** (**MA**) server, collectively. Each server is described individually in detail in their respective manuals.

The pages, tabs, fields, menu items, and functions that you see in the utility depend on your configuration, application, or mode.

1.1 platcfg Overview

The `platcfg` utility is a Command Line Interface (CLI) tool that simplifies the execution of tasks that cannot be included in the application software. These tasks include those that affect operating system operations or platform services that are invisible to an application or that are not accessible from the application management controls.

The `platcfg` utility simplifies task execution and reduces the chance of user errors through the use of wizard-like menu options and forms.

You access `platcfg` menus by logging in from a console or logging in remotely. The `platcfg` security actions are centralized at the active CMP server, with all functions propagated automatically to all connected servers.

1.2 Accessing platcfg

- Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
  - To access the platcfg utility from the system console:
    1. Log in as **root**.
    2. Enter `su - platcfg`.
  - To access the platcfg utility through an SSH remote session:
    1. Log in as **admusr**.
    2. Enter `sudo su - platcfg`.

> **Note**
>
> The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

1.3 Using Keyboard Actions in the platcfg Utility

Use the following keyboard actions to move and enter information within the platcfg utility:

- Up and down arrows—Moves the action up or down.
- Left and right arrows—Moves the action sideways.
- Enter key—Enters the selected item and moves to the next menu or feature screen.
- Tab Key—Moves from one option item to another option item.

1.4 Using the Save Platform Debug Logs Menu to Troubleshoot

Use **Save Platform Debug Logs** to help troubleshoot If a system failure occurs.

> **Note**
>
> The CMP Save Log function includes CMP Audit logs for the previous two months.

1.4.1 Saving Platform Debug Logs

The **Save Platform Debug Logs** menu is used to help you troubleshoot a system failure. You can adjust two settings to limit the size of the saved log files.

Information saved in the logs includes the current state of all logs, all the configuration files, all the system procedure entries, and several miscellaneous files. Output from this process is a single tar/gzip file.

To use the menu:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

   > **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.

   > ⓘ **Note**
   >
   > The NetBackup Configuration menu selection only opens if the server is a CMP server.

3. Select **Save Platform Debug Logs** from the Policy Configuration Menu screen and press **Enter**.

4. In the screen that opens, enter values for the following fields:

   - **Record limit for qptrace**
     This field specifies the maximum number of qptrace messages to save. Do not change this setting when generating a save log to debug a problem; only reduce the default number messages when instructed to do so by Customer Support.
   - **Record limit for AppEventLog**
     This field specifies the maximum number of AppEventLog records to save. Do not change this setting when generating a save log to debug a problem; only reduce the default number records when instructed to do so by Customer Support.
   - **Remember count limit settings**
     This field specifies whether or not to retain limit setting from previous log.
   - **Include trace/subact/sync log**
     This field indicates whether to include the extra trace/subact/sync debug records.
   - **Savelogs Path**
     This field lists the path where savelogs file will be saved.

   > ⓘ **Note**
   >
   > **Include trace/subact/sync log** should be left set to **No** unless directed to be set to **Yes** by My Oracle Support.

5. Select **OK** and press **Enter** to save variable changes and generate the tar/gzip file.

   The file is generated and saved in the location you specified.

2

Performing Initial Server Configuration

This chapter describes the initial platcfg setup steps.

2.1 Setting the Policy Management Mode

To select the Policy Management mode:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

> **Note**
>
> The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.

   The Policy Configuration Menu opens.
3. Select **Set Policy Mode** from the Policy Configuration Menu screen and press **Enter**.
4. Select the "Wireless" mode for your system, then select **OK** and press **Enter**.
5. If the **Select Network Layout** screen opens, you will need to select the appropriate Network layout profile. See Table 2-1 for information about the network layout choices.

Table 2-1 Server Network Layouts

Network Layout Profile	Network Layout Detail	Description

common	PMAC=bond0
	OAM=bond0.<VLAN>
	SIGA=bond0.<VLAN>
	SIGB=bond0.<VLAN>
		This is the default layout assigned after the policy product is installed.

segregated	PMAC=bond0
	OAM=bond0.<VLAN>
	SIGA=bond1.<VLAN>
	SIGB=bond1.<VLAN>
		This layout is used by MPE and MRA devices for traffic segregation.
		If the server is upgraded from an earlier release with traffic segregation enabled, this layout is automatically selected.

Table 2-1 (Cont.) Server Network Layouts

Network Layout Profile	Network Layout Detail	Description

bkup	PMAC=bond0
	OAM=bond0.<VLAN>
	SIGA=bond0.<VLAN>
	SIGB=bond0.<VLAN>
	BKUP=bond2
		This layout is used by CMP server where an extra BKUP interface is used.
		If the server is a CMP upgraded from an earlier release with segregation turned off, this layout is automatically selected.

segregated_with_bkup	PMAC=bond0
	OAM=bond0.<VLAN>
	SIGA=bond1.<VLAN>
	SIGB=bond1.<VLAN>
	BKUP=bond2
		This layout is used by CMP server where an extra BKUP interface is used.
		If the server is a CMP upgraded from an earlier release with segregation turned on, this layout is automatically selected

common_with_sigc	OAM=bond0.<VLAN>
	PMAC=bond0
	SIGA=bond0.<VLAN>
	SIGB=bond0.<VLAN>
	SIGC=bond0.<VLAN>
		This layout is used by a customer using the Wireless mode to provide separate external SCTP multi-homing and internal traffic by using an additional signaling interface.

cloudinit	OAM=eth0
	SIGA=eth1
	SIGB=eth2
	SIGC=eth3
	REP=eth4
	BKUP=eth5
		This layout is recommended for VM deployments. The number of interfaces available would depend on the available NICs and VLANs.

2.2 Setting Up the Initial Configuration

This section describes how to perform the initial configuration on the CMP servers in your system.

To perform the initial configuration of the system:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

> **Note**
>
> The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.
3. Select **Perform Initial Configuration** from the Policy Configuration Menu screen and press **Enter**.

   The **Initial Configuration** screen opens.
4. Enter values for the configuration fields in the Initial Configuration screen, which will include some of the following:
   - **HostName**—The unique name of the host for the device being configured.
   - **OAM Real IP Address**—The IP address that is permanently assigned to this device.
   - **OAM Real IPv4 Address**—The IPv4 address that is permanently assigned to this device.
   - **OAM Default Route**—The default route of the OAM network.
   - **OAM IPv4 Default Route**—The IPv4 default route of the OAM network.
   - **OAM Real IPv6 Address**—The IPv6 address that is permanently assigned to this device.
   - **OAM IPv6 Default Route**—The IPv6 default route of the OAM network.
   - **NTP Server** (required)—A reachable **NTP** server on the OAM network.
   - **DNS Server A** (optional)—A reachable **DNS** server on the OAM network.
   - **DNS Server B** (optional)—A second reachable DNS server on the OAM network.
   - **DNS Search**—A directive to a DNS resolver (client) to append the specified domain name (suffix) before sending out a DNS query.
   - **OAM Device**—The bond interface of the OAM device. Note that the default value should be used, as changing this value is not supported.

   > **Note**
   >
   > **DNS Server** and **DNS Search** are optional fields, but it is recommended to enter values for them.

   > **Note**
   >
   > Every network service and IP flow that is supported by IPv4 is also supported by IPv6. Either interface or a combination of the two can be configured.

5. Select **OK** and the configuration is saved and applied .

   The screen pauses for approximately one minute. This is normal behavior.

You have successfully set up the initial configuration.
If SIG-C is selected, proceed to the Add Route screen.

2.2.1 Changing an NTP Server on an MPE/MRA Device

To change an NTP server on an MPE/MRA device:

1. From the CMP server:

   a. Set the MPE/MRA device to **forced standby**.
   b. **SSH** to the **standby server**.
   c. Become the **root** user by using `su` or `sudo`.
   d. Enter `su - platcfg`.

2. In platcfg:
   a. Select **Policy Configuration**.
   b. Select **Routing Configuration**.
   c. Select **Display Routes**.
   d. Write down the routes.
3. In platcfg:
   a. Select **Policy Configuration**.
   b. Select **Initial Configuration**.
   c. Modify the **NTP Server Value** to the correct **value**.
   d. Click **OK**.
4. Click **Save**.
5. At the menu prompt:
   a. Select **Routing Config**.
   b. Select **Display Routes**.

   > **Note**
   >
   > Make sure the route is the one you wrote down in 2d. If it is not the same, you will need to use **Add Route** and **Delete Route** to make the route the same as the one you wrote down in 2d.

6. To generate the NTP health report, open the platcfg utility, got to **Policy Configuration** and select **Verify Initial Configuration**.
7. In the command line interface, use `# chronyc ntpdata` to ensure that the server is reaching the new NTP server.

   For example:

```
[root@CMP5207 camiant]# chronyc ntpdata

Remote address : 10.250.32.10 (0AFA200A)
Remote port : 123
Local address : 192.168.5.207 (C0A805CF)
Leap status : Normal
Version : 4
Mode : Server
Stratum : 3
Poll interval : 10 (1024 seconds)
Precision : -24 (0.000000060 seconds)
Root delay : 0.074646 seconds
Root dispersion : 0.095230 seconds
Reference ID : 0A4B0007 ()
Reference time : Fri Nov 17 09:19:28 2023
```

```
Offset : -0.000163211 seconds
Peer delay : 0.001340960 seconds
Peer dispersion : 0.000000096 seconds
Response time : 0.000068799 seconds
Jitter asymmetry: +0.00
NTP tests : 111 111 1111
Interleaved : No
Authenticated : No
TX timestamping : Kernel
RX timestamping : Kernel
Total TX : 45
Total RX : 45
Total valid RX : 45
```

> **Note**
>
> If the offset is very large, you might have to execute the procedure Process for Very Large NTP Offset to manually adjust it. If not, continue with this procedure.

8. Check that >`prod.state` is:

   ```
   ...prod.state (RUNID=00)...
           ...getting current state...
   Current state: A (product under procmgr in a START state)
   ```

   Where:

   Current state: A product under `procmgr` in a START state. If the current state is not Active, stop executing this procedure and call Oracle Support.

9. In the current active server, enter `# netstat -nap | grep 3868 | wc` to obtain a count of diameter connections.
10. In the CMP server, select the cluster and use **switch force standby** to failover the MPE/MRA device.
11. In the new active MPE/MRA device:
    a. Use `# netstat -nap | grep 3868 | wc` to determine if the diameter connections have been re-established.

    > **Note**
    >
    > If not, use the CMP interface to **switch force standby** again and call Oracle Support.

    b. If Diameter link has been re-established and the modified server with the new NTP is working properly, log into Linux as **root** on the current standby server.

    c. Enter `su - platcfg`.
12. Select **Policy Configuration**, then click **Initial Configuration**:
    a. Modify the NTP server value and click **OK**.

    b. Click **Save**.
13. When the platcfg menu returns, select **Routing Config**.

14. Select **Display Routes**.

   > **Note**
   >
   > Make sure it is the same with the routes written down in step 2d. If it is not the same, you need to use **Add Route** and **Delete Route** to make it the same.

15. Exit platcfg and wait two minutes before proceeding to next step.
16. Use the command: `#chronyc ntpdata` to ensure that the server is reaching the new NTP server.

   > **Note**
   >
   > It the offset is very large, you also need to execute extra steps. See Process for Very Large NTP Offset for more information.

17. Execute `prod.state` to ensure that the **Current state** is **Active**.

   > **Note**
   >
   > If the current state is not **Active**, stop executing this procedure and call Oracle Support.

   > **Note**
   >
   > If you cancel the forced standby for the server in CMP interface, there might be some alarms raised, but they should be automatically cleared.

2.2.2 Process for Very Large NTP Offset

If the NTP offset is very large:

1. To verify the NTP server is configured correctly and works on the MPE/MRA device, use `chronyc tracking`.
2. If the MPE device has the active role in the cluster, please run a switch over of this cluster to make this device use standby role.
3. Perform these commands in order:
   a. `service qp_procmgr stop`
   b. `service comcol stop`
   c. `systemctl stop chronyd`
   d. reset chronyd using this command : `chronyd -q 'server <ntp server ip> iburst'`
   e. Wait one minute for the sync between device and the NTP server to complete.
   f. `systemctl start chronyd`
   g. `date`

h. `hwclock`

i. `chronyc ntpdata`

j. Check sync is done and the time is accurate for the server time and BIOS clock.

k. `service comcol start`

l. `service qp_procmgr start`

4. Monitor the system for several minutes and then verify the system status is functioning normally, and that all the alarms are cleared.

2.3 Verifying the Initial Configuration

This section describes how to verity the initial configuration on the CMP servers in your system after you have completed the initial configuration.

To verify the initial configuration of the system:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

> **Note**
>
> The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Verify Initial Configuration** from the Policy Configuration Menu screen and press **Enter**.

   A screen opens to display your initial configuration settings.
3. Select **Exit** and press **Enter**.

2.4 Verifying the Server Status

After you have made and verified your initial configuration settings, to verify the server status:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.

b. Enter `sudo su - platcfg`.

> **Note**
>
> The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Verify Server Status** from the Policy Configuration Menu menu and press **Enter**.

   After a server is fully configured, it will show the **Server Role** as **Active** or **Standby** (or **Spare** in the **Index Table of Contents** screen, if this is a Policy Management server configured for georedundancy). **Unknown** is a valid state during initial configuration because the cluster has not been formed. Policy Process Management Status should always be **Running**.

2.5 Cleaning Up the Cluster Configuration

After removing a server from a cluster and before adding the server to another cluster, clean up the cluster:

1. If at the **admusr** prompt, enter:

   ```
   sudo su - platcfg
   ```

   > **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Cluster Configuration Removal** from the Policy Configuration Menu screen and press **Enter**.
3. Select **Cluster Information Cleanup** from the Cleanup Configuration Menu screen and press **Enter**.
4. Select **Yes** or **No** from the Cleaning up cluster information screen and press **Enter**.

