

**Oracle® Communications
Policy Management**

Platform Configuration User's Guide

Release 12.1

E62447 Revision 01

September 2015

Oracle® Communications Policy Management Platform Configuration User's Guide, Release 12.1

Copyright © 2013, 2015, Oracle and/or its affiliates. All rights reserved.

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

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

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

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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

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

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

This software or hardware and documentation may provide access to or information about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.

Table of Contents

Chapter 1: About This Guide.....	14
How This Guide is Organized.....	15
Intended Audience.....	15
Documentation Admonishments.....	15
Related Publications.....	16
Locate Product Documentation on the Oracle Technology Network Site.....	16
Customer Training.....	16
My Oracle Support (MOS).....	17
Emergency Response.....	17
Chapter 2: Introduction.....	18
Accessing the Platcfg Utility.....	19
Using the Platcfg Utility.....	19
Troubleshooting Using the Policy Configuration Menu.....	19
Saving Platform Debug Logs.....	20
Chapter 3: Performing Initial Server Configuration.....	23
Set Policy Mode.....	24
Initial Configuration.....	27
Verifying the Initial Configuration.....	31
Verifying the Server Status.....	33
Cluster Configuration Removal.....	35
Configuring Routing on Your Server.....	36
Configuring Routing.....	36
Deleting a Route.....	39
Displaying Configure Routes.....	41
Exporting a Route.....	42
Importing a Route.....	43
Restarting the Application.....	43
Configuring Firewall Settings.....	45
Displaying Firewall Settings.....	51
Configuring DSCP.....	54
Adding a DSCP Configuration.....	54

Viewing DSCP Configurations.....	57
Editing a DSCP Configuration.....	57
Deleting a DSCP Configuration.....	60
Syncing DSCP Configurations.....	60
Chapter 4: Managing Certificates.....	62
Description of Security Certificates.....	63
Managing SSL Security Certificates.....	63
Creating a Self-Signed Certificate.....	63
Verifying the Self-Signed Certificate.....	65
Using a Local Certificate to Establish a Secure HTTP (https) Web-Browser Session.....	67
Establishing a Secure Connection Between a CMP System and a CMP Device.....	68
Exporting the Certificate Signed Request to the Policy Management Servers.....	69
Importing the Peer Certificate.....	70
Creating a CA Third-party Signed Certificate.....	72
Remove the Pre-existing Local Certificate.....	72
Generating a Certificate Signature Request, Exporting for Signing, Re-importing, and Verifying.....	73
Chapter 5: Synchronizing Files.....	79
Managing Cluster Sync Configurations.....	80
Reading Destination from COMCOL.....	80
Adding a Sync File.....	81
Deleting a Sync File.....	83
Showing Sync Configuration.....	84
Showing Sync Destination.....	85
Showing Sync Status.....	86
Performing File Synchronization.....	87
Chapter 6: Custom Ethtool Options.....	89
Edit Network Interface Ethernet Parameters (Policy Configuration Method).....	90
Edit Network Interface Ethernet Parameters (TPD Method).....	92
Chapter 7: Performing System and Server Backups and Restores....	95
Performing a Server Backup.....	96
Performing a System Backup.....	98
Displaying Backup Files.....	99
Configuring Local Archive Settings.....	102

Configuring Remote Archive Settings.....	103
Configuring a Remote Archive.....	103
Editing a Remote Archive Configuration.....	105
Deleting a Remote Archive Configuration.....	106
Displaying a Remote Archive Configuration.....	107
Scheduling Backups.....	109
Scheduling a Backup.....	109
Editing a Scheduled Backup.....	110
Deleting a Scheduled Backup.....	112
Displaying Scheduled Backups.....	112
Performing a System Restore.....	113
Performing a Server Restore.....	114
Glossary.....	116

List of Figures

Figure 1: Main Menu.....	19
Figure 2: Main Menu--Policy Configuration.....	20
Figure 3: Policy Configuration Menu--Save Platform Debug Logs.....	21
Figure 4: Save Platform Debug Logs.....	22
Figure 5: Policy Configuration Menu--Set Policy Mode.....	24
Figure 6: Select Policy Mode.....	25
Figure 7: Select Network Layout--CMP Server.....	25
Figure 8: Select Network Layout--Policy Management Server.....	26
Figure 9: Select Network Layout--MRA Server, SIGC.....	26
Figure 10: Policy Configuration Menu--Perform Initial Configuration.....	28
Figure 11: Initial Configuration--Wireless.....	28
Figure 12: Initial Configuration--Wireless, c-Class hardware.....	29
Figure 13: Initial Configuration--Cable.....	29
Figure 14: Initial Configuration - Wireless, MRA Support.....	30
Figure 15: Policy Configuration Menu--Verify Initial Configuration.....	31
Figure 16: Index Table of Contents--Wireless.....	32
Figure 17: Index Table of Contents--Cable.....	32
Figure 18: Index Table of Contents--Wireline.....	33
Figure 19: Policy Configuration Menu--Verify Server Status.....	34
Figure 20: Index Table of Contents--Server Status.....	34
Figure 21: Policy Configuration Menu--Cluster Configuration Removal.....	35
Figure 22: Cleanup Configuration Menu.....	35

Figure 23: Cleaning up cluster information.....	36
Figure 24: Policy Configuration Menu--Routing Config.....	37
Figure 25: Route Configuration Menu--Add Route.....	37
Figure 26: Add Route--Wireless.....	38
Figure 27: Route Configuration Menu--Delete Route.....	40
Figure 28: Main Routing Table.....	40
Figure 29: Route Configuration Menu--Display Routes.....	41
Figure 30: Main Routing Table.....	41
Figure 31: Route Configuration Menu--Export Routes.....	42
Figure 32: Export Routes To File.....	42
Figure 33: Routing Configuration Menu--Import Routes.....	43
Figure 34: Import Routes From File.....	43
Figure 35: Policy Configuration Menu--Restart Application.....	44
Figure 36: Restart qp_procmgr.....	44
Figure 37: Policy Configuration Menu--Firewall.....	45
Figure 38: Firewall Configuration Menu--Enable/Disable Firewall.....	46
Figure 39: Firewall status screen.....	46
Figure 40: Enable/Disable Firewall Feature Menu.....	47
Figure 41: Enable iptables?.....	47
Figure 42: Enable/Disable Firewall Features Menu--Enable custom rules.....	47
Figure 43: Enable custom prefer feature?.....	48
Figure 44: Enable/Disable Firewall Features Menu--Enable custom prefer.....	48
Figure 45: Enable custom prefer feature?.....	48
Figure 46: Firewall Configuration Menu--Customize Firewall.....	49
Figure 47: Firewall Custom Rules.....	49

Figure 48: Connection Action Menu.....	49
Figure 49: Customize Firewall--Wireless.....	50
Figure 50: Customize Firewall--Cable.....	50
Figure 51: Customize Firewall--CMCC Wireless.....	51
Figure 52: Firewall Configuration Menu--Save and Apply Configuration.....	51
Figure 53: Firewall Configuration Menu--Display Firewall.....	52
Figure 54: Display Firewall Menu.....	52
Figure 55: Display Firewall Status.....	52
Figure 56: Display Factory Rules.....	53
Figure 57: Display Custom Rules.....	53
Figure 58: Policy Configuration Menu--DSCP Config.....	54
Figure 59: DSCP Configuration Menu--Add New DSCP Configuration.....	55
Figure 60: Select Interface.....	55
Figure 61: Input Source IP and Destination IP.....	56
Figure 62: Code Point selection.....	56
Figure 63: DSCP Configuration Menu--View DSCP Configuration.....	57
Figure 64: View DSCP Configuration.....	57
Figure 65: DSCP Configuration Menu--Edit DSCP Configuration.....	58
Figure 66: Edit DSCP Configuration Menu.....	58
Figure 67: Select Interface.....	58
Figure 68: Input Source IP and destination IP.....	59
Figure 69: Code Point selection.....	59
Figure 70: DSCP Configuration Menu--Delete DSCP Configuration.....	60
Figure 71: Current DSCP.....	60
Figure 72: DSCP Configuration Menu--Sync DSCP Configuration.....	61

Figure 73: (Sync DSCP) Message.....	61
Figure 74: Policy Configuration Menu--SSL Key Configuration.....	64
Figure 75: Configure SSL keys Menu- Configure keystore.....	64
Figure 76: Operate keystore Menu.....	65
Figure 77: Input Parameters.....	65
Figure 78: Operate keystore Menu--View Key.....	66
Figure 79: Keystore Parameters.....	66
Figure 80: Select keystore item Menu.....	66
Figure 81: Verify Self-Signed Certificate.....	67
Figure 82: Operate keystore Menu - Export key.....	69
Figure 83: Export Certificate.....	70
Figure 84: Certificate Message.....	70
Figure 85: Operate keystore Menu.....	71
Figure 86: Input Parameters--Keystore Password.....	71
Figure 87: Import Certificate.....	71
Figure 88: Configure SSL keys Menu.....	72
Figure 89: Operate keystore Menu.....	73
Figure 90: Select keystore item Menu.....	73
Figure 91: Delete existing certificate.....	73
Figure 92: Operate keystore Menu--Create Certificate Signature Request (CSR).....	74
Figure 93: Message--CSR success.....	75
Figure 94: Export Certificate.....	75
Figure 95: Export Success Message.....	76
Figure 96: Policy Configuration Menu--Cluster File Sync.....	80
Figure 97: Cluster Configuration Sync Menu--Cluster Sync Config.....	81

Figure 98: Config the Destination of Cluster Sync Menu--Read Destination from COMCOL.....	81
Figure 99: Detecting destination servers.....	81
Figure 100: Config the Destination of Cluster Sync Menu--Add Sync File.....	82
Figure 101: Add a Sync File.....	82
Figure 102: Config the Destination of Cluster Sync Menu--Delete Sync File.....	83
Figure 103: Main Routing Table.....	83
Figure 104: Cluster Configuration Sync Menu--Show Sync Config.....	84
Figure 105: The Sync File.....	85
Figure 106: Cluster Configuration Sync Menu--Show Sync Destination.....	86
Figure 107: The Sync Destination.....	86
Figure 108: Cluster Configuration Sync Menu--Show Sync Status.....	87
Figure 109: The Sync Status.....	87
Figure 110: Cluster Configuration Sync Menu--Start Synchronizing.....	88
Figure 111: Policy Configuration Menu--Ethernet Interface Parameter Settings.....	90
Figure 112: Network Interfaces Menu.....	90
Figure 113: Edit <linkname> Link Options.....	91
Figure 114: Network Interfaces Menu--Edit an Interface.....	92
Figure 115: Example view of Connection to edit Menu.....	93
Figure 116: Example view of Interface Statistics.....	93
Figure 117: Example view of Interface Options.....	94
Figure 118: Policy Configuration Menu--Backup and Restore.....	96
Figure 119: Backup and Restore Menu.....	97
Figure 120: Set backup location.....	97
Figure 121: Backup creation message.....	97
Figure 122: Backup and Restore Menu.....	98

Figure 123: Set system backup location.....	98
Figure 124: Creating backup archive.....	99
Figure 125: Backup and Restore Menu--Display Backup Files.....	100
Figure 126: Display Backup Files Menu--Display Local Archive.....	100
Figure 127: Local Archives.....	101
Figure 128: Display Backup Files Menu--Display Remote Archive.....	101
Figure 129: Remote Archives.....	102
Figure 130: Backup and Restore Menu.....	103
Figure 131: Local Archive Settings.....	103
Figure 132: Remote Archive Settings Menu.....	104
Figure 133: Remote Archive Settings Menu.....	104
Figure 134: Add Remote Archive.....	104
Figure 135: Remote Archive Settings Menu--Edit Remote Archive.....	105
Figure 136: Remote Archives Menu.....	105
Figure 137: Edit Remote Archive.....	106
Figure 138: Remote Archive Settings Menu.....	106
Figure 139: Remote Archives Menu.....	106
Figure 140: Confirm deletion.....	107
Figure 141: Remote Archive Settings Menu.....	107
Figure 142: Display Remote Archive For Server-Backup.....	108
Figure 143: Display Remote Archive For System-Backup.....	108
Figure 144: Backup and Restore Menu--Scheduled Backup Settings.....	109
Figure 145: Scheduled Backup Settings Menu.....	110
Figure 146: Schedule parameters.....	110
Figure 147: Backup and Restore Menu--Scheduled Backup Settings.....	111

Figure 148: Scheduled Backup Settings Menu.....	111
Figure 149: Scheduled Backup for server backups Menu.....	111
Figure 150: Scheduled Backup for server backups Menu.....	112
Figure 151: Scheduled Backups.....	113
Figure 152: Select tarball to restore from.....	114
Figure 153: Select iso to restore from screen.....	115

List of Tables

Table 1: Admonishments.....	15
Table 2: Server Network Layouts.....	26
Table 3: Detailed Behavior of Preferred Source Addr.....	39
Table 4: Certificate Management Terminology.....	63
Table 5: Ethtool speed compatibility matrix.....	91

Chapter 1

About This Guide

Topics:

- *How This Guide is Organized.....15*
- *Intended Audience.....15*
- *Documentation Admonishments.....15*
- *Related Publications.....16*
- *Locate Product Documentation on the Oracle Technology Network Site.....16*
- *Customer Training.....16*
- *My Oracle Support (MOS).....17*
- *Emergency Response.....17*

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.
- [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 Management 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> .)

Icon	Description
 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 and equipment damage</i> .)

Related Publications

For information about additional publications that are related to this document, refer to the *Related Publications Reference* document, which is published as a separate document on the Oracle Technology Network (OTN) site. See [Locate Product Documentation on the Oracle Technology Network Site](#) for more information.

Locate Product Documentation on the Oracle Technology Network Site

Oracle customer documentation is available on the web at the Oracle Technology Network (OTN) 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 Technology Network site at <http://docs.oracle.com>.
2. Click **Industries**.
3. Under the Oracle Communications subheading, click the **Oracle Communications documentation** link.
The Oracle Communications Documentation page appears with Tekelec shown near the top.
4. Click the **Oracle Communications Documentation for Tekelec Products** link.
5. Navigate to your Product and then the Release Number, and click the **View** link (the Download link will retrieve the entire documentation set).
A list of the entire documentation set for the selected product and release appears.
6. To download a file to your location, right-click the **PDF** link, select **Save target as**, 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 (MOS)

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

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

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

You will be connected to a live agent who can assist you with MOS registration and opening a support ticket.

MOS 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 (CAS) 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.

Chapter

2

Introduction

Topics:

- [Accessing the Platcfg Utility.....19](#)
- [Using the Platcfg Utility.....19](#)
- [Troubleshooting Using the Policy Configuration Menu.....19](#)

This chapter describes how to use the Platform Configuration (Platcfg) utility to configure Policy Management on Configuration Management Platform (CMP) servers and **Policy Management servers**. The term **Policy Management servers** will be used throughout this document to refer to the Multimedia Policy Engine (MPE), Multi-Protocol Routing Agent (MRA), Bandwidth on Demand (BoD), Message Distribution Function (MDF) and Management Agent (MA) collectively. Each server is described individually in detail in their respective manuals.

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

Accessing the Platcfg Utility

To access the Platcfg utility, complete the following procedures:

1. Log in to your system as **root** if logging in from the system console. Otherwise, SSH into your system as **admusr**.
2. At the **root** prompt, enter the following command:
`su - platcfg`
3. Or, at the **admusr** prompt, enter the following command:
`sudo su - platcfg`

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

The following screen is displayed.

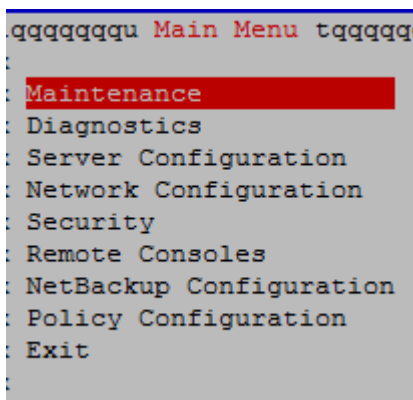


Figure 1: Main Menu

Using the Platcfg Utility

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

- 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.
- 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 procedures:

1. Log in to your system as `root` if logging in from the system console. Otherwise, SSH into your system as `admusr`.
2. At the **root** prompt, enter the following command:
`su - platcfg`
3. Or, at the **admusr** prompt, enter the following command:
`sudo su - platcfg`
4. Select **Policy Configuration** from the **Main Menu** and press **Enter**.

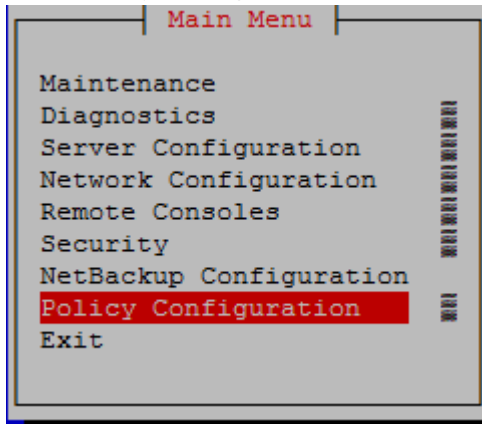


Figure 2: Main Menu--Policy Configuration

Note: NetBackup Configuration menu selection will only appear if the server is a CMP.

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

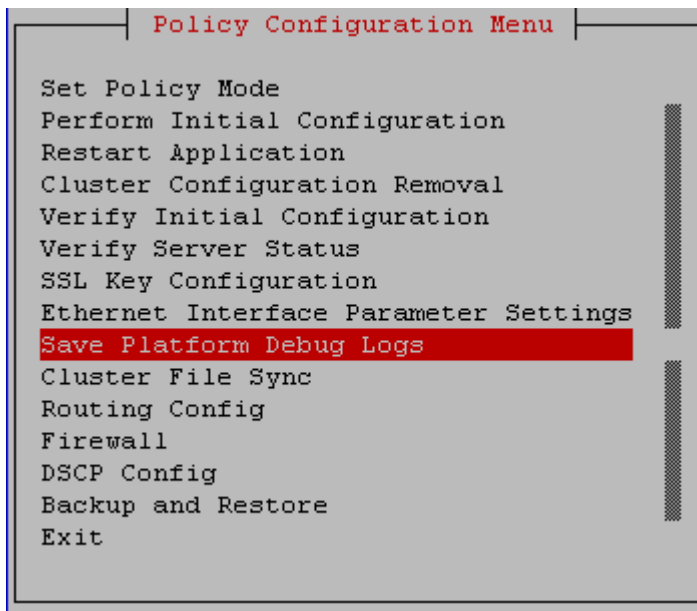


Figure 3: Policy Configuration Menu--Save Platform Debug Logs

6. In the screen that appears, enter values, where:

- **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.
- **Include trace/subact/sync log**--Indicates whether to include the extra trace/subact/sync debug records.
- **Save as**--Lists the path and filename of the file being saved.

