

**Oracle®Communications
Policy Management**

Platform Configuration User's Guide

Release 9.7

E53124 Revision 01

April 2014

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

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

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

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

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

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

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

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

Table of Contents

Chapter 1: About This Guide.....	7
Introduction.....	8
Conventions.....	8
How This Guide is Organized.....	8
Intended Audience.....	8
Documentation Admonishments.....	9
Customer Care Center.....	9
Emergency Response.....	12
Related Publications.....	12
Locate Product Documentation on the Customer Support Site.....	13
Chapter 2: Accessing and Using the Platform Configuration Utility.....	14
Accessing the Platcfg Utility.....	15
Using the Platcfg Utility.....	15
Troubleshooting Using the Policy Configuration Menu.....	15
Saving Platform Debug Logs.....	16
Chapter 3: Performing Initial Server Configuration.....	17
Initial Configuration.....	18
Verifying the Initial Configuration.....	19
Verifying the Server Status.....	20
Exchanging SSH Key with Mate(s).....	20
Configuring Routing on Your Server.....	21
Configuring Routing	21
Deleting a Route.....	22
Displaying Configure Routes.....	23
Exporting a Route.....	23
Importing a Route.....	24
Restarting the Application.....	24
Configuring Firewall Settings.....	25
Displaying Firewall Settings.....	28

Chapter 4: Managing Certificates.....	30
Managing SSL Security Certificates.....	31
Creating a Self-Signed Certificate.....	31
Verifying the Generated Certificate.....	32
Using a Local Certificate to Establish a Secure HTTP (https) Web-Browser Session.....	33
Establishing a Secure Connection Between a CMP System and an MPE/MRA/MDF Device.....	34
Exporting the Local Certificate to the MPE/MRA/MDF Servers.....	35
Importing the Peer Certificate.....	36
Creating a Third-party CA Signed Certificate.....	37
Remove the Pre-existing Local Certificate.....	37
Generating a Local Certificate, Exporting for Signing, and Re-importing.....	38
Chapter 5: Synchronizing Files.....	43
Managing Cluster Sync Configurations.....	44
Reading Destination from COMCOL.....	44
Adding a Sync File.....	45
Deleting a Sync File.....	46
Showing Sync Configuration.....	48
Showing Sync Destination.....	49
Showing Sync Status.....	49
Performing File Synchronization.....	50
Chapter 6: Performing System and Server Backups and Restores.....	52
Performing a Server Backup.....	53
Performing a System Backup.....	54
Displaying Backup Files.....	55
Configuring Local Archive Settings.....	55
Configuring Remote Archive Settings.....	56
Configuring a Remote Archive.....	56
Editing a Remote Archive Configuration.....	57
Deleting an Archive Configuration.....	57
Scheduling Backups.....	58
Scheduling a Backup.....	58
Editing a Scheduled Backup.....	59
Deleting a Scheduled Backup.....	59
Displaying Scheduled Backups.....	59
Performing a System Restore.....	60

Performing a Server Restore.....	60
Glossary.....	62

List of Tables

Table 1: Admonishments.....	9
-----------------------------	---

Chapter 1

About This Guide

Topics:

- *Introduction.....8*
- *How This Guide is Organized.....8*
- *Intended Audience.....8*
- *Documentation Admonishments.....9*
- *Customer Care Center.....9*
- *Emergency Response.....12*
- *Related Publications.....12*
- *Locate Product Documentation on the Customer Support Site.....13*

Introduction

This guide describes how to use the Platform Configuration utility to configure Policy Management, as are described in their respective manuals.

Conventions

Your view of the product may vary from the figures used as examples in this guide; the pages, tabs, fields, and functions that you see depend on your configuration or application.

The MPE device is the Policy server. The terms *policy server* and *MPE device* are synonymous.

The following conventions are used throughout this guide to emphasize certain information, such as user input, page options and output, and menu selections.

Italics -Indicates book titles and user input variables.

Monospace - Indicates program output.

Monospace bold - Indicates user input.

Monospace *italics* - Indicates variables in commands.

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.
- [*Accessing and Using the Platform Configuration Utility*](#) describes how to access the Platform Configuration (Platcfg) utility, how to use the utility interface in a policy environment, and troubleshooting.
- [*Performing Initial Server Configuration*](#) describes how to access the Platform Configuration (Platcfg) utility and configure your applications initial configuration, and then how to verify the configuration.
- [*Managing Certificates*](#) describes how to access the Platform Configuration (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.
- [*Performing System and Server Backups and Restores*](#) describes how to perform system and server backups and restores.
- Glossary

Intended Audience

This guide is intended for the following trained and qualified service personnel who are responsible for operating policy servers and related support equipment:

- System operators
- System administrators

Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

Table 1: Admonishments

Icon	Description
 DANGER	Danger: (This icon and text indicate the possibility of <i>personal injury</i> .)
 WARNING	Warning: (This icon and text indicate the possibility of <i>equipment damage</i> .)
 CAUTION	Caution: (This icon and text indicate the possibility of <i>service interruption</i> .)
 TOPPLE	Topple: (This icon and text indicate the possibility of <i>personal injury</i> and <i>equipment damage</i> .)

Customer Care Center

The Tekelec Customer Care Center is your initial point of contact for all product support needs. A representative takes your call or email, creates a Customer Service Request (CSR) and directs your requests to the Tekelec Technical Assistance Center (TAC). Each CSR includes an individual tracking number. Together with TAC Engineers, the representative will help you resolve your request.

The Customer Care Center is available 24 hours a day, 7 days a week, 365 days a year, and is linked to TAC Engineers around the globe.

Tekelec TAC Engineers are available to provide solutions to your technical questions and issues 7 days a week, 24 hours a day. After a CSR is issued, the TAC Engineer determines the classification of the trouble. If a critical problem exists, emergency procedures are initiated. If the problem is not critical, normal support procedures apply. A primary Technical Engineer is assigned to work on the CSR and provide a solution to the problem. The CSR is closed when the problem is resolved.

Tekelec Technical Assistance Centers are located around the globe in the following locations:

Tekelec - Global

Email (All Regions): support@tekelec.com

- **USA and Canada**

Phone:

1-888-367-8552 (toll-free, within continental USA and Canada)

1-919-460-2150 (outside continental USA and Canada)

TAC Regional Support Office Hours:

8:00 a.m. through 5:00 p.m. (GMT minus 5 hours), Monday through Friday, excluding holidays

- **Caribbean and Latin America (CALA)**

Phone:

+1-919-460-2150

TAC Regional Support Office Hours (except Brazil):

10:00 a.m. through 7:00 p.m. (GMT minus 6 hours), Monday through Friday, excluding holidays

- **Argentina**

Phone:

0-800-555-5246 (toll-free)

- **Brazil**

Phone:

0-800-891-4341 (toll-free)

TAC Regional Support Office Hours:

8:00 a.m. through 5:48 p.m. (GMT minus 3 hours), Monday through Friday, excluding holidays

- **Chile**

Phone:

1230-020-555-5468

- **Colombia**

Phone:

01-800-912-0537

- **Dominican Republic**

Phone:

1-888-367-8552

- **Mexico**

Phone:

001-888-367-8552

- **Peru**

Phone:

0800-53-087

- **Puerto Rico**

Phone:

1-888-367-8552

- **Venezuela**

Phone:

0800-176-6497

- **Europe, Middle East, and Africa**

Regional Office Hours:

8:30 a.m. through 5:00 p.m. (GMT), Monday through Friday, excluding holidays

- **Signaling**

Phone:

+44 1784 467 804 (within UK)

- **Software Solutions**

Phone:

+33 3 89 33 54 00

- **Asia**

- **India**

Phone:

+91-124-465-5098 or +1-919-460-2150

TAC Regional Support Office Hours:

10:00 a.m. through 7:00 p.m. (GMT plus 5 1/2 hours), Monday through Saturday, excluding holidays

- **Singapore**

Phone:

+65 6796 2288

TAC Regional Support Office Hours:

9:00 a.m. through 6:00 p.m. (GMT plus 8 hours), Monday through Friday, excluding holidays

Emergency Response

In the event of a critical service situation, emergency response is offered by the Tekelec Customer Care Center 24 hours a day, 7 days a week. 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 the Tekelec Customer Care Center.

Related Publications

The Policy Management product set includes the following publications, which provide information for the configuration and use of Policy Management products in the following environments:

Cable

- *Feature Notice*
- *Cable Release Notes*
- *Roadmap to Hardware Documentation*
- *CMP Cable User's Guide*
- *Troubleshooting Reference*
- *SNMP User's Guide*
- *OSSI XML Interface Definitions Reference*
- *Platform Configuration User's Guide*
- *Bandwidth on Demand Application Manager User's Guide*
- *PCMM specification PKT-SP-MM-I06* (third-party document, used as reference material for PCMM)

Wireless

- *Feature Notice*
- *Wireless Release Notes*
- *Roadmap to Hardware Documentation*
- *CMP Wireless User's Guide*
- *Multi-Protocol Routing Agent User's Guide*
- *Troubleshooting Reference*

- *SNMP User's Guide*
- *OSSI XML Interface Definitions Reference*
- *Analytics Data Stream Reference*
- *Platform Configuration User's Guide*
- *Message Distribution Function Reference*

Wireline

- *Feature Notice*
- *Wireline Release Notes*
- *Roadmap to Hardware Documentation*
- *CMP Wireline User's Guide*
- *Troubleshooting Reference*
- *SNMP User's Guide*
- *OSSI XML Interface Definitions Reference*
- *Platform Configuration User's Guide*

Locate Product Documentation on the Customer Support Site

Access to Tekelec's Customer Support site is restricted to current Tekelec customers only. This section describes how to log into the Tekelec Customer Support site and locate a document. Viewing the document requires Adobe Acrobat Reader, which can be downloaded at www.adobe.com.

1. Log into the [Tekelec Customer Support](#) site.

Note: If you have not registered for this new site, click the **Register Here** link. Have your customer number available. The response time for registration requests is 24 to 48 hours.

2. Click the **Product Support** tab.
3. Use the Search field to locate a document by its part number, release number, document name, or document type. The Search field accepts both full and partial entries.
4. Click a subject folder to browse through a list of related files.
5. To download a file to your location, right-click the file name and select **Save Target As**.

Chapter 2

Accessing and Using the Platform Configuration Utility

Topics:

- *Accessing the Platcfg Utility.....15*
- *Using the Platcfg Utility.....15*
- *Troubleshooting Using the Policy Configuration Menu.....15*

This chapter describes how to access the Platform Configuration (Platcfg) utility and use the utility interface in the Policy Management environment.

Accessing the Platcfg Utility

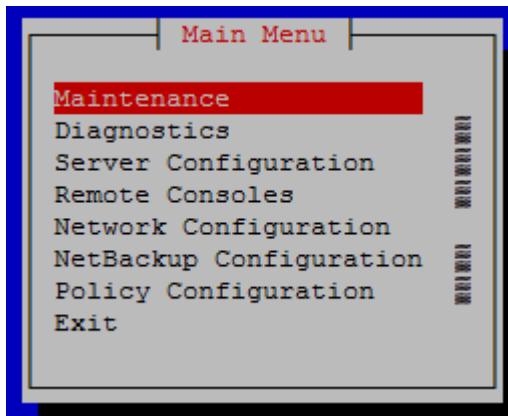
To access the Platcfg utility, complete the following:

1. Log in to your system as root.
2. At the root prompt, enter the following command:

```
# su - platcfg
```

Note: The dash (-) is required in the su - platcfg command to ensure proper permissions.

The following screen is displayed.



Using the Platcfg Utility

To move and enter information within the Platcfg utility, use the following:

- Up and down arrows - moves the action up or down.
- Left and right arrows - moves the action sideways.
- Enter key - enters the desired information and moves to the next menu item or feature.
- First letter - Select the first letter of a menu item to move to that item.

Troubleshooting Using the Policy Configuration Menu

If a system failure occurs, use the Save Platform Debug Logs menu option on the Policy Configuration Menu to help debug the issue.

Saving Platform Debug Logs

The Save Platform Debug Logs option is used to troubleshoot a system failure. This option varies from the standard Platcfg save debug log option by providing two settings that allow you to limit the size of the Save Log files.

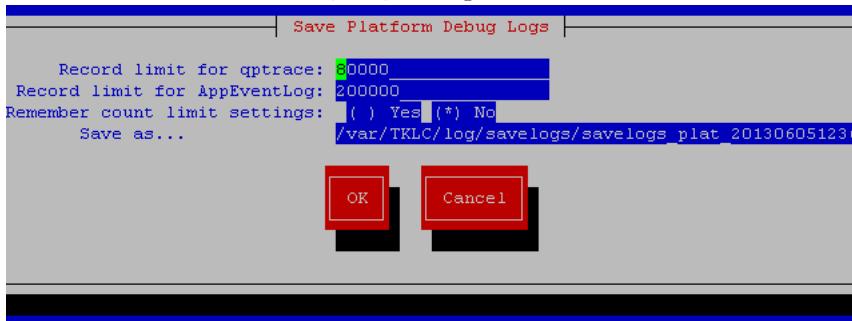
Information saved in the logs includes the current state of all logs, all the configuration files, all the system proc entries, and several miscellaneous files. Output from this process is a single tar/gzip file.

To access this utility, complete the following:

1. Log in to your system as root.
2. At the root prompt, enter the following command:

```
# su - platcfg
```

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



5. Edit variables as needed:
 - *Record limit for qptrace*: 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*: 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*: Specifies whether or not to retain limit setting from previous log.
 - *Save as*: Lists the path and filename of the file being saved.
6. Select **OK** and press **Enter** to save variable changes and generate the tar/gzip file. The file is generated and saved in the specified location.

Chapter 3

Performing Initial Server Configuration

Topics:

- *Initial Configuration.....18*
- *Verifying the Initial Configuration.....19*
- *Verifying the Server Status.....20*
- *Exchanging SSH Key with Mate(s).....20*
- *Configuring Routing on Your Server.....21*
- *Restarting the Application.....24*
- *Configuring Firewall Settings.....25*
- *Displaying Firewall Settings.....28*

This chapter describes how to access the Platform Configuration (Platcfg) utility and configure your Policy Management initial configuration, and then how to verify the configuration. Specifically described:

- Initial Platcfg configuration
- Verifying the configuration
- Verifying the cluster status
- Restarting the application

Initial Configuration

This section describes how to perform the initial configuration on the Configuration Management Platform (CMP), Multimedia Policy Engine (MPE) , Message Distribution Function (MDF) , and Multi-Protocol Routing Agent (MRA) .