The cluster configuration is cleaned up.

2.6 Managing Routes on Your Server

This section describes how to manage routes on your server:

- Configuring a Route
- Deleting a Route
- Displaying Configured Routes
- Exporting a Route
- Importing a Route

2.6.1 Configuring a Route

To configure a route:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

   > **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.
3. Select **Routing Config** from the Policy Configuration Menu screen and press **Enter**.
4. Select **Add Route** from the Route Configuration Menu screen and press **Enter**.

   The Add Route screen opens.
5. Edit the information displayed on the Add Route screen:
   a. Select the **IP Type**.

      This field setting specifies whether this will be an **IPv4** or **IPv6** route.
   b. Select the **Route Type**.

      This field setting specifies whether this route will be for a specific destination (**host**), a specific network segment (**net**), or a **default** route.

      > **Note**
      >
      > This option is provided to allow the default route to be moved to a different interface; only one default route per address family (IPv4 or IPv6) should exist on a system at one time.

   c. Select the **Network**.

      This field setting specifies whether this route will be created on the BKUP, OAM, REP (replication), SIGA, SIGB, SIGC interface.

      > **Note**
      >
      > When creating routes for an interface that does not have an active IP address, such as the SIG-A interface on the standby server you receive a warning stating that the route cannot be applied at this time but it will be saved. These routes show as **INACT** on the display routes section.

   d. Select the **Preferred Source Addr**.

      This field setting specifies the source address selection for outgoing traffic. Options include:

- **NONE**, which refers to no VIP or STATIC IP assignment.
- **VIP,** which is the virtual IP configured in the CMP GUI.
- **STATIC**, which includes:
  - OAM IP address configured in Policy Initial Configuration
  - Static IP configured in the CMP **Topology** action.
  - An IP address assigned by netAdm or ifconfig or `ip addr add`
  - An IP address added by manual editing of the ifcfg file

See table for details about the behavior of **Preferred Source Addr**.

e. Enter the **Destination** IP address.

f. Enter the **Gateway Address**.

Table 2-2 Detailed Behavior of Preferred Source Addr

Preference/status	Prefer None	Prefer VIP	Prefer STATIC
No VIP, no static IP	Not applied. On Active server, alarm 70015 is raised. On Standby or Spare server, this error is ignored.	Not applied. If VIP is not configured, Alarm 70016 is raised. On Active server, alarm 70015 is also raised.	Not applied. Alarm 70017 is raised.
No VIP, one or more static IP	Applied without "src" option specified to kernel. Kernel will use the first static IP as source address automatically.	Not applied. If VIP is not configured, Alarm 70016 is raised. On Active server, alarm 70015 is also raised.	Applied to the first static IP
One VIP, no static IP	Applied without "src" option specified to kernel. Kernel will use the VIP as source address automatically.	Applied to VIP	Not applied. Alarm 70017 is raised.
One VIP, one or more static IP	Applied without "src" option specified to kernel. Kernel will use the VIP as source address automatically.	Applied to VIP	Applied to first static IP
Two or more VIPs, no static IP	Applied without "src" option specified to kernel. Kernel will use the first VIP as source address automatically.	Applied to first VIP	Not applied. Alarm 70017 is raised.
Two or more VIPs, one or more static IP	Applied without "src" option specified to kernel. Kernel will use the first static IP as source address automatically.	Applied to first VIP	Applied to first static IP

6. When finished editing, select **OK** and press **Enter**.
7. Press **Enter** again to save changes.

2.6.2 Deleting a Route

To delete a route:

1. If at the **admusr** prompt, enter:

   ```
   sudo su - platcfg
   ```

   > **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.
3. Select **Routing Config** from the Policy Configuration Menu screen and press **Enter**.
4. Select **Delete Route** from the Route Configuration Menu screen and press **Enter**.

   The Main Routing Table screen appears.

5. Select the route to delete by pressing the space bar, select **OK** and press **Enter**.

   Use the **Top**, **Bottom**, **Prev,** and **Next** buttons to scroll through the list.

   > **Note**
   >
   > More than one route can be deleted at a time.

   > **Note**
   >
   > The route is deleted without confirmation.

2.6.3 Displaying Configured Routes

To display configured routes:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

> **Note**
>
> The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.
3. Select **Routing Config** from the Policy Configuration Menu screen and press **Enter**.
4. Select **Display Routes** from the Route Configuration Menu screen and press **Enter**.

   The Main Routing Table screen opens to display the configured routes.

The status of each route displays as either **ACT** (active and currently running) or **INACT** (save in the configuration, but cannot be activated at this time). An inactive route may mean that an interface for which the route is configured does not currently have an IP address; for example, a standby server on an interface that only has a **VIP**. An inactive route may also mean that a route has been configured incorrectly, with the gateway IP address not on the same subnet as the interface IP address.

2.6.4 Exporting a Route

Routes can be exported from one server and imported into another or exported and modified with a text editor before importing.

To export all existing routes in a route list:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

> **Note**
>
> The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.
3. Select **Routing Config** from the Policy Configuration Menu screen and press **Enter**.
4. Select **Export Route** from the Route Configuration Menu screen and press **Enter**.

   The Export Routes To File screen appears.

5. Specify the location and filename of the routes in a route list that are to be exported, then select **OK** and press **Enter**.

   Routes in a route list are exported to the specified directory and filename.

2.6.5 Importing a Route

> **Note**
>
> Exported routes can be modified with a text editor before importing.

To import all existing routes within a route list into the routing configuration:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

   > **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.
3. Select **Routing Config** from the Policy Configuration Menu screen and press **Enter**.
4. Select **Import Routes** from the Routing Configuration Menu and screen press **Enter**.

   The Import Routes From File page appears.
5. Specify the location and filename of the routes in a route list that are to be imported, select **OK** and press **Enter**.

   Routes in a route list are imported into the routing configuration from the specified directory and filename.

2.7 Restarting the Application

> **Note**
>
> Restarting the application will interrupt service on a server if it is in an active role. However, restarting the application does not log out users.

To restart the application:

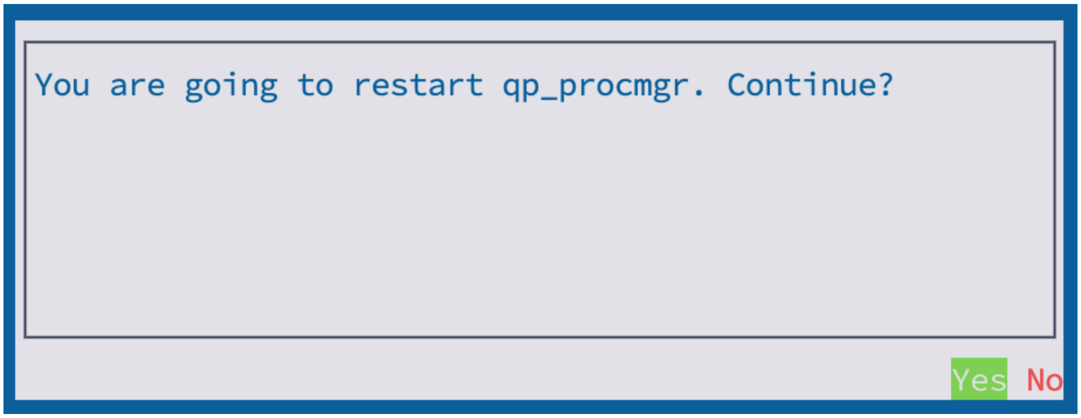
1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:

   a. Log in as **root**.
   b. Enter `su - platcfg`.
- To access the platcfg utility through an SSH remote session:
   a. Log in as **admusr**.
   b. Enter `sudo su - platcfg`.

> **Note**
>
> The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu screen and press **Enter**
3. Select **Restart Application** from the Policy Configuration Menu screen and press **Enter**.
4. Select **Yes** and press **Enter** to restart `qp_procmgr`.

Figure 2-1 Restart qp_procmgr



```
You are going to restart qp_procmgr. Continue?
```

> **Note**
>
> Following this procedure restarts `qp_procmgr`, which controls all Policy Management specific processes, and the entire application is restarted. It does not restart High Availability (**HA**) or database software, although the failure of the application on the active server will trigger an HA failure.

2.8 Configuring Firewall Settings

> **Note**
>
> During the editing of firewall configuration settings, if an attempt is made to leave the Firewall Configuration Menu screen with unsaved changes, you are presented with the options to save changes and exit, exit without saving changes, or to return to the Firewall Configuration Menu screen to continue.

> **Note**
>
> When all firewall configuration setting changes are completed, be sure to use **Save and Apply Configuration** from the Firewall Configuration Menu screen to commit the changes made to the firewall configuration files and restart the firewall.

To configure firewall settings:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

   > **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.
3. Select **Firewall** from the Policy Configuration Menu screen, and press **Enter**.
4. Select **Enable/Disable Firewall** from the Firewall Configuration Menu screen and press **Enter**.
5. Select **Edit** from the Firewall Status screen and press **Enter**.
6. To enable the IPv4 or IPv6 firewall , select **Enable iptables** or **Enable ip6tables** from the list of interfaces on the Enable/Disable Firewall Features Menu screen and press **Enter**.
7. When prompted to continue, select **Yes** from the Enable iptables? screen or other appropriate dialog screen that opens and press **Enter**.
8. (Optional) To open additional ports in the firewall, select **Enable Custom Rules** from the Enable/Disable Firewall Features Menu screen.
9. Select **Yes** from the Enable custom rules? screen to confirm that custom rules are to be enabled or select **No** to cancel.
10. To set custom rules to be used instead of default firewall rules, select **Enable custom prefer** from the Enable/Disable Firewall Features Menu screen.

    If a custom rule conflicts with a default rule, the default rule is used, but the default rule can be overridden if the custom prefer option is enabled. Rules conflict if they have matching protocols (TCP, UDP) and ports (80, 443, etc.).
11. Select **Yes** from the Enable custom prefer feature? screen to confirm custom rules are to be preferred over default rules or select **No** to cancel.
12. To add, edit, or delete custom firewall rules, select **Customize Firewall** from the Firewall Configuration Menu screen and press **Enter**.
13. Select **Edit** from the Firewall Custom Rules screen and press **Enter**.

14. To add a new rule or edit an existing rule, select **Add Rule** or **Edit Rule** from the Connection Action Menu screen and press **Enter**.
15. Enter information to customize the firewall rule, then select **OK** and press **Enter**.

    > **Note**
    >
    > The term **All** indicates open access to any interface, for example: BKUP, REP, OAM, SIG-A, SIG-B, and SIG-C.

16. Enter field values, select **OK** and press **Enter**.
17. To delete an existing custom rule, select **Delete Rule** from the Connection Action Menu screen and press **Enter**.
18. Select the rule to be deleted from the Select Rule Menu and press **Enter**.
19. When all editing is complete, save and apply the changes to the system:
    a. If not at the Firewall Configuration Menu screen, select **Exit** to return to the Firewall Configuration Menu screen.
    b. Select **Save and Apply Configuration** from the Firewall Configuration Menu screen and press **Enter** to save all changes.

       A dialog box will open to confirm that the request to apply the changes is successful.

       > **Note**
       >
       > During the editing of firewall configuration settings, if an attempt is made to leave the Firewall Configuration Menu screen with unsaved changes, you are presented with a screen where you can save changes and exit, exit without saving changes, or return to the Firewall Configuration Menu to continue.

       > **Note**
       >
       > When all firewall configuration setting changes are completed, be sure to use menu item **Save and Apply Configuration** from the Firewall Configuration Menu screen to commit the changes made to the firewall configuration files and restart the firewall.

       > **Note**
       >
       > In the preceding configuration steps, the term **All** indicates open access to any interface, for example: Backplane, PMAC, REP, OAM, SIG-A, and SIG-B.

2.9 Displaying Firewall Settings

To display current firewall settings:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:

a. Log in as **root**.

b. Enter `su - platcfg`.

- To access the platcfg utility through an SSH remote session:

a. Log in as **admusr**.

b. Enter `sudo su - platcfg`.

> **Note**
>
> The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.
3. Select **Firewall** from the Policy Configuration Menu screen and press **Enter**.
4. Select **Display Firewall** from the Firewall Configuration Menu screen and press **Enter**.
5. To verify firewall configurations, select a firewall option from the Display Firewall Menu screen, and press **Enter**.

   If **Display Firewall Status** is selected, the Display Firewall Status screen opens to indicate which firewalls are enabled or disabled:

   If **Display Factory Rules** is selected, the Display Factory Rules screen opens:

   If **Display Custom Rules** is selected, the Display Custom Rules screen opens:

2.10 Managing Differentiated Services Code Points (DSCP) Configurations

Use the options on the **DSCP Configuration Menu** screen to manage **DSCP** configurations. These configurations allow you to operate DSCP on network interfaces (SIG-A, SIG-B, and SIG-C) for MPE or MRA devices. The configurations are persistent during system power off, reboot, and upgrade. Configurations can also synchronize to other servers within a cluster.

2.10.1 Adding a DSCP Configuration

> **Note**
>
> Each DSCP configuration is saved to the configuration file in the order in which it is added.

To add a DSCP configuration:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.

- To access the platcfg utility from the system console:

a. Log in as **root**.

b. Enter `su - platcfg`.

- To access the platcfg utility through an SSH remote session:

a. Log in as **admusr**.

b. Enter `sudo su - platcfg`.

> **Note**
>
> The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **DSCP Config** from the Policy Configuration Menu screen and press **Enter**.
3. Select **Add New DSCP Configuration** from the DSCP Configuration Menu screen and press **Enter**.
4. Select the appropriate interface for the new configuration from the Select Interface screen, then select **OK** and press **Enter**, where:
   - **SIG-A** is used to connect to the customer signaling A network,
   - **SIG-B** is used to connect to the customer signaling B network,
   - **SIG-C** is used to connect to the customer signaling C network and is used to internally connect to either MRA or MPE devices when both SIG-A and SIG-B are used for SCTP multi-homing, and
   - **OAM** is used to connect to the customer management network and for internal connection between the cluster and site.