Note: Include trace/subact/sync log should be left set to **No** unless directed to be set to **Yes** by *My Oracle Support (MOS)*.

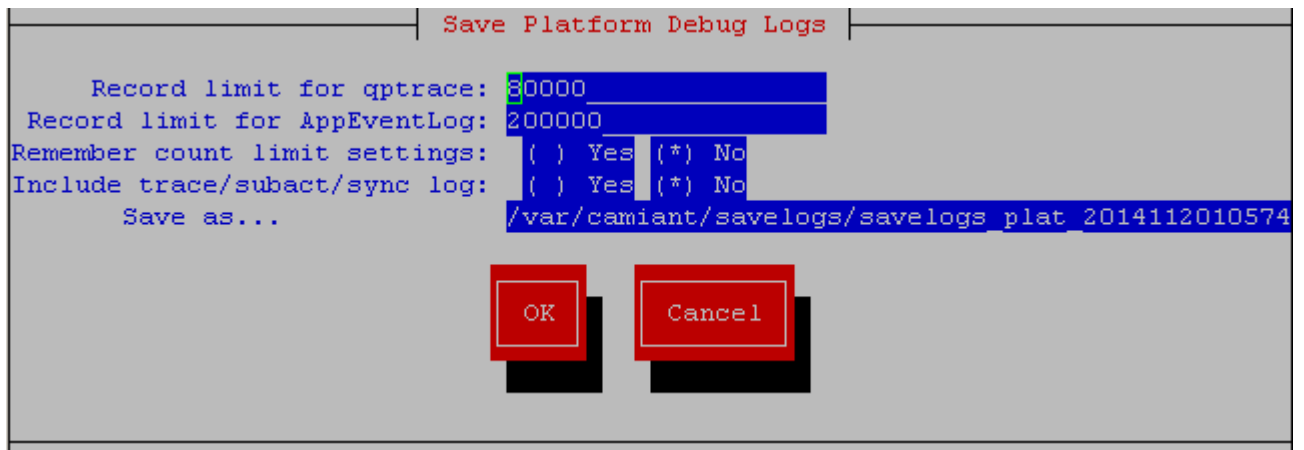


Figure 4: Save Platform Debug Logs

7. 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:

- *Set Policy Mode.....24*
- *Initial Configuration.....27*
- *Verifying the Initial Configuration.....31*
- *Verifying the Server Status.....33*
- *Cluster Configuration Removal.....35*
- *Configuring Routing on Your Server.....36*
- *Restarting the Application.....43*
- *Configuring Firewall Settings.....45*
- *Displaying Firewall Settings.....51*
- *Configuring DSCP.....54*

This chapter describes how to access the Platcfg utility, set the Policy Management configuration mode, configure the initial configuration, and then how to verify the configuration.

Set Policy Mode

This section describes how to set the Policy mode on CMP servers and other Policy Management servers for new system installations or upgrades.

To select the Policy Management mode, complete the following procedures:

1. Log in to your system as **root** if logging in from the system console. Otherwise, SSH into your system as **admusr**.
2. At the **root** prompt, enter the following command:
`su - platcfg`
3. Or, at the **admusr** prompt, enter the following command:
`sudo su - platcfg`
4. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
5. The following menu is displayed. Select **Set Policy Mode** from the **Policy Configuration Menu** and press **Enter**.

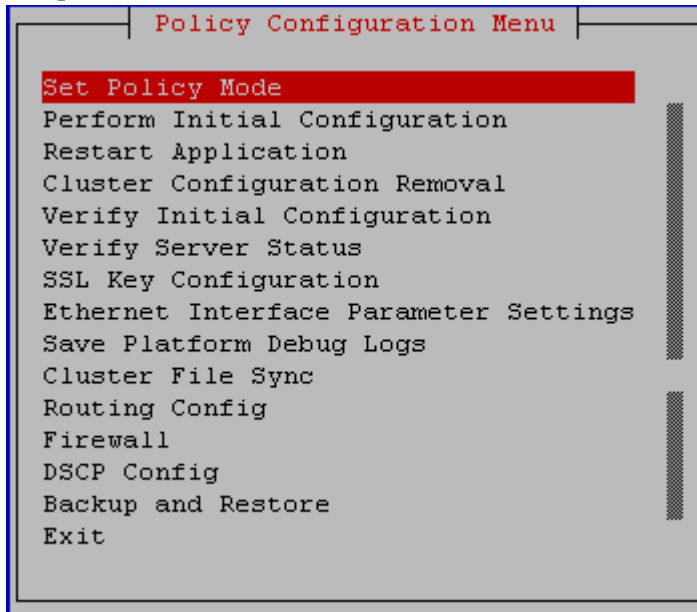


Figure 5: Policy Configuration Menu--Set Policy Mode

6. Select the appropriate mode and press **OK**.

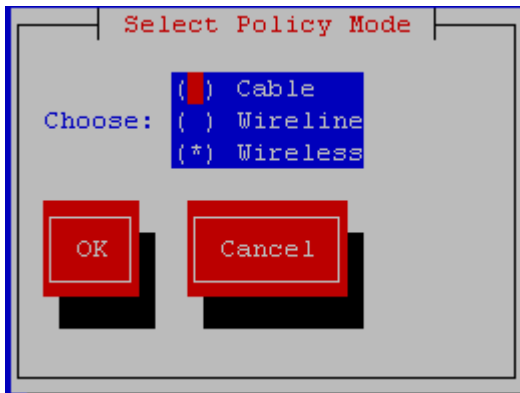


Figure 6: Select Policy Mode

7. After selecting the mode, if the **Select Network Layout** screen is displayed, you will need to select the appropriate network layout. Refer to the table below for more information about the network layout choices.
 - a) If you have an optional Ethernet Mezzanine card installed, one of the two following screens will display: one for CMP servers only and another for other Policy Management servers. For a CMP server, select either **bkup**, **common**, or **segregated_with_bkup**, from the **Select Network Layout** menu, select **OK**, and press **Enter**.

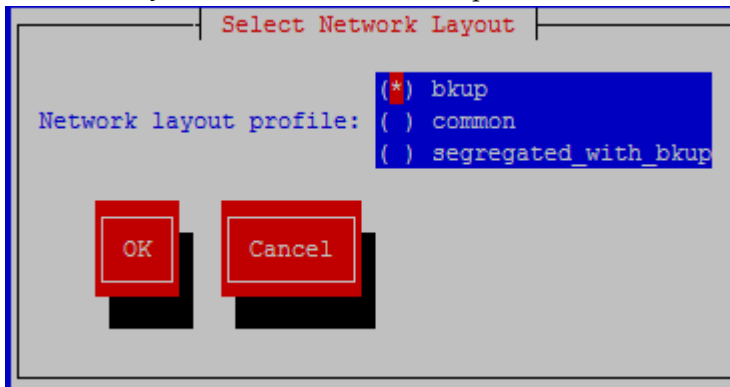


Figure 7: Select Network Layout--CMP Server

For other Policy Management servers, select either **common** or **segregated**, select **OK**, and press **Enter**.

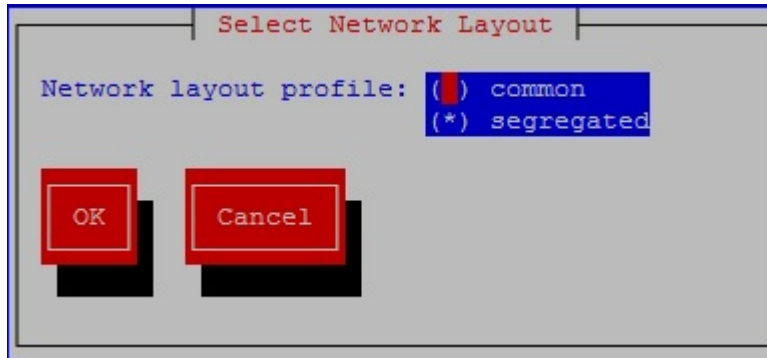


Figure 8: Select Network Layout--Policy Management Server

Note: To enable traffic segregation in a system, an Ethernet Mezzanine card is required and a selection other than **common** in the **Select Network Layout** screen is required.

Note: If the system does not have an Ethernet Mezzanine card, the **Select Network Layout** screen is not displayed, and the network layout of **Common** is applied automatically.

- b) If you have an MRA server and you are using Hewlett Packard (HP) c-Class or Sun Netra hardware to provide separate external SCTP multi-homing and internal traffic by using an additional signaling interface, select **common_with_sigc** from the **Select Network Layout** menu, select **OK**, and press **Enter**.

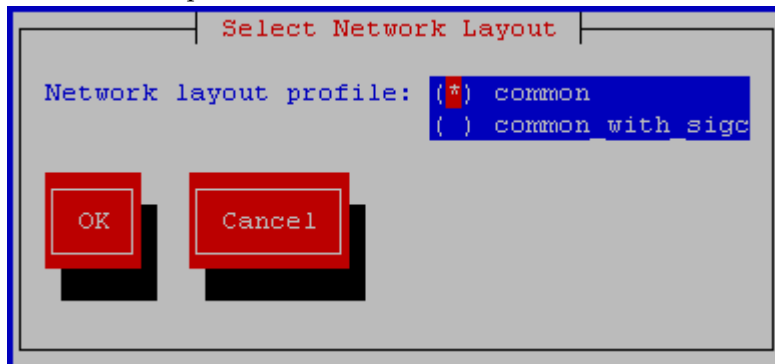


Figure 9: Select Network Layout--MRA Server, SIGC

Table 2: Server Network Layouts

Network Layout Name	Network Layout Detail	Description
common	PMAC=bond0 OAM=bond0.<VLAN> SIGA=bond0.<VLAN> SIGB=bond0.<VLAN>	This is the default layout after policy product is installed. With this layout, the mezzanine cards are not used. The product behaves exactly like an ordinary c-Class server.
segregated	PMAC=bond0 OAM=bond0.<VLAN>	This mode is used by MPE and MRA for traffic segregation.

Network Layout Name	Network Layout Detail	Description
	SIGA=bond1.<VLAN> SIGB=bond1.<VLAN>	If the server is upgraded from an earlier release with traffic segregation enabled, this layout is automatically selected.
bkup	PMAC=bond0 OAM=bond0.<VLAN> SIGA=bond0.<VLAN> SIGB=bond0.<VLAN> BKUP=bond2	This mode is used by CMP 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 mode is used by CMP 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 mode is used by a customer using an MRA server only in the Wireless mode with c-Class or Netra hardware to provide separate external SCTP multi-homing and internal traffic by using an additional signaling interface.

Initial Configuration

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

To perform the initial configuration of the system, complete the following procedures:

1. Log in to your system as `root` if logging in from the system console. Otherwise, SSH into your system as `admusr`.
2. At the **root** prompt, enter the following command:
`su - platcfg`
3. Or, at the **admusr** prompt, enter the following command:
`sudo su - platcfg`
4. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **Perform Initial Configuration** from the **Policy Configuration Menu** and press **Enter**.