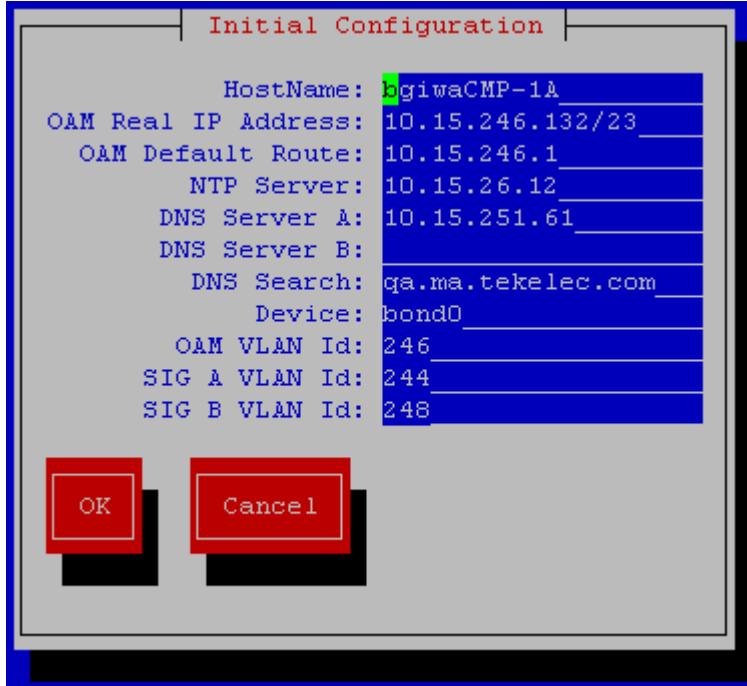
To perform your system initial configuration, complete the following:

1. Log in to your system as root.
2. At the root prompt, enter the following command:

```
# su - platcfg
```

3. Select the **Policy Configuration Menu** and press **Enter**. The following menu is displayed.
4. Select **Perform Initial Configuration** and press **Enter**. The initial Configuration screen is displayed.

For example:



Where (all of the following fields are required, with the exception of the DNS Server and DNS Search which are optional but recommended):

- HostName - the unique hostname for the device being configured.
- OAM Real IP Address - the IP address that is permanently assigned to this device.
- OAM Default Route - the default route of the OAM network.
- NTP Server (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 - is a directive to a DNS resolver (client) to append the specified domain name (suffix) before sending out a DNS query.
- Device - the bond interface of the OAM device. Note that the default value should be used, as changing this value is not supported.
- OAM VLAN Id - the OAM network VLAN Id (only applies to c-Class blades; field doesn't display otherwise).
- SIG A VLAN Id - the Signaling-A network VLAN Id (only applies to c-Class blades; field doesn't display otherwise).
- SIG B VLAN Id - the Signaling-B network VLAN Id (only applies to c-Class blades; field doesn't display otherwise).

5. Enter the configuration and then select **OK**.

NOTE: If you have the optional Ethernet Mezzanine card installed, you will be prompted to enable traffic segregation at this point. Selecting yes, enabling traffic segregation will segregate the SIG-A and SIG-B interfaces onto the optional second pair of 6120XG enclosure switches.

6. When finished, select **OK** to save and apply the configuration. At this point the screen pauses for around a minute. This is normal behavior, while the configuration updates.

Verifying the Initial Configuration

Once you have made your initial configuration settings, from the Policy Configuration Menu, select **Verify Initial Configuration** and press **Enter**. Your initial configuration settings are displayed. For example:

```
Index Table of Contents
Date/Time: 05/11/2011 13:12:00
Hardware Type: ProLiantBL460cG6
HostName="jeffCMP-A"
SIGBVLAN="280"
ServIpAddr="10.15.26.103/23"
DefaultGv="10.15.26.1"
NtpServIpAddr="10.15.26.11"
DNSServer="10.15.29.59"
DNSSearch="qa.ma.teklaes.com ma.teklaes.com teklaes.com"
Device="bond0"
OAMVLAN="260"
SIGAVLAN="240"
NTP Status:
    remote           refid      st t when poll reach  delay  offset  jitter
=====
[Red Buttons]
  Forward  Backward  Top  Bottom  Exit
[Text at bottom]
Use arrow keys to move between options | <Enter> selects
```

Note: Use the Forward and Backward buttons to page up and down through the list.

Verifying the Server Status

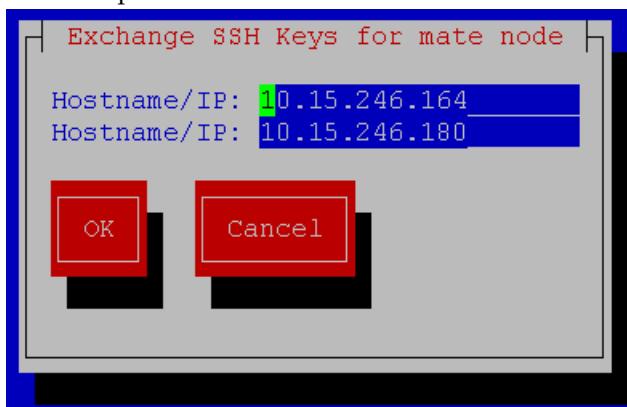
To view the Server Role and Policy Process Management Status, once you have made your initial configuration settings, from the Policy Configuration Menu, select **Verify Server Status** and press **Enter**. Once fully configured, a server will show the server role as Active or Standby (or Spare, if this is an MPE or MRA configured for PCRF Geo Redundancy), based on whether it is the active server in the cluster. It is valid for it to be Unknown during initial configuration, as the cluster hasn't been formed yet. Policy Process Management Status should always be running. For example:



Exchanging SSH Key with Mate(s)

Use this option to allow two or three servers in a cluster to SSH to each other without entering a password. This simplifies back-end operations that rely on SSH. This step is required in the initial configuration of a cluster, but must be done after the topology is defined in the CMP GUI. Note that the SSH keys exchange must be within the cluster (executed from one blade only). To perform the exchange, complete the following:

1. From within the Policy Configuration Menu screen, select the **Exchange SSH Key with Mate** menu item and press **Enter**. A screen similar to the following is displayed:



2. Enter the hostname or IP address of the server's mate(s) and select **OK**.
SSH keys are exchanged between the two servers.
3. The SSH key is exchanged between all servers in the cluster: in a two-server cluster, execute the exchange from one server to the other; in a three-server PCRF Geo-Redundant cluster, execute the exchange from two different servers; in a four-server Geo-Redundant cluster, execute the exchange from three different servers.

Configuring Routing on Your Server

This section describes how to configure routes on your server.

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

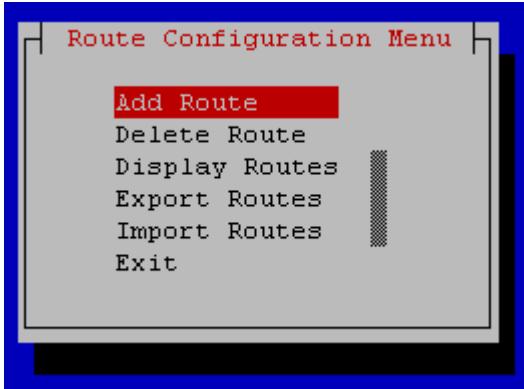
Configuring Routing

To configure routing, complete the following:

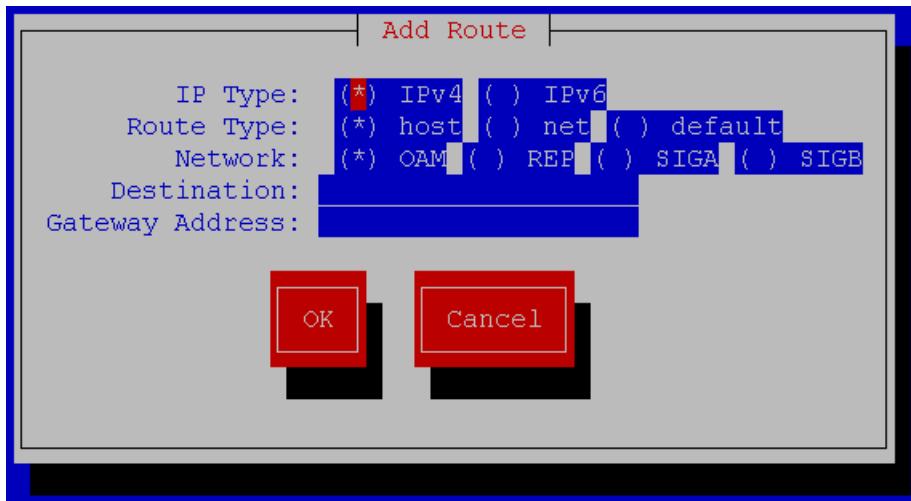
1. Log in to your system as root.
2. At the root prompt, enter the following command:

```
# su - platcfg
```

3. Select the **Policy Configuration Menu**, **Routing Config**, and press **Enter**.



4. Select **Add Route** and press **Enter**. The initial Add Route configuration screen is displayed. For example:



Where:

- **IP Type** - Defines whether this will be an IPv4 or IPv6 route.
- **Route Type** - Defines whether this route will be for a specific destination (Host), a specific network segment (Net), or a default route. Note that 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.
- **Network** - whether this route will be created on the OAM, REP (replication), SIGA, or SIGB interface. Note that the BKUP network is only available on CMP servers with the optional mezzanine card installed.
- **Destination** - the destination IP address.
- **Gateway Address** - the gateway address.

5. Enter the desired information, and when you have finished select **OK** and press **Enter**. You are prompted to continue, press **Enter** again to save changes.

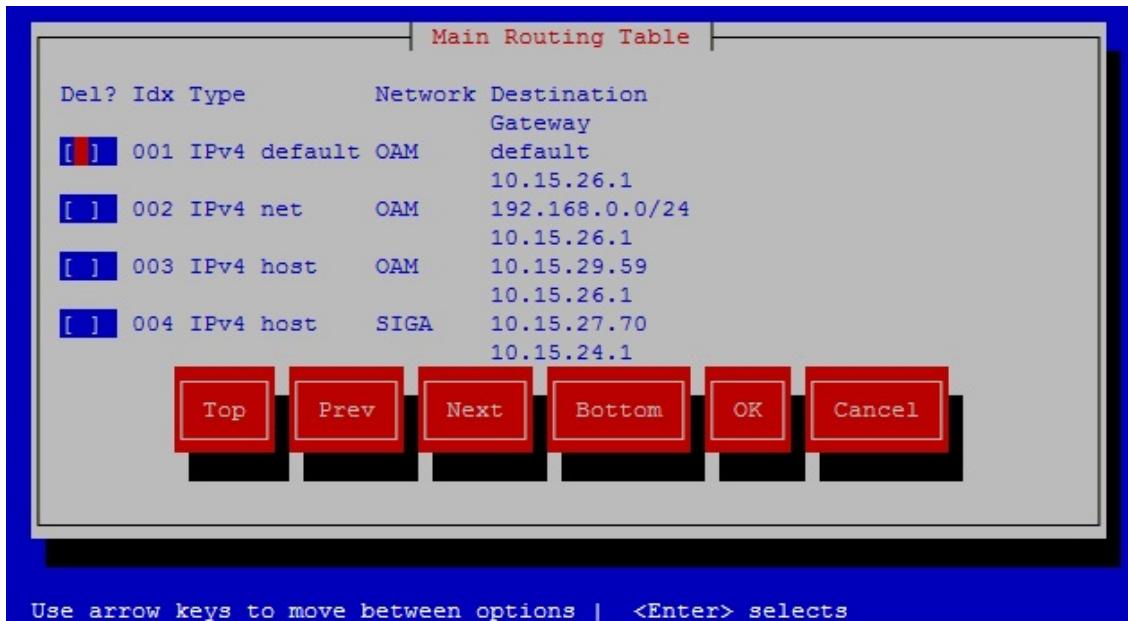
Deleting a Route

To delete an existing route, complete the following:

1. Log in to your system as root.
2. At the root prompt, enter the following command:

```
# su - platcfg
```

3. From the Policy Configuration Menu, select **Routing Config** and press **Enter**.
4. Select **Delete Route** and press **Enter**. The main routing page is displayed. For example:



5. Select the route to be deleted by pressing the space bar, then select **OK** and press **Enter**. More than one route can be deleted at a time. Use the **Top**, **Bottom**, **Prev**, and **Next** buttons to scroll through the list if needed. **Note:** The route is deleted without warning.

Displaying Configure Routes

To display the configured routes, complete the following:

1. Log in to your system as root.
2. At the root prompt, enter the following command:

```
# su - platcfg
```

3. From the Policy Configuration Menu, select **Routing Config** and press **Enter**.
4. Select **Display Routes** and press **Enter**. The configured routes are displayed. For example:

The status of each route displays as either ACT or INACT. ACT means the route is active and currently running. INACT means that the route is saved in configuration, but cannot be activated at this time. The reason for an inactive route may be that the 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), or it may mean that a route has been misconfigured, and the gateway IP is not on the same subnet as the IP address on the interface.

Exporting a Route

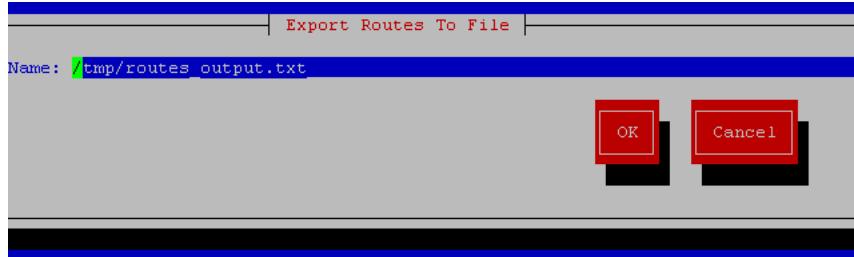
To export all existing routes, complete the following:

1. Log in to your system as root.

2. At the root prompt, enter the following command:

```
# su - platcfg
```

3. From the Policy Configuration Menu, select **Routing Config** and press **Enter**.
4. Select **Export Route** and press **Enter**. The export routing page is displayed. For example:



5. Specify the location and filename to which routes are to be exported, then select **OK** and press **Enter**.
Routes are exported to the specified directory and filename.