> **Note**
>
> If more than one DSCP configuration is added on the same network interface (for example, SIG-A), the output packets sent from this interface are from the latest DSCP configuration added. The new DSCP configuration (with the same or greater scope in output packets of this network interface) takes precedence over any previous DSCP configurations.

> **Note**
>
> If one interface has both VIP and IP and associates DSCP only with VIP, the packets sent from this interface may not be marked with DSCP as expected because the application may send packets from the server IP instead of the VIP.

5. Specify the **IP Protocol Version**, **Source IP Address**, and **Destination IP Address** to associate with the new configuration on the Input Source IP and Destination IP screen.

> **Note**
>
> If settings are not specified, default settings are used.

6. Select **OK** and press **Enter**.
7. Select the **Code Point** to use with this configuration from the Code Point selection screen, then select **OK** and press **Enter**.

2.10.2 Viewing a DSCP Configuration

To view a DSCP configuration:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

   > **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **View DSCP Configuration** from the DSCP Configuration Menu screen and press **Enter**.

2.10.3 Editing a DSCP Configuration

To edit an existing DSCP configuration:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

   > **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **DSCP Config** from the Policy Configuration Menu screen and press **Enter**.
3. Select **Edit DSCP Configuration** from the DSCP Configuration Menu screen and press **Enter**.
4. Select the DSCP configuration you want to edit from the Edit DSCP Configuraton Menu screen and press **Enter**.

5. Select the interface you want to use for the configuration from the Select Interface screen, then select **OK** and press **Enter**.
6. Enter values for the **IP Protocol Version**, **Source IP Address**, and **Destination IP Address** on the Input Source IP and Destination IP screen, select **OK** and press **Enter**.

> **Note**
>
> If settings are not specified, the previous settings are used.

7. Select the **Code Point** to use with this configuration on the Code Point selection screen, then select **OK** and press **Enter**.

2.10.4 Deleting a DSCP Configuration

To delete a DSCP configuration:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

> **Note**
>
> The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **DSCP Config** from the Policy Configuration Menu screen and press **Enter**.
3. Select **Edit DSCP Configuration** from the DSCP Configuration Menu screen and press **Enter**.
4. Select the DSCP configuration you want to delete by pressing the space bar (more than one configuration can be deleted at a time), then select **OK** and press **Enter**.

   The selected configurations are deleted.

> **Note**
>
> When a configuration is deleted for a network interface that has more than one configuration defined, priority is given to the most current remaining DSCP configuration regarding output packet processing.

2.10.5 Syncing a DSCP Configuration

DSCP configurations on one server can be synced with other servers in the same cluster. It is recommended the sync be performed from the active server to all other servers (standby or standby and spare) in a one site or two site cluster.

To sync a DSCP configuration:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

   > **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **DSCP Config** from the Policy Configuration Menu screen and press **Enter**.
3. Select **Sync DSCP Configuration** from the DSCP Configuration Menu screen and press **Enter**.

   > **Note**
   >
   > If the sync is performed from a server that is not the Active server, a warning message opens, giving you the option to stop the sync process.

4. Select **Yes** to continue the sync process.

   After the process is complete, a confirmation message screen opens. The configurations are copied to the other servers and take effect.

3 Managing Certificates

This chapter describes how to use the platcfg utility to manage secure sockets layer (SSL) security certificates, which allow systems to interact with a high level of security.

3.1 About Security Certificates

To establish a secure (HTTPS) connection between servers in the Policy Management network, or to establish secure connections with third-party systems, you need to create and exchange secure sockets layer (SSL) security certificates, which allow for encrypted communication, before putting the system into production. The platcfg utility supports two types of security certificates: self-signed and third-party.

- Self-signed certificates are created locally on each server using the platcfg utility, then synchronized throughout the Policy Management network to allow encrypted communications between servers. A connection is established between the active servers of a cluster. Because any server in a cluster may become the active server, certificates must be exchanged between all servers in all clusters. To function correctly, the certificates must be current and valid. Self-signed certificates are inherently less secure than third-party signed certificates, so they are not recommended for use in a production environment. Additionally, some external systems may not allow the use of self-signed certificates, which may necessitate the use of third-party certificates.
- Third-party signed certificates are created by an external signing authority. Third-party signed certificates are generated in response to a **Certificate Signature Request** (CSR), which you create locally using the platcfg utility and then send to the third-party signing authority. You then combine it with a current and valid self-signed certificate and synchronize it throughout the Policy Management network.

The following terms relate to the management of certificates:

Certificate
Used by SSL to verify a trusted server; sometimes referred to in platcfg as a Key.

CN (Common Name)
The primary ID inside of a certificate. The Keystore Input Parameters page refers to the CN as **First and Last Name**.

First and Last Name
The primary ID inside of a certificate, also known as the CN.

Key
Another name sometimes used in platcfg to refer to a Certificate.

Local keystore
A file, protected by password-based encryption, that stores self-signed certificates generated on the local servers of a cluster. All servers in a cluster share the same local keystore.

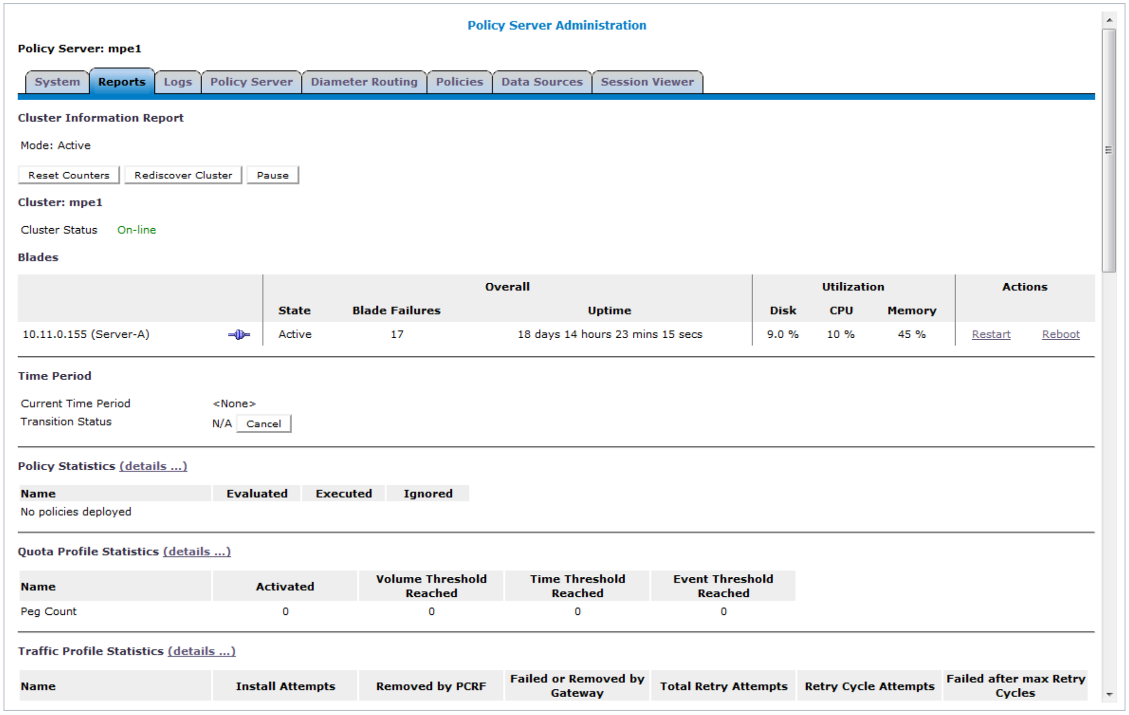
Certificate keystore
A file, protected by password-based encryption, that stores imported certificates generated on other clusters.

When a secure connection is established between the CMP system and a Policy Management cluster:

- An HTTPS session is established and displayed in the URL
- The **System** tab for the cluster displays **Yes** in the **Secure Connection** field
- The **Reports** tab for the cluster displays statistics

Figure 3-1 shows an example of statistics information displayed on the **Reports** tab of the Policy Server Administration page over a secure connection for an MPE cluster.

Figure 3-1 Statistics Displayed Over a Secure Connection



Policy Server Administration

Policy Server: mpe1

Cluster Information Report

Mode: Active

Cluster: mpe1

Cluster Status On-line

Blades

	Overall			Utilization			Actions	
	State	Blade Failures	Uptime	Disk	CPU	Memory		
10.11.0.155 (Server-A)	Active	17	18 days 14 hours 23 mins 15 secs	9.0 %	10 %	45 %	Restart	Reboot

Time Period

Current Time Period <None>
Transition Status N/A

Policy Statistics (details ...)

Name	Evaluated	Executed	Ignored
No policies deployed			

Quota Profile Statistics (details ...)

Name	Activated	Volume Threshold Reached	Time Threshold Reached	Event Threshold Reached
Peg Count	0	0	0	0

Traffic Profile Statistics (details ...)

Name	Install Attempts	Removed by PCRF	Failed or Removed by Gateway	Total Retry Attempts	Retry Cycle Attempts	Failed after max Retry Cycles

3.2 Managing SSL Security Certificates

This section describes how to create and verify self-signed certificates for secure communication between servers and systems.

3.2.1 Creating a Self-signed Certificate

A certificate is used by SSL to verify a trusted server. Certificate creation is performed on the active server in each cluster in the topology and then shared with the other servers of each cluster. This local certificate acts as a Private certificate for the local server and enables encrypted information to be transferred through a secure connection.

> **Note**
>
> Common Name (CN) is the primary ID inside of a certificate. The Keystore Input Parameters page refers to the CN as **First and Last Name**.

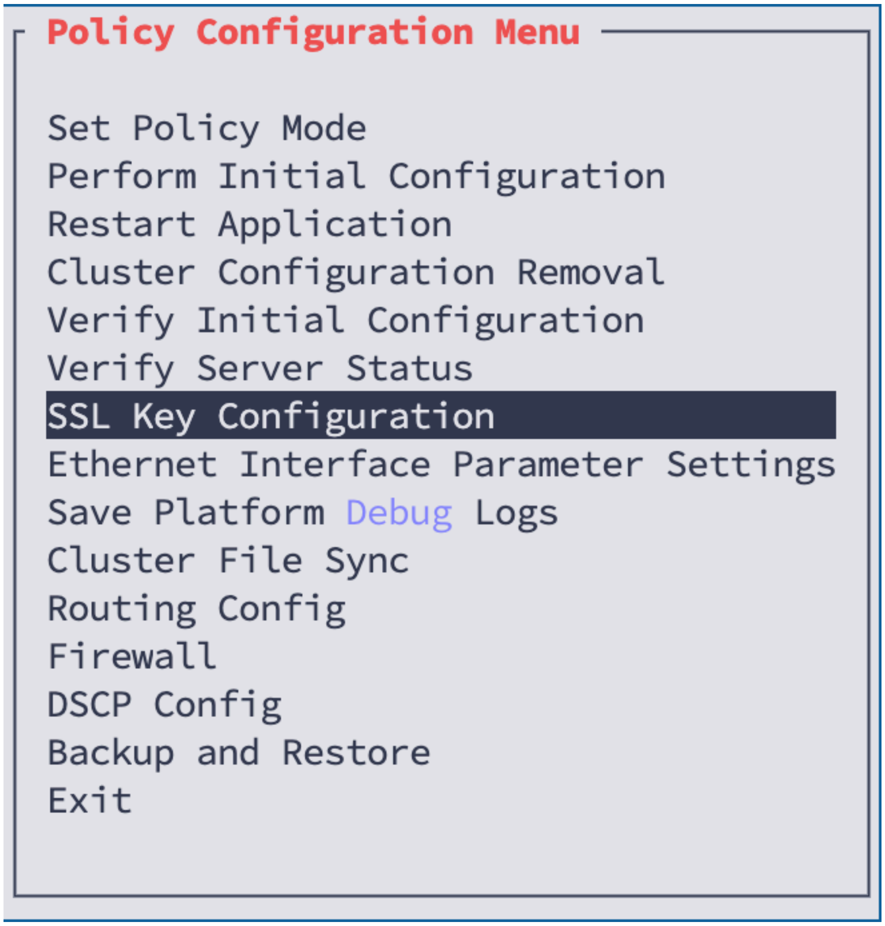
To create a self-signed certificate for a cluster and then synchronize it across the cluster:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

   > **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

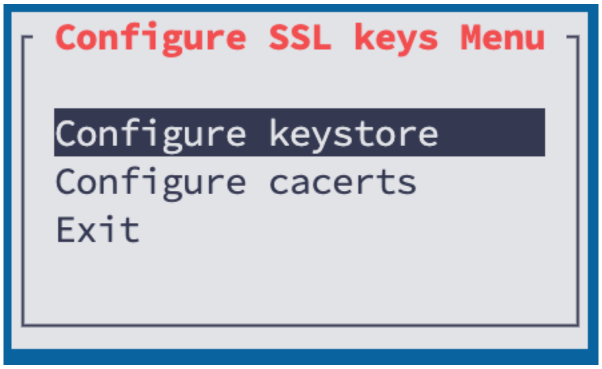
2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.
3. Select **SSL Key Configuration** from the Policy Configuration Menu screen and press **Enter**.