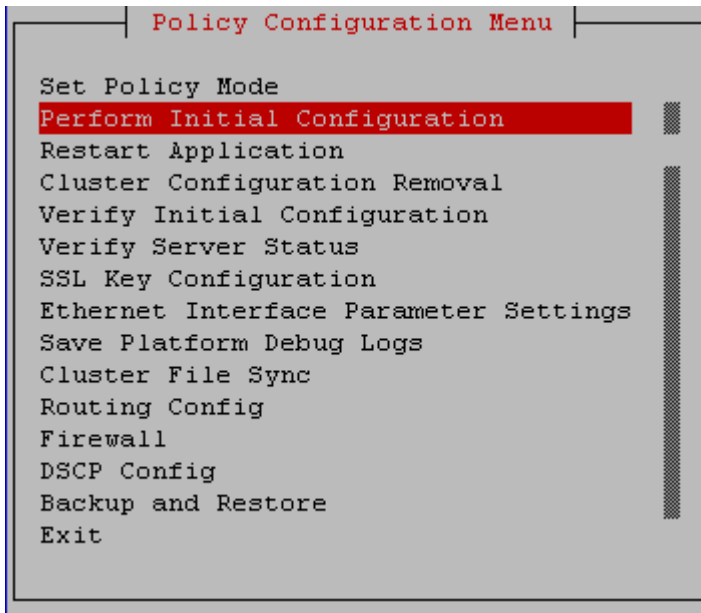


Figure 10: Policy Configuration Menu--Perform Initial Configuration

6. The **Initial Configuration** screen is displayed.

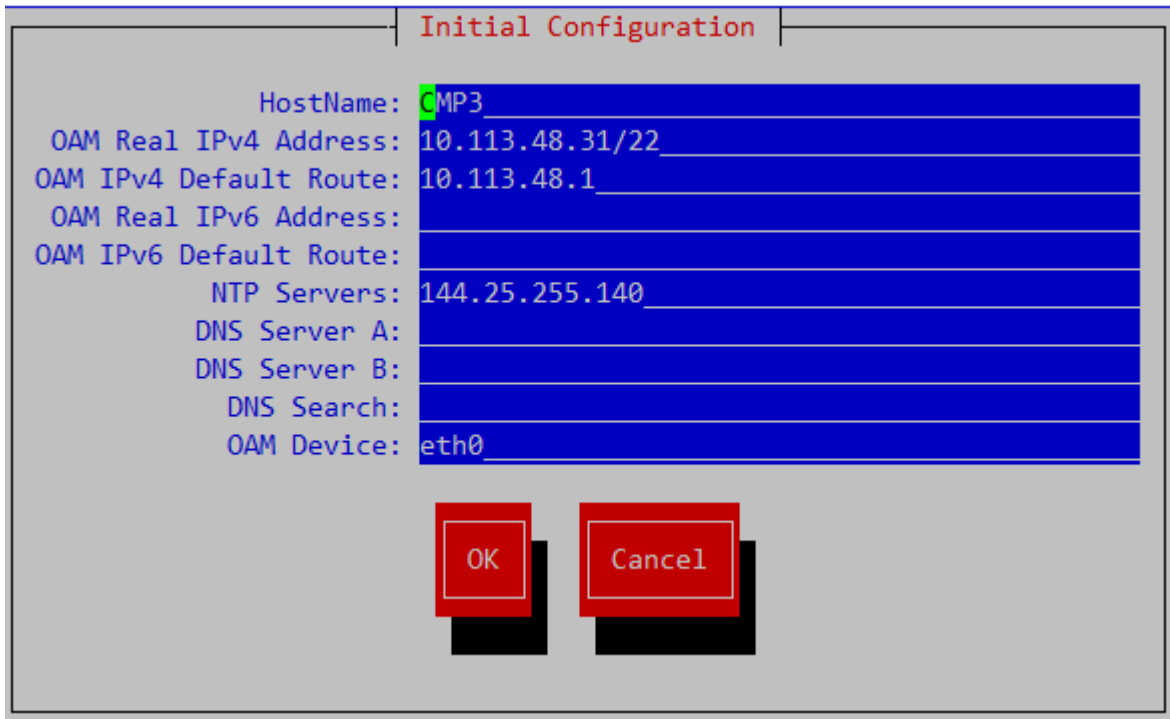


Figure 11: Initial Configuration--Wireless

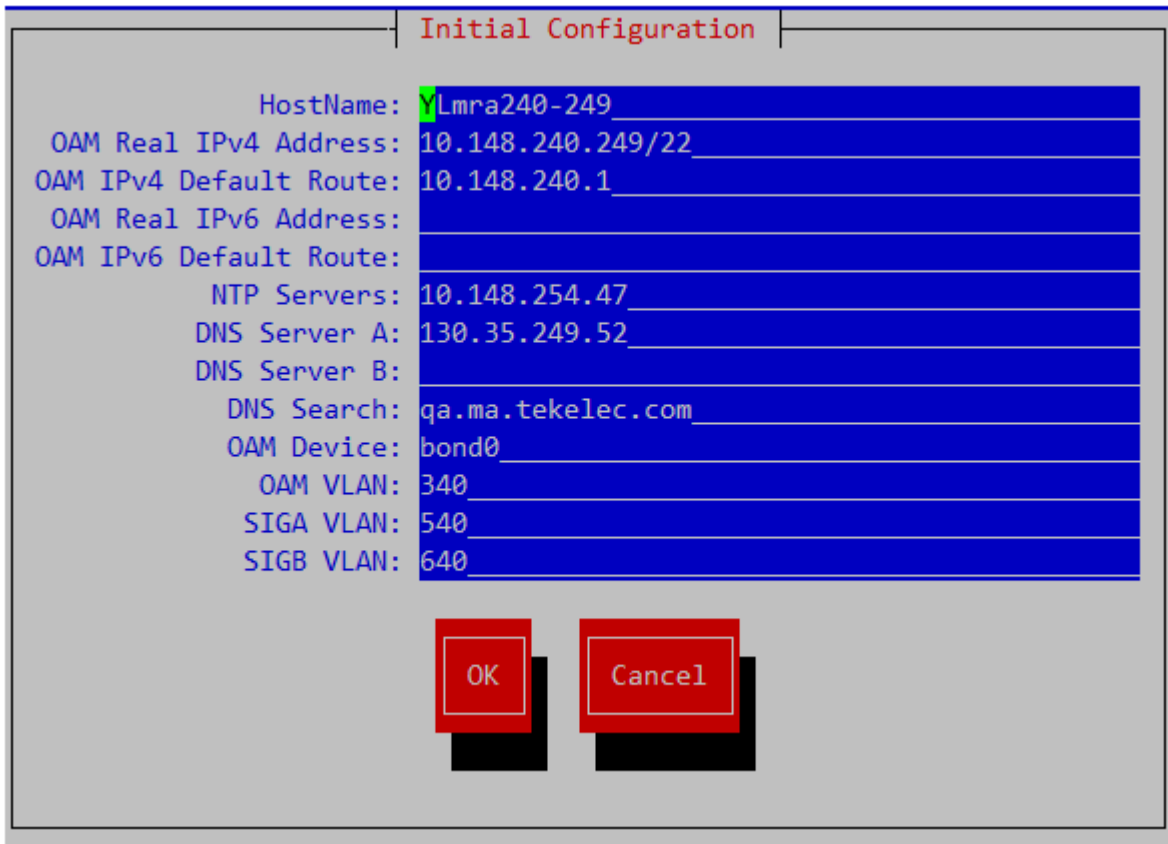


Figure 12: Initial Configuration--Wireless, c-Class hardware

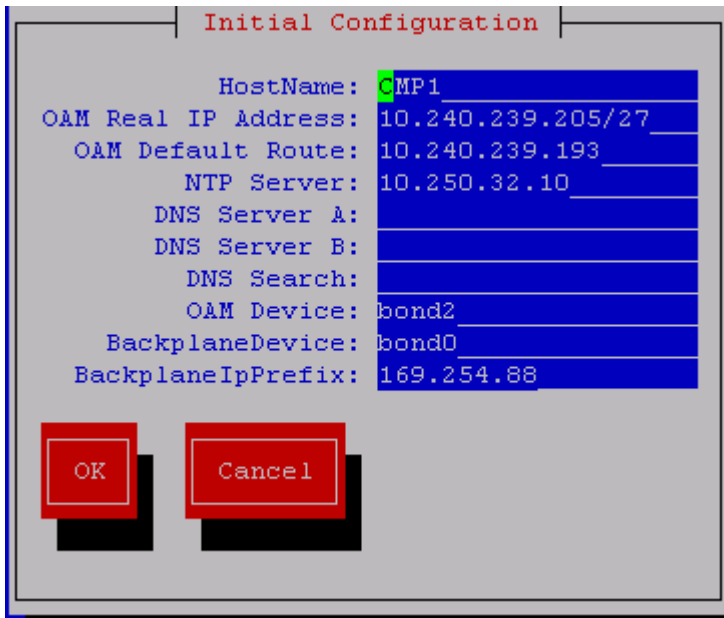


Figure 13: Initial Configuration--Cable

```

Initial Configuration
-----
HostName: live1-mra-cmcc-1
OAM Real IP Address: 10.60.32.60/24
OAM Default Route: 10.60.32.1
NTP Server: 10.60.27.191
DNS Server A: 10.60.2.15
DNS Server B:
DNS Search:
OAM Device: bond0
OAM VLAN Id: 32
SIGA VLAN Id: 500
SIGB VLAN Id: 600
SIGC VLAN Id: 700
-----
[OK] [Cancel]
    
```

Figure 14: Initial Configuration - Wireless, MRA Support

Enter the configuration values and then select **OK**, where:

- **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.
- **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**--The OAM network VLAN Id (only applies to c-Class servers or Netra X3-2 RMS; field does not display otherwise).
- **SIG A VLAN Id**--The Signaling-A network VLAN Id (only applies to c-Class servers or Netra X3-2 RMS; field does not display otherwise).
- **SIG B VLAN Id**--The Signaling-B network VLAN Id (only applies to c-Class servers or Netra X3-2 RMS; field does not display otherwise).
- **SIG C VLAN Id**--The Signaling-C network VLAN Id (only applies to c-Class servers or Netra X3-2 RMS; field does not display otherwise).
- **BackplaneDevice**--The backplane bond interface of the OAM device.
- **BackplaneIpPrefix**--The backplane bond interface IP Prefix of the OAM device.

Note: All of the fields listed above are required, except for fields *DNS Server* and *DNS Search*, which are optional but recommended

Note: If you have the optional Ethernet Mezzanine card installed, you will be prompted to select a network layout after you *Set Policy Mode*. If traffic segregation is available and is defined, the SIG-A and SIG-B interfaces will be segregated onto the optional second pair of 6120XG/6125XLG enclosure switches. Do not enable traffic segregation if a second pair of 6120XG/6125XLG enclosure switches are not available. Setting traffic separation information previously occurred after **Initial Configuration** activities, but is now set in the **Set Policy Mode** activities.

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

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

Verifying the Initial Configuration

Once you have made the initial configuration settings, verify the configuration by completing the following procedure:

1. Select **Verify Initial Configuration** from the **Policy Configuration Menu**, and press **Enter**.

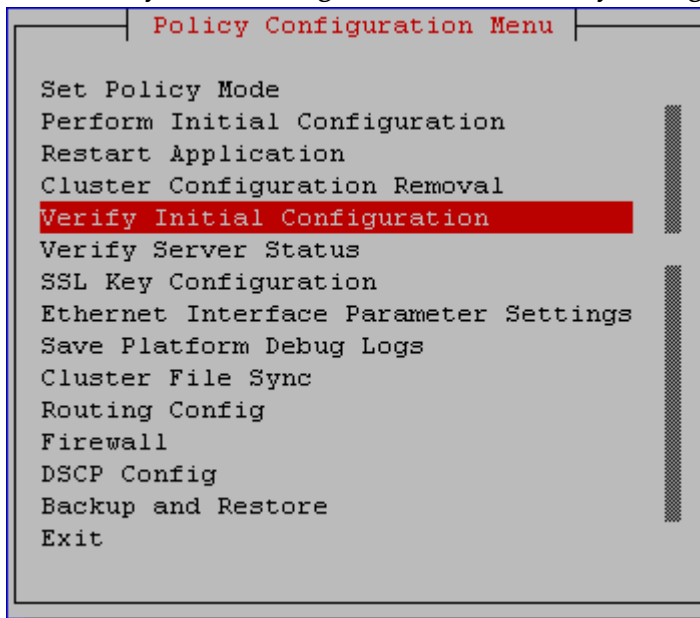


Figure 15: Policy Configuration Menu--Verify Initial Configuration

2. Your initial configuration settings are displayed. For example:

Performing Initial Server Configuration

```
Copyright (C) 2003, 2014, Oracle and/or its affiliates. All rights reserved.
Hostname: cmp241-18

Date/Time: 11/03/2014 09:59:29
Hardware Type: ProLiantBL460cGen8
DNSSearch="qa.ma.tekelec.com"
DNSServerA="130.35.249.52"
DNSServerB=""
DefaultGw="10.148.240.1"
Device="bond0"
HostName="cmp241-18"
LayoutProfile="common"
NtpServIpAddr="10.148.254.47"
OAMDevice="bond0"
OAMVLAN="340"
PMACDevice="bond0"
SIGADevice="bond0"
SIGAVLAN="540"
SIGBDevice="bond0"
SIGBVLAN="640"
ServIpAddr="10.148.241.18/22"
NTP Status:
  remote      refid      st t when poll reach  delay  offset  jitter
-----
*10.148.254.47 10.148.224.1 4 u 753 1024 377 0.130 2.586 1.530
```

Figure 16: Index Table of Contents--Wireless

```
Index Table of Contents
Date/Time: 11/11/2014 13:53:41
Hardware Type: ProLiantDL360G6
BackplaneDevice="bond0"
BackplaneEnable="1"
BackplaneIpPrefix="169.254.88"
DNSSearch=""
DNSServerA=""
DNSServerB=""
DefaultGw="10.240.239.193"
Device="bond2"
HostName="CMP1"
LayoutProfile="directlink"
NtpServIpAddr="10.250.32.10"
OAMDevice="bond2"
SIGADevice="bond1"
SIGBDevice="bond3"
ServIpAddr="10.240.239.205/27"
NTP Status:
  remote      refid      st t when poll reach  delay  offset  jitter
-----
*10.250.32.10 192.5.41.209 2 u 634 1024 377 1.239 -2.515 2.494

[Forward] [Backward] [Top] [Bottom] [Exit]
```

Figure 17: Index Table of Contents--Cable


```

Copyright (C) 2003, 2014, Oracle and/or its affiliates. All rights reserved.
Hostname: brbg-g6-cmp-a                               Index Table of Contents
Date/Time: 11/07/2014 17:03:03
Hardware Type: ProLiantBL4s0eG6
DNSSearch=""
DNSServerA=""
DNSServerB=""
DefaultGW="10.250.84.1"
Device="bond0"
HostName="brbg-g6-cmp-a"
LayoutProfile="common"
TopServIPAddr="10.250.32.10"
S1MDevice="bond0"
S1MVLAN="90"
P1MDevice="bond0"
S1GDevice="bond0"
S1GVLAN="91"
S1ODevice="bond0"
S1OVLAN="92"
ServIPAddr="10.250.84.43/24"
NTP Status:
=====
remote      refid      st t When poll reach  delay  offset jitter
=====
*10.250.32.10  192.5.41.209  2 u 255 1024 377  0.361  -2.846  1.240
    
```

Figure 18: Index Table of Contents--Wireline

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

Verifying the Server Status

After you have made your initial configuration settings, view the **Policy Process Management Status** and the **Server Role** by completing the following procedure:

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

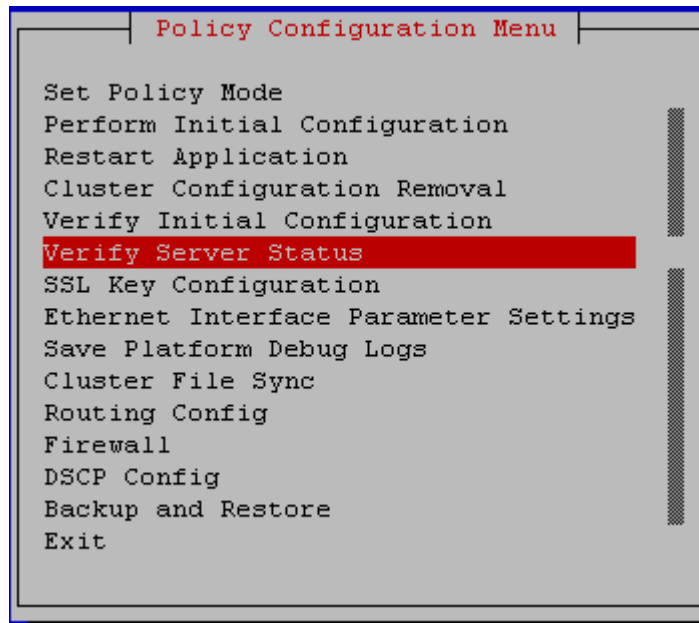


Figure 19: Policy Configuration Menu--Verify Server Status

2. Once fully configured, a server will show the server role as **Active** or **Standby**, (or **Spare**, 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**.

For example:

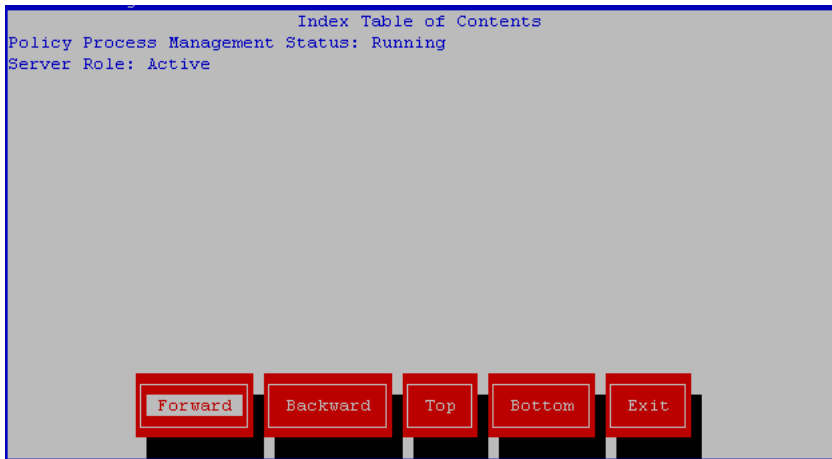


Figure 20: Index Table of Contents--Server Status

Cluster Configuration Removal

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

1. Select **Cluster Configuration Removal** from the **Policy Configuration Menu** screen and press **Enter**.

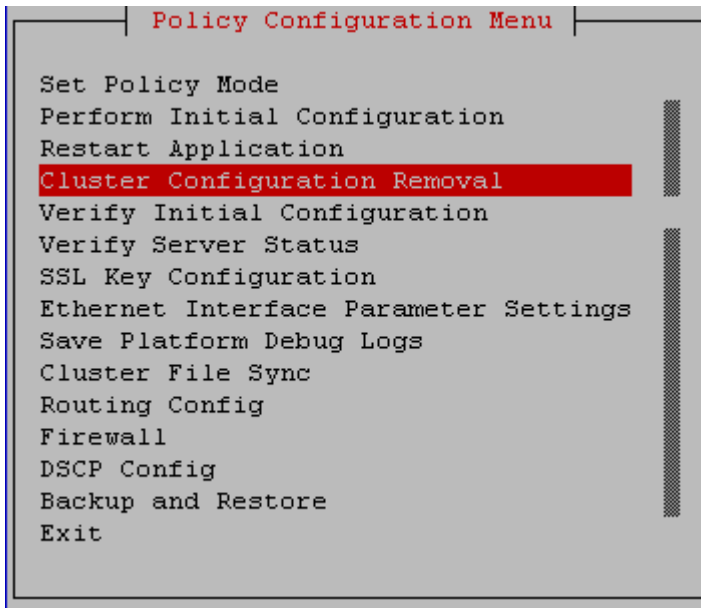


Figure 21: Policy Configuration Menu--Cluster Configuration Removal

2. Select **Cluster Information Cleanup** from the **Cleanup Configuration Menu** screen and press **Enter**.

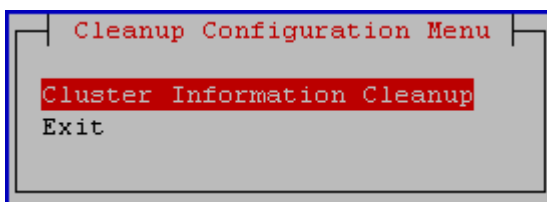


Figure 22: Cleanup Configuration Menu

3. Select **Yes** or **No** from the **Cleaning up cluster information** screen and press **Enter**.

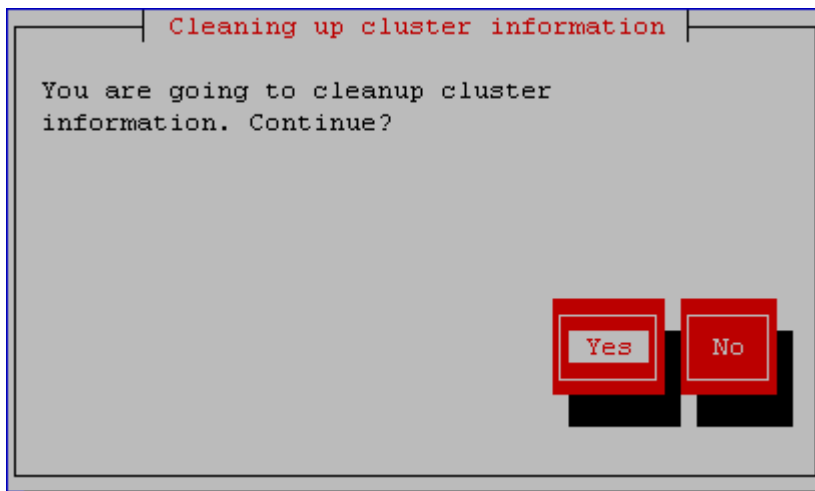


Figure 23: Cleaning up cluster information

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 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.

Configuring Routing

To configure routing, complete the following procedures:

1. Log in to your system as `root` if logging in from the system console. Otherwise, SSH into your system as `admusr`.
2. At the **root** prompt, enter the following command:
`su - platcfg`
3. Or, at the **admusr** prompt, enter the following command:
`sudo su - platcfg`
4. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **Routing Config** from the **Policy Configuration Menu** and press **Enter**.

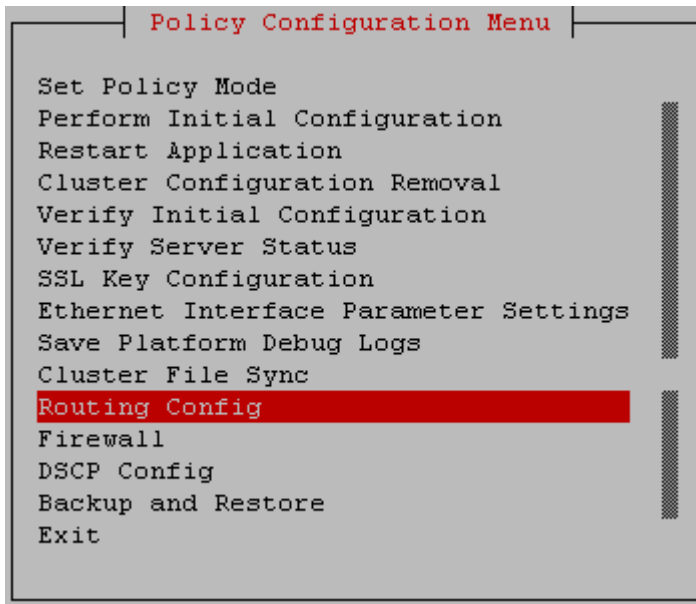


Figure 24: Policy Configuration Menu--Routing Config

6. Select Add Route from the Route Configuration Menu and press Enter.

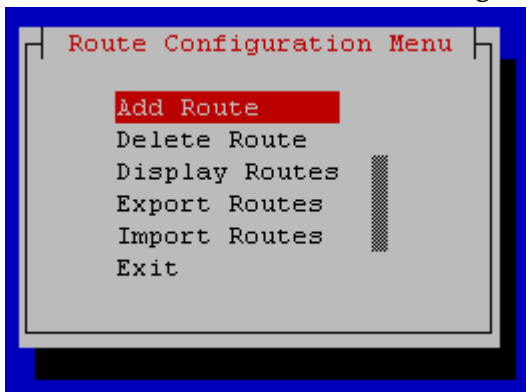


Figure 25: Route Configuration Menu--Add Route

The Add Route configuration screen is displayed. For example:

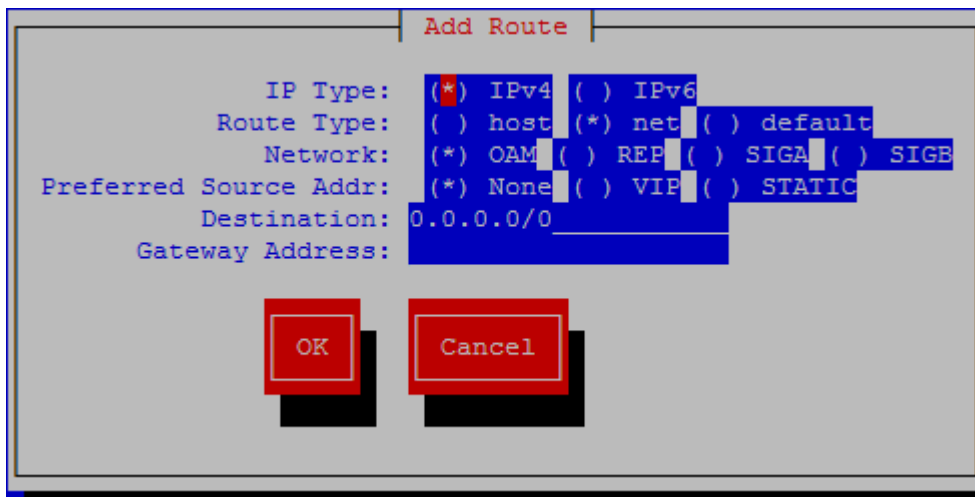


Figure 26: Add Route--Wireless

Note: This screen shot displays a representative example of what available Network choices may be displayed. The actual Network choices will vary depending on product type, hardware type, and operating mode.