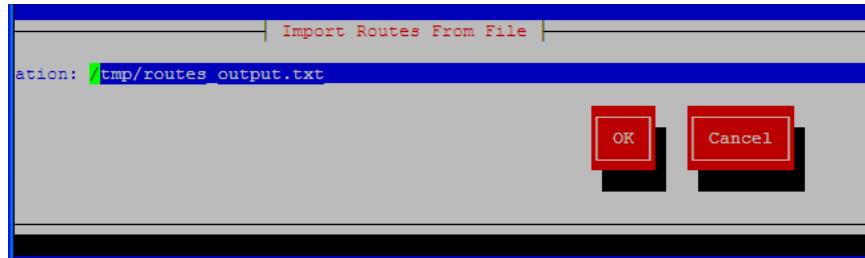
Importing a Route

To import existing routes into the routing configuration, complete the following:

1. Log in to your system as root.
2. At the root prompt, enter the following command:

```
# su - platcfg
```

3. From the Policy Configuration Menu, select **Routing Config** and press **Enter**.
4. Select **Import Routes** and press **Enter**. The import routes page is displayed. For example:

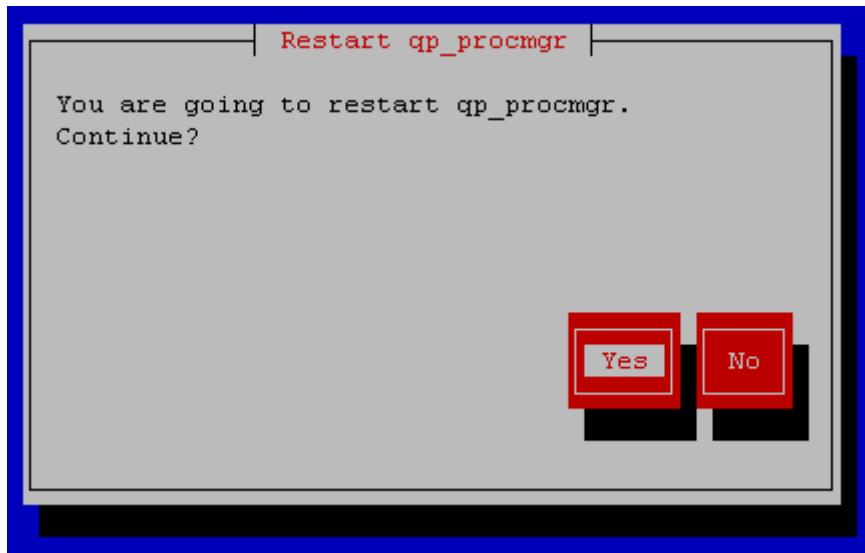


5. Specify the directory and filename from which routes are to be imported, then select **OK** and press **Enter**.
Routes are imported into the routing configuration from the specified directory and filename.

Restarting the Application

To restart your application, from the Policy Configuration Menu:

1. Select **Restart Application** and press **Enter**. You are prompted to continue. For example:



This action restarts qp_procmgr, which controls all Policy Management specific processes, and the entire application is restarted. It does *not* restart HA or database software, although the failure of the application will trigger an HA failover.

Configuring Firewall Settings

Note: When configuring firewall settings, be sure to use the menu item **Save and Apply Configuration**, as it is the only way changes will be saved. The "Save and Apply" action takes your edits, commits them to the firewall config files, and restarts the firewall. If you leave this menu before initiating "Save and Apply" your changes will be lost.

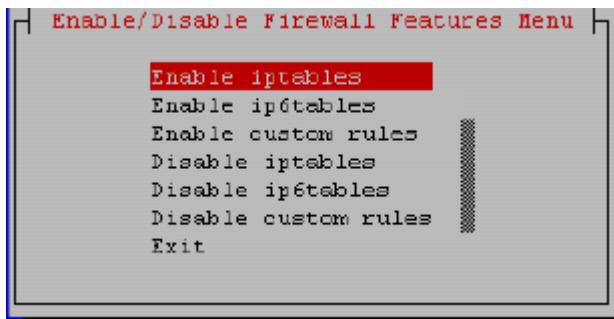
To configure firewall settings on the server, that restrict access to non-standard ports, complete the following.

Note: In the following process, the term "all" indicates open access to any interface (For example: OAM, SIG-A, and SIG-B).

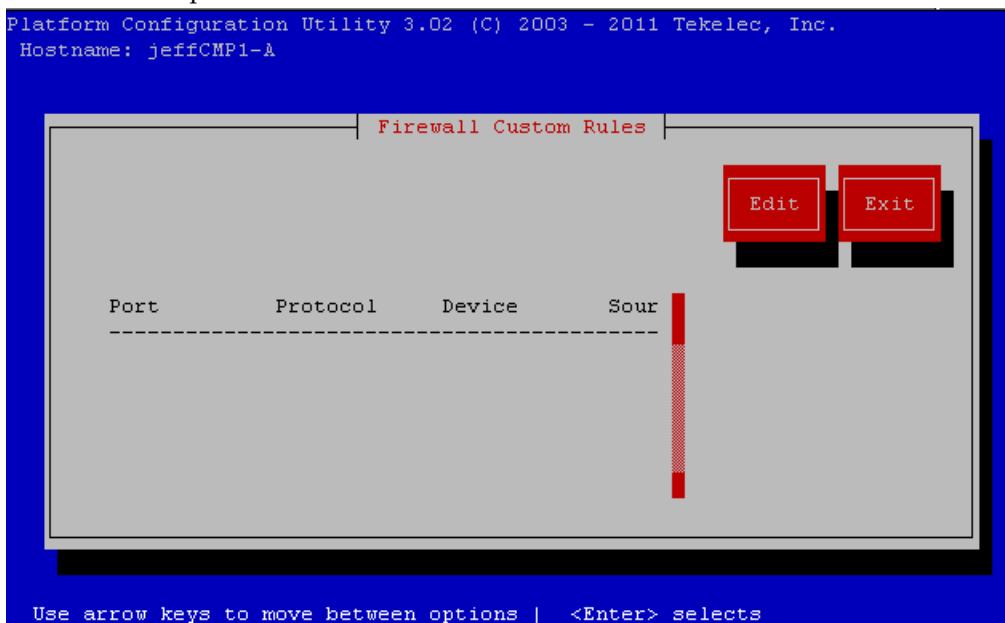
1. Log in to your system as root.
2. At the root prompt, enter the following command:

```
# su - platcfg
```

3. Select the **Policy Configuration Menu**, **Firewall**, and press **Enter**.
4. Select **Customize Firewall** and press **Enter**.



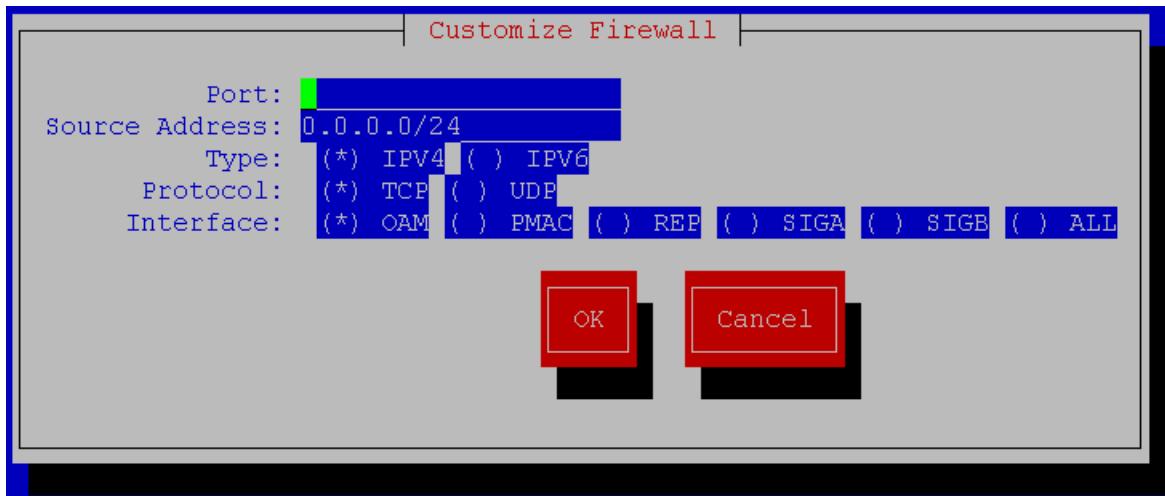
5. Select **Edit** and press **Enter**.



6. Select **Add** or **Edit** (if the rule already exists) and press **Enter**.



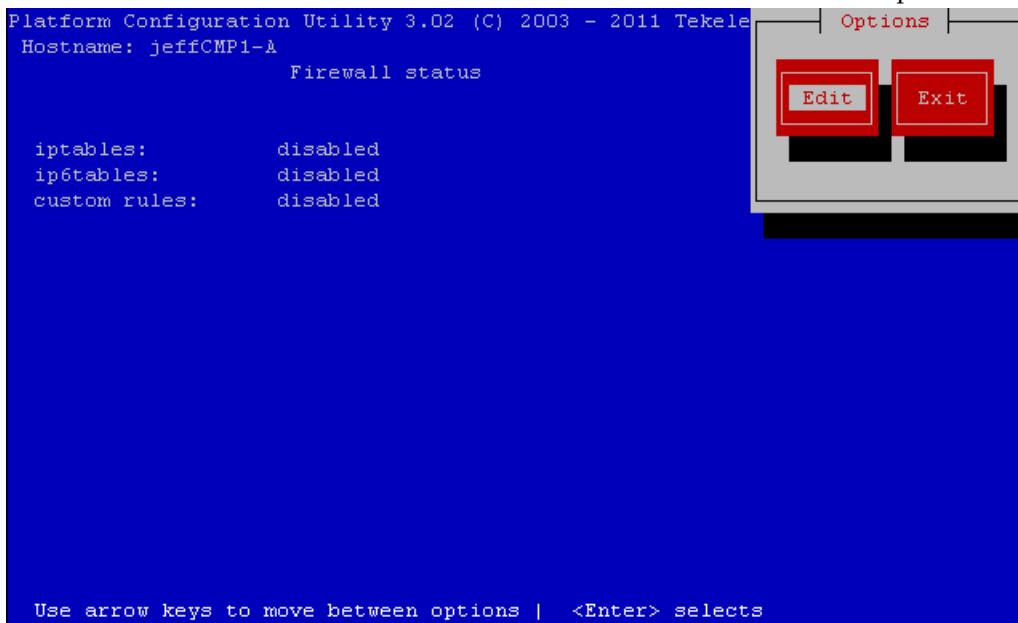
7. Enter the desired information, when finished, select **OK** and press **Enter**.



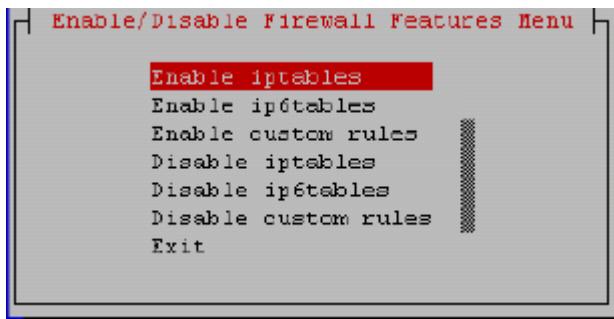
If configuring a CMP with the optional Ethernet mezzanine card, an additional interface appears called **BKUP**. This interface is used as a dedicated interface for performing remote archive activities for CMP backup operations. The BKUP will be included if **ALL** is selected.

If configuring an MPE or MRA, and replication is enabled, an additional interface appears called **REP**.

8. Return to the **Firewall Configuration Menu**, select **Enable/Disable Firewall** and press **Enter**. Be sure to select **Save and Apply Configuration** to save this change.
9. Select **Edit** to define which IPv4 and IPv6 firewalls to enable or disable and press **Enter**.



10. Select the desired interfaces and press **Enter**. The firewall is disabled by default. By enabling iptables or ip6tables, you are turning on the firewall with a default set of rules (don't forget to save and apply!). These default rules are enough to allow the product to function as needed, however it may be considered desirable to open up additional ports. To do this you must enable the Custom rules. When you add or remove a firewall rule, you are making changes to this custom rule set (the default firewall rules cannot be changed).

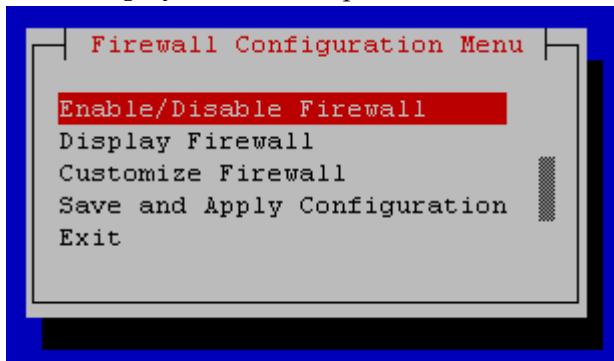


11. You are prompted to continue, select **Yes** and press **Enter**. Be sure to select **Save and Apply Configuration** to save this change.

Displaying Firewall Settings

To display current firewall settings, complete the following:

- From the **Policy Configuration Menu**, select **Firewall** and press **Enter**.
- Select **Display Firewall** and press **Enter**.

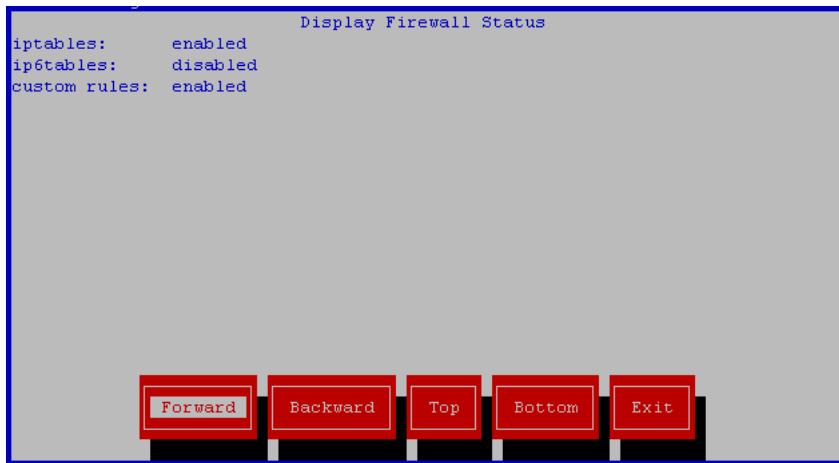


- Select the desired Firewall feature and press **Enter**.