Figure 3-2 Policy Configuration Menu—SSL Key Configuration



4. Select **Configure keystore** from the Configure SSL keys Menu screen and press **Enter**.

Figure 3-3 Configure SSL keys Menu—Configure keystore

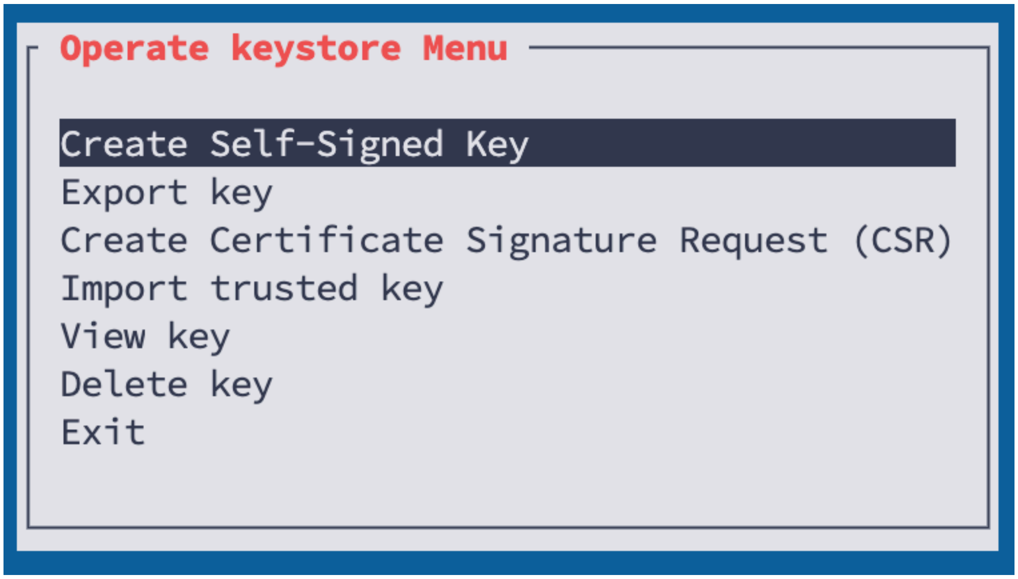


```
Configure SSL keys Menu

Configure keystore
Configure cacerts
Exit
```

5. Select **Create Self-Signed Key** from the Operate keystore Menu and press **Enter**.

Figure 3-4 Operate keystore Menu

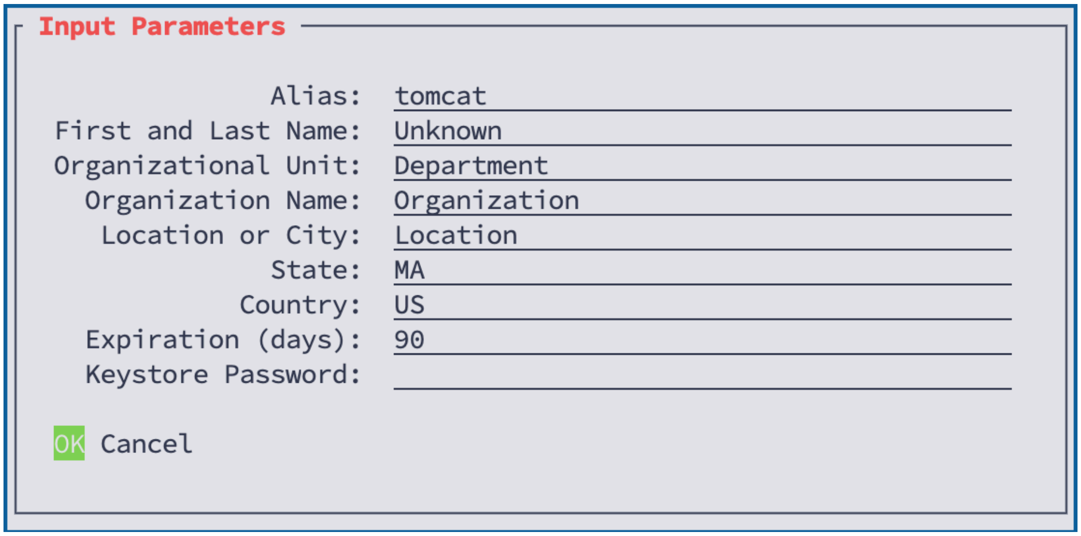


```
Operate keystore Menu

Create Self-Signed Key
Export key
Create Certificate Signature Request (CSR)
Import trusted key
View key
Delete key
Exit
```

6. Enter information on the Input Parameters screen.

Figure 3-5 Input Parameters



```
 Input Parameters

                   Alias:  tomcat
     First and Last Name:  Unknown
     Organizational Unit:  Department
       Organization Name:  Organization
        Location or City:  Location
                   State:  MA
                 Country:  US
       Expiration (days):  90
       Keystore Password:

 OK  Cancel
```

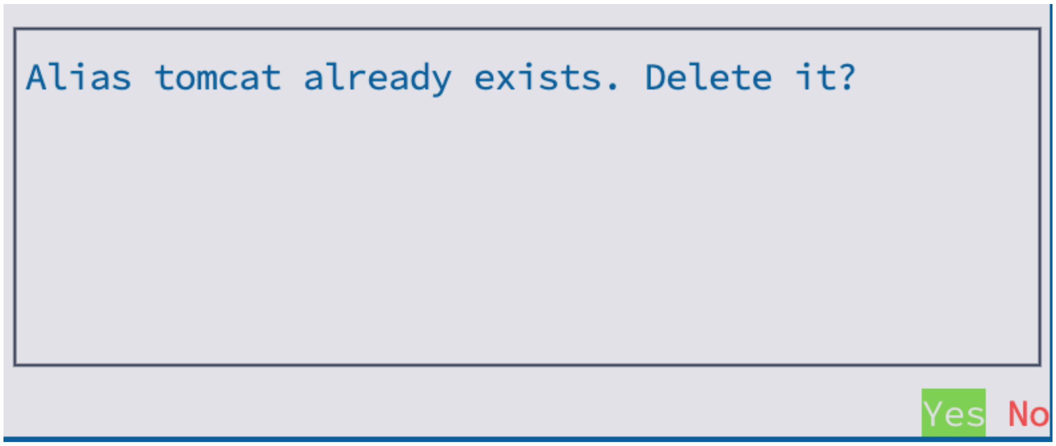
> **Note**
>
> For the **Alias** field, enter `tomcat`.

> **Note**
>
> For the **First and Last Name** field (the CN value), create a unique cluster ID name.

> **Note**
>
> The **Keystore Password** is **changeit**

7. When finished entering values, select **OK** and press **Enter**.
8. If there is an existing certificate with the same **Alias** name, the following screen opens:

Figure 3-6 Delete existing certificate

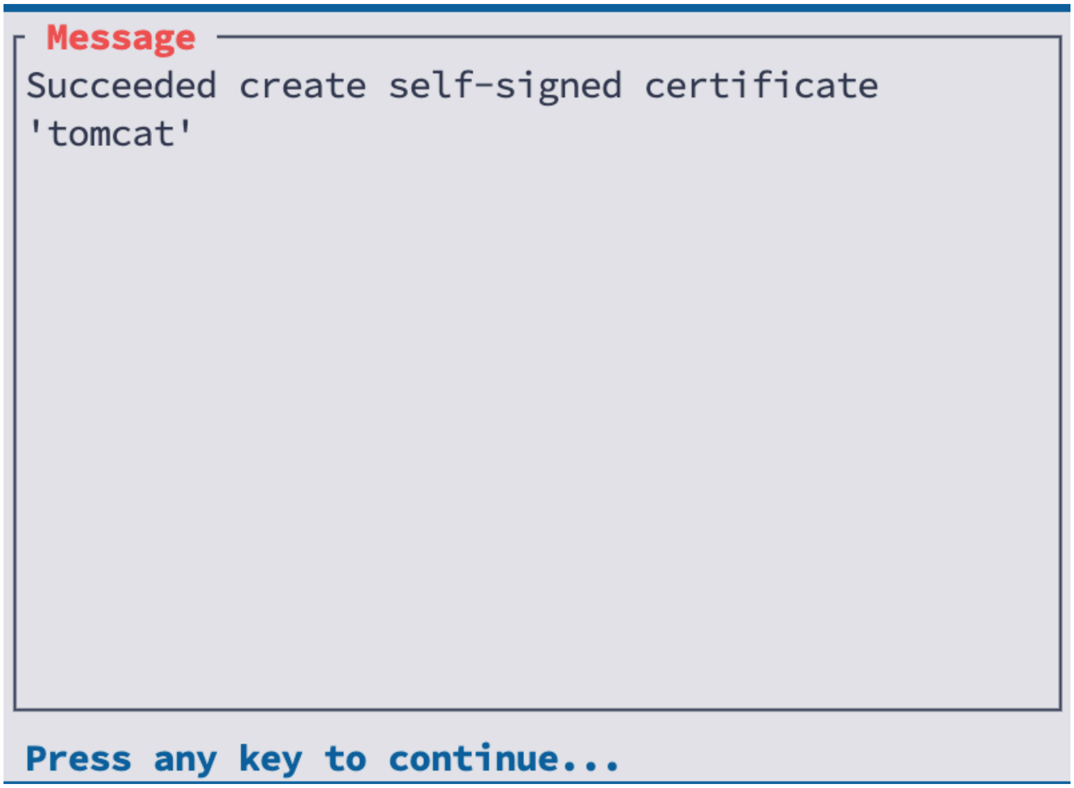


```
Alias tomcat already exists. Delete it?
```

Select **Yes** to remove the old certificate and replace it with a new one with the same name.

9. The following screen opens when the SSL creation is successful.

Figure 3-7 Message



```
Message
Succeeded create self-signed certificate
'tomcat'

Press any key to continue...
```

Press **Enter** to return to the previous screen.

10. Select **Cluster File Sync** from the Policy Configuration Menu screen and press **Enter**.

    The self-signed certificate is synchronized to the others servers of the cluster.

11. Select **Restart Application** from the Policy Configuration Menu screen and press **Enter**.

    The Policy Management application (the qp_procmgr process) on the active server restarts.

Repeat this procedure for every cluster in the Policy Management network.

3.2.2 Verifying a Self-signed Certificate

After an SSL certificate has been created, verify its attributes before attempting to import or export the certificate to create your secure connection. If the certificate on the host is not the same after it is imported into its peer, the secure connection will not be allowed.

To verify a self-signed certificate:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
    - To access the platcfg utility from the system console:
        a. Log in as **root**.
        b. Enter `su - platcfg`.
    - To access the platcfg utility through an SSH remote session:
        a. Log in as **admusr**.
        b. Enter `sudo su - platcfg`.

    > ⓘ **Note**
    >
    > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.
3. Select **SSL Key Configuration** from the Policy Configuration Menu screen and press **Enter**.
4. Select **Configure keystore** from the Configure SSL keys Menu screen and press **Enter**.
5. Select **View key** and press **Enter**.
6. Enter the password, select **OK**, and press **Enter**.
7. Select the certificate and press **Enter**.

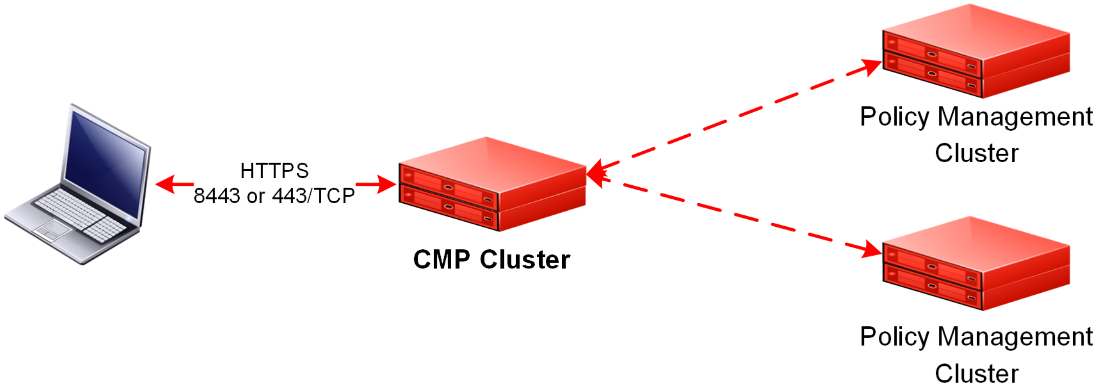
    The certificate opens.
8. Verify the certificate information in the Verify Self-Signed Certificate screen.

    The most important portions of the certificate are the **Alias name**, **Owner**, and **Issuer**. These settings are exported and imported to the other server to establish the secure **HTTP** session.
9. Select **Exit** and press **Enter**.

3.3 Establishing a Secure HTTPS WebBrowser Session

An HTTPS connection is created between an end user (web browser) and the CMP system by passing a predefined certificate to the end user.

Figure 3-8 Establishing a Secure Session



> **Note**
>
> Web browsers function differently based on their configuration. Review your browser settings before using SSL certificates.

> **Note**
>
> For more information, refer to Creating a Self-signed Certificate and Configuring Firewall Settings.

To force end users to establish an HTTPS session with the CMP system:

1. Exchange and import SSL certificates between the CMP server and the workstation.
2. Enable the firewall on the CMP server.
3. Enable **prefer custom**.
4. Create two customized firewall rules (one for port 80 and one for port 8080) where the allowed host is 0.0.0.0/32.

   > **Note**
   >
   > Because the ports 80 and 8080 conflict with the factory rule that allows anyone access to these ports, using the **prefer custom** option discards this rule, and instead uses the custom rule which allows only 0.0.0.0 to connect via 80 or 8080, which locks down the unencrypted HTTP ports.

To establish a HTTPS session with the web browser using CMP GUI, the PCRF CMP application certificate must be signed. The certificate can be signed by a third-party known CA or a local CA can be created to sign the certificate.

The following step must be done on the PCRF Active CMP:

- Creating local CA and Generating the Root Certificate

The root certificate is used to sign the application, or PCRF certificate. If a root certificate, for example, caroot.cert, is not already available, a user can generate the root certificate. Local

CA is not needed if a third-party CA is used to sign the application certificates so skip creating the local CA, if third-party CA is used.