7. Edit the information, 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**--Indicates whether this route will be created on the OAM, REP (replication), SIGA, or SIGB interface. Note that the BKUP network is available on CMP servers with the optional mezzanine card installed and also on all Oracle RMS including X3-2 NETRA and X5-2 (non-NETRA only) for all products including CMP, MPE, and MRA.
- **Preferred Source Addr**--Indicates the source address selection for outgoing traffic.

Options include None, VIP, and STATIC. where:

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

Note: See [Table 3: Detailed Behavior of Preferred Source Addr](#) for details about the behavior of Preferred Source Addr.

- **Destination**--Indicates the destination IP address.
- **Gateway Address**--Indicates the gateway address.

Table 3: 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

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

Deleting a Route

To delete an existing route, complete the following procedures:

1. Log in to your system as `root` if logging in from the system console. Otherwise, SSH into your system as `admusr`.
2. At the `root` prompt, enter the following command:
`su - platcfg`

3. Or, at the **admusr** prompt, enter the following command:
`sudo su - platcfg`
4. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **Routing Config** from the **Policy Configuration Menu** and press **Enter**.
6. Select **Delete Route** from the **Route Configuration Menu** and press **Enter**.

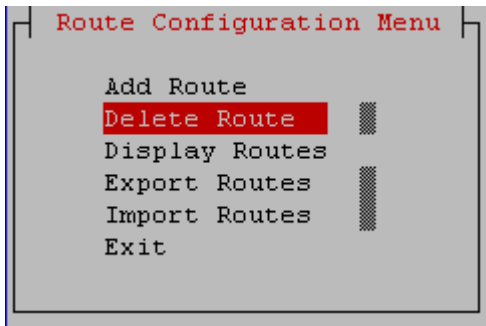


Figure 27: Route Configuration Menu--Delete Route

The **Main Routing Table** screen is displayed. For example:

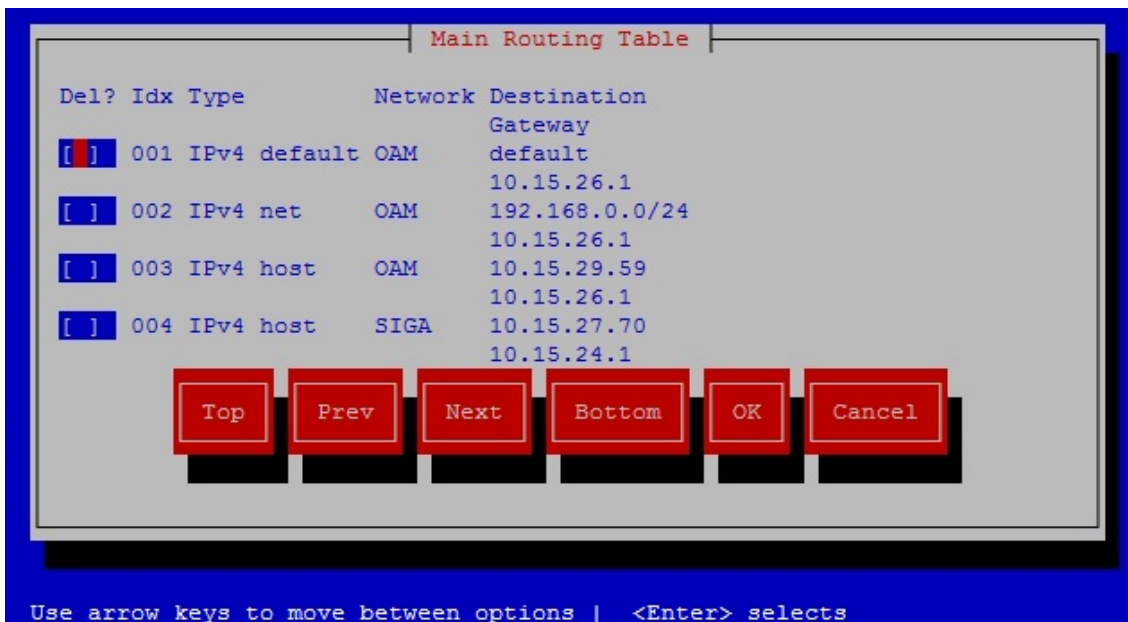


Figure 28: Main Routing Table

7. Select the route to delete by pressing the space bar, then select **OK** and press **Enter**. Use the **Top**, **Bottom**, **Prev**, and **Next** buttons to scroll through the list. More than one route can be deleted at a time.

Note: The route is deleted without warning.

Displaying Configure Routes

To display the configured routes, complete the following procedures:

1. Log in to your system as `root` if logging in from the system console. Otherwise, SSH into your system as `admusr`.
2. At the `root` prompt, enter the following command:
`su - platcfg`
3. Or, at the `admusr` prompt, enter the following command:
`sudo su - platcfg`
4. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **Routing Config** from the **Policy Configuration Menu** and press **Enter**.
6. Select **Display Routes** from the **Route Configuration Menu** and press **Enter**.

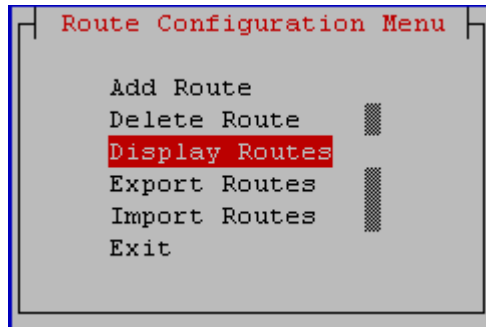


Figure 29: Route Configuration Menu--Display Routes

The configured routes are displayed. For example:

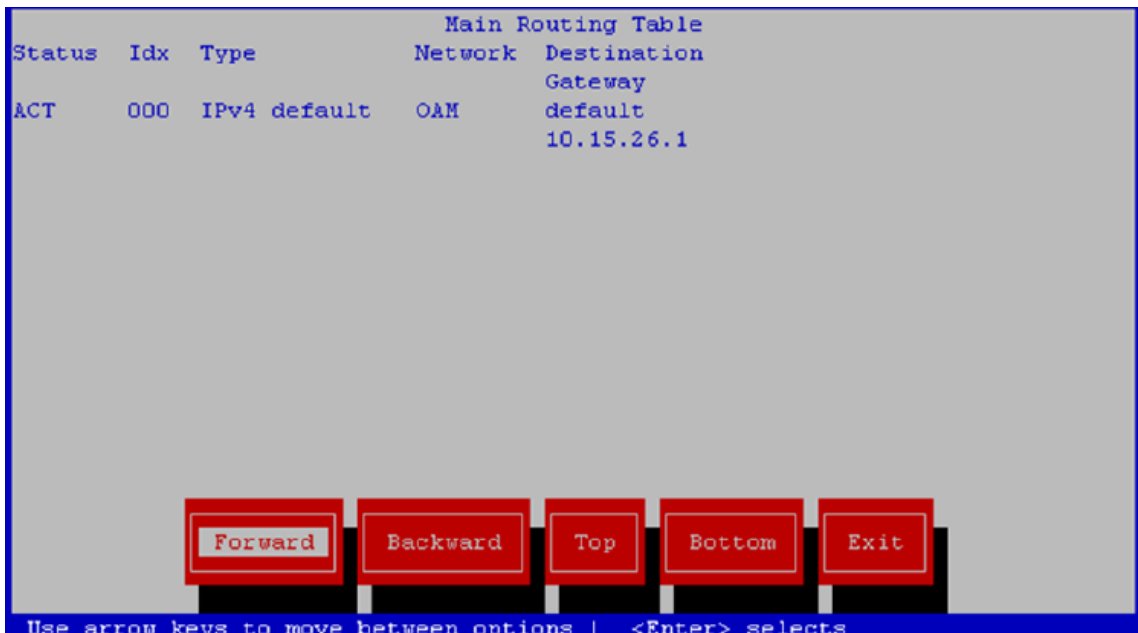


Figure 30: Main Routing Table

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. 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.

Exporting a Route

To export all existing routes, complete the following procedures:

1. Log in to your system as `root` if logging in from the system console. Otherwise, SSH into your system as `admusr`.
2. At the `root` prompt, enter the following command:
`su - platcfg`
3. Or, at the `admusr` prompt, enter the following command:
`sudo su - platcfg`
4. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **Routing Config** from the **Policy Configuration Menu** and press **Enter**.
6. Select **Export Route** from the **Route Configuration Menu** and press **Enter**.

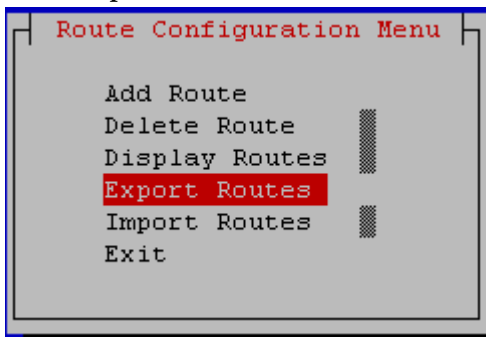


Figure 31: Route Configuration Menu--Export Routes

The **Export Routes To File** screen is displayed. For example:

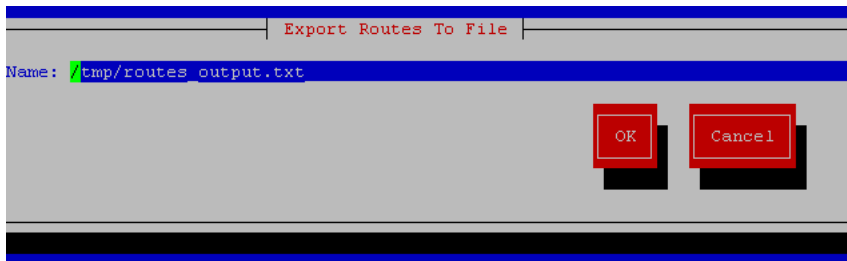


Figure 32: Export Routes To File

7. Specify the location and filename of the routes that 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 procedures:

1. Log in to your system as `root` if logging in from the system console. Otherwise, SSH into your system as `admusr`.
2. At the `root` prompt, enter the following command:
`su - platcfg`
3. Or, at the `admusr` prompt, enter the following command:
`sudo su - platcfg`
4. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **Routing Config** from the **Policy Configuration Menu** and press **Enter**.
6. Select **Import Routes** from the **Routing Configuration Menu** and press **Enter**.

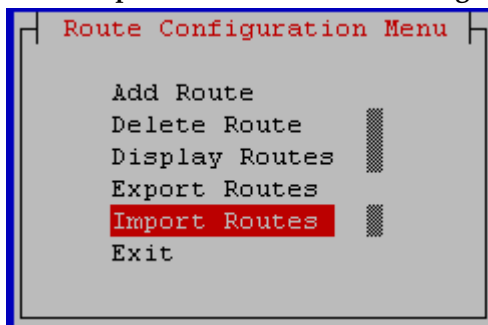


Figure 33: Routing Configuration Menu--Import Routes

The **Import Routes From File** page is displayed. For example:

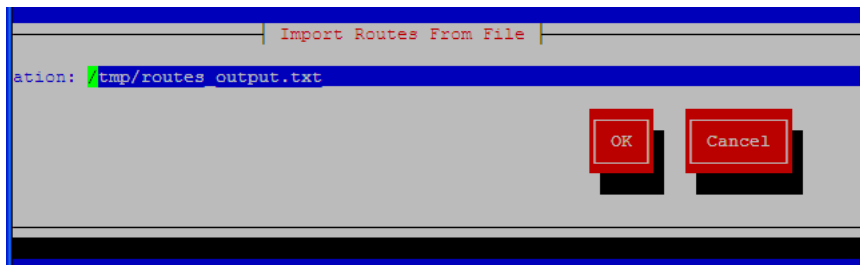


Figure 34: Import Routes From File

7. Specify the location and filename of the routes that 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 the application, enter the following procedures:

Performing Initial Server Configuration

1. Log in to your system as root if logging in from the system console. Otherwise, SSH into your system as admusr.
2. At the **root** prompt, enter the following command: `su - platcfg`
3. Or, at the **admusr** prompt, enter the following command: `sudo su - platcfg`
4. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **Restart Application** from the **Policy Configuration Menu** and press **Enter**.

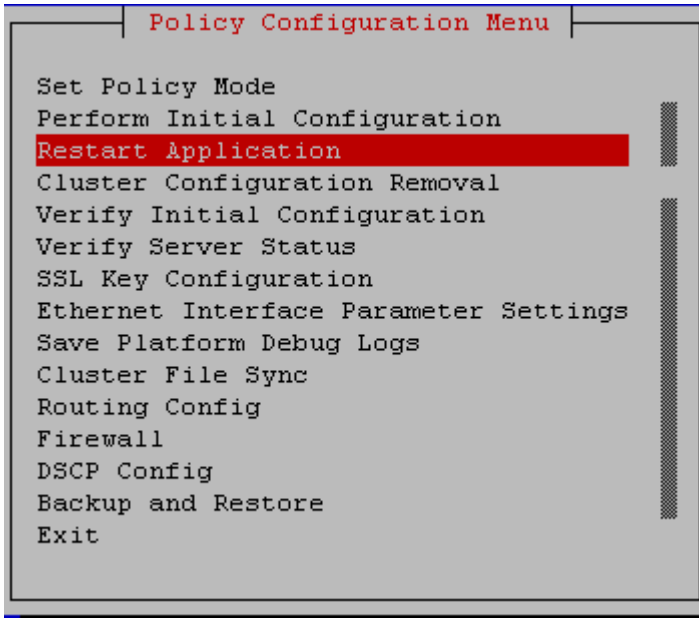


Figure 35: Policy Configuration Menu--Restart Application

You are prompted to continue:



Figure 36: Restart qp_procmgr

Selecting **Yes** 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 will trigger an HA failover.

Configuring Firewall Settings

Note: During the editing of firewall configuration settings, if an attempt is made to leave the **Firewall Configuration Menu** with unsaved changes, you are presented with the options to save changes and exit, exit without saving changes, and to 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** to commit the changes made to the firewall configuration files and restart the firewall.

Note: In the following process, the term **All** indicates open access to any interface, for example: PMAC, REP, OAM, SIG-A, and SIG-B.

To configure firewall settings on the server and restrict access to non-standard ports, complete the following procedures:

1. Log in to your system as `root` if logging in from the system console. Otherwise, SSH into your system as `admusr`.
2. At the `root` prompt, enter the following command:
`su - platcfg`
3. Or, at the `admusr` prompt, enter the following command:
`sudo su - platcfg`
4. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **Firewall** from the **Policy Configuration Menu**, and press **Enter**.

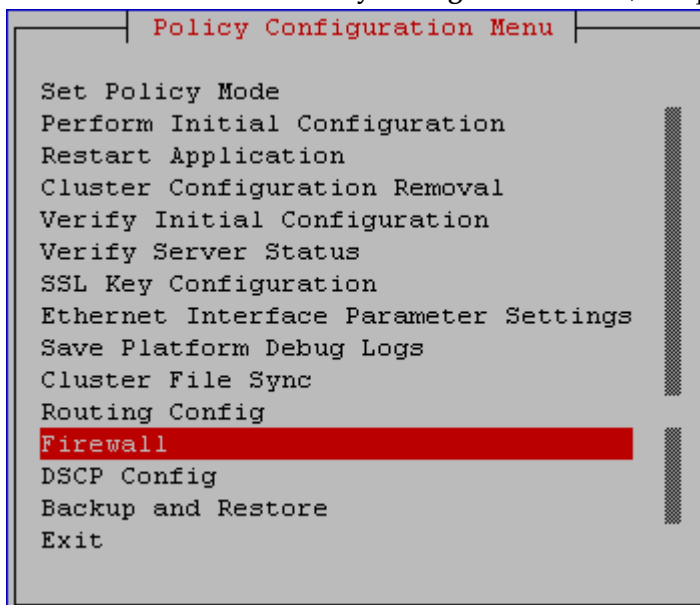


Figure 37: Policy Configuration Menu--Firewall

- To enable the firewall, select **Enable/Disable Firewall** from the **Firewall Configuration Menu** and press **Enter**.