This is an example of the Display Firewall Status screen:

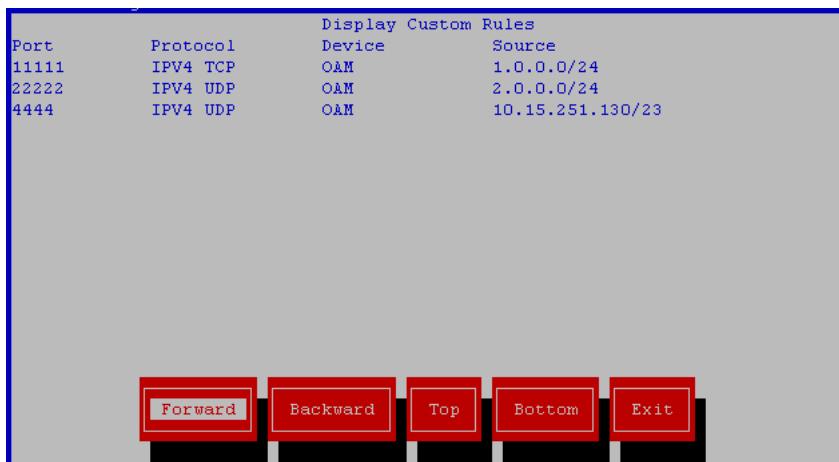
Performing Initial Server Configuration



This is an example of the Display Factory Rules screen:



And this is an example of the Display Custom Rules screen:



Chapter 4

Managing Certificates

Topics:

- *Managing SSL Security Certificates.....31*
- *Using a Local Certificate to Establish a Secure HTTP (https) Web-Browser Session.....33*
- *Establishing a Secure Connection Between a CMP System and an MPE/MRA/MDF Device.....34*
- *Creating a Third-party CA Signed Certificate...37*

Normal web traffic is sent unencrypted over the Internet, which allows anyone with access to the right tools to snoop and view all of that traffic and data. This can lead to problems, especially where security and privacy is necessary. To combat this, the Secure Socket Layer (SSL) is used to encrypt the data stream between the web server and the web client (the browser).

Each SSL Certificate consists of a public key and a private key. The public key is shared with other SSL clients and is used to set up secure sessions, while the private key never leaves the server. When a Web browser points to a secured domain, an SSL handshake authenticates the server and the client.

This chapter describes how to access the Platform Configuration (platcfg) utility to manage SSL security certificates, which allow two systems to interact with a high level of security.

Within this chapter, the following terms are used:

- Local certificate - The certificate created on the local system and then exported to the peer system.
- Peer certificate - The certificate created on the peer system that is imported by the local system.
- Private/Public Key - As previously stated, the public key is used to encrypt information and the private key is used to decipher it.

The information and configuration steps that are provided in this chapter are primarily implemented within the platcfg utility. However, Secure Connections must be enabled within the CMP Graphical User Interface (GUI) for the MPE devices used in the certificate exchange.

Managing SSL Security Certificates

Creating a Self-Signed Certificate

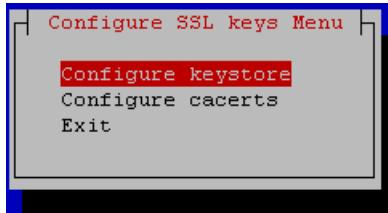
Certificate creation is performed on the local server, and depending on your implementation, on the remote server, as well. This local certificate acts as a Private key for the local server.

To create a self-signed key, using the default value of “tomcat” or another value, complete the following:

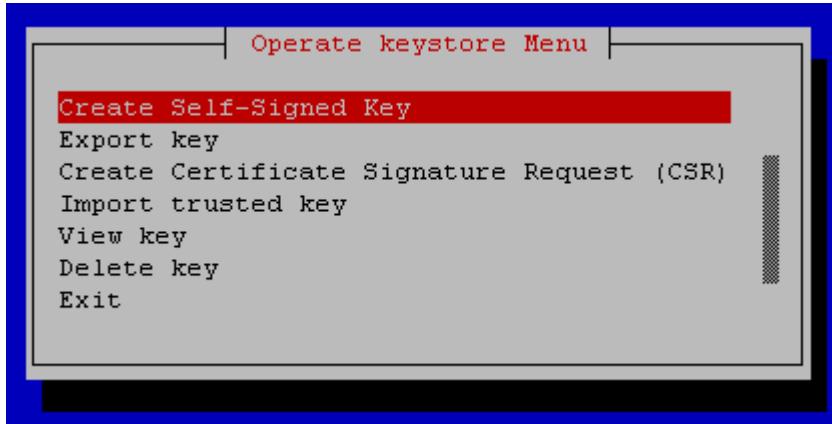
1. Log in to your server as root.
2. At the root prompt, enter the following command:

```
# su - platcfg
```

3. Select the **Policy Configuration Menu, SSL Key Configuration** and press **Enter**.
4. Select **SSL Key Configure** and press **Enter**.

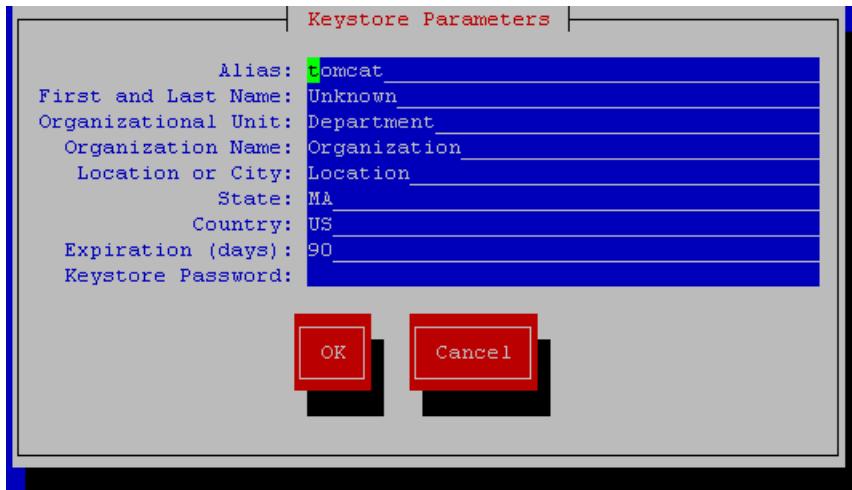


5. Select **Create Self-Signed Key** and press **Enter**.



6. Enter the desired keystore information and then click **OK**. If you desire to change this alias name, the default alias “tomcat” will need to be deleted to ensure that the correct SSL certificate is used.

Note: To avoid confusion when creating the certificate, use the default alias “tomcat”. Also, the default password ‘changeit’ must be used throughout the creation process or the certificate will not work.



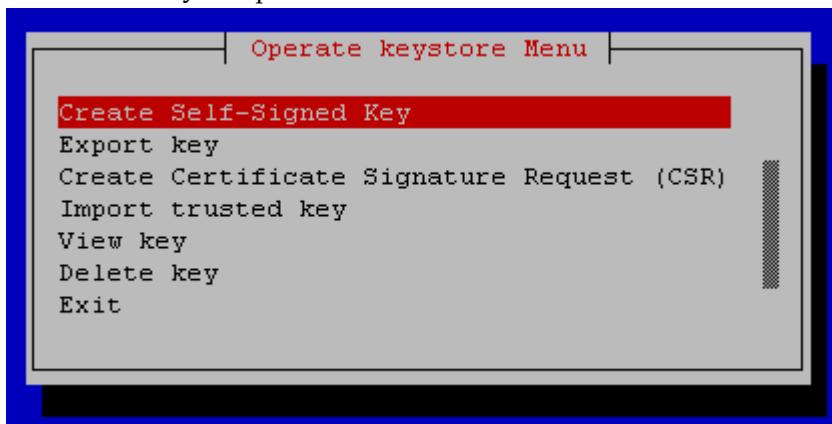
- When you have finished, select **OK** and press **Enter**.

Verifying the Generated Certificate

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

To verify the SSL Certificate's attributes, complete the following:

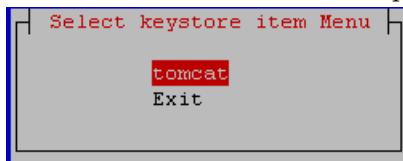
- From the **Policy Configuration Menu**, **SSL Key Configuration** and press **Enter**.
- Select **Configure Keystore** and press **Enter**.
- Select **OK** to accept the keystore destination, and press **Enter**.
- Select **View key** and press **Enter**.



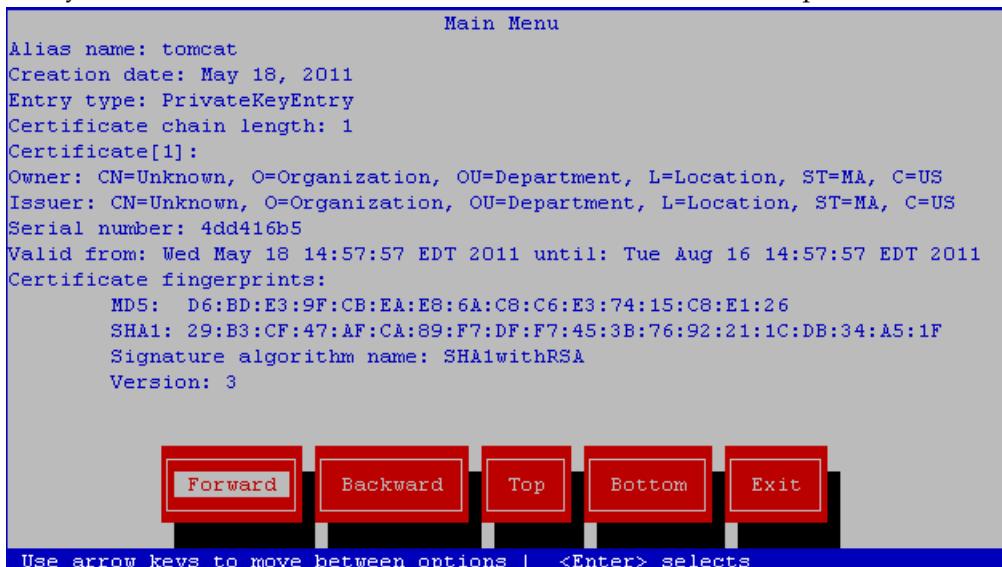
- Enter the password (changeit), select **OK** and press **Enter**.



6. Select the desired certificate and press **Enter**.



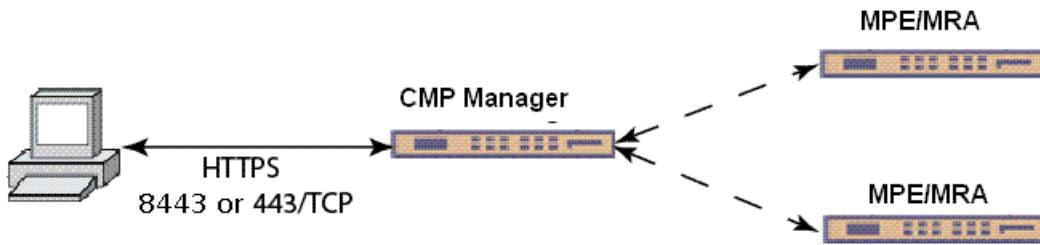
7. Verify all certificate information and when finished, select **Exit** and press **Enter**. For example:



From the previous display, the key portions of the certificate are the Alias name, Owner, and issuer, as these attributes are exported and imported to the other server to establish the secure HTTP session.

Using a Local Certificate to Establish a Secure HTTP (https) Web-Browser Session

To ensure a safe and secure TCP connection between an end-user (PC Web-browser) and the CMP system, an https session can be created between the two by passing a predefined certificate to the end-user. Once the end-user accepts the certificate, the https session is created.



Also, Web browsers may behave differently, based on their configuration. Be sure to understand your browser settings before using SSL certificates.

To force end-users to establish an https session with the CMP system, complete the following steps:

1. Create the local certificate as described in [Creating a Self-Signed Certificate](#).
2. Clear firewall settings.
3. Once the local certificate has been created, the end-user will need to accept the certificate before access to the MPE/MRA is granted.

Establishing a Secure Connection Between a CMP System and an MPE/MRA/MDF Device

Note: Procedures used in this chapter may require the rebooting of one or more blades. Subsequently, for HA to operate correctly in a clustered system, the active blade of the cluster must not be rebooted unless the cluster is in the "online" state. Before rebooting any blade, check cluster status using the CMP Manager Graphical User Interface. If a cluster is labeled Degraded, but the blade detail does not show any failed or disconnected equipment, the blade is performing a database synchronization operation and until the synchronization process has completed, the standby blade cannot perform as the active blade.

Also, when a new certificate is configured, the synchronization will cause HA on the standby blade to restart.

It should be noted that 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 establish a secure connection between a CMP system and an MPE/MRA server, both the CMP system and the MPE/MRA/MDF server must exchange certificates. The following figure provides an example of this:

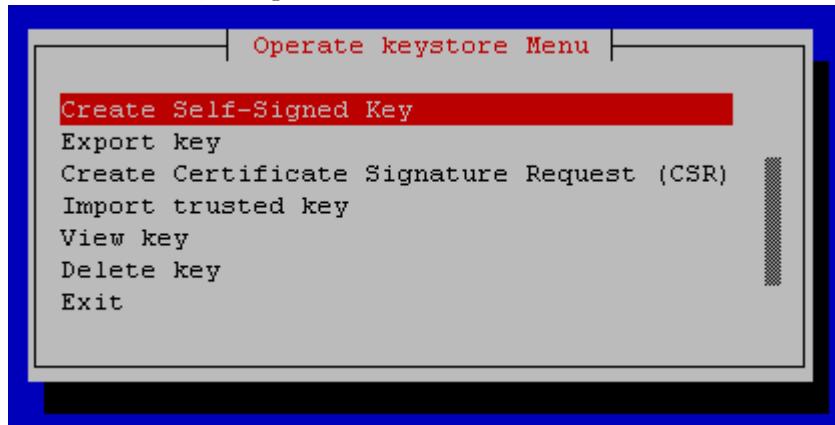
Within this figure, the SSL Certificate is shared within the cluster, with the following certificate exchange occurring:

1. The CMP system creates a local certificate and exports the certificate to the MPE/MRA/MDF server.
2. The MPE/MRA/MDF server imports the peer certificate (local certificate created by the CMP system) into its trust store.
3. The MPE/MRA/MDF 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 MPE/MRA/MDF server) into its trust store.