Perform the following steps to create a root CA key and certificate to be used to sign the application certificate:

1. Generate a root CA key with the following command:

   ```
   openssl genrsa 2048 > <path_to_root_key>
   ```

   For example,

   ```
   openssl genrsa 2048 > caroot.key
   ```

2. Generate a "caroot" certificate with the following command:

   ```
   openssl req -new -x509 -nodes -days 1000 -key <path_to_root_key>
   ><path_to_root_certificate>
   ```

   For example,

   ```
   openssl req -new -x509 -nodes -days 1000 -key caroot.key > caroot.cer
   ```

   You will be asked to enter information that will be incorporated into your certificate request. You need to enter a Distinguished Name (DN). Few fields can be left blank while entering the DN. For some fields, there will be a default value. If you enter '.', the field will be left blank.

   - Country Name (2 letter code) [XX]:IN
   - State or Province Name (full name) []:KA
   - Locality Name (for example, city) [Default City]:BLR
   - Organization Name (for example, company) [Default Company Ltd]:ORACLE
   - Organizational Unit Name (for example, section) []:CGBU
   - Email Address []:[cloud-user@star23-bastion-1 cert]$
     Common Name for caroot certificate can be anything.

Generating Application or Client Certificate

The application key and CSR must be generated so that it can signed by either the local CA or third party CA.

Perform the following steps to create and edit the ssl.conf file:

1. In the **alt_names** section, list the IPs, such as IP.1, IP.2, and so on, that are used to access the PCRF GUI:

   [req]

   default_bits = 4096

   distinguished_name = req_distinguished_name

   req_extensions = req_ext

   [req_distinguished_name]

   countryName = Country Name (2 letter code)

```
countryName_default = <Country_Name>
stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = <State_Name>
localityName = Locality Name (eg, city)
localityName_default = <Locality_Name>
organizationName = Organization Name (eg, company)
organizationName_default = <Org_Name>
commonName = Common Name (e.g. server FQDN or YOUR name)
commonName_max = 64
commonName_default = CMP
[ req_ext ]
keyUsage = critical, digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth, clientAuth
asicConstraints = critical, CA:FALSE
subjectAltName = critical, @alt_names
[alt_names]
IP.1 = 127.0.0.1
IP.2 = <IP2>
IP.3 = <IP3>
IP.4 = <IP4>
IP.5 = <IP5>
IP.6 = <IP6>
DNS.1 = localhost
```

For example,

```
[ req ]
default_bits = 4096
distinguished_name = req_distinguished_name
req_extensions = req_ext
[ req_distinguished_name ]
countryName = Country Name (2 letter code)
countryName_default = <Country_Name>
stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = <State_Name>
localityName = Locality Name (eg, city)
localityName_default = <Locality_Name>
organizationName = Organization Name (eg, company)
organizationName_default = <Org_Name>
commonName = Common Name (e.g. server FQDN or YOUR name)
```

commonName_max = 64

commonName_default = CMP

[req_ext]

keyUsage = critical, digitalSignature, keyEncipherment

extendedKeyUsage = serverAuth, clientAuth

basicConstraints = critical, CA:FALSE

subjectAltName = critical, @alt_names

[alt_names]

IP.1 = 127.0.0.1

IP.2 = 10.75.217.5

IP.3 = 10.75.217.76

DNS.1 = localhost

2. Create a Certificate Signing Request (CSR) with the following command:

   ```
   openssl req -config ssl.conf -newkey rsa:2048 -days 1000 -nodes -keyout
   <path_to_application_certificate_key> >
   <path_to_certificate_signing_request>
   ```

   For example,

   ```
   openssl req -config ssl.conf -newkey rsa:2048 -days 1000 -nodes -keyout
   rsa_private_key_pkcs1.key >ssl_rsa_certificate.csr
   ```

   The following output is displayed: Ignoring -days; not generating a certificateGenerating a RSA private key...++++........++++writing new private key to 'rsa_private_key_pkcs1.key' You will be asked to enter information that will be incorporated into your certificate request. You need to enter a Distinguished Name (DN). Few fields can be left blank while entering the DN. For some fields, there will be a default value. If you enter '.', the field will be left blank.

   - Country Name (2 letter code) [IN]:
   - State or Province Name (full name) [KA]:
   - Locality Name (for example, city) [BLR]:
   - Organization Name (for example, company) [ORACLE]:
   - Common Name (e.g. server FQDN or YOUR name) [pcrf]:
   - Email Address []:[cloud-user@star23-bastion-1 cert]$

   Provide the Common name as hostname of your Active CMP server.

3. Display the components of the file and verify the configurations with the following command:

   ```
   openssl req -text -noout -verify -in ssl_rsa_certificate.csr
   ```

   Ensure all fields entered for application certificate are correct.

Signing the application CSR

If the third-party CA is used to sign the application CSR, then provide the CSR and IPs to the third party CA to sign. The third-party CA should return a ca root certificate and a signed application certificate. If local CA is used, then follow the steps to sign the Application CSR:

1. Sign in to this CSR file with the CA root certificate with the following command:

   ```
   openssl x509 -extfile ssl.conf -extensions req_ext -req -in
         <path_to_certificate_signing_request> -days 1000 -
   CA<path_to_root_certificate> -CAkey <path_to_root_key> -set_serial 04>
   <path_to_application_certificate>
   ```

   For example,

   ```
   openssl x509 -extfile ssl.conf -extensions req_ext -req -in
   ssl_rsa_certificate.csr -days 1000 -CA ../caroot.cer -CAkey ../caroot.key -
   set_serial 04 >ssl_rsa_certificate.crt
   ```

   The following output is displayed: Signature oksubject=C = IN, ST = KA, L = BLR, O = ORACLE, CN = ocatsGetting CA Private Key[cloud-user@star23-bastion-1 cert]$

2. Verify that the certificate is properly signed by the CA root certificate with the following command:

   ```
   openssl verify -
   CAfile<path_to_root_certificate><path_to_application_certificate>
   ```

   For Example,

   ```
   openssl verify -CAfile caroot.cer ssl_rsa_certificate.crt
   ```

   The following output is displayed: ssl_rsa_certificate.crt: OK

3. Save the generated application certificates and the root certificates.

Importing Certificates:

1. If a third-party CA used is which is known by the browsers, then skip this step. The known CA on the browsers can be checked by navigating into settings->certificates-> trusted root authorities. If local CA or an unknown third party CA is used, then add the caroot.cer of the CA to the browser as a trusted author. For more information, see Adding Root Certificate to Web Browser.

2. Delete old keys of tomcat in keystore and cacerts by using platcfg options, remove any other keys as well.

3. Import the signed certificate to the default CMP keystore. The key to be used is the one generated in previous step. If third-party signed certificate is used, the format must be openssl x509 only.

   ```
   openssl pkcs12 -inkey <path_to_application_certificate_key> -in
   <path_to_signed_application_certificate> -export -out /opt/camiant/tomcat/
   conf/.keystore -name "<Cert alias>
   ```

For example,

```
openssl pkcs12 -inkey rsa_private_key_pkcs1.key -in
ssl_rsa_certificate.crt -export -out /opt/camiant/tomcat/conf/.keystore -
name "Cert1"
```

4. Importing keystore in default CMP cacerts

   ```
   keytool -importkeystore -srckeystore /opt/camiant/tomcat/conf/.keystore -
   srcstoretype pkcs12 -destkeystore /opt/camiant/tomcat/conf/cacerts.jks -
   deststoretype JKS
   ```

5. Perform Cluster file sync from Active CMP.
6. If CMP site2 cluster is present, import the certificate in Site2 Active CMP by repeating Step 3 and Step 4 with the same file. Then perform a cluster file sync on Site2 Active CMP.
7. Reboot all CMP Nodes one by one.

Adding Root Certificate to Web Browser

This section describes how to add a root certificate on Google Chrome and Mozilla Firfox forWindows and Mac laptop.

Adding a Certificate on Google Chrome in Windows Laptop:

1. In the Chrome browser, navigate to the settings and search for security.
2. Click the security option that appears next to search.
3. Click the Manage Device Certificate option.
4. Click the Trusted root certification authorities bar.
5. Import the caroot certificate.
6. Save and restart the browser.

Adding a Certificate on Google Chrome in Mac Laptop:

1. In the Chrome browser, navigate to the settings and search for security.
2. Click the security option that appears next to search.
3. Click the Manage Device Certificate option. The Keychain Access window opens.
4. Search the tab certificate and drag and drop the downloaded caroot certificate.
5. Find the uploaded certificate in the list, usually listed by a temporary name.
6. Double click the certificate and expand the Trust option.
7. When using this certificate option, assign it to "always trust".
8. Close the window and validate if it asks for the password.
9. Save and restart the browser.

Adding a Certificate on Mozilla Firefox for Windows and Mac Laptop:

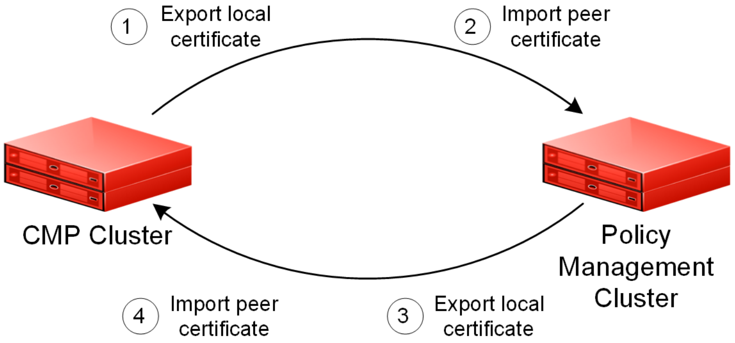
1. In the Mozilla Firefox browser, navigate to the settings and search for certificates.
2. Click the View Certificate that appears next to search. This opens a Certificate Manager window.
3. Navigate to the Authorities section, click the Import button, and upload the caroot certificate.

4. Click the Trust options in the pop-up window and click OK.
5. Save and restart the browser.

3.4 About Establishing a Secure Connection Between a CMP System and a Policy Management Server

To establish a secure connection between a CMP system and a Policy Management server, both the CMP system and the Policy Management server must exchange certificates.

Figure 3-9 Exchanging Certificates



The figure shows how the SSL certificate is shared between the clusters. The following certificate exchange is done:

1. The CMP system creates a local certificate and exports the certificate to the Policy Management server.
2. The Policy Management server imports the peer certificate (local certificate created by the CMP system) into its trust store.
3. The Policy Management server creates a local certificate and exports the certificate to the CMP system.
4. The CMP system imports the peer certificate (local certificate created by the Policy Management server) into its trust store.

> **Note**
>
> Procedures used in this chapter may require the reboot of one or more servers. Subsequently, for high availability (HA) to operate correctly in a clustered system, the active server of the cluster must not be rebooted unless the cluster is in the **online** state. Before rebooting any server, check cluster status using the CMP interface. If a cluster is labeled **Degraded**, but the server detail does not show any failed or disconnected equipment, the server is performing a database synchronization operation and until the synchronization process has completed, the standby server cannot perform as the active server.
> When a new certificate is configured, the synchronization causes the HA on the standby server to restart.
>
> SSL certificates are created on a per-cluster basis, and to ensure that the cluster has the same certificate installed, you should force a system synchronization.
>
> To exchange certificates in a large Policy Management network with many servers, see Bulk Certificate Exchange.

3.4.1 Exporting a Local Certificate to a Policy Management Server

To export a local certificate through a secure connection between the CMP system and a Policy Management server:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

   > **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.
3. Select **SSL Key Configuration** from the Policy Configuration Menu screen and press **Enter**.
4. Select **Configure Keystore** from the Configure SSL keys Menu screen and press **Enter**.
5. Select **Export key** from the Operate keystore Menu screen and press **Enter**.
6. Enter the **Keystore Password**, select **OK**, and press **Enter**.
7. Press **Enter** to accept the alias `tomcat`.

   The Export Certificate screen opens.

8. Select the certificate type **binary**, enter the local certificate file path, select **OK**, and press **Enter**.

   The certificate is exported.

9. When the certificate is exported, a successful completion message displays.

   Press **Enter**.

10. Log in as **admusr** on the active server of the CMP cluster and enter the following commands:

    a. `sudo su -`

    b. `scp admusr@`*`active_server_addr`*`:`*`remote_path/file`*`.cer `*`local_path`*

    In this example, *active_server_addr* is `mpe-01`, *remote_path* is `/tmp`, *file* is `mpe-a.cer`, and *local_path* is `/tmp`:

    ```
    # scp admusr@mpe01:/tmp/mpe-a.cer /tmp
    mpe-a.cer
    #
    ```

    The certificate is copied to the active CMP server.

3.4.2 Importing a Peer Certificate

This procedure imports a certificate to a Policy Management server and enables a secure connection. This includes certificates generated by other servers including certificates signed by a third party or similar.

After you have exported the local certificate, to import the peer certificate (that is, the certificate you exported) to the certificate keystore of a Policy Management server:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.

   - To access the platcfg utility from the system console:

     a. Log in as **root**.

     b. Enter `su - platcfg`.

   - To access the platcfg utility through an SSH remote session:

     a. Log in as **admusr**.

     b. Enter `sudo su - platcfg`.

   > **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.

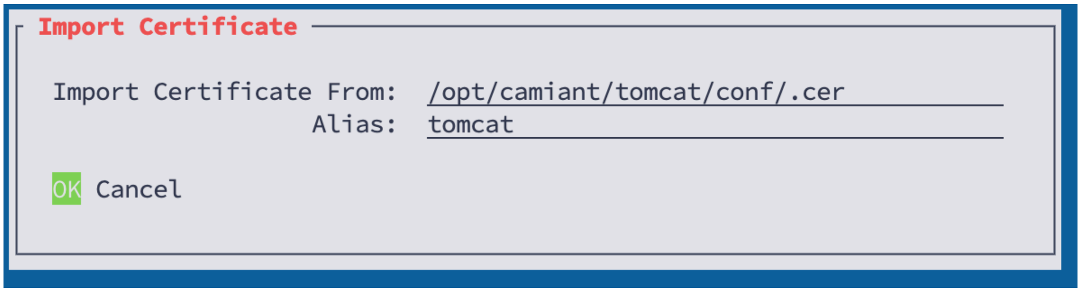
3. Select **SSL Key Configuration** from the Policy Configuration Menu screen and press **Enter**.