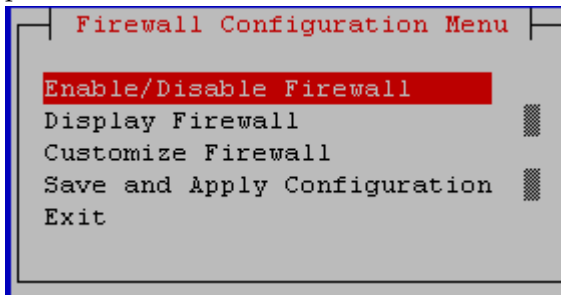


Figure 38: Firewall Configuration Menu--Enable/Disable Firewall

- Select **Edit** from the **Firewall Status** screen and press **Enter**.

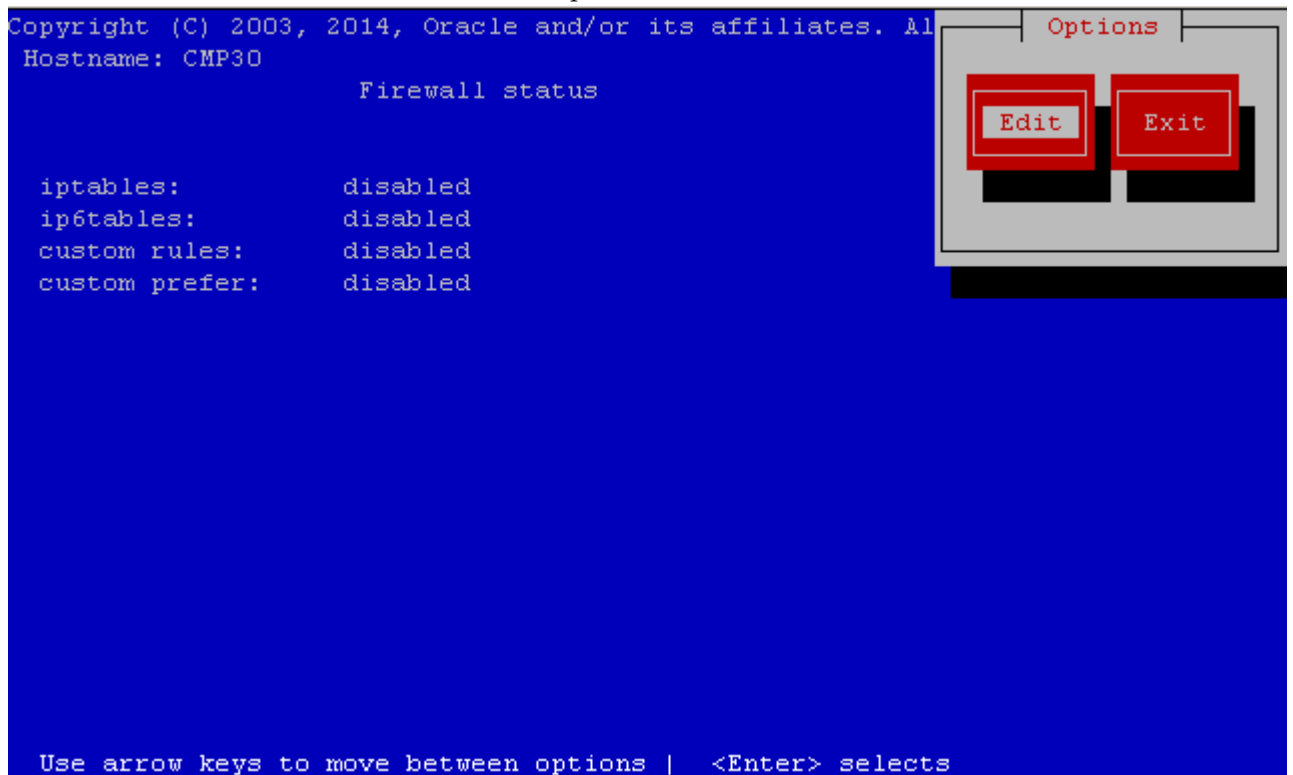


Figure 39: Firewall status screen

- To define which IPv4 and IPv6 firewall to enable or disable, select from the list of interfaces on the **Enable/Disable Firewall Features Menu** and press **Enter**.

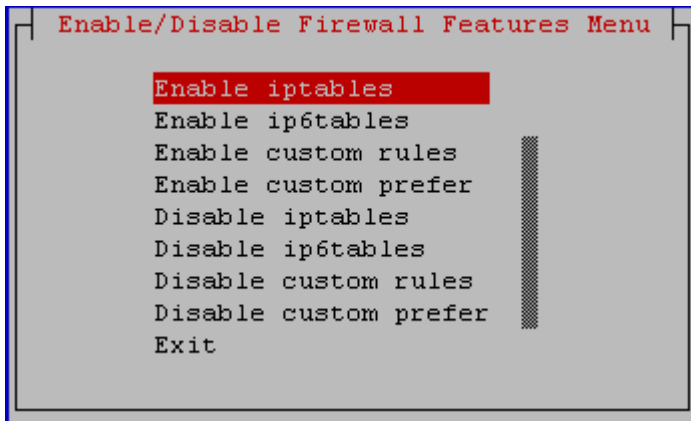


Figure 40: Enable/Disable Firewall Feature Menu

- When prompted to continue, select **Yes** from the **Enable iptables?** or other appropriate dialog screen that appears and press **Enter**.

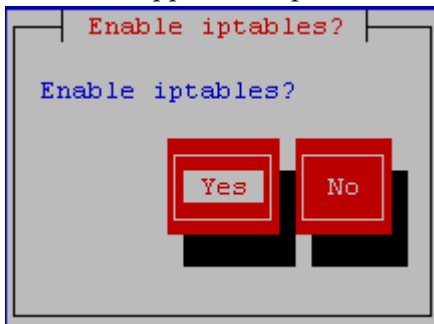


Figure 41: Enable iptables?

Note: By enabling iptables or ip6tables, firewalls are set up with a default set of rules. Default rules allow the product to function as needed, but it may be necessary to open up additional ports.

- The Factory Firewall Rule Set cannot typically be changed, but you may wish to open additional ports in the firewall by enabling custom rules. To open additional ports, select **Enable Custom Rules** from the **Enable/Disable Firewall Features Menu**.

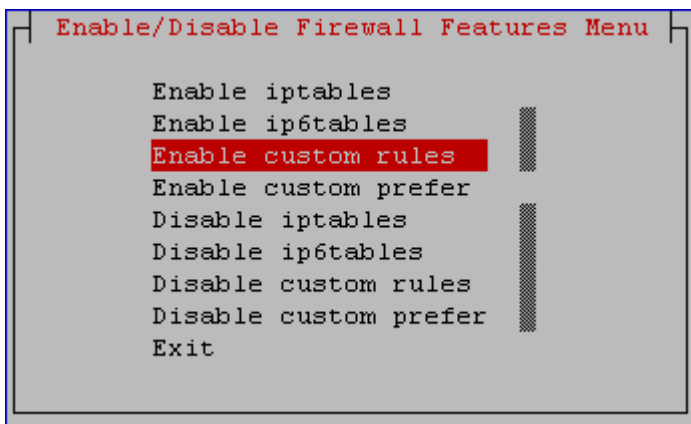


Figure 42: Enable/Disable Firewall Features Menu--Enable custom rules

11. Select **Yes** from the **Enable custom rules?** screen to confirm that custom rules are to be enabled or select **No** to cancel.

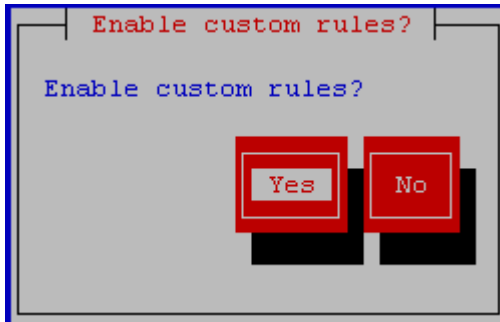


Figure 43: Enable custom prefer feature?

12. 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.). To set custom rules to be used instead of default firewall rules, select **Enable custom prefer** from the **Enable/Disable Firewall Features Menu**.

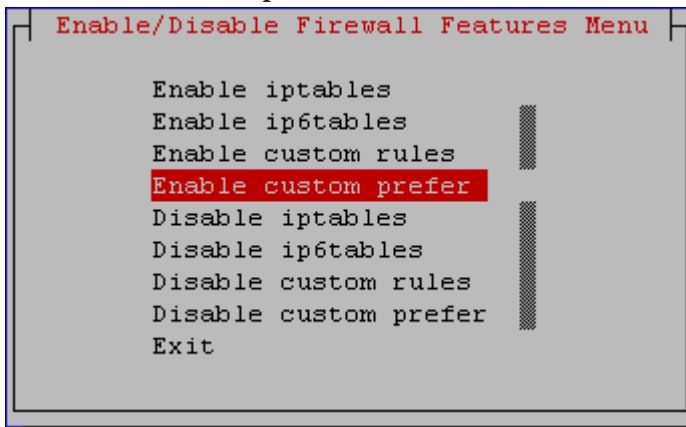


Figure 44: Enable/Disable Firewall Features Menu--Enable custom prefer

13. 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.

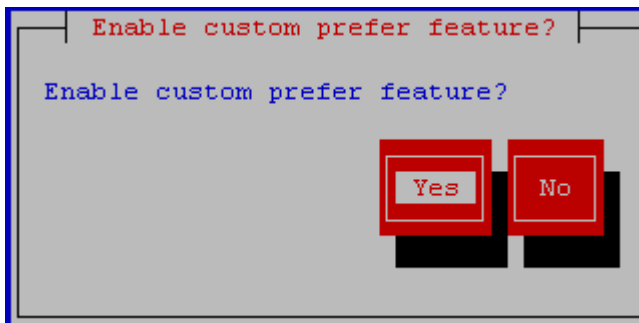


Figure 45: Enable custom prefer feature?

- To add, edit or delete custom firewall rules, select **Customize Firewall** from the **Firewall Configuration Menu**, and press **Enter**.

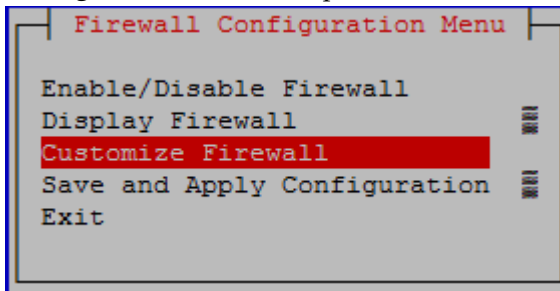


Figure 46: Firewall Configuration Menu--Customize Firewall

- Select **Edit** from the **Firewall Custom Rules** screen and press **Enter**.

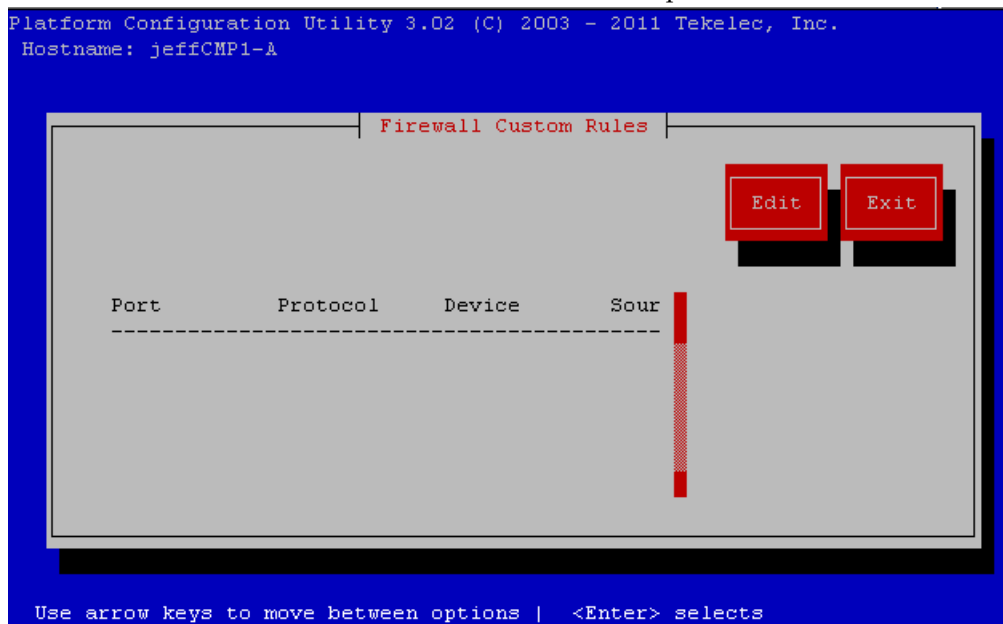


Figure 47: Firewall Custom Rules

- To add a new rule or edit an existing rule, select **Add Rule** or **Edit Rule** from the **Connection Action Menu** and press **Enter**.



Figure 48: Connection Action Menu

- Enter information to customize the firewall rule, then select **OK** and press **Enter**.

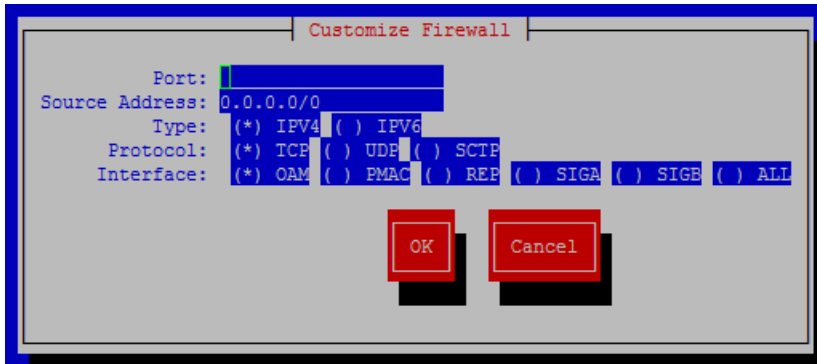


Figure 49: Customize Firewall--Wireless

Note: This screen shot displays a representative example of what available Network choices may be displayed. The actual Network choices will vary depending on product type, hardware type, and operating mode.

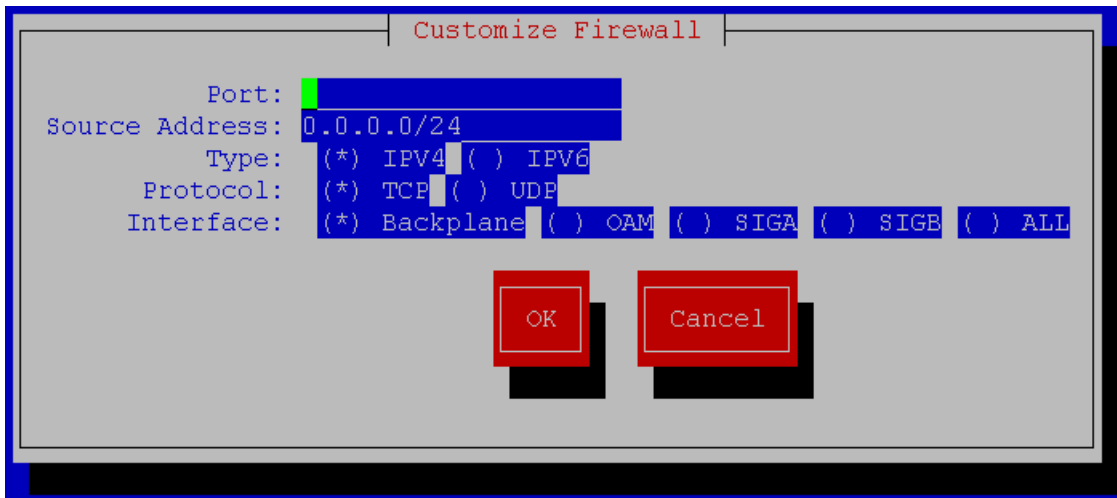


Figure 50: Customize Firewall--Cable

Enter field values. When completed, select **OK** and press **Enter**.

Note: If configuring a CMP with the optional Ethernet mezzanine card or any product on any mode on the Sun Netra X3-2, an additional interface appears called **BKUP**. This interface is dedicated to perform remote archive activities for CMP backup operations. **BKUP** is included if **ALL** is selected for **Interface** on the **Customize Firewall** screen.

The **REP** network selection will appear in the **Interface** screen only for c-Class MPE and MRA servers if a static IP is set in the topology for MPE and MRA. The **REP** selection will not appear for a CMP server or any other Policy Management server.

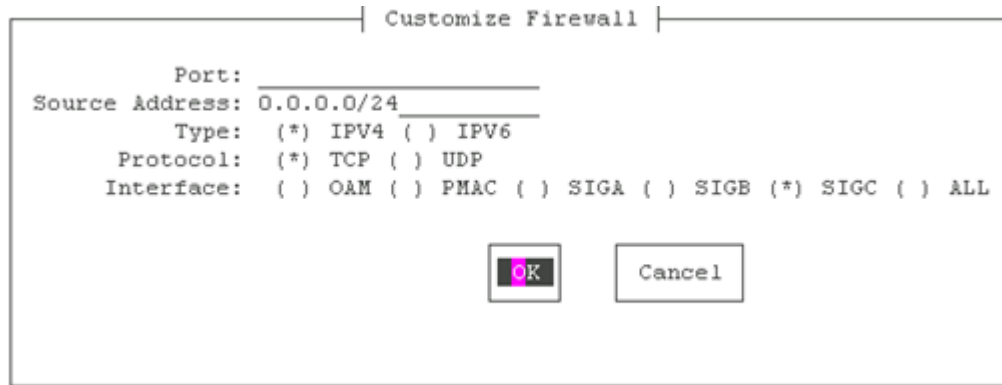


Figure 51: Customize Firewall--CMCC Wireless

Note: Use this screen to customize firewall when using a SIGC interface in a Wireless mode MRA server with c-Class or Netra hardware.

18. To delete an existing custom rule, select **Delete Rule** from the **Connection Action Menu** and press **Enter**. Then, 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**, select **Exit** to return to the **Firewall Configuration Menu**. Then, select **Save and Apply Configuration** from the **Firewall Configuration Menu** and press **Enter** to save all changes.