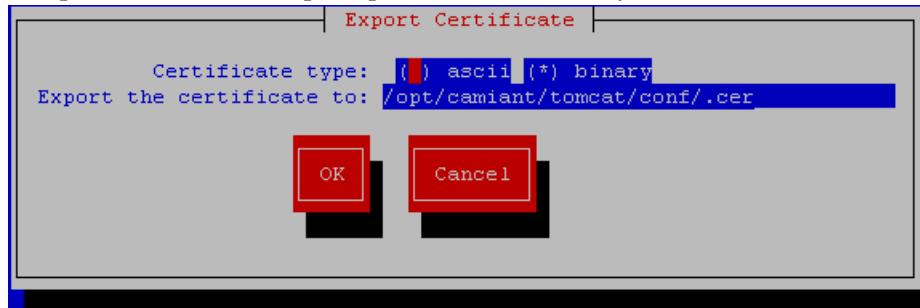
Exporting the Local Certificate to the MPE/MRA/MDF Servers

To establish a secure connection between the CMP system and an MPE/MRA/MDF server, complete the following:

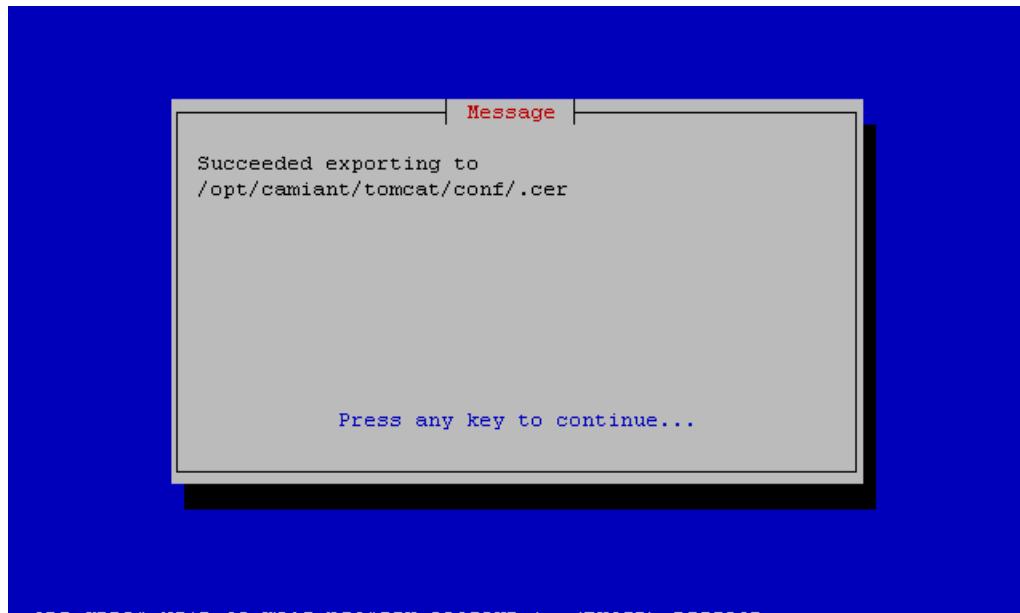
1. Create the local certificate on each server or cluster, as described in [Creating a Self-Signed Certificate](#).
2. From within the Platcfg utility, complete the following:
 - a) From the **Policy Configuration Menu**, select **SSL Key Configuration** and press **Enter**.
 - b) Select **Configure Keystore** and press **Enter**.
 - c) Select **OK** to accept the keystore destination, and press **Enter**.
 - d) Select **Export key** and press **Enter**.



- e) Enter the Keystore Password (changeit), select **OK** and press **Enter**.
- f) Press **Enter** to accept the alias "tomcat" or enter the alias previously created for the certificate and press **Enter**. You are prompted to create a binary or ascii certificate.



- g) Select **OK** and press **Enter** to accept the default value of "binary". The certificate is exported.

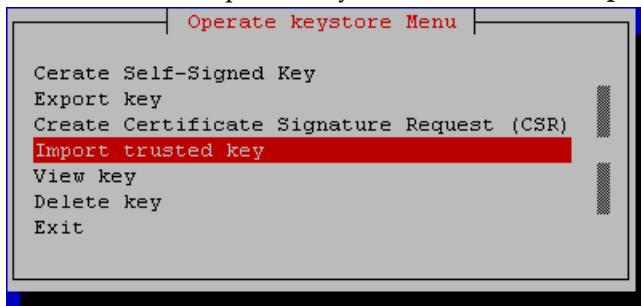


Importing the Peer Certificate

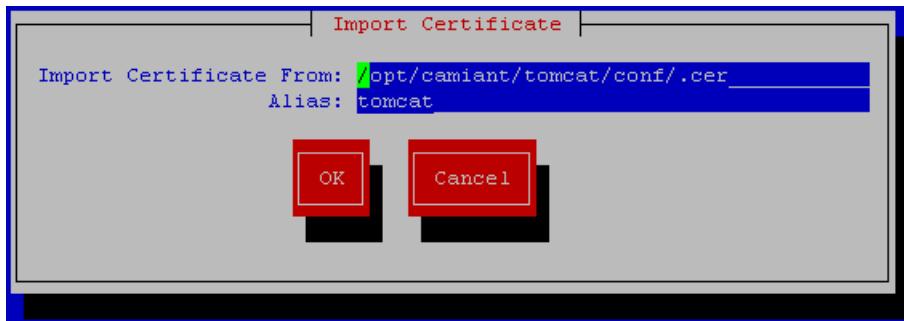
Once you have exported the local certificate, return to the Operate Keystore Menu item of the platcfg utility and import the peer certificate (this is the certificate that was exported from the other system).

Note: The process that follows is used to import a certificate to the peer machine. This includes certificates generated by other servers including certificates signed by a third party or similar.

1. From within the Operate Keystore Menu, select **Import trusted key** and press **Enter**.



2. Enter the **Keystore Password** (changeit), select **OK** and press **Enter**.
3. You are prompted for the location and alias for the certificate.



4. Enter the **Alias** for certificate (tomcat), select **OK** and press **Enter**. You are then presented with the certificate data for verification. To avoid confusion, though they may be different, ensure that the "Owner" and "Issuer" names used for the certificate match that of the certificate it is being created on.
5. If the certificate data is correct, select **OK** and press **Enter**.
6. Log in to the CMP system, enter the desired Policy Server, and click on the **Secure Connections** checkbox, located under the Policy Server System tab. Refer to the *CMP User Guide* to do this.

Creating a Third-party CA Signed Certificate

Note: This section assumes that no SSL certificates have previously been generated on or imported into the servers. If there are any other pre-existing certificates on the system (besides the default tomcat certificate), please consult with Technical Support to determine its use and importance. Also, read this method in its entirety before starting the operations presented herein.

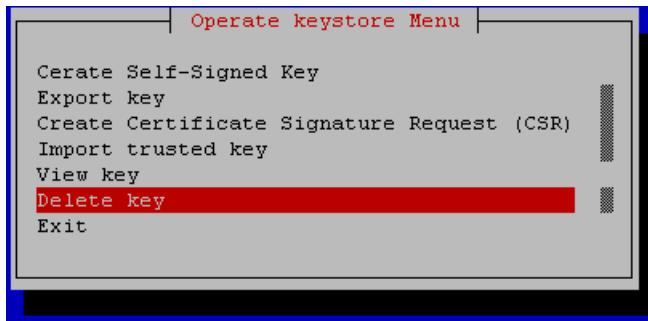
Third-party certificates are implemented as follows:

- Remove pre-existing local certificate
- Generate local certificate, export for signing, and re-import
- Import the third-party peer certificate
- Synchronize and reboot Policy Management cluster

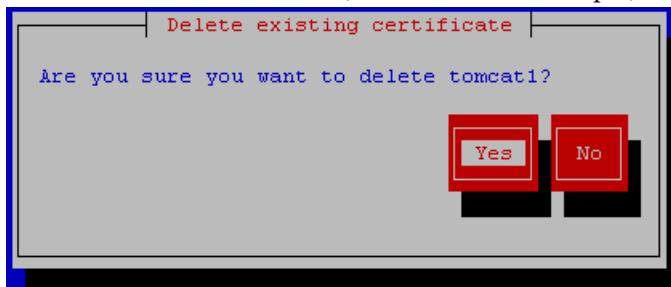
Remove the Pre-existing Local Certificate

Typically on most MPE/MRA installations, there is a pre-existing certificate in the store that has an alias name of "tomcat". This certificate needs to be removed before continuing with any of the other required certificate generation, or import/export functions. To do this:

1. From the **Policy Configuration Menu**, select **SSL Key Configuration** and press **Enter**.
2. Select **Configure Keystore** and press **Enter**.
3. Select **OK** to accept the keystore destination, and press **Enter**.



4. Select **Delete key** and press **Enter**.
5. Enter the Keystore Password (changeit), select **OK** and press **Enter**.
6. Select the desired certificate (tomcat1 in this example) and press **Enter**.



7. You are prompted to delete the selected certificate. Select **Yes** to delete the certificate or **No** to leave it as is, and then press **Enter**.

You are now ready to generate the local certificate, export it for signing, and then re-import it.

Generating a Local Certificate, Exporting for Signing, and Re-importing

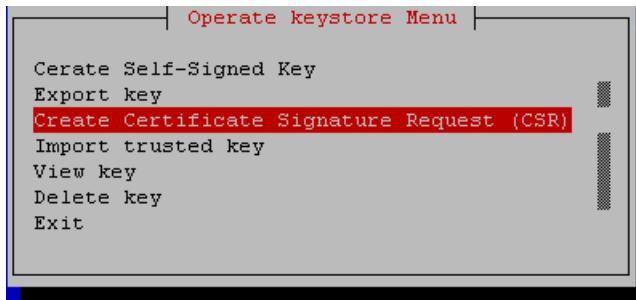
To generate the third-party signed local certificate you need to complete the following:

- Generate a certificate signature request
- Export certificate from the system
- Re-import the third-party signed certificates
- Verify that the certificates are stored

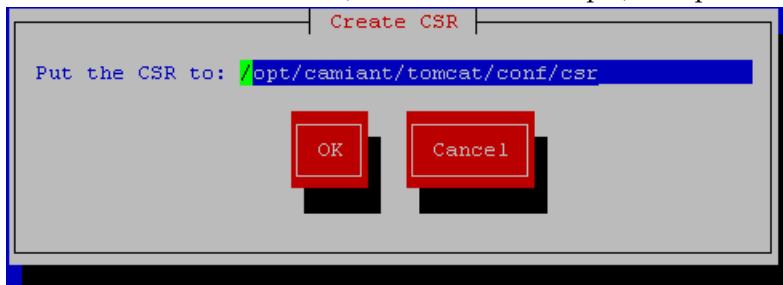
Generate a Certificate Signature Request

To do this:

1. From the Policy Configuration Menu, select **SSL Key Configuration** and press **Enter**.
2. Select **Configure Keystore** and press **Enter**.
3. Select **OK** to accept the keystore destination, and press **Enter**.

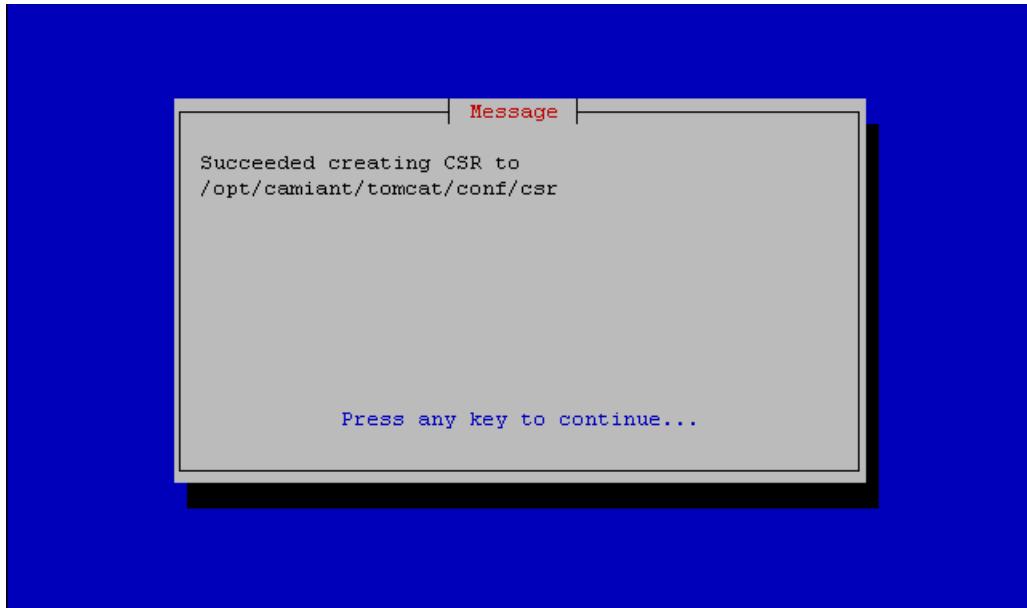


4. Select **Create Certificate Signature Request (CSR)** and press **Enter**.
5. Enter the Keystore Password (changeit), select **OK** and press **Enter**.
6. Select the desired certificate (tomcat, in this example) to export for signature and press **Enter**.



Note: The alias (certificate) value will be used later for re-importing the certificate after signing by a third party. Use a name 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 as not to expire before any peer certificates. A value preventing expiration before 2019 would be advisable.

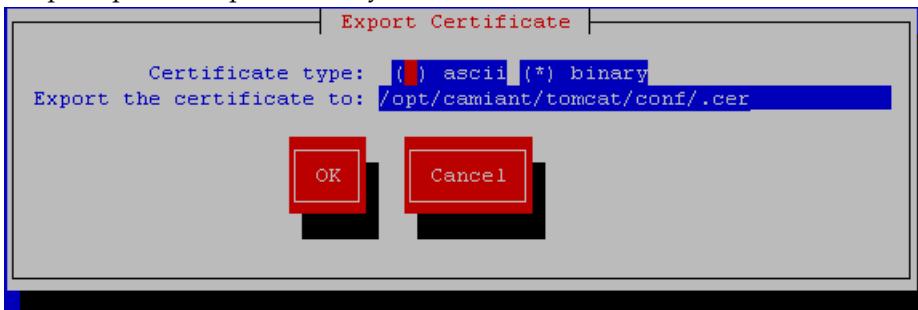
7. Select **OK** to accept the keystore destination, and press **Enter**.