4. Select **Configure cacerts** from the Configure SSL keys Menu screen and press **Enter**.

5. Select **Import trusted key** from the Operate keystore Menu screen and press **Enter**.

6. Enter the **Keystore Password**, select **OK**, and press **Enter**.
7. Enter the import location and **Alias** for the certificate, as set previously for the **CN** name, select **OK**, and press **Enter**.

Figure 3-10 Import Certificate



```
Import Certificate

  Import Certificate From:  /opt/camiant/tomcat/conf/.cer
                    Alias:  tomcat
```

You are then presented with the certificate data for verification. Ensure that the **CN** name, **Owner**, and **Issuer** names of the input file name match that of the previous export file.

8. After you have verified that the certificate data is correct, select **OK** and press **Enter**.

   When the certificate is imported, a successful import message displays.
9. Press **Enter**.
10. Select **Cluster File Sync** from the Policy Configuration Menu screen and press **Enter**.

    The imported peer certificate is synchronized to the others servers of the cluster.
11. Select **Restart Application** from the Policy Configuration Menu screen and press **Enter**.

    The Policy Management application (the `qp_procmgr` process) on the active server restarts.

> **Tip**
>
> You can verify that SSH keys have been fully exchanged between servers by logging in to the active CMP server as **admusr** and entering the following commands:
>
> ```
> sudo su - /opt/camiant/bin/qpSSHKeyProv.pl --check --verbose
> ```

Once certificates are exchanged, to enable an HTTPS connection to the Policy Management cluster, log on to the active CMP server, select the cluster, select the **Secure Connection** check box from the **Policy Server** tab, and click **Save**. You are prompted, "The `configuration was applied successfully`," and **Secure Connection** displays **Yes**. See the appropriate *CMP User's Guide* for more information.

> **Tip**
>
> If instead you are prompted that the Policy server is unavailable, there may be a problem with the certificates.

3.4.3 Bulk Certificate Exchange

Before beginning this procedure, you must have created self-signed certificates (see Creating a Self-signed Certificate).

This procedure imports certificates from multiple MPE andMRA clusters and enables a secure connection. You would use this procedure, in place of the procedures Exporting a Local Certificate to a Policy Management Server and Importing a Peer Certificate, to save time when exchanging certificates in a large Policy Management network.

You cannot use this procedure for connections between a Network Configuration Management Platform (NW-CMP) system and a System Configuration Management Platform (S-CMP) system.

From the primary site active CMP or S-CMP server:

1. Log in as **admusr**.
2. Enter `sudo su -`.
3. To exchange SSH keys between the CMP system and MPE and MRA servers, enter `/opt/camiant/bin/qpSSHKeyProv.pl --prov --relax`.

   The argument `--relax` causes SSH keys to be provisioned from MPE and MRA systems to the CMP system.
4. Enter `/opt/camiant/bin/qpRunInTopo.py --cmd="sslKeyUtil --exportToCmp --target=active_cmp_addr --sshUser=<UserName> --sshPasswd=<UserPasswd>" --pool-size=1 --prod=mpe,mra --ha-role=Active [--show]`.

   The optional argument `--show` displays execution details.

   UserName - the user who has sudo permissions. For example, admusr.

   UserPasswd - the password of the user

   The utility `sslKeyUtil` executes on the active server of each MPE and MRA cluster. It exports the certificate from the local keystore to a local file; copies the file to the specified CMP server; and imports the file into the certificate keystore on the CMP server.
5. Synchronize the certificates across the other servers in the CMP cluster. For more information, see Synchronizing Cluster Files.

Example 3-1 Example

This example shows a successful execution of `qpRunInTopo.py`. The certificate file `mpe-a.cer` is imported from the MPE server `mpe01` to the active CMP server at IP address `nn.nn.nn.nn`.

```
# /opt/camiant/bin/qpRunInTopo.py --cmd="sslKeyUtil --exportToCmp --
target=nn.nn.nn.nn --sshUser=admusr --sshPasswd=<admusrPasswd>" --pool-size=1
--prod=mpe,mra --ha-role=Active --show
Command will be run on following servers:
["mpe01"]
Continue? [yes|no]: yes
[   {   'errput': 'FIPS integrity verification test failed.\r\nCertificate
stored in file </tmp/mpe01_mpe-a.cer>\n',
        'id': 'configUser@mpe01: sslKeyUtil --exportToCmp --
target=nn.nn.nn.nn --sshUser=admusr --sshPasswd=<admusrPasswd>',
        'output': "Export to cmp\nGoing to export key tomcat\nImporting to
cacerts.jks in target nn.nn.nn.nn\nSSHRun returns 0\n output : FIPS integrity
verification test failed.\r\r\n
SYSTEM\r\nThis system is intended to be used solely by authorized users in
the\r\ncourse of legitimate corporate business.  Users are monitored to
the\r\nextent necessary to properly administer the system, to
identify\r\nunauthorized users or users operating beyond their proper
authority,\r\nand to investigate improper access or use. By accessing this
system,\r\nyou are consenting to this monitoring.\r\n\r\nadmusr@nn.nn.nn.nn's
password: \r\nCertificate was added to keystore\r\n[Storing /opt/camiant/
tomcat/conf/cacerts.jks]\r\n \n",,
        'ret_code': 0}]
=======================================
Suceeded.
#
```

Once certificates are exchanged, to enable an HTTPS connection, log on to the active CMP server, select the Policy Management cluster, and select the **Secure Connections** check box, located on the **Policy Server** tab. See the appropriate *CMP User's Guide* for more information.

3.5 About Creating CA Third-Party Signed Certificates

> **Note**
>
> This section assumes that no SSL certificates have previously been generated on or imported into the servers. If pre-existing certificates exist on the system (besides the default `tomcat` certificate, which you must keep), contact My Oracle Support to determine their purpose and importance. Read this section in its entirety before starting the operations.

To create CA third-party certificates, execute the following procedures:

1. Deleting an SSL Certificate
2. Generating a Certificate Signature Request
3. Exporting the Certificate Signature Request from the System
4. Provide the Certificate Signature Request to the third party who signs and returns the certificate request.
5. Importing Third-party Peer Certificates
6. Importing the Third-party Signed Certificates
7. Synchronizing and Rebooting the Cluster

3.5.1 Deleting an SSL Certificate

> **Note**
>
> You can also use this procedure to delete an expired SSL certificate.

Before continuing with any of the other required certificate generation or import/export functions, delete any other user-created pre-existing certificates.

> ⚠ **Caution**
>
> The default certificate has the alias `tomcat`. You may need to replace it with a current certificate, but do not delete it, or else you will not be able to complete subsequent procedures.

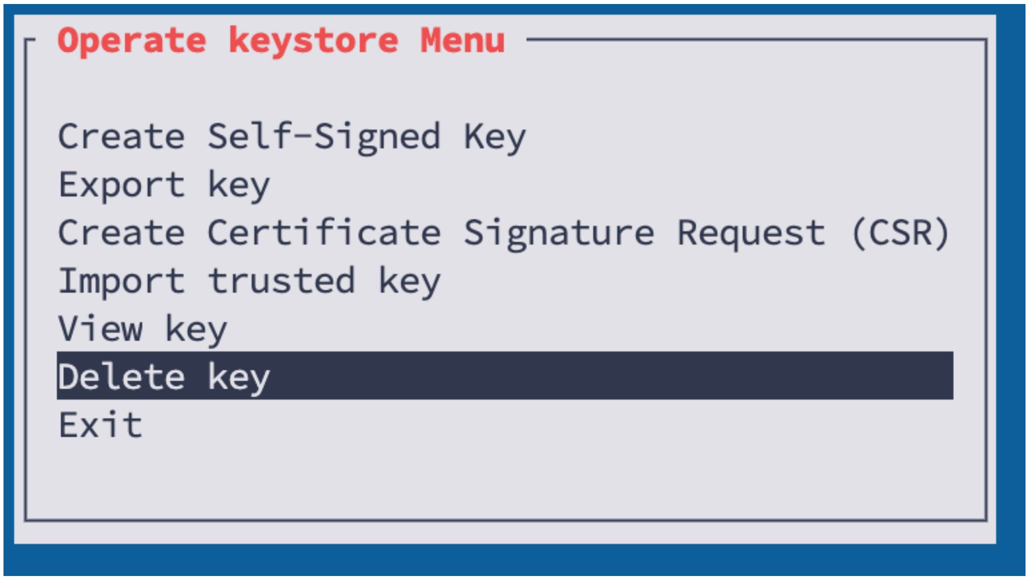
To delete an SSL certificate:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

   > ⓘ **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

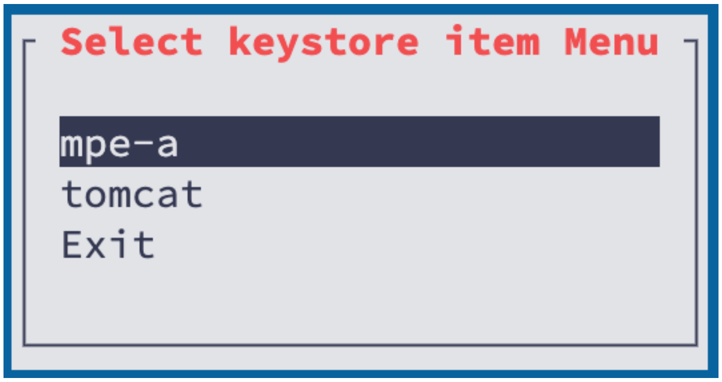
2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.
3. Select **SSL Key Configuration** from the Policy Configuration Menu screen and press **Enter**.
4. Select **Configure Keystore** from the Configure SSL keys Menu screen and press **Enter**.
5. Select **Delete key** from the Operate keystore Menu screen and press **Enter**.

Figure 3-11 Operate keystore Menu



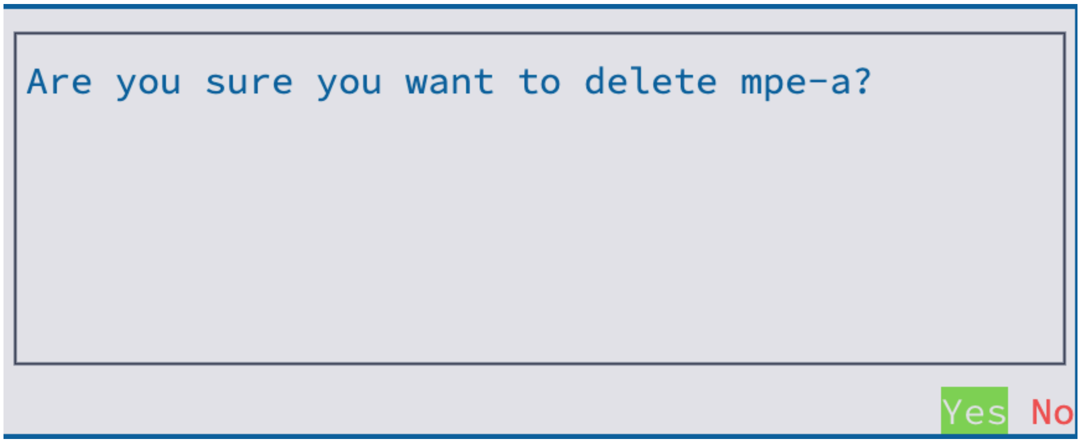
6. Enter the **Keystore Password**, select **OK**, and press **Enter.**
7. Select the certificate to be deleted and press **Enter**.

Figure 3-12   Select keystore item Menu



8. You are prompted to delete the selected certificate.

Figure 3-13   Delete existing certificate


Are you sure you want to delete mpe-a?

Select **Yes** to delete the certificate or **No** to leave it as is, then press **Enter**.
You are now ready to generate the local certificate, export it for signing, and then re-import the signed certificate.

3.5.2 About Generating a Certificate Signature Request

To generate the third-party signed local certificate, execute the following procedures:

1. Generating a Certificate Signature Request
2. Exporting the Certificate Signature Request from the System
3. Send the Certificate Signature Request to a third-party certifying authority for signing
4. Receive the signed Certificate Signature Request
5. Importing the Third-party Signed Certificates

6. Verifying a Self-signed Certificate

3.5.2.1 Generating a Certificate Signature Request

To generate a certificate signature request:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

   > **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu and press **Enter**.
3. Select **SSL Key Configuration** from the Policy Configuration Menu screen and press **Enter**.
4. Select **Configure keystore** from the Configure SSL keys Menu screen and press **Enter**.
5. Select **Create Certificate Signature Request (CSR)** from the Operate keystore Menu screen and press **Enter**.
6. Enter the **Keystore Password**, select **OK**, and press **Enter**.
7. Select the certificate name that you want to export for signature from the Create CSR screen and press **Enter**.

   > **Note**
   >
   > The alias of the certificate is used later for re-importing the certificate after signing by a third party. Use an alias that allows the certificate to be identified with a specific system. Also of importance is the **Expiration** attribute, which should be set to a sufficiently large value so that the certificate does not expire before any peer certificates. Oracle recommends a value preventing expiration for three years.

8. Edit the destination path from the Create CSR screen to change it or select **OK** to accept it, and press **Enter**.

3.5.2.2 Exporting the Certificate Signature Request from the System

To export a locally generated certificate signature request:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.

- To access the platcfg utility from the system console:
  a. Log in as **root**.
  b. Enter `su - platcfg`.
- To access the platcfg utility through an SSH remote session:
  a. Log in as **admusr**.
  b. Enter `sudo su - platcfg`.

> **Note**
>
> The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.
3. Select **SSL Key Configuration** from the Policy Configuration Menu screen and press **Enter**.
4. Select **Configure keystore** from the Configure SSL keys Menu screen and press **Enter**.
5. Select **SSL Key Configuration** from the Policy Configuration Menu screen and press **Enter**.
6. Select **Export key** from the Operate keystore Menu screen and press **Enter**.
7. Enter the **Keystore Password**, select **OK** and press **Enter**.
8. Select the certificate to export for signature and press **Enter**.
9. Select the certificate **ascii** and enter the certificate export location, then select **OK** and press **Enter**.