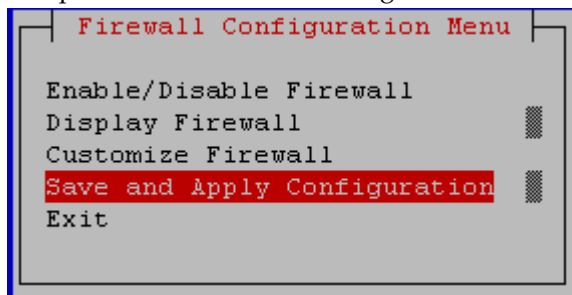


Figure 52: Firewall Configuration Menu--Save and Apply Configuration

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

Displaying Firewall Settings

To display current firewall settings, complete the following procedures:

1. Log in to your system as `root` if logging in from the system console. Otherwise, SSH into your system as `admusr`.
2. At the `root` prompt, enter the following command:


```
su - platcfg
```
3. Or, at the `admusr` prompt, enter the following command:


```
sudo su - platcfg
```

4. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **Firewall** from the **Policy Configuration Menu**, and press **Enter**.
6. Select **Display Firewall** from the **Firewall Configuration Menu** and press **Enter**.

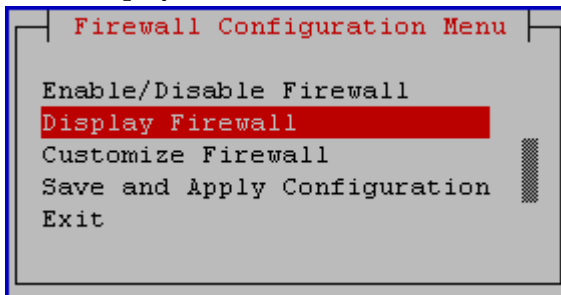


Figure 53: Firewall Configuration Menu--Display Firewall

7. Select the firewall action from the **Display Firewall Menu** and press **Enter**.

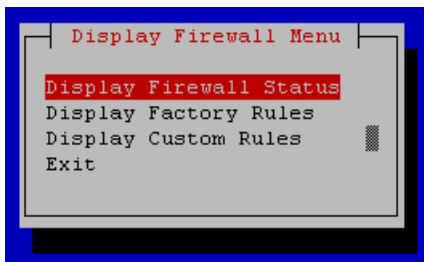


Figure 54: Display Firewall Menu

The following is an example of the **Display Firewall Status** screen:

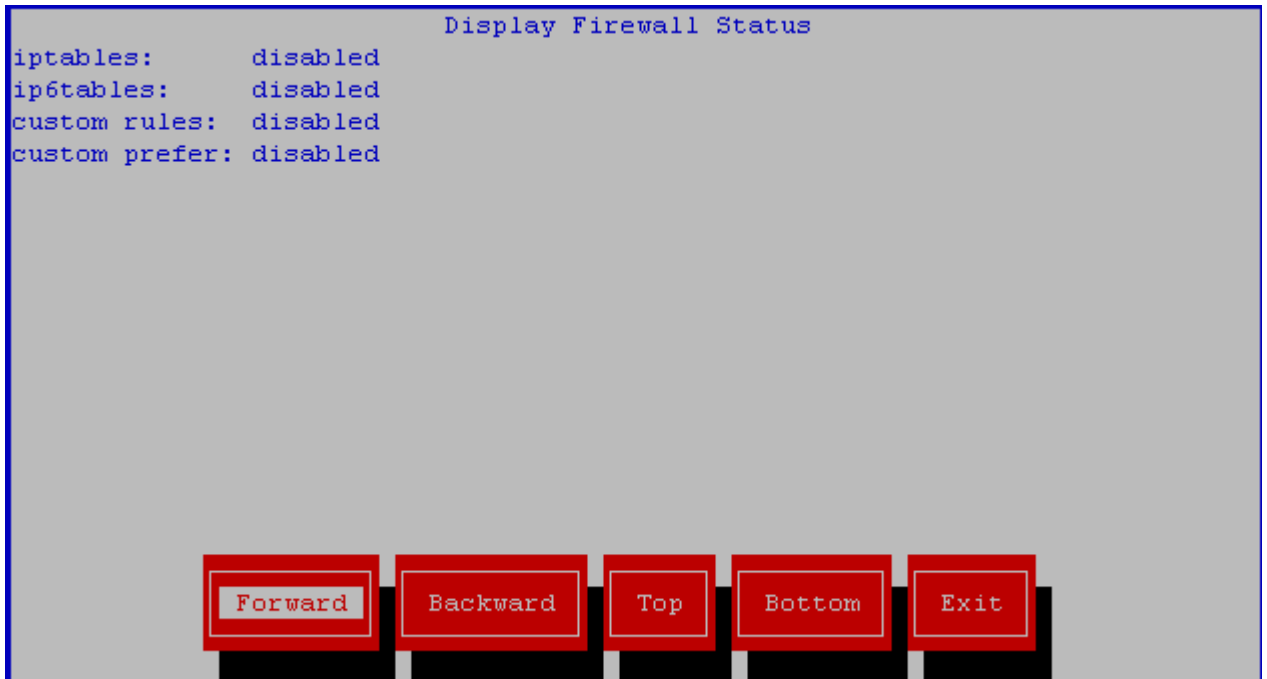


Figure 55: Display Firewall Status

The following is an example of the **Display Factory Rules** screen:

Display Factory Rules						
STATUS	PROTO	SOURCE	IPVER	INTERFACE	PORT	
FW_OFF	tcp	all	both	OAM	mysql	
FW_OFF	tcp	all	both	ALL	http	
FW_OFF	tcp	all	both	ALL	webcache	
FW_OFF	tcp	all	both	ALL	https	
FW_OFF	tcp	all	both	ALL	pcsync-https	
FW_OFF	udp	all	both	ALL	9663	
FW_OFF	tcp	all	both	ALL	ssh	
FW_OFF	udp	all	both	ALL	ntp	
FW_OFF	tcp	all	both	ALL	16810	
FW_OFF	tcp	all	both	ALL	16426	
FW_OFF	tcp	all	both	ALL	16878	
FW_OFF	tcp	all	both	ALL	41207	

Figure 56: Display Factory Rules

The following is an example of the **Display Custom Rules** screen:

Copyright (C) 2003, 2014, Oracle and/or its affiliates. All rights reserved.
 Hostname: netramRA-1C

Display Custom Rules						
STATUS	PROTO	SOURCE	IPVER	INTERFACE	PORT	
ACTIVE	TCP	10.196.100.12/32	IPV4	SIGB	14219	
ACTIVE	TCP	10.196.12.0/23	IPV4	SIGB	14219	
ACTIVE	TCP	10.148.244.0/23	IPV4	ALL	443	

Use arrow keys to move between options | <Enter> selects

Figure 57: Display Custom Rules

Configuring DSCP

Use the options on the DSCP (Differentiated Services Code Point) Configuration menu to manage DSCP configurations. These configurations allow you to operate DSCP on network interfaces (SIG A, SIG B) for a Policy Management device. The configurations are persistent during system power off, reboot, and upgrade. Configurations can also sync to other servers within a cluster.

Menu options include:

- Add a DSCP configuration
- View existing DSCP configurations
- Edit a DSCP configuration
- Delete a DSCP configuration
- Sync a configuration to other servers in cluster

Adding a DSCP Configuration

Use **Add New DSCP Configuration** to add a new DSCP configuration on the network interface and begin DSCP marking of specified packets. Each DSCP configuration is saved to the configuration file in the order in which it is added.

To add a new DSCP configuration, complete the following procedure:

1. Select **DSCP Config** from the **Policy Configuration Menu** and press **Enter**.

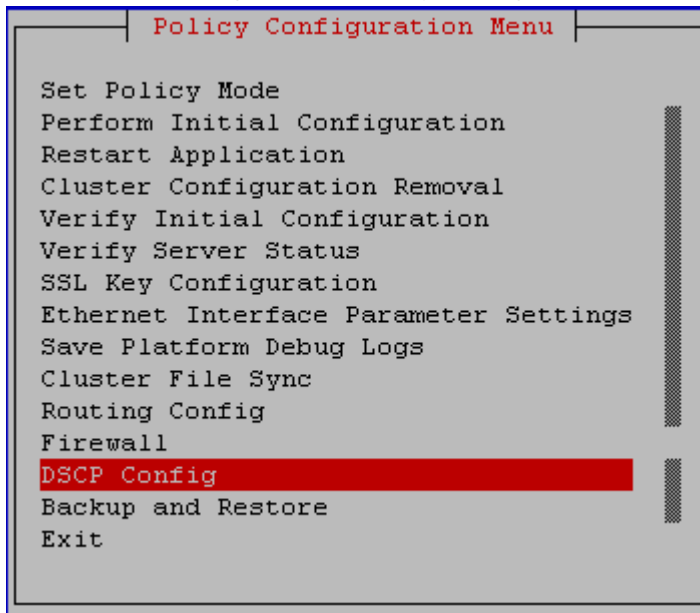


Figure 58: Policy Configuration Menu--DSCP Config

2. Select **Add New DSCP Configuration** from the **DSCP Configuration Menu** and press **Enter**.

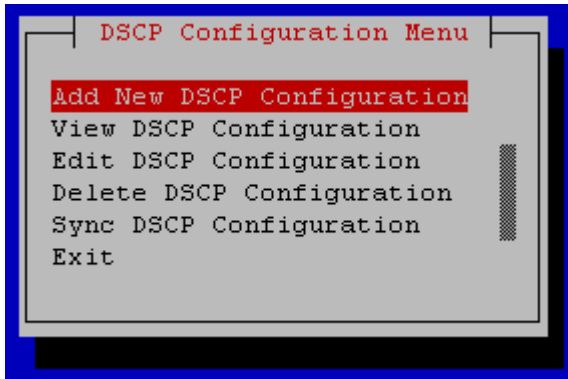


Figure 59: DSCP Configuration Menu--Add New DSCP Configuration

3. Select the desired interface for the new configuration from the **Select Interface** screen, then select **OK** and press **Enter**.

In the Policy Management architecture, network interfaces are segregated into SIGA, SIGB, SIGC, and OAM. The interface SIGA is used to connect to the customer signaling A network; SIGB is used to connect to the customer signaling B network; SIGC is used to connect to the customer signaling C network SIGC is used on MRA only to internally connect to MPE when both SIGA and SIGB were 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. The Configuration includes interface SIGA, SIGB, and SIGC but does not include OAM. Select either SIGA or SIGB for the current DSCP configuration.

If more than one DSCP configuration is added on the same network interface (for example, SIGA), 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.

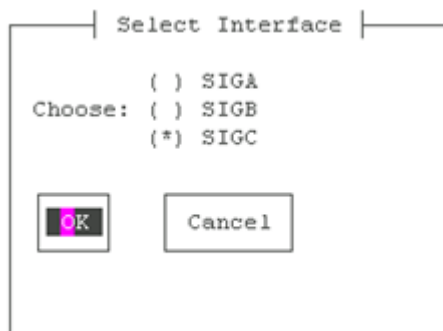


Figure 60: Select Interface

4. Specify the **IP Protocol Version**, **Source IP Address**, and **Destination IP Address** to associate with the new configuration from the **Input Source IP and Destination IP** screen. If no settings are specified here, default settings are used.

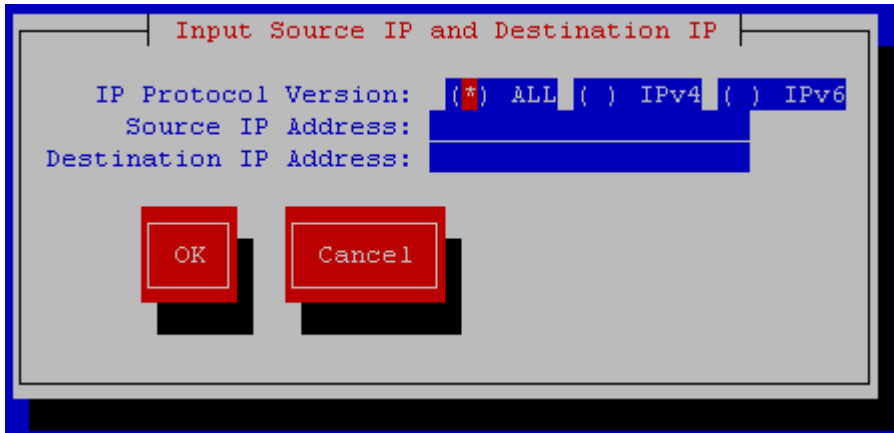


Figure 61: Input Source IP and Destination IP

Select **OK** and press **Enter** to save setting selections and continue to **Code Point selection**.

5. Select the **Code Point** to use with this configuration from the **Code Point selection** window, then select **OK**, and press **Enter**. When the configuration has been saved, DSCP marking begins on the specified packets.

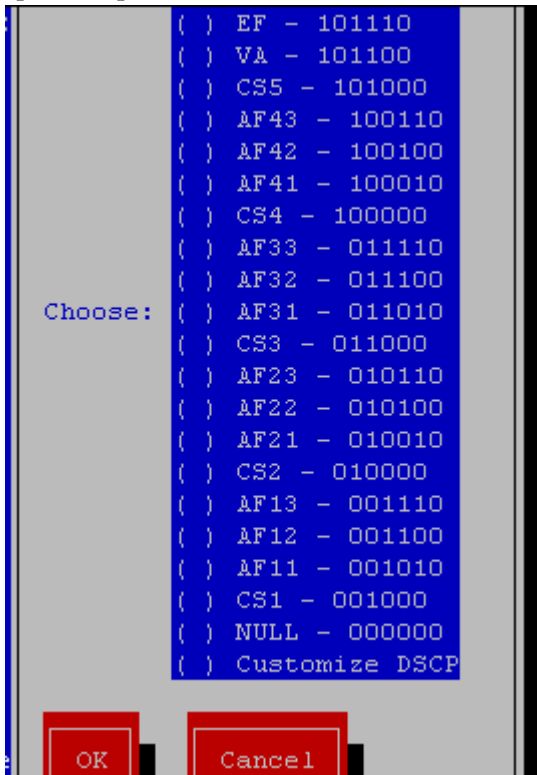


Figure 62: Code Point selection

Viewing DSCP Configurations

To display existing DSCP configurations, complete the following procedures:

1. Select **DSCP Config** from the **Policy Configuration Menu** and press **Enter**.
2. Select **View DSCP Configuration** from the **DSCP Configuration Menu** and press **Enter**

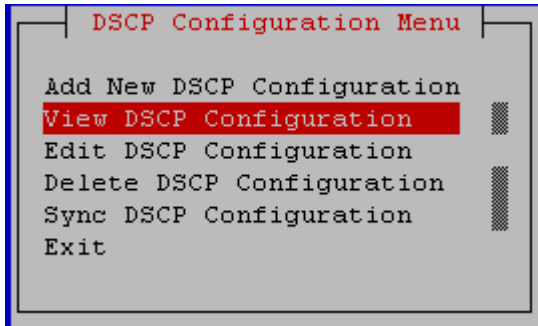


Figure 63: DSCP Configuration Menu--View DSCP Configuration

3. All existing DSCP configurations are displayed.

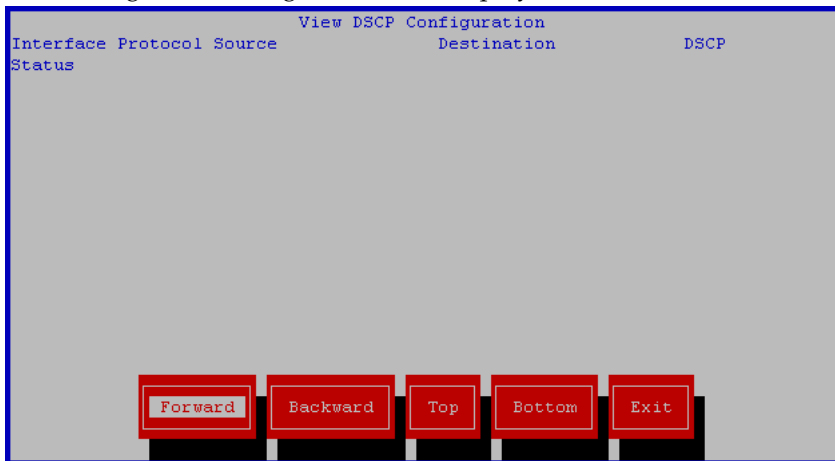


Figure 64: View DSCP Configuration

Editing a DSCP Configuration

To edit an existing DSCP configuration, complete the following procedure:

1. Select **DSCP Config** from the **Policy Configuration Menu** and press **Enter**.
2. Select **Edit DSCP Configuration** from the **DSCP Configuration Menu** and press **Enter**

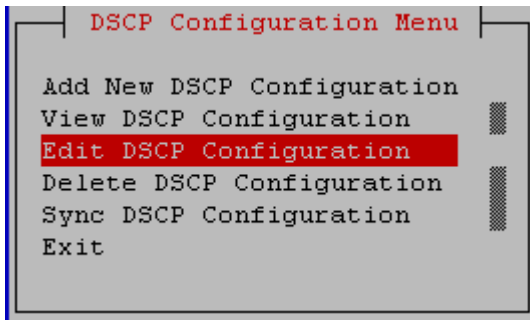


Figure 65: DSCP Configuration Menu--Edit DSCP Configuration

3. All existing DSCP configurations are displayed. Select the configuration to change from the **Edit DSCP Configuration Menu** and press **Enter**.

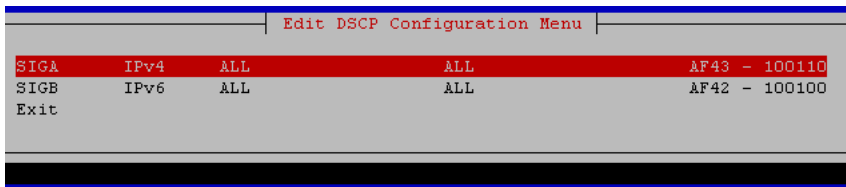


Figure 66: Edit DSCP Configuration Menu

4. Select the interface to use for the configuration from the **Select Interface** screen, then select **OK**, and press **Enter**.