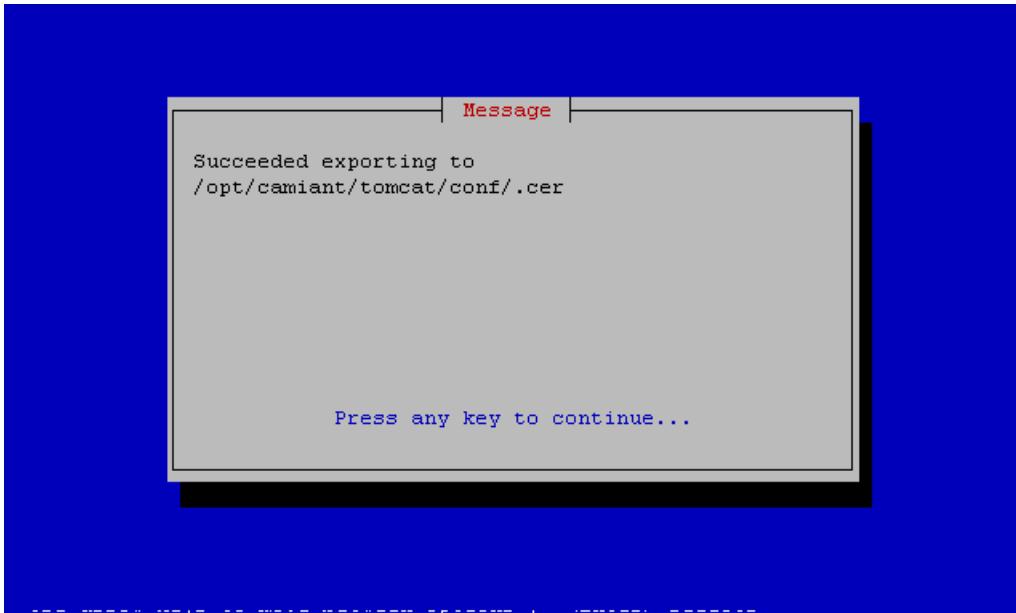
Export the Certificate Signature Request from the System

To export a locally generated certificate signature request:

1. From the Policy Configuration Menu, select **SSL Key Configuration** and press **Enter**.
2. Select **Configure Keystore** and press **Enter**.
3. Select **OK** to accept the keystore destination, and press **Enter**.
4. Select **Export key** and press **Enter**.
5. Enter the Keystore Password (changeit), select **OK** and press **Enter**.
6. Select the desired certificate (tomcat, in this example) to export for signature and press **Enter**. You are prompted to export a binary or ascii certificate.



7. Select **OK** and press **Enter** to accept the default value of "binary". The certificate is exported.



After the certificate file is exported, provide it to the third party who will be signing and returning the certificate request.

Re-import the Third-party Signed Certificates

Once the certificate has been signed by the third party, two certificate files should be returned by them for importing into the MPE/MRA system. One of these files will be a signed, local client certificate,

and the other a certificate authority (CA), peer certificate. Both of these need to be imported into the system for proper SSL communication.

Note: It may be necessary to edit the returned files to remove extraneous debugging-type information in the certificate. This must be accomplished using Linux-based editor to preserve line termination style. The only contents that should be in the files, are the blocks of data headlined by “----BEGIN CERTIFICATE----” and concluded by “----END CERTIFICATE----”. All other text above or below these blocks should be removed.

In addition, to remove extra text in the certificate files, a further modification needs to be made to the signed local client certificate. In order for the MPE/MRA to be able to import this local certificate successfully, the CA certificate needs to be merged into this file as well. To do this, the BEGIN/END certificate text block from the CA cert needs to be copied and then pasted into the local client certificate below its BEGIN/END certificate text block. The final result will be the original local client certificate text block immediately followed by the certificate text block of the CA cert 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 MPE/MRA in advance, or store them somewhere on the network accessible via SCP. They can now be imported back into the system for use in securing the communication channel with the third-party system. To do this:

1. From the **Policy Configuration Menu**, select **SSL Key Configuration** and press **Enter**.
2. Select **Configure Keystore** and press **Enter**.
3. Select **OK** to accept the keystore destination, and press **Enter**.
4. Select **Import trusted key** and press **Enter**.
5. Enter the Keystore Password (changeit), select **OK** and press **Enter**. You are prompted for the location of the certificate to be imported.
6. 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.

You are then presented with the certificate data for verification. To avoid confusion, though they may be different, ensure that the “Owner” and “Issuer” names used for the certificate matches the hostname 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.

Import the Third-party Peer Certificates

In addition to the certificates that were imported in the previous section, it is also necessary to import a pair of peer certificates from the third party to connect to and communicate with their server (versus their client communicating with the CMP/MPE/MRA servers).

The third party will provide a set of new client and CA certificate files, both of which will be imported to the CMP/MPE/MRA system as peer certificates. This process will be almost identical to that which was followed previously.

Note: It may be necessary to edit the returned files to remove extraneous debugging-type information in the certificate. The only contents that should be in the files, are the blocks of data headlined by “----BEGIN CERTIFICATE----” and concluded by “----END CERTIFICATE----”. All other text above or below these blocks should be removed.

To import the peer certificates, either copy these certificate files to the CMP/MPE/MRA in advance, or store them somewhere on the network accessible via SCP. To import the certificate:

1. From the Policy Configuration Menu, select **SSL Key Configuration** and press **Enter**.
2. Select **Configure cacerts** and press **Enter**.
3. Select **OK** to accept the keystore destination and press **Enter**.
4. Select **Import trusted key** and press **Enter**.
5. Enter the Keystore Password (changeit), select **OK** and press **Enter**. You are prompted for the location of the certificate to be imported.
6. 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.

Synchronize and Reboot the Cluster

In order for the new certificates to take effect, all blades of the cluster must be synchronized so they have the set of certificates necessary, and then also rebooted for the certificates to take effect on the MPE/MRA system. To do this, refer to the *CMP User Guide*.

Chapter 5

Synchronizing Files

Topics:

- *Managing Cluster Sync Configurations.....44*
- *Showing Sync Configuration.....48*
- *Showing Sync Destination.....49*
- *Showing Sync Status.....49*
- *Performing File Synchronization.....50*

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

Files should be synchronized using Cluster File Sync after any of the following are configured:

- Routes (Routing Config)
- Firewall (Firewall)

Functionality described includes:

- Cluster Sync Config
- Show Sync Config
- Show Sync Destination
- Show Sync Status
- Start Synchronizing

Managing Cluster Sync Configurations

Use the Cluster Sync Config menu to manage cluster sync configurations. Functionality available on this menu includes:

- Read destination from COMCOL
- Add Sync File
- Delete Sync File

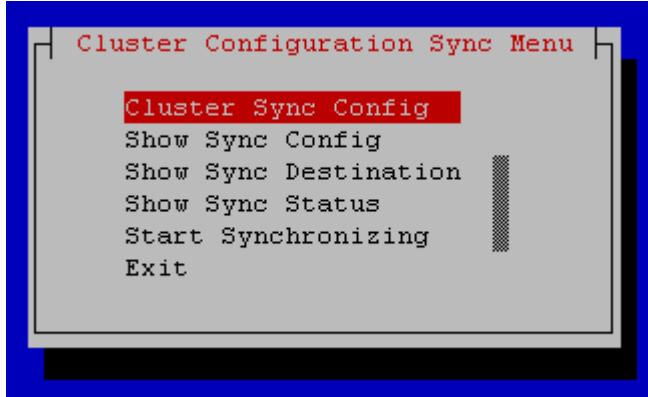
Reading Destination from COMCOL

Select this option to read the cluster sync destination from COMCOL. To perform this step, complete the following:

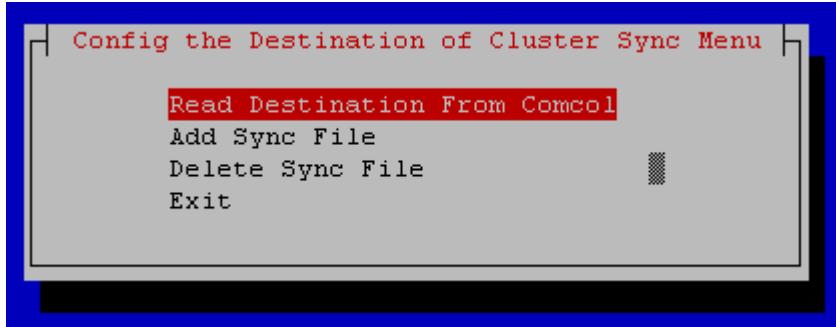
1. Log in to your system as root.
2. At the root prompt, enter the following command:

```
# su - platcfg
```

3. Select the Policy Configuration Menu, and press **Enter**.
4. Select **Cluster File Sync** and press **Enter**. The Cluster Configuration Sync Menu is displayed.



5. Select **Cluster Sync Config** and press **Enter**.



The Config Destination of Cluster Sync menu is displayed.

6. Select **Read Destination from Comcol** and press **Enter**.

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

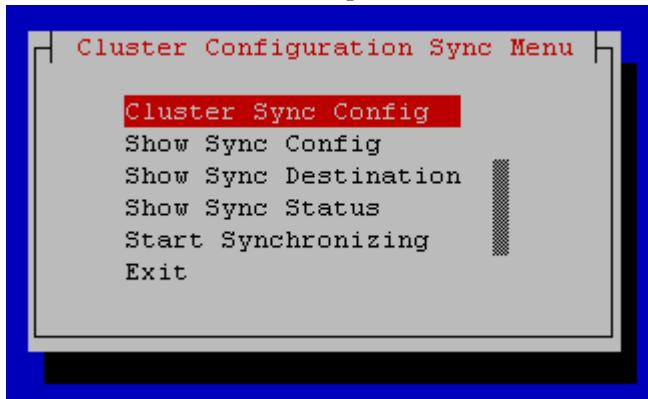
Adding a Sync File

To create a new cluster sync configuration file, complete the following:

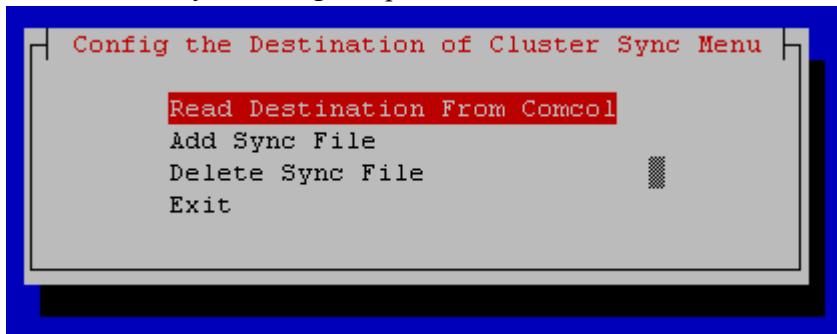
1. Log in to your system as root.
2. At the root prompt, enter the following command:

```
# su - platcfg
```

3. Select the **Policy Configuration Menu**, and press **Enter**.
4. Select **Cluster File Sync** and press **Enter**. The Cluster Configuration Sync Menu is displayed.

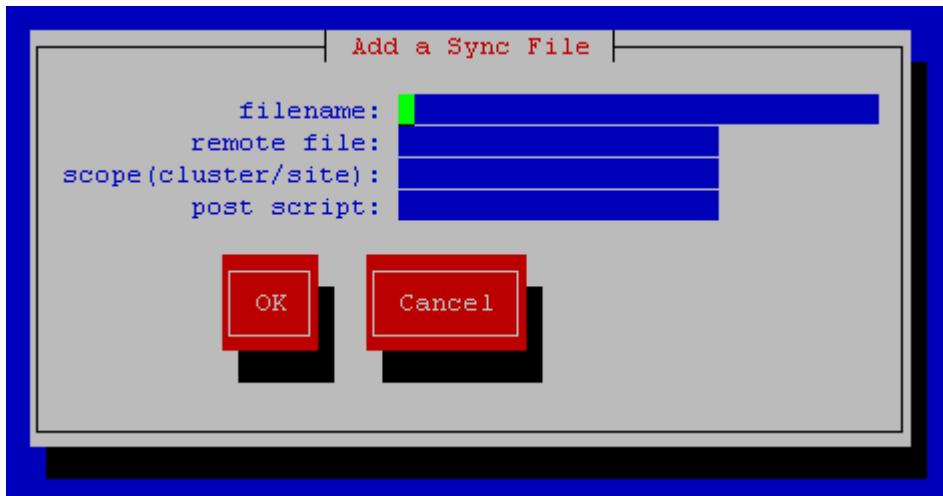


5. Select **Cluster Sync Config** and press **Enter**.



The Config Destination of Cluster Sync menu is displayed.

6. Select **Add Sync File** and press **Enter**.



The Add a Sync File screen is displayed.

7. Enter data into the fields, as needed.

1. **Filename**

2. **Remote file**

3. **Scope (cluster/site)** - Scope lists where each file is being synced: Site indicates just to servers at the local site, Cluster indicates to all servers at all sites. Files that need to be in sync at all sites (like certificates) should be listed as Cluster; IP-related files that may not be valid at other sites (like firewall and static routes) should be listed as Site.

4. **Post script**

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

The new cluster sync configuration is saved.

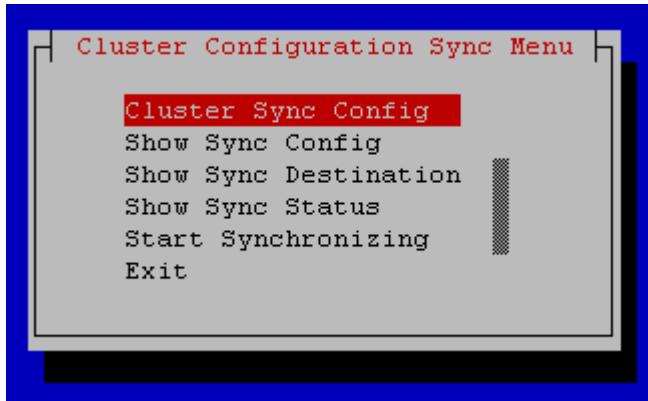
Deleting a Sync File

To delete an existing cluster sync configuration file, complete the following:

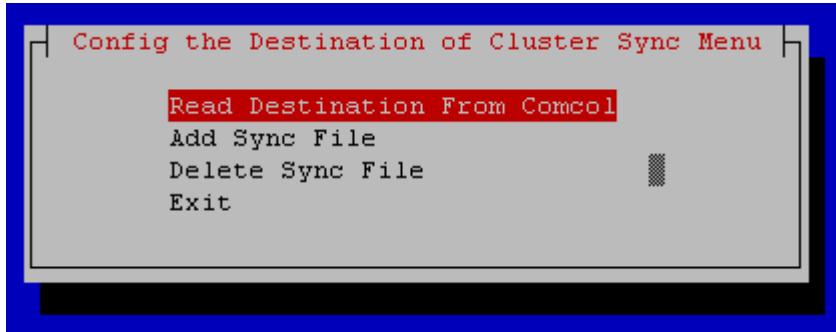
1. Log in to your system as root.
2. At the root prompt, enter the following command:

```
# su - platcfg
```

3. Select the **Policy Configuration Menu**, and press **Enter**.
4. Select **Cluster File Sync** and press **Enter**. The Cluster Configuration Sync Menu is displayed.