   The **Message** screen opens to confirm that the certificate was exported.

After the certificate file is exported, send it to the third party who signs and returns the certificate request.

3.5.2.3 Importing the Third-party Signed Certificates

After the certificate has been signed by the third-party certifying authority, two certificate files are returned by the authority for importing into the Policy Management servers:

- A signed local client certificate (with the file suffix `.crt`)
- A certificate authority (**CA**) peer certificate (with the file suffix `.pem`)

Both certificates must be imported into the active CMP system for proper SSL communication.

> **Note**
>
> It may necessary to edit the returned files to remove extraneous debugging information in the certificate. You must use a Linux-based editor to preserve line termination style.

The only content in the files should be the blocks of data beginning with:

```
----BEGIN CERTIFICATE-----
```

and ending with:

```
-----END CERTIFICATE-----
```

All other text above or below these blocks should be removed.

A further modification needs to be made to the signed local client certificate.

For the Policy Management servers to be able to import the local certificate successfully, the CA peer certificate must be merged into the signed local client certificate. Copy the `BEGIN/END` certificate text block from the CA peer certificate into the local client certificate below the `BEGIN/END` certificate text block. The final result is the original local client certificate text block immediately followed by the certificate text block of the CA peer certificate that was provided by the third-party signer. An example of what this should look like is as follows:

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAligAwIBAgIBBTANBgkqhkiG9w0BAQUFADCBjDELMAkGA1UEBhMCVVMx
<text removed>
gJeTRnZwMJEXv71V85NGobVGqb1uR94kIQazFP5HC2b2C0Q=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDjTCCAvagAwIBAgIJAJCKgXrXbhQ/MA0GCSqGSIb3DQEBBQUAMIGMMQswCQYD
<text removed>
YVPOATiFnrt1B9Qb1P8kW8lwPmG88Gg6nqttolhAnIi/lWBcp+QZfJMxPBcMkH2k7A==
-----END CERTIFICATE-----
```

Either copy these certificate files to the Policy Management server in advance, or store them somewhere on the network accessible via SCP. They can be imported back into the system to secure the communication channel with the third-party system.

To import the certificates:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

   > **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.
3. Select **SSL Key Configuration** from the Policy Configuration Menu screen and press **Enter**.
4. Select **Configure keystore** from the Configure SSL keys Menu screen and press **Enter**.
5. To import the local signed certificate, select **Import trusted key** from the Operate keystore Menu screen and press **Enter**.

6. Enter the **Keystore Password**, select **OK**, and press **Enter**.

   You are prompted for the location of the certificate to be imported.

7. Select or enter the location where the local signed certificate is located and the certificate alias name, select **OK**, and press **Enter**.

   The certificate data screen opens for verification. To avoid confusion, though they may be different, ensure that the **Owner** and **Issuer** names used for the certificate match the host name of the server where the certificate is being created.

   > **Note**
   >
   > The alias entered must match the alias originally used to create the certificate request.

8. To import the CA signed certificate as a peer certificate, select **Import trusted key** from the Operate cacerts Menu and press **Enter**.

9. Enter the **Keystore Password**, select **OK**, and press **Enter**.

   You are prompted for the location of the certificate to be imported.

10. Select or enter the location where the CA peer certificate is located and the certificate alias name, select **OK**, and press **Enter**.

    The certificate data screen opens for verification. To avoid confusion, though they may be different, ensure that the **Owner** and **Issuer** names used for the certificate match the host name of the server the certificate is being created on. If all certificate information is correct, the next operation is to import the CA certificate as a peer certificate.

    > **Note**
    >
    > The alias entered must match the alias originally used to create the Certificate Request.

3.6 Importing Third-party Peer Certificates

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.

   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

   > **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu and press **Enter**.
3. Select **SSL Key Configuration** from the Policy Configuration Menu and press **Enter**.
4. Select **Configure keystore** from the Configure SSL keys Menu and press **Enter**.
5. Select **Import trusted key** from the Operate keystore Menu and press **Enter**.
6. Enter the **Keystore Password**, select **OK**, and press **Enter**.

   You are prompted for the location of the certificate to be imported.
7. Select or enter the location where the certificate is located and the certificate alias name, select **OK**, and press **Enter**.

> **Note**
>
> The alias entered here must match the alias originally used to create the Certificate Request.

3.7 Establishing a Secure Connection over REST interface between CMP and UDR

To establish a secure connection, UDR's certificate which is present on UDR at `/usr/TKLC/udr/ssl`, needs to be imported into CMP's Truststore which is present at `/opt/camiant/tomcat/conf/cacerts.jks`, and CMP's certificate needs to be added to CMP's Keystore which is present at `//opt/camiant/tomcat/conf/.keystore`.

How UDR-CMP Secure Connection Works

Certificate Exchange between UDR and CMP

1. CMP sends "Client Hello" message to UDR.
2. UDR responds with "Server Hello", its certificate (**/usr/TKLC/udr/ssl/serverCert.pem**) and a Certificate Request. The Certificate Request contains **/usr/TKLC/udr/ssl/tklcCaCert.pem** and is a request from UDR to CMP for a certificate.
3. CMP first verifies the certificate sent by UDR, that is, **serverCert.pem** by checking for it in the Truststore: `/opt/camiant/tomcat/conf/cacerts.jks`. After it finds a match CMP checks the keystore for a certificate that has been verified by the certificate received in the Certificate Request. Once CMP finds such a certificate it sends it to the UDR, and this certificate is then validated by the UDR.

Steps to exchange the certificate between UDR and CMP

Following is an example to exchange the certificate between CMP and UDR. Here *clientCert.p12* is the CMP's certificate and *serverCert.pem* is the UDR's certificate as per the instructions given in *Oracle Communications User Data Repository REST Provisioning Interface Specification document*.

1. Copy **/usr/TKLC/udr/ssl/serverCert.pem** from UDR on CMP.
2. Run the following command to import **serverCert.pem** into the CMP's Truststore:`keytool -import -alias newUDR -file serverCert.pem -keystore /opt/camiant/tomcat/conf/cacerts.jks`

3. Run the following command to import CMP’s certificate into the Keystore:`keytool -v -importkeystore -srckeystore clientCert.p12 -srcstoretype PKCS12 -destkeystore /opt/camiant/tomcat/conf/.keystore -deststoretype JKS`

3.8 Synchronizing and Rebooting the Cluster

After exchanging certificates, all cluster servers must be synchronized and rebooted.

- Synchronizing a cluster shares the keystore. To synchronize, see Synchronizing Cluster Files.
- To reboot, see the *CMP User's Guide* corresponding to the system mode.

4
Synchronizing Files

This chapter describes how and when to synchronize files in clusters.

Files should be synchronized after either of the following items are configured:

- Routes (Routing Config)
- Firewall (Firewall)

4.1 Managing Cluster Sync Configurations

Use the **Cluster Sync Config** menu to manage cluster sync configurations:

- Reading Destination from COMCOL
- Adding Sync File
- Deleting Sync File

4.1.1 Reading Destination from COMCOL

To read the cluster sync destination from COMCOL:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

   > **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.
3. Select **Cluster File Sync** from the Policy Configuration Menu screen and press **Enter**.
4. Select **Cluster Sync Config** from the Cluster Configuration Sync Menu screen and press **Enter**.
5. Select **Read Destination from Comcol** from the Config the Destination of Cluster Sync Menu screen and press **Enter**.

   The destination of the cluster sync file is read from COMCOL.

4.1.2 Adding a Sync File

To add a cluster sync configuration file:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

   > **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.
3. Select **Cluster File Sync** from the Policy Configuration Menu screen and press **Enter**.
4. Select **Cluster Sync Config** from the Cluster Configuration Sync Menu screen and press **Enter**.
5. Select **Add Sync File** from the Config the Destination of Cluster Sync Menu screen and press **Enter**.

   The Add a Sync File screen opens.
6. Enter data into the fields:
   - **filename**—The name of the sync file.
   - **remote file**—The name of the sync file if different at the remote site.
   - **scope (cluster/site/clusterGroup)**—Lists where each file is to be synced:
     – **cluster**—Indicates access to all servers at all sites. Files that need to be in sync at all sites (such as certificates) should be listed as Cluster.
     – **site**—Indicates access to servers at the local site. IP-related files that may not be valid at other sites (such as firewall and static routes) should be listed as Site.
     – **clusterGroup**—Indicates access to all servers only in multiple CMP, MPE, or MRA clusters.
   - **post script**— Indicates a note or description of the scope (cluster/site/clusterGroup).
7. Select **OK** and press **Enter**.

   The new cluster sync configuration is saved.

4.1.3 Deleting a Sync File

To delete an cluster sync configuration file:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

   > **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.
3. Select **Cluster File Sync** from the Policy Configuration Menu screen and press **Enter**.
4. Select **Cluster Sync Config** from the Cluster Configuration Sync Menu screen and press **Enter**.
5. Select **Delete Sync File** from the Config the Destination of Cluster Sync Menu screen and press **Enter**.

   The Main Routing Table screen opens.
6. Select the cluster sync configuration file to delete from the list, select **OK** and press **Enter**.

   The selected cluster sync configuration is deleted.

4.2 Displaying a Sync Configuration

Displaying a sync configuration is useful when georedundancy is implemented.

To display a sync configuration:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

   > **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.

3. Select **Cluster File Sync** from the Policy Configuration Menu screen and press **Enter**.
4. Select **Show Sync Config** from the Cluster Configuration Sync Menu screen and press **Enter**.

   The **Sync File** screen is displayed.

   The **Scope** column lists where each file is being synced:

   - **Site** indicates that the file is synced to servers at the local site
   - **Cluster** indicates that the file is synced to all servers at all sites

   > **Note**
   >
   > Files that must be in sync at all sites (like certificates) are listed as **Cluster**; IP-related files that are not valid at other sites (like firewall and static routes) are listed as **Site**.

4.3 Displaying a Sync Destination

To display a sync destination (for example, hostname, IP address, and location):

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

   > **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.
3. Select **Cluster File Sync** from the Policy Configuration Menu screen and press **Enter**.
4. Select **Show Sync Destination** from the Cluster Configuration Sync Menu screen and press **Enter**.

   The Sync Destination screen opens.

4.4 Displaying a Sync Status

To display a cluster sync status:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:

   a. Log in as **root**.
   b. Enter `su - platcfg`.
- To access the platcfg utility through an SSH remote session:
   a. Log in as **admusr**.
   b. Enter `sudo su - platcfg`.

> ⓘ **Note**
>
> The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.
3. Select **Cluster File Sync** from the Policy Configuration Menu screen and press **Enter**.
4. Select **Show Sync Status** from the Cluster Configuration Sync Menu screen and press **Enter**.

   A screen opens to display the sync status.

4.5 Synchronizing Cluster Files

> ⓘ **Note**
>
> File synchronization (or cluster sync) copies configuration files from the target server to the remaining servers in the cluster. Performing a cluster sync will launch **`qp_procmgr`** on the target servers, so this action should only be performed from the Active server, or else a failure occurs. A warning screen opens before continuing with the sync to help prevent this issue from occurring. There is a separate sync operation for DSCP configurations.

To synchronize the cluster files:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
      a. Log in as **root**.
      b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
      a. Log in as **admusr**.
      b. Enter `sudo su - platcfg`.

> ⓘ **Note**
>
> The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.

3. Select **Cluster File Sync** from the Policy Configuration Menu screen and press **Enter**.
4. Select **Start Synchronizing** from the Cluster Configuration Sync Menu screen and press **Enter**.

   > ⓘ **Note**
   >
   > A warning message screen opens, indicating that a cluster sync will launch `qp_procmgr` on the target servers.

   > ⚠ **Warning**
   >
   > This action should only be performed from the Active server, otherwise a failure will occur.

5. Select **OK** and press **Enter**.

   Configuration files are synced to the other servers in the cluster, and `qp_procmgr` is restarted on the target servers.

5

Editing Network Interface Ethernet Parameters

This chapter describes how to edit Ethtool options, including auto-negotiation, speed, and duplex transmission parameters, on the interface controller for a wireline network installation. Two methods are used, the policy configuration method and the TPD method.

Configuration settings are persistent over system upgrades and reboots.

5.1 About Settings Link Options

Keep the following information in mind when configuring link options:

- The **Speed** is configurable only when the device supports 100baseT/Full.
- The physical device might support several **Speed** modes, but 100baseT/Full is the only candidate in the platcfg interface.
- If the interface is a bond device, then the **Speed** and duplex settings for the active secondary device is fetched from kernel and displayed on the platcfg interface. If any secondary device of the bond interface is not linked, the bond interface is not configurable.
- If the interface is a bond device, then primary_reselect is configurable.
- If the two secondary devices in a bond device are running in different modes, a warning message is displayed before the window is updated.
- It is strongly recommended that the auto-negotiation option is set to autoneg on at both ends. If it is set to autoneg off, a warning message is displayed when **OK** is selected.
- The link behavior is undefined if one end has autoneg on while the other end has autoneg off.
- When **OK** is selected, the setting is applied to the interface immediately. For a bond device, the setting is applied to both of the secondary devices.
- If the applied mode is not compatible with the switch, it is possible that the link may go down. This utility does not try to detect or correct this situation.

Table 5-1 Ethtool speed compatibility matrix

Speed Setting: server/ switch	Default (autoneg on)	100baseT/Full, Autoneg on	100baseT/Full, Autoneg off
Default (autoneg on)	OK (case 1)	OK (case 2)	Undefined
100baseT/Full, Autoneg on	OK (case 2)	OK (case 3)	Undefined
100baseT/Full, Autoneg off	Undefined	Undefined	OK (case 4)

5.2 Editing Network Interface Ethernet Parameters (Policy Configuration Method)

This section describes how to edit Network Interface Ethernet parameter settings using the Policy Configuration method. See About Settings Link Options for additional information.

To edit network interface ethernet parameter settings:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

   > **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu and press **Enter**.
3. Select **Ethernet Interface Parameter Settings** from the Policy Configuration Menu and press **Enter**.
4. Select a network from the list on the **Network Interfaces List Menu** and press **Enter**.

   Each line in this display represents a physical interface (OAM, SIGA or SIGB) using logical names instead of physical names. If multiple logical interfaces share a physical interface, those interfaces are grouped on a single line.
5. Select **Set EthTool Options of <linkname>** from the Interface <linkname> Menu and press **Enter**.
6. Select from the options on the Edit <linkname> Link Options screen, select **OK** and press **Enter**.

   Selection changes are made on both devices of a bond interface at the same time.

5.3 Editing Network Interface Ethernet Parameters (TPD Method)

This section describes how to edit network interface ethernet parameter settings using the TPD platform method. If none of the options are specified, auto-negotiation is assumed.

To edit network interface ethernet parameter settings:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:

    a. Log in as **root**.
    b. Enter `su - platcfg`.

- To access the platcfg utility through an SSH remote session:
    a. Log in as **admusr**.
    b. Enter `sudo su - platcfg`.

> ⓘ **Note**
>
> The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Network Configuration** from the Main Menu - Network Configuration and press **Enter**.
3. Select **Network Interfaces** from the Network Configuration Menu and press **Enter**.
4. Select **Edit an Interface** from the Network Interfaces Menu and press **Enter**.
5. Select a Network Interface name from the Connection to edit Menu choices.
6. To continue to the network Interface Options menu, select **Edit** from the **Options** menu on the screen. Otherwise, select **Exit** to return to the previous menu.
7. Select the required speed and duplex options from the Interface Options menu, select **OK** and press **Enter.**

6 Backing Up and Restoring the System and Server

This chapter describes how to back up and restore the system and server.

6.1 Backing Up a Server

The server backup file contains OS-level information that is configured in the platcfg utility such as **IP**, **NTP**, and **DNS** addresses. This type of backup is unique to a server and should be created for every server within a cluster.

To back up a server:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

   > **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select the **Policy Configuration** from the Main Menu screen and press **Enter**.
3. Select **Backup and Restore** from the Policy Configuration Menu screen and press **Enter**.

   System Backup and **System Restore** actions are only allowed on a CMP server or **MA Server**, so these options are not available on the menu for other types of servers.
4. Select **Server Backup** from the Backup and Restore Menu screen and press **Enter**.
5. Accept the default backup directory or enter the **ISO** path to save the backup file.

   The naming convention used for the backup file is:

   hostname-camiant-*release*-serverbackup-*datetime*.iso
6. Select **OK** and press **Enter**.

   The backup file is created.

6.2 Backing Up the System

The system backup file contains application-level information such as Topology, Network Element, and Policy Management configurations that are configured in the CMP system. This backup file saves the information for an entire deployment and should be created on the active server of the Primary CMP cluster.

When the backup file is created, the file contains a specific name and is located in a specific directory. Transfer this backup to the **FTP** server.

To back up the system:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

   > **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.
3. Select **Backup and Restore** from the Policy Configuration Menu screen and press **Enter**.
4. Select **System Backup** from the Backup and Restore Menu screen and press **Enter**.
5. Enter the tar.gz path to save the backup file.
6. Accept the default backup directory or enter a desired directory.

   The naming convention used for the backup file is:

   hostname-camiant-*release*-systembackup-*datetime*.tar.gz
7. Select **OK** and press **Enter**.

   The backup file is created.

6.3 Displaying Backup Files

To display current local archive and remote archive backup files:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.

- To access the platcfg utility through an SSH remote session:
   a. Log in as **admusr**.
   b. Enter `sudo su - platcfg`.

> **Note**
>
> The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select the **Policy Configuration** from the Main Menu screen and press **Enter**.
3. Select **Backup and Restore** from the Policy Configuration Menu screen and press **Enter**.
4. Select **Display Backup Files** from the Backup and Restore Menu screen and press **Enter**.
5. From the Display Backup Files Menu screen, select either the local archive or the remote archive:
   - Select **Display Local Archive** and press **Enter**.
     The Local Archives screen opens.
   - Select **Display Remote Archive** and press **Enter**.
     The Remote Archives screen opens.

6.4 Configuring Local Archive Settings

You can store up to three archives for both the server and system backup files. To configure local archive settings:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
      a. Log in as **root**.
      b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
      a. Log in as **admusr**.
      b. Enter `sudo su - platcfg`.

> **Note**
>
> The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.
3. Select **Backup and Restore** from the Policy Configuration Menu screen and press **Enter**.
4. Select **Local Archive Settings** from the Backup and Restore Menu screen and press **Enter**.
5. Specify the number of archives for the server and system backups.

> **Note**
>
> The server backup option is only available on a CMP system or MA Server.

6. When finished, select **OK** and press **Enter**.

   The archive settings are configured.

6.5 Configuring Remote Archive Settings

This section describes how to manage remotely stored system and server archives.

6.5.1 Adding a Remote Archive

To add a remote archive:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

   > **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.
3. Select **Backup and Restore** from the Policy Configuration Menu screen and press **Enter**.
4. Select **Remote Archive Settings** from the Backup and Restore Menu screen and press **Enter**.
5. Select **Remote Archive for Server Backups** or **Remote Archive for System Backups** from the Remote Archive Settings Menu screen and press **Enter**.

   > **Note**
   >
   > The server backups option is available only on a CMP system or MA Server.

6. Select **Add Remote Archive** from the second Remote Archive Settings Menu screen and press **Enter**.
7. Enter the remote access information, where:
   - **user** and **password**—Valid SSH login credentials for the target server.
   - **host**—A reachable IP address or a resolvable hostname.

- **folder**—A directory on the target server where the Policy Management server will attempt to copy backups. The directory must already exist; it will not be created on demand.
- **comment**—The name of the remote archive when viewed in platcfg.

8. Select **OK** and press **Enter**.

   The remote archive is added.

6.5.2 Editing a Remote Archive Configuration

To edit a remote archive configuration:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

   > **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select either **Remote Archive for Server Backups** or **Remote Archive for System Backups** from the Remote Archive Settings Menu screen and press **Enter**.
3. Select **Edit Remote Archive** from the Remote Archive Settings Menu screen and press **Enter**.
4. Select the remote archive to edit from the Remote Archives Menu screen and press **Enter**.
5. Enter the remote archive information, select **OK**, and press **Enter**.

   The remote archive settings are updated.

6.5.3 Deleting a Remote Archive Configuration

To delete a remote archive configuration:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

> **Note**
>
> The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select either **Remote Archive for Server Backups** or **Remote Archive for System Backups** from the Remote Archive Settings Menu screen and press **Enter**.
3. Select **Delete Remote Archive** and press **Enter**.
4. Select the remote archive to delete from the Remote Archives Menu screen and press **Enter**.
5. Select **Yes** from the Confirm deletion screen and press **Enter**.

   The remote archive is deleted.

6.5.4 Displaying a Remote Archive Configuration

To display a remote archive configuration:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

> **Note**
>
> The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select either **Remote Archive for Server Backups** or **Remote Archive for System Backups** from the Remote Archive Settings Menu screen and press **Enter**.
3. Select **Display Remote Archive** from the second Remote Archive Settings Menu screen and press **Enter**.

   Either the **Display Remote Archive For Server-Backup** or the **Display Remote Archive For System-Backup** screen opens.

6.6 Scheduling Backups

You can configure your system or server to conduct backups on a scheduled basis. This section describes how to manage backup schedules.

6.6.1 Scheduling a Backup

To schedule a backup:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

   > ⓘ **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.
3. Select **Backup and Restore** from the Policy Configuration Menu screen and press **Enter**.
4. Select **Scheduled Backup Settings** from the Backup and Restore Menu screen and press **Enter**.
5. Select either **Scheduled Backup for Server Backups** or **Scheduled Backup for System Backups** from the Scheduled Backup Settings Menu screen and press **Enter**.
6. Select **Add Schedule** from the **Scheduled Backup for server backups Menu** screen and press **Enter**.

   The Schedule parameters screen opens.
7. Enter the following information:
   - **Name**—A unique name identifying the scheduled backup.
   - **Min**—Minute to perform backup. Valid values are 0 to 59, with a default of 0.
   - **Hour**—Hour to perform backup. Valid values are 0 to 23, with a default of 0.
   - **Weekly**—Select to have the backup performed weekly. When **Weekly** is selected, the **Days of the Month** value is ignored. The default backup is performed weekly.
   - **Days of Week**—Specifies that the backup is performed on specific days. Valid values are sun, mon, tue, wed, thu, fri, and sat.
   - **Monthly**—Select to have the backup performed monthly. When **Monthly** is selected, the **Days of the Week** value is ignored.
   - **Days of the Month**—Day to perform backup. Valid values include 1 and 15.

   > ⓘ **Note**
   >
   > When **Weekly** is selected, the **Days of the Month** field is ignored, and when **Monthly** is selected, the **Days of the Week** field is ignored.

8. Select **OK** and press **Enter**.

   The backup is scheduled.

6.6.2 Editing a Backup Schedule

To edit a backup schedule:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

   > **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select the **Policy Configuration** from the Main Menu screen and press **Enter**.
3. Select **Backup and Restore** from the Policy Configuration Menu screen and press **Enter**.
4. Select **Scheduled Backup Settings** from the Backup and Restore Menu screen and press **Enter**.
5. Select either **Scheduled Backup for Server Backups** or **Scheduled Backup for System Backups** from the Scheduled Backup Settings Menu screen and press **Enter**.
6. Select **Edit Schedule** from the **Scheduled Backup for server backups Menu** screen or from the Scheduled Backup for system backups Menu screen and press **Enter**.
7. Edit the following Information:
   - **Name**—A unique name identifying the scheduled backup.
   - **Min**—Minute to perform backup. Valid values are 0 to 59, with a default of 0.
   - **Hour**—Hour to perform backup. Valid values are 0 to 23, with a default of 0.
   - **Weekly**—Select to have the backup performed weekly. When **Weekly** is selected, the **Days of the Month** value is ignored. The default backup is performed weekly.
   - **Days of Week**—Specifies that the backup is performed on specific days. Valid values are sun, mon, tue, wed, thu, fri, and sat.
   - **Monthly**—Select to have the backup performed monthly. When **Monthly** is selected, the **Days of the Week** value is ignored.
   - **Days of the Month**—Day to perform backup. Valid values include 1 and 15.

   > **Note**
   >
   > When **Weekly** is selected, the **Days of the Month** field is ignored, and when **Monthly** is selected, the **Days of the Week** field is ignored.

8. Select **OK** and press **Enter**.

6.6.3 Deleting a Backup Schedule

To delete a backup schedule:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

   > **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.
3. Select **Backup and Restore** from the Policy Configuration Menu screen and press **Enter**.
4. Select **Backup and Restore** from the Policy Configuration Menu screen and press **Enter**.
5. Select **Scheduled Backup Settings** from the Backup and Restore Menu screen and press **Enter**.
6. Select either **Scheduled Backup for Server Backups** or **Scheduled Backup for System Backups** from the Scheduled Backup Settings Menu screen and press **Enter**.
7. Select **Delete Schedule** from the **Scheduled Backup for server backups Menu** screen or from the Scheduled Backup for system backups Menu screen and press **Enter**.
8. Select **OK** and press **Enter**.

   The schedule is deleted.

6.6.4 Displaying a Backup Schedule

To a display a backup schedule:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

> **Note**
>
> The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu and press **Enter**.
3. Select **Backup and Restore** from the Policy Configuration Menu screen and press **Enter**.
4. Select **Backup and Restore** from the Policy Configuration Menu screen and press **Enter**.
5. Select **Scheduled Backup Settings** from the Backup and Restore Menu screen and press **Enter**.
6. Select **Display Scheduled Backups** from the Scheduled Backup Settings Menu screen and press **Enter**.

   The backup schedule list screen opens.

6.7 Restoring a System

Restoring a System restores the Policy Management information that is unique to this system, including topology, policies, and feature configuration.

To restore a system:

1. Stop QP and COMCOL on the standby server using the CMP interface, by entering the commands:

   ```
   service qp_procmgr stop
   service comcol stop
   ```

2. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

   > **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

3. Select the **Policy Configuration** from the Main Menu screen and press **Enter**.
4. Select **Backup and Restore** from the Policy Configuration Menu screen and press **Enter**.
5. Select **System Restore** from the Backup and Restore Menu screen and press **Enter**.
6. Input the requested information, where:.

7. Select **OK** and press **Enter**.

   The system restores to the backup version specified.

8. Restart QP and COMCOL on the standby server using the CMP interface, by entering the commands:

   ```
   service comcol start
   service qp_procmgr start
   ```

   > ⓘ **Note**
   >
   > For more information about how to use the CMP interface, refer to the *CMP User's Guide* that corresponds to the mode of the system.

6.8 Performing a Server Restore

The server restore restores the OS information unique to the server. This operation applies the data from a previously saved server configuration backup file.

To perform a server restore:

1. Log in to the platcfg utility using one of two methods, either from the system console using **root** or through an SSH remote session using **admusr**.
   - To access the platcfg utility from the system console:
     a. Log in as **root**.
     b. Enter `su - platcfg`.
   - To access the platcfg utility through an SSH remote session:
     a. Log in as **admusr**.
     b. Enter `sudo su - platcfg`.

   > ⓘ **Note**
   >
   > The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

2. Select **Policy Configuration** from the Main Menu screen and press **Enter**.
3. Select **Backup and Restore** from the Policy Configuration Menu screen and press **Enter**.
4. Select **Server Restore** from the Backup and Restore Menu screen and press **Enter**.
5. Enter the path to the backup file, select **OK**, and press **Enter**.

   The system restores to the backup version specified.