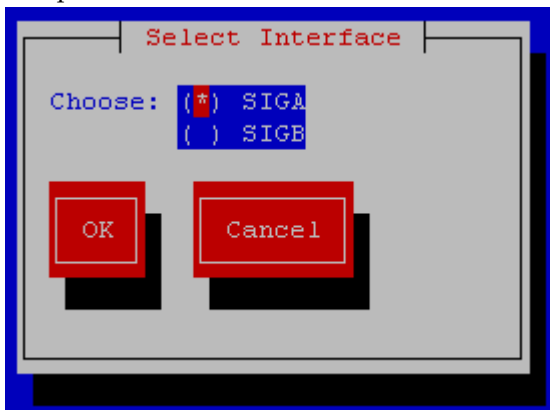


Figure 67: Select Interface

5. Specify the **IP Protocol Version**, **Source IP Address**, and **Destination IP Address** from the **Input Source IP and Destination IP** screen to associate with the configuration. If no settings are specified here, the previous settings are used. Select **OK** and press **Enter** to save setting selections and continue to **Code Point selection**

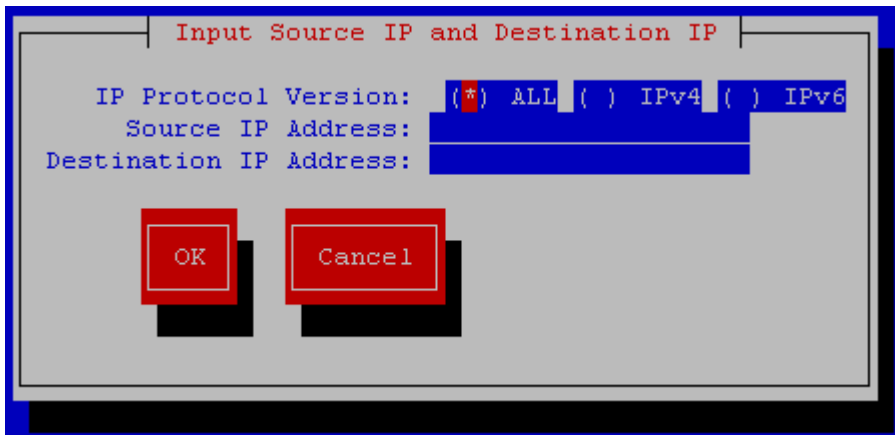


Figure 68: Input Source IP and destination IP

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

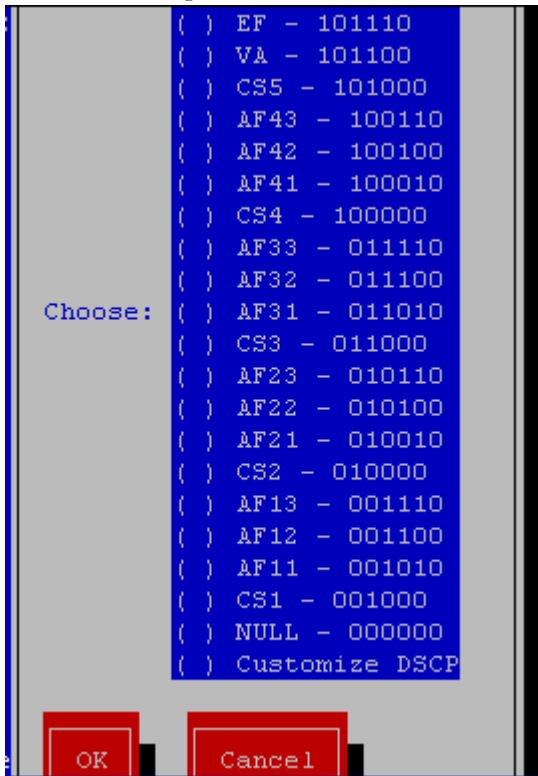


Figure 69: Code Point selection.

Once **OK** is selected, the changes are saved for the configuration, and DSCP marking begins on the specified packets.

Deleting a DSCP Configuration

To delete an existing DSCP configuration, complete the following procedure:

1. Select **DSCP Config** from the **Policy Configuration Menu** and press **Enter**.
2. Select **Edit DSCP Configuration** from the **DSCP Configuration Menu** and press **Enter**

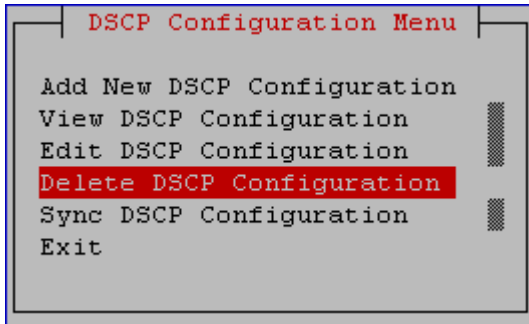


Figure 70: DSCP Configuration Menu--Delete DSCP Configuration

All existing DSCP configurations are then displayed.

3. Select the configuration to delete by pressing the space bar; more than one configuration can be deleted at a time. and Select **OK** and press **Enter**. The selected configuration(s) are deleted.

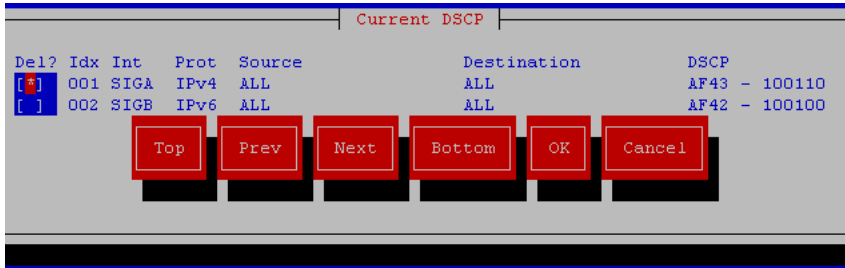


Figure 71: Current DSCP

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.

Syncing DSCP Configurations

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 existing DSCP configurations, complete the following procedure:

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

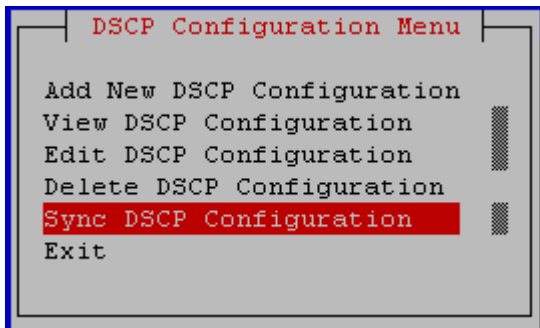


Figure 72: DSCP Configuration Menu--Sync DSCP Configuration

All existing DSCP configurations are then displayed.

3. If the sync is performed from a server that is not the Active server, a warning message appears, giving you the option to abort the sync process. If you select **Yes** to continue, the sync process begins. Once the process is complete, the following message is displayed:

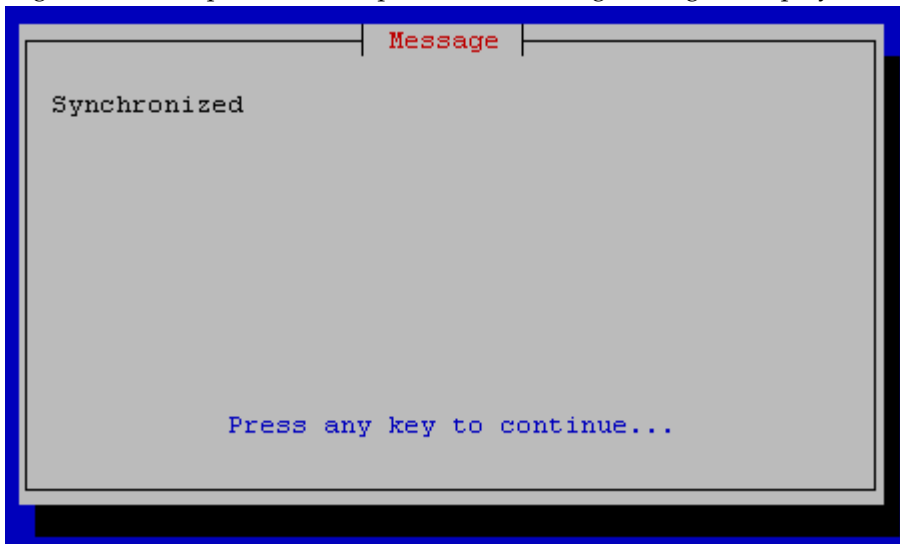


Figure 73: (Sync DSCP) Message

The configurations are copied to the other servers and take effect. The sync status is displayed for each remote server.

Managing Certificates

Topics:

- *Description of Security Certificates.....63*
- *Managing SSL Security Certificates.....63*
- *Using a Local Certificate to Establish a Secure HTTP (https) Web-Browser Session.....67*
- *Establishing a Secure Connection Between a CMP System and a CMP Device.....68*
- *Creating a CA Third-party Signed Certificate...72*

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

Description of Security Certificates

There are two types of security certificates used in a system: self-signed or signed by a 3rd party.

- Self-signed certificates are created locally on each server in platcfg, then synchronized throughout the system to allow encrypted communications between servers. Self-signed certificates are inherently less secure than 3rd 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 3rd party certificates.
- A Certificate Signature Request (CSR) is created locally in the platcfg utility, then is sent to a 3rd party signing authority who generates a signed certificate based on your request. You then synchronize this certificate throughout the system.

The following terminology is related to the management of certificate.

Table 4: Certificate Management Terminology

Term	Definition
Certificate	Used by SSL to verify a trusted server, also known as a Key.
CN (Common Name)	CN is the primary ID inside of a certificate. The Keytool allows you to set this. Keytool refers to the CN as First and Last Name.
First and Last Name	First and Last Name is the primary ID inside of a certificate, also know as the CN. First and Last Name is the way the Keytool refers to this ID.
Key	Used by SSL to verify a trusted server, also known as a Certificate.

Managing SSL Security Certificates

Creating a Self-Signed Certificate

A Certificate, commonly known as a Key, is used by SSL to verify a trusted server. Certificate creation is performed on the local server, and depending on your implementation, on the remote server. This local certificate acts as a Private key for the local server.

Common Name (CN) is the primary ID inside of a certificate. The Keytool allows you to set this; however, the Keytool refers to the CN as First and Last Name.

To create a self-signed key, complete the following:

1. Log in to your system as root if logging in from the system console. Otherwise, SSH into your system as admusr.

2. At the **root** prompt, enter the following command:
`su - platcfg`
3. Or, at the **admusr** prompt, enter the following command:
`sudo su - platcfg`
4. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **SSL Key Configuration** from the **Policy Configuration Menu** and press **Enter**.

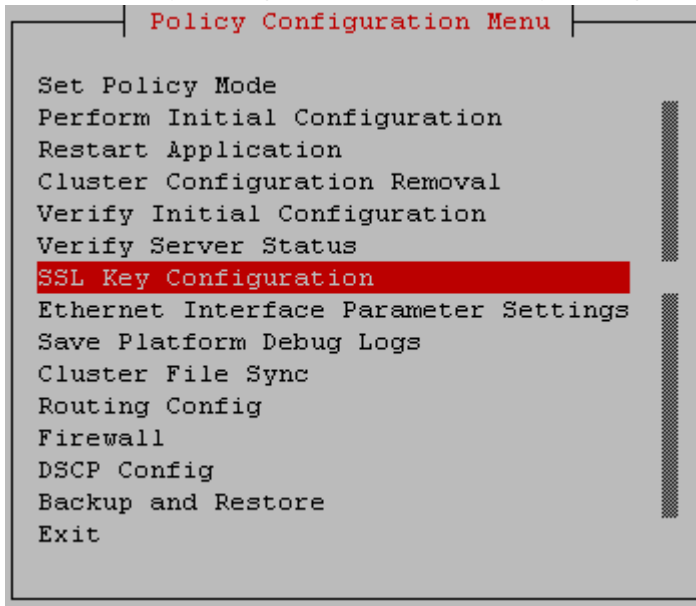


Figure 74: Policy Configuration Menu--SSL Key Configuration

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

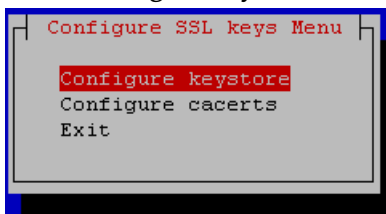


Figure 75: Configure SSL keys Menu- Configure keystore

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

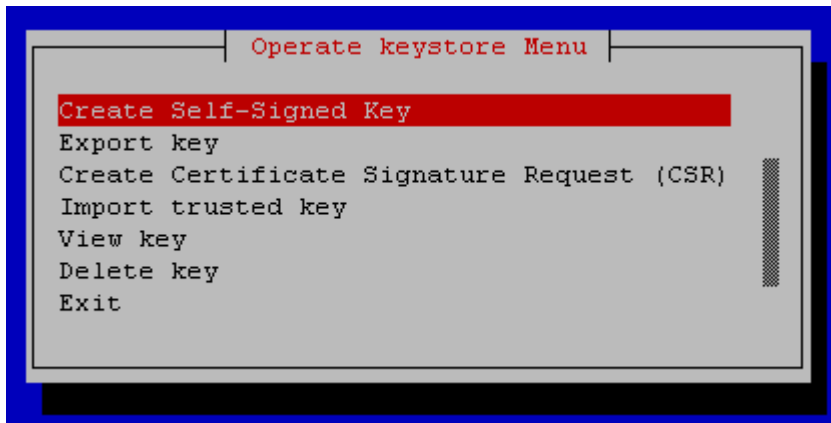


Figure 76: Operate keystore Menu

8. Enter information on the **Keystore Parameters** screen,

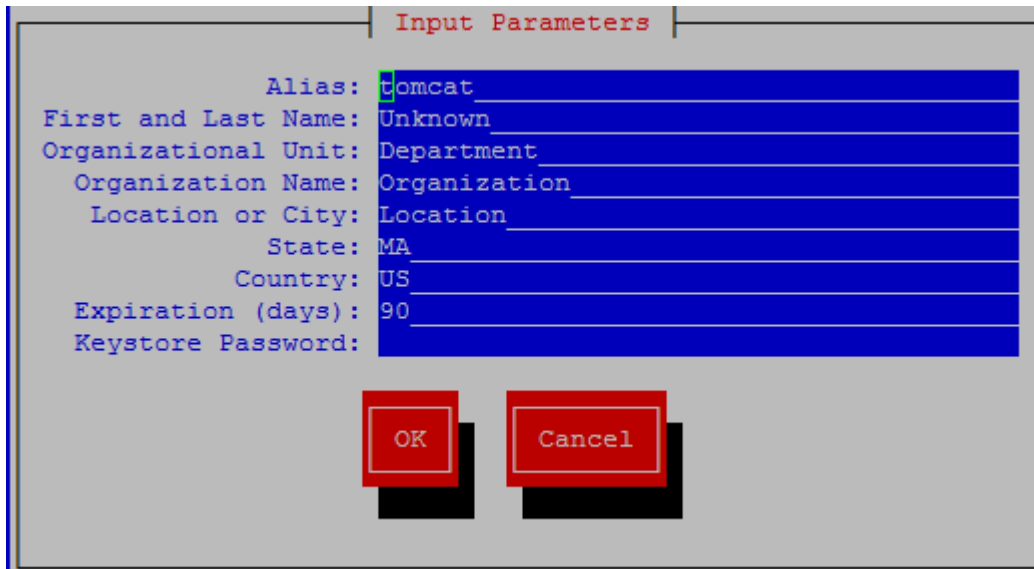


Figure 77: Input Parameters

Note: tomcat must be used for the **Alias** field.

Note: A unique cluster ID name should be used in the **First and Last Name** field (the CN value).

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

Verifying the Self-Signed 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 it is imported into its peer, the secure connection will not be allowed.

To verify the attributes for the SSL certificate, complete the following procedures:

1. Log in to your system as root if logging in from the system console. Otherwise, SSH into your system as admusr.
2. At the **root** prompt, enter the following command:
su - platcfg
3. Or, at the **admusr** prompt, enter the following command:
sudo su - platcfg
4. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **SSL Key Configuration** from the **Policy Configuration Menu** and press **Enter**.
6. Select **Configure keystore** from the **Configure SSL keys Menu** and press **Enter**.
7. Select **View key** and press **Enter**.