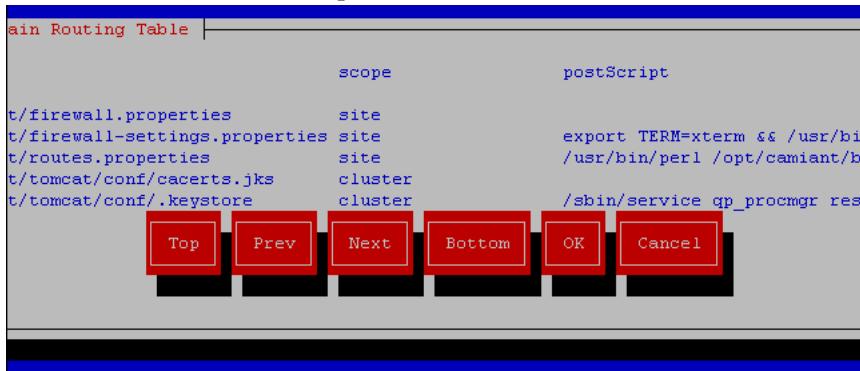


5. Select **Cluster Sync Config** and press **Enter**.



The Config Destination of Cluster Sync menu is displayed.

6. Select **Delete Sync File** and press **Enter**.



The Main Routing Table screen is displayed.

7. Select the cluster sync configuration file to delete from the list, select **OK**, and press **Enter**. The selected cluster sync configuration is deleted.

Showing Sync Configuration

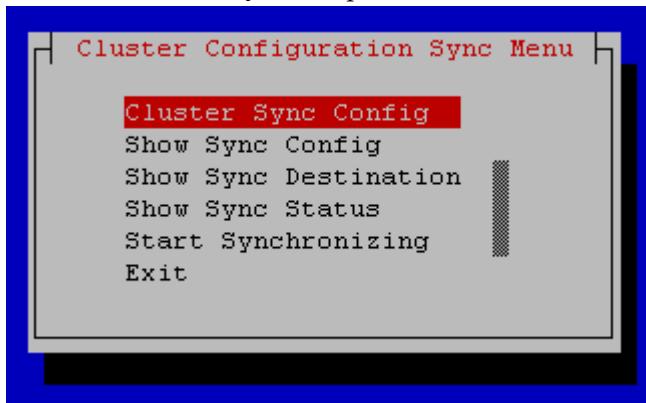
Use this option to view where files are synced; this is useful when georedundancy is implemented. The Scope column lists where each file is being synced: Site indicates just to servers at the local site, Cluster indicates to all servers at all sites. Files that need to be in sync at all sites (like certificates) are listed as Cluster; IP-related files that may not be valid at other sites (like firewall and static routes) are listed as Site.

To display cluster sync filenames and their scope, complete the following:

1. Log in to your system as root.
2. At the root prompt, enter the following command:

```
# su - platcfg
```

3. Select the Policy Configuration Menu, and press **Enter**.
4. Select **Cluster File Sync** and press **Enter**. The Cluster Configuration Sync Menu is displayed.



5. Select **Show Sync Config** and press **Enter**.

The Sync File			
Filename	Scope	PostScript	
/etc/camiant/firewall.properties	site		
/etc/camiant/firewall-settings.properties	site	export TERM=xterm	
@@ /usr/bin/perl /opt/camiant/bin/applyFirewallRules.pl 2>&1 > /dev/null			
/etc/camiant/routes.properties	site	/usr/bin/perl	
/opt/camiant/bin/fixRoute.pl --quiet 2>&1 > /dev/null			
/opt/camiant/tomcat/conf/cacerts.jks	cluster		
/opt/camiant/tomcat/conf/.keystore	cluster	/sbin/service	
qp_procmgr restart			

At the bottom of the screen are five red buttons labeled 'Forward', 'Backward', 'Top', 'Bottom', and 'Exit'.

The Sync File screen is displayed.

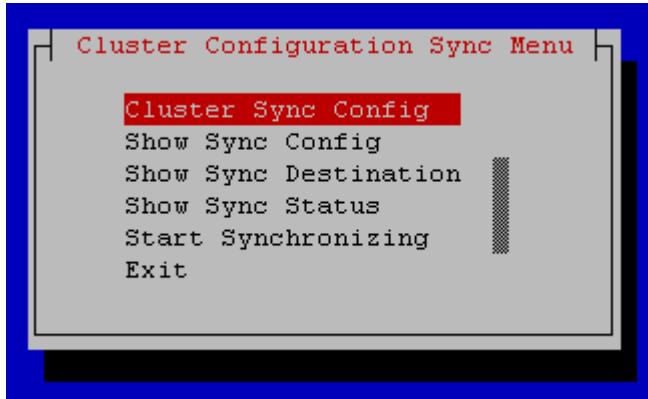
Showing Sync Destination

To display cluster sync destinations (hostname, IP address, and Location), complete the following:

1. Log in to your system as root.
2. At the root prompt, enter the following command:

```
# su - platcfg
```

3. Select the **Policy Configuration Menu**, and press **Enter**.
4. Select **Cluster File Sync** and press **Enter**. The Cluster Configuration Sync Menu is displayed.



5. Select **Show Sync Destination** and press **Enter**.



The Sync Destination screen is displayed.

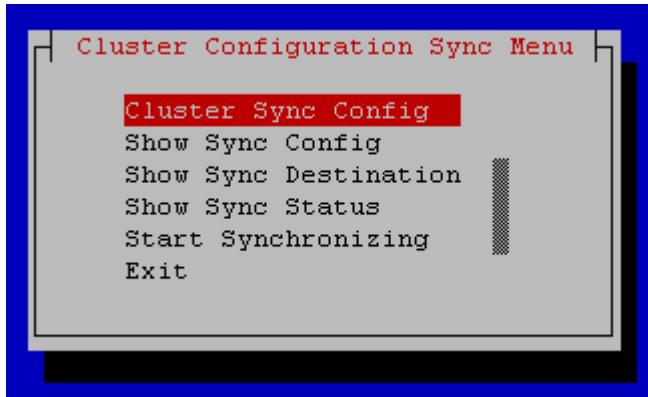
Showing Sync Status

To display cluster sync status, complete the following:

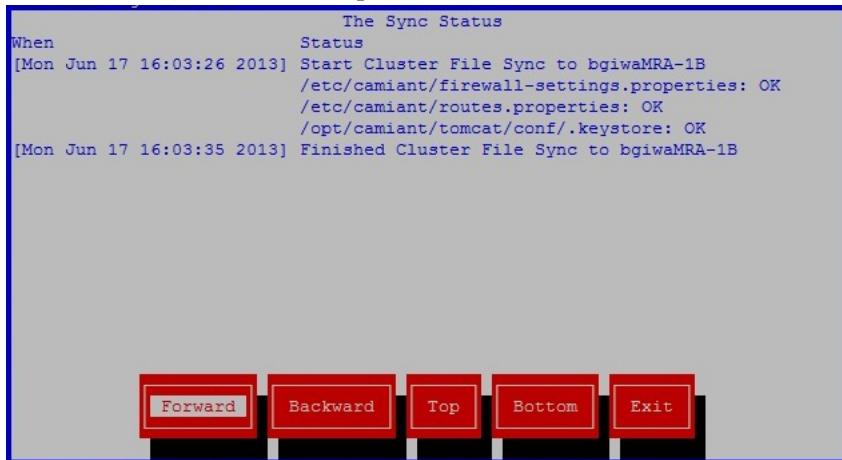
1. Log in to your system as root.
2. At the root prompt, enter the following command:

```
# su - platcfg
```

3. Select the Policy Configuration Menu, and press Enter.
4. Select Cluster File Sync and press Enter. The Cluster Configuration Sync Menu is displayed.



5. Select Show Sync Status and press Enter.



The Sync Status screen is displayed.

Performing File Synchronization

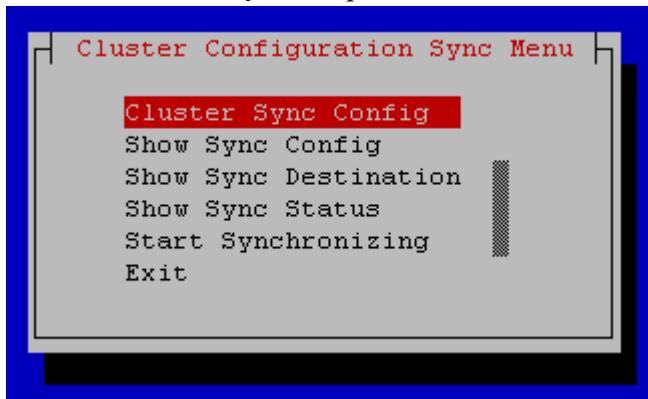
File synchronization (or cluster sync) copies configuration files from the target server to the remaining servers in the cluster. Performing a cluster sync restarts qp_procmgr on the target blade(s), so this action should only be performed from the Active server, otherwise a failover will occur. A warning displays on the screen before continuing with the sync, to help prevent this issue from occurring. Note that the cluster file sync doesn't currently handle DSCP configurations; there is a separate DSCP-specific sync operation for this.

To perform the cluster sync, complete the following:

1. Log in to your system as root.
2. At the root prompt, enter the following command:

```
# su - platcfg
```

3. Select the Policy Configuration Menu and press Enter.
4. Select Cluster File Sync and press Enter. The Cluster Configuration Sync Menu is displayed.



5. Select Start Synchronizing and press Enter.

A warning message is displayed, warning that a cluster sync restarts qp_procmgr on the target blade(s). This action should only be performed from the Active server, otherwise a failover will occur.

6. Select OK to continue.

Configuration files are synced to the other servers in the cluster, and qp_procmgr is restarted on the target blade(s).

Chapter

6

Performing System and Server Backups and Restores

Topics:

- *Performing a Server Backup.....53*
- *Performing a System Backup.....54*
- *Displaying Backup Files.....55*
- *Configuring Local Archive Settings.....55*
- *Configuring Remote Archive Settings.....56*
- *Scheduling Backups.....58*
- *Performing a System Restore.....60*
- *Performing a Server Restore.....60*

This chapter describes how to perform system and server backups and restores.

Performing a Server Backup

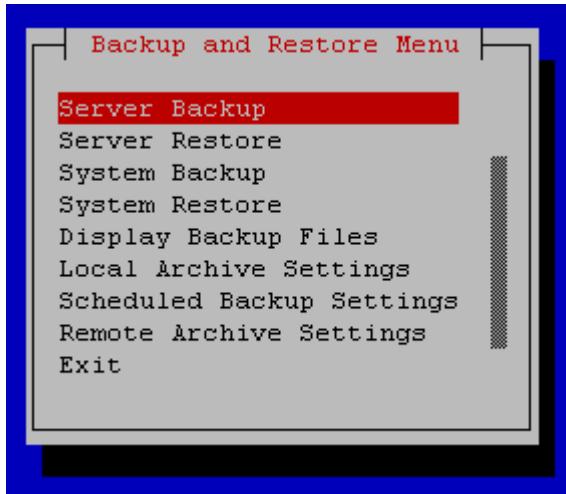
The server backup contains OS-level information such as IP, NTP, and DNS information, basically what gets configured in Platcfg. This type of backup is therefore unique to a server and should be created for each server within a cluster.

To back up your server settings, complete the following:

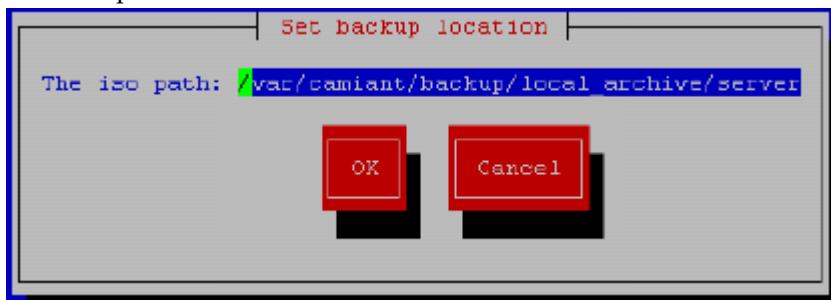
1. Log in to your system as root.
2. At the root prompt, enter the following command:

```
# su - platcfg
```

3. Select the **Policy Configuration Menu** and press **Enter**.
4. Select **Backup and Restore** and press **Enter**. The Backup and Restore Menu is displayed. Note that System Backup and System Restore are only allowed on the CMPsystem, so these options don't appear on the menu for other types of blades.



5. Select **Server Backup** and press **Enter**. You are prompted for the ISO path to save the backup file. For example:



Accept the default backup directory or enter a desired directory. The file naming convention used for the backup file is:

`<hostname>-camiant-<release>-serverbackup-<datetimestamp>.iso`

- When you are done, select **OK** and press **Enter**. The backup is created.

```
Creating backup archive... OK
Removing oldest archives... OK
Rsync copying local archive to remote archive... OK
```

```
PRESS ANY KEY TO RETURN TO THE PLATCFG MENU.
```

Performing a System Backup

The system backup contains application-level information such as Topology, Network Element, and PCRF configurations, almost anything that is configured in the CMP GUI. This type of backup will save information for an entire deployment and should be created on the active blade of the Primary CMP cluster only.

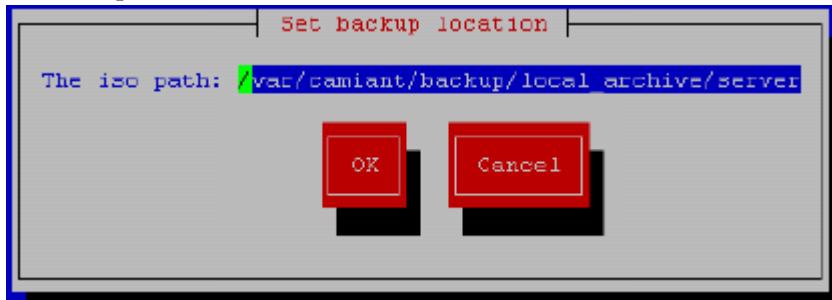
When the backup file is created it contains a specific name and is located in a specific directory. Transfer this backup to the FTP server and/or to the PMAC server.

To back up your server settings, complete the following:

- Log in to your server as root
- At the root prompt, enter the following command:

```
# su - platcfg
```

- Select the **Policy Configuration Menu** and press **Enter**.
- Select **Backup and Restore** and press **Enter**.
- Select **System Backup** and press **Enter**. You are prompted for the ISO path to save the backup file. For example:



- Accept the default backup directory or enter a desired directory. The file naming convention used for the backup file is:
`<hostname>-camiant-<release>-systembackup-<datetime>.tar.gz`
- When you are done, select **OK** and press **Enter**. The backup is created.

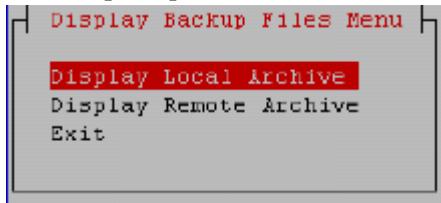
Displaying Backup Files

To display current backup files, complete the following:

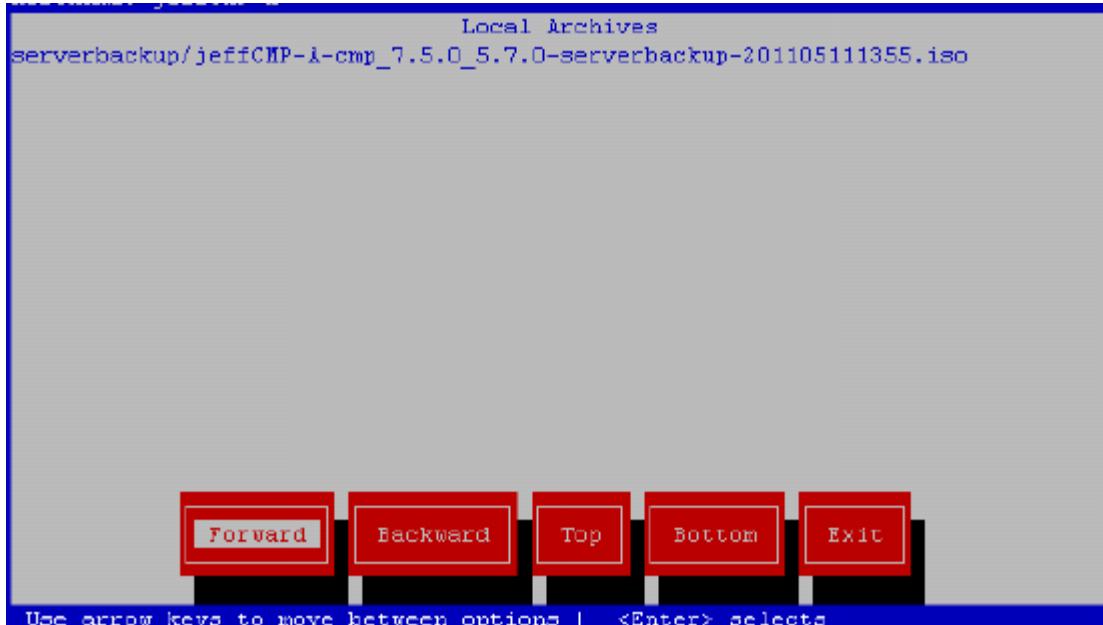
1. Log in to your system as root.
2. At the root prompt, enter the following command:

```
# su - platcfg
```

3. Select the **Policy Configuration Menu** and press **Enter**.
4. Select **Backup and Restore** and press **Enter**.
5. Select **Display Backup Files** and press **Enter**.
6. You are prompted for Local or Remote backup archive.



7. Select the desired archive and press **Enter**. The archive is displayed. For example:



Configuring Local Archive Settings

You can store up to three archives for both the server and system backup files. To configure this setting, complete the following:

1. Log in to your system as root.
2. At the root prompt, enter the following command:

```
# su - platcfg
```

3. Select the **Policy Configuration Menu** and press **Enter**.
4. Select **Backup and Restore** and press **Enter**.
5. Select **Local Archive Settings** and press **Enter**.
6. You are prompted for the desired number of archives for both the server and system backups. Note that the following example shows both the number of Server Backups and System Backups to keep; the Server Backup line will only appear on a CMP system.



7. Select the desired number for each archive and when you are done, select **OK** and press **Enter**.

Configuring Remote Archive Settings

You can store system and server archives remotely. These archives have separate directories for each host. This section describes how to configure, edit, and delete system or server remote archives.

Configuring a Remote Archive

To configure this setting, complete the following:

1. Log in to your system as root.
2. At the root prompt, enter the following command:

```
# su - platcfg
```

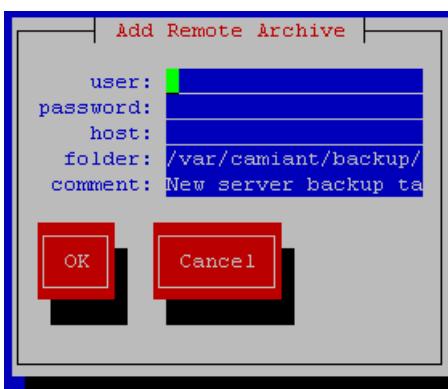
3. Select the **Policy Configuration Menu** and press **Enter**.
4. Select **Backup and Restore** and press **Enter**.
5. Select **Remote Archive Settings** and press **Enter**.

6. You are prompted for the desired archive type (server or system). Note that the Server Backups option only appears on a CMP system. Select the desired archive type and press **Enter**.



The **Add Remote Archive** screen displays.

7. Enter all remote access information:



- a) **user** and **password**: must be valid SSH login credentials for the target server.
- b) **host**: must be either a reachable IP address or a resolvable hostname.
- c) **folder**: must be a directory on the target server where the Policy Management server will attempt to copy backups to. The directory must already exist; it will not be created on demand.
- d) **comment**: is just the name of the remote archive when viewed in Platcfg.

8. When you are done, select **OK** and press **Enter**.

Editing a Remote Archive Configuration

To edit an archive configuration, complete the following:

1. From the Backup and Restore Menu, select **Remote Archive Settings** and press **Enter**.
2. Select the desired archive type and press **Enter**.
3. Select **Edit Remote Archive** and press **Enter**.
4. Enter all remote access information and when you are done, select **OK** and press **Enter**.

Deleting an Archive Configuration

To delete an archive configuration, complete the following:

1. From the Backup and Restore Menu, select **Remote Archive Settings**, and press **Enter**.
2. Select the desired archive type and press **Enter**.
3. Select **Delete Remote Archive** and press **Enter**.

4. Select the desired archive to delete and press **Enter**. The archive is removed from the system.

Scheduling Backups

You can configure your system or server to conduct backups on a scheduled basis. This section describes how to schedule, edit, delete, and view scheduled backups.

Note: When "Daily" is selected, the Days of the month field is ignored, and when "Monthly" is selected, the Days of the week field is ignored.

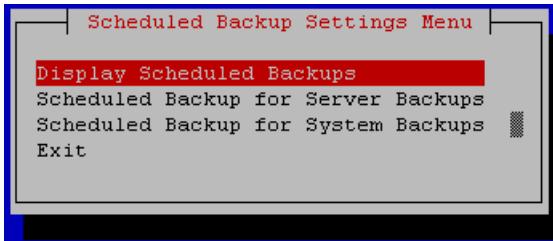
Scheduling a Backup

To schedule a backup, complete the following:

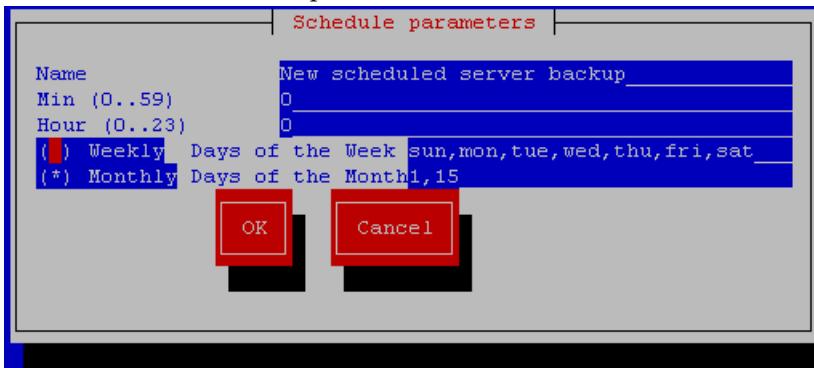
1. Log in to your system as root.
2. At the root prompt, enter the following command:

```
# su - platcfg
```

3. Select the **Policy Configuration Menu**, and press **Enter**.
4. Select **Backup and Restore** and press **Enter**.
5. You are prompted for the desired backup type (server or system). Select the desired backup type and press **Enter**. For example:



6. Select **Add Schedule** and press **Enter**.



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 - day to perform backup. Valid values include the days of the week and All.
- 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 through 31.

8. When you have finished, select **OK** and press **Enter**.

Editing a Scheduled Backup

To edit an existing scheduled backup, complete the following:

1. From the Policy Configuration Menu, select **Backup and Restore** and press **Enter**.
2. Select **Scheduled backup settings** and press **Enter**.
3. You are prompted for the desired backup type (server or system). Select the desired backup type and press **Enter**.
4. Select **Edit Schedule** and press **Enter**.
5. Edit the following Information, as desired.
 - 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. The default backup is performed weekly.
 - Days of Week - day to perform backup. Valid values include the days of the week and All.
 - Monthly - select to have the backup performed monthly.
 - Days of the Month - day to perform backup. Valid values include 1 through 31.
6. When you have finished, select **OK** and press **Enter**.

Deleting a Scheduled Backup

To delete an existing scheduled backup, complete the following:

1. From the Policy Configuration Menu, select **Backup and Restore** and press **Enter**.
2. Select **Scheduled backup settings** and press **Enter**.
3. You are prompted for the desired backup type (server or system). Select the desired backup type and press **Enter**.
4. Select **Delete Schedule** and press **Enter**.
5. When you have finished, select **OK** and press **Enter**.

Displaying Scheduled Backups

To display the scheduled backups, complete the following:

1. From the Policy Configuration Menu, select **Backup and Restore** and press **Enter**.
2. Select **Scheduled backup settings** and press **Enter**.

3. Select **Display Scheduled Backups** and press **Enter**. The scheduled backups are displayed.

Performing a System Restore

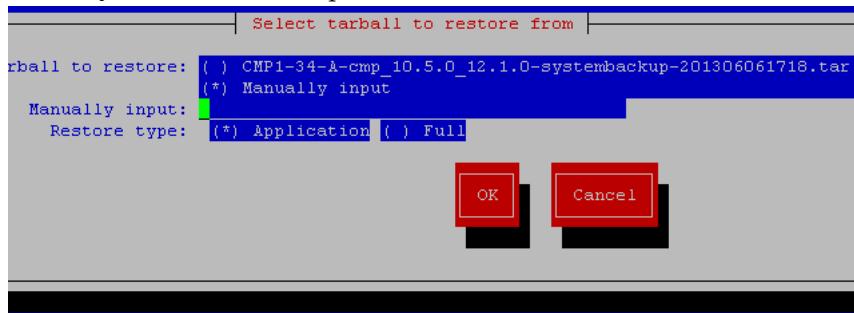
The system restore restores the PCRF information that is unique to this system. Information such as: topology, policies, and feature configuration.

To perform a system restore, complete the following:

1. Log in to your system as root.
2. At the root prompt, enter the following command:

```
# su - platcfg
```

3. Select the **Policy Configuration Menu** and press **Enter**.
4. Select **Backup and Restore** and press **Enter**.
5. Select **System Restore** and press **Enter**.



6. Enter the path of the location that contains the backup, and select either Application or Full for the type of restore. When you are finished, select **OK** and press **Enter**. The system restores to the backup version specified.

Performing a Server Restore

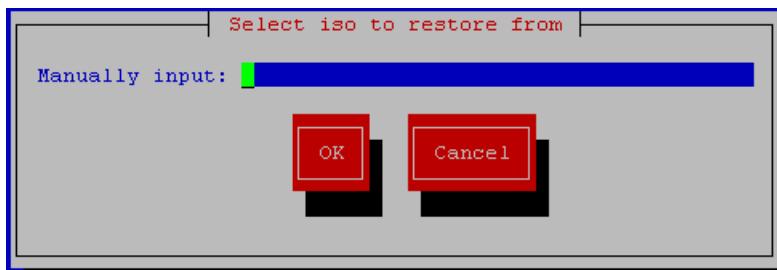
The server restore restores the OS information unique to the server. This operation applies the data from a previously saved server configuration backup file.

To perform a server restore, complete the following:

1. Log in to your system as root.
2. At the root prompt, enter the following command:

```
# su - platcfg
```

3. Select the **Policy Configuration Menu**, press **Enter**.
4. Select **Backup and Restore** and press **Enter**.
5. Select **Server Restore** and press **Enter**.



6. Enter the path of the location that contains the backup, select OK, and press Enter. The system restores to the backup version specified.

Glossary

C

CA	<p>Canada (NPAC Region)</p> <p>Conditioning Action</p> <p>NPP CAs indicate what digit conditioning actions to execute when processing a digit string.</p> <p>Certificate Authority: An entity that issues digital certificates</p>
----	--

CMP	<p>Configuration Management Platform</p> <p>A centralized management interface to create policies, maintain policy libraries, configure, provision, and manage multiple distributed MPE policy server devices, and deploy policy rules to MPE devices. The CMP has a web-based interface.</p>
-----	---

D

DNS	<p>Domain Name Services</p> <p>Domain Name System</p> <p>A system for converting Internet host and domain names into IP addresses.</p>
-----	--

G

GUI	<p>Graphical User Interface</p> <p>The term given to that set of items and facilities which provide the user with a graphic means for manipulating screen data rather than being limited to character based commands.</p>
-----	---

H

H

HTTP	Hypertext Transfer Protocol
------	-----------------------------

I

IP	Intelligent Peripheral
	Internet Protocol
	IP specifies the format of packets, also called datagrams, and the addressing scheme. The network layer for the TCP/IP protocol suite widely used on Ethernet networks, defined in STD 5, RFC 791. IP is a connectionless, best-effort packet switching protocol. It provides packet routing, fragmentation and re-assembly through the data link layer.

ISO	International Standards Organization
-----	--------------------------------------

M

MDF	Message Distribution Function. A standalone hardware system, situated between a Mediation Gateway and an Oracle Communications subscriber profile repository (SPR), that exchanges messages between a Mediation Gateway and SPR systems
-----	---

MPE	Multimedia Policy Engine
	A high-performance, high-availability platform for operators to deliver and manage differentiated services over high-speed data networks. The MPE includes a protocol-independent policy rules engine that provides authorization for services based on policy conditions such as subscriber information, application

M

information, time of day, and edge resource utilization.

MRA

Multi-Protocol Routing Agent

Scales the Policy Management infrastructure by distributing the PCRF load across multiple Policy Server devices.

N**NTP**

Network Time Protocol

P**PCRF**

Policy and Charging Rules Function. The ability to dynamically control access, services, network capacity, and charges in a network.

Maintains rules regarding a subscriber's use of network resources. Responds to CCR and AAR messages. Periodically sends RAR messages. All policy sessions for a given subscriber, originating anywhere in the network, must be processed by the same PCRF.

PMAC

Platform Management & Configuration (also referred to as PM&C)

Provides hardware and platform management capabilities at the site level for Tekelec platforms. The PMAC application manages and monitors the platform and installs the TPD operating system from a single interface.

V**VLAN**

Virtual Local Area Network

V

A logically independent network. A VLAN consists of a network of computers that function as though they were connected to the same wire when in fact they may be physically connected to different segments of a LAN. VLANs are configured through software rather than hardware. Several VLANs can co-exist on a single physical switch.