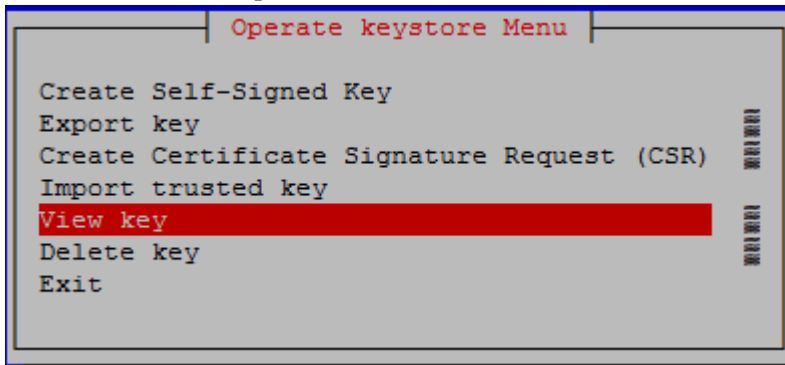


Figure 78: Operate keystore Menu--View Key

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

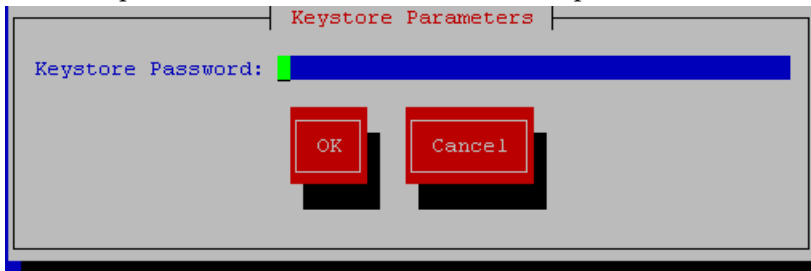


Figure 79: Keystore Parameters

9. Select the certificate and press **Enter**.

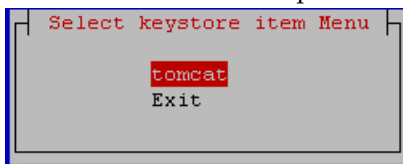


Figure 80: Select keystore item Menu

10. Verify the certificate information. For example:

```

Copyright (C) 2003, 2014, Oracle and/or its affiliates. All rights reserved.
Hostname: cmp241-19

Alias name: cmp243-18
Creation date: Jun 19, 2014
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=Mehul Gogri, O=Oracle, OU=QA, L=Marlborough, ST=MA, C=US
Issuer: CN=Mehul Gogri, O=Oracle, OU=QA, L=Marlborough, ST=MA, C=US
Serial number: c884736
Valid from: Thu Jun 19 15:43:00 EDT 2014 until: Wed Sep 17 15:43:00 EDT 2014
Certificate fingerprints:
    MD5: C5:F8:58:A1:CC:02:95:15:CC:44:16:D3:2B:FF:42:83
    SHA1: 82:40:BF:46:23:77:98:3E:03:AD:E7:79:FF:43:C4:54:07:78:82:9C
    SHA256: 93:96:1C:8A:50:C9:E6:B6:37:75:C7:48:86:6E:45:F7:8B:3C:45:63:35:FF
    Signature algorithm name: SHA256withRSA
    Version: 3

Extensions:
#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: DE 17 AB A7 74 35 32 AD   3B 00 A7 1E 1F 8E 65 25   ....t52.;.....e$
0010: 34 AC E5 7D                               4...
]
]

```

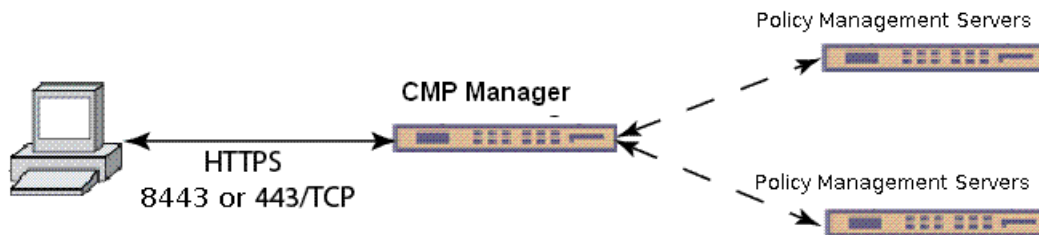
Figure 81: Verify Self-Signed Certificate

From the example, the key portions of the certificate are the **Alias name**, **Owner**, and **Issuer**. These attributes are exported and imported to the other server to establish the secure HTTP session.

11. Select **Exit** and press **Enter**

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.



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

To force end-users to establish an HTTPS session with the CMP system, refer to [Creating a Self-Signed Certificate](#) and [Configuring Firewall Settings](#) to complete the following steps:

1. Exchange and import SSL keys between the CMP and the workstation as described in
2. Enable the firewall on the CMP,
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 will discard this rule, and instead use the custom rule which will allow only 0.0.0.0 to connect via 80 or 8080, which locks down the unencrypted http ports.

Establishing a Secure Connection Between a CMP System and a CMP Device

Note: Procedures used in this chapter may require the rebooting of one or more servers. Subsequently, for 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 Manager Graphical User 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.

Also, when a new certificate is configured, the synchronization will cause HA on the standby server 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 a CMP device server, both the CMP system and the CMP device 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 CMP device server.
2. The CMP device server imports the peer certificate (local certificate created by the CMP system) into its trust store.
3. The CMP device 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 CMP device server) into its trust store.

Exporting the Certificate Signed Request to the Policy Management Servers

To establish a secure connection between the CMP system and a Policy Management server, first ensure that the local certificate signed request has been created on each server or cluster, as described in [Creating a Self-Signed Certificate](#), then complete the following:

1. Log in to your system as `root` if logging in from the system console. Otherwise, SSH into your system as `admusr`.
2. At the `root` prompt, enter the following command:
`su - platcfg`
3. Or, at the `admusr` prompt, enter the following command:
`sudo su - platcfg`
4. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **SSL Key Configuration** from the **Policy Configuration Menu** and press **Enter**.
6. Select **Configure Keystore** from the **Configure SSL keys Menu** and press **Enter**.
7. Select **Export key** from the **Operate keystore Menu** and press **Enter**.

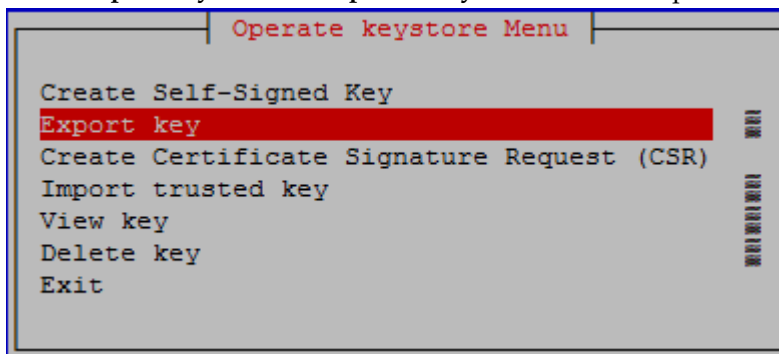


Figure 82: Operate keystore Menu - Export key

8. Enter the **Keystore Password** (changeit), select **OK** and press **Enter**.
9. Press **Enter** to accept the alias tomcat or enter the alias previously created for the certificate.
10. Select a certificate type of binary or ascii from the **Export Certificate** screen, then select **OK** and press **Enter**.

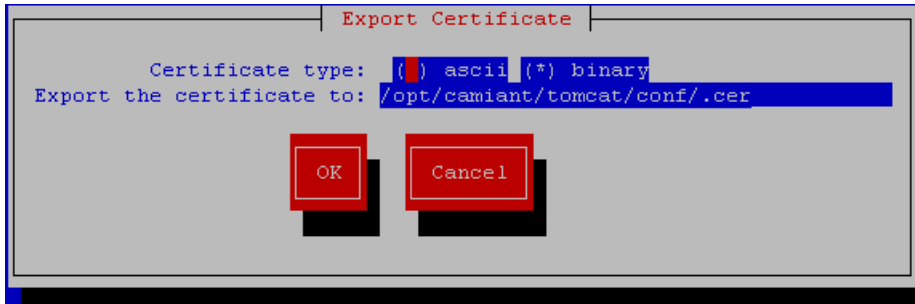


Figure 83: Export Certificate

11. The certificate is exported.

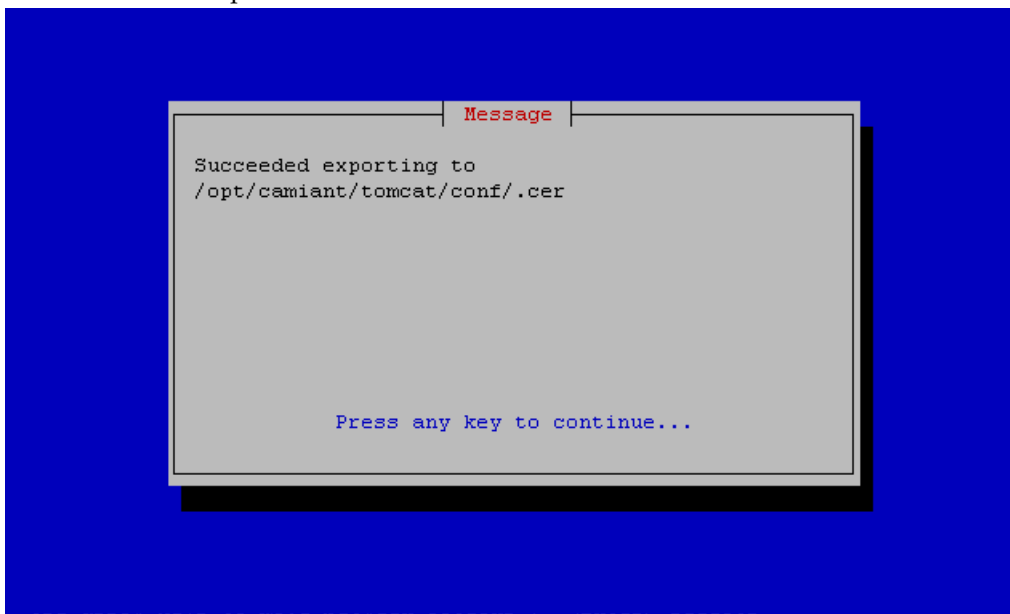


Figure 84: Certificate Message

Importing the Peer Certificate

Once you have exported the local certificate, import the peer certificate (this is the certificate that was exported from the other system) by completing the following procedures:

Note: This procedure 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. Log in to your system as **root** if logging in from the system console. Otherwise, SSH into your system as **admusr**.
2. At the **root** prompt, enter the following command:

```
su - platcfg
```

3. Or, at the **admusr** prompt, enter the following command:

```
sudo su - platcfg
```
4. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **SSL Key Configuration** from the **Policy Configuration Menu** and press **Enter**.
6. Select **Configure cacerts** from the **Configure SSL keys Menu** and press **Enter**.
7. Select **Import trusted key** from the **Operate keystore Menu** and press **Enter**.

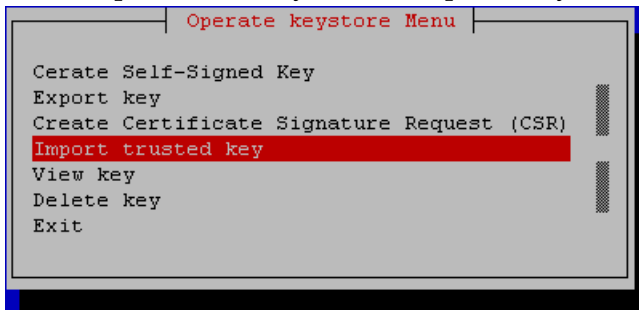


Figure 85: Operate keystore Menu

8. Enter the **Keystore Password** (changeit), select **OK** and press **Enter**.

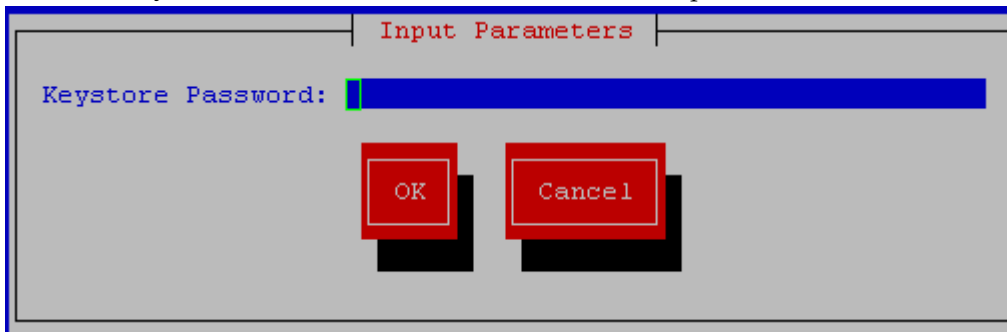


Figure 86: Input Parameters--Keystore Password

9. You are prompted for the import location and alias for the certificate.

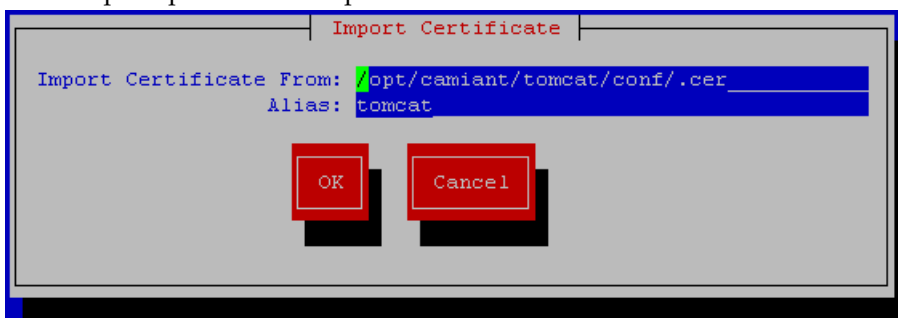


Figure 87: Import Certificate

10. Enter the **Alias** for the certificate, as set previously for the **CN** name, select **OK** and press **Enter**. 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.

11. If the certificate data is correct, select **OK** and press **Enter**.
12. Log in to the CMP system, select the Policy Management server, and click the **Secure Connections** checkbox, located on the **Policy Server** tab. Refer to the CMP user's guide that corresponds to the mode of the system for more information.

Creating a CA Third-party Signed Certificate

Note: This section assumes that no SSL certificates have previously been generated on or imported into the servers. If there are pre-existing certificates on the system (besides the default `tomcat` certificate), please contact [My Oracle Support \(MOS\)](#) to determine its use and importance. Also, read this method in its entirety before starting the operations.

Third-party certificates are implemented as follows:

1. *Remove the Pre-existing Local Certificate*
2. *Generate a Certificate Signature Request, Exporting the Certificate Signed Request to the Policy Management Servers, and Re-import the Third-party Signed Certificates.*
3. *Import the Third-party Peer Certificates*
4. *Synchronize and Reboot the Cluster*

Remove the Pre-existing Local Certificate

On most Policy Management servers, 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, complete the following procedures:

1. Log in to your system as `root` if logging in from the system console. Otherwise, SSH into your system as `admusr`.
2. At the `root` prompt, enter the following command: `su - platcfg`.
3. Or, at the `admusr` prompt, enter the following command: `sudo su - platcfg`.
4. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **SSL Key Configuration** from the **Policy Configuration Menu**, and press **Enter**.
6. Select **Configure Keystore** from the **Configure SSL keys Menu** and press **Enter**.

Figure 88: Configure SSL keys Menu

7. Select **Delete key** from the **Operate keystore Menu** and press **Enter**.

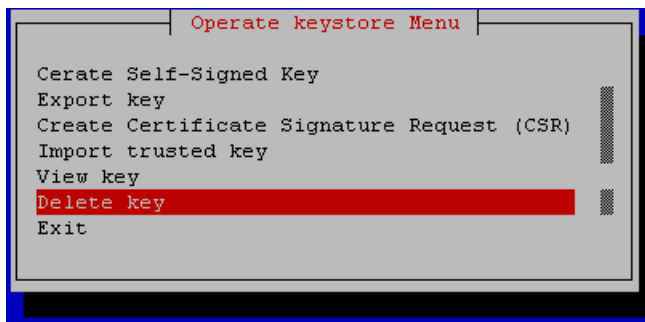


Figure 89: Operate keystore Menu

8. Enter the Keystore Password (changeit), select **OK** and press **Enter**.
9. Select the certificate to be deleted (**tomcat** in this example) and press **Enter**.

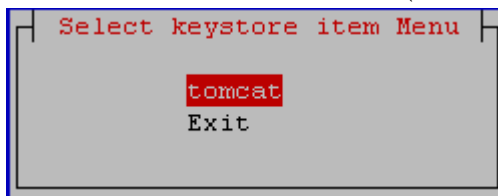


Figure 90: Select keystore item Menu

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**.

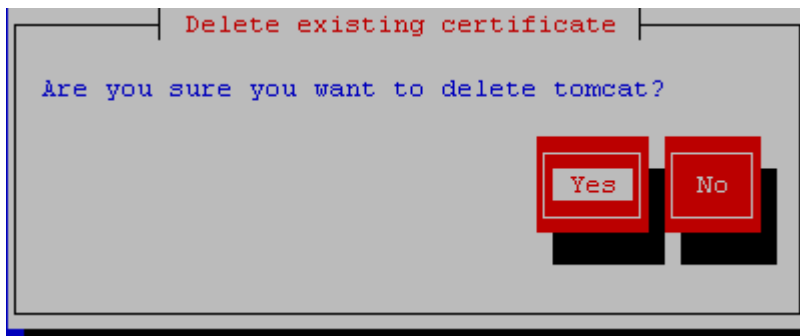


Figure 91: Delete existing certificate

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

Generating a Certificate Signature Request, Exporting for Signing, Re-importing, and Verifying

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

1. *Generate a Certificate Signature Request*
2. *Export the Certificate Signature Request from the System*
3. *Re-import the Third-party Signed Certificates*
4. *Verifying the Self-Signed Certificate*

Generate a Certificate Signature Request

To generate a certificate signature request, complete the following procedures:

1. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
2. Select **SSL Key Configuration** from the **Policy Configuration Menu** and press **Enter**.
3. Select **Configure keystore** from the **Configure SSL keys Menu** and press **Enter**.
4. Select **Create Certificate Signature Request (CSR)** from the **Operate keystore Menu** and press **Enter**.

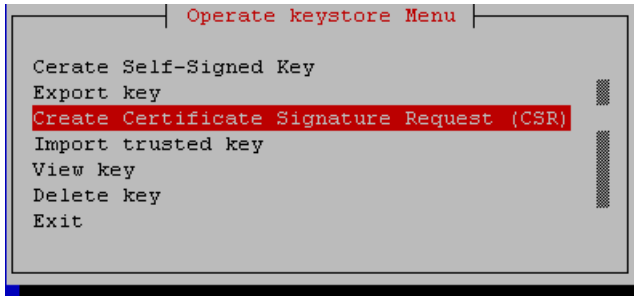
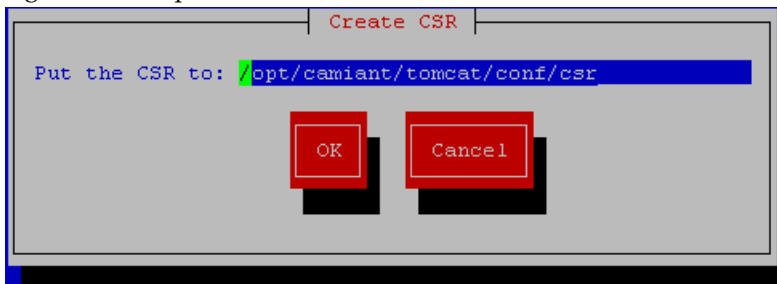


Figure 92: Operate keystore Menu--Create Certificate Signature Request (CSR)

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



Note: The alias (certificate) value is 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 that the certificate does not expire before any peer certificates. A value preventing expiration before 2019 is recommended.

7. Select **OK** to accept the keystore destination, and press **Enter**. The following screen is displayed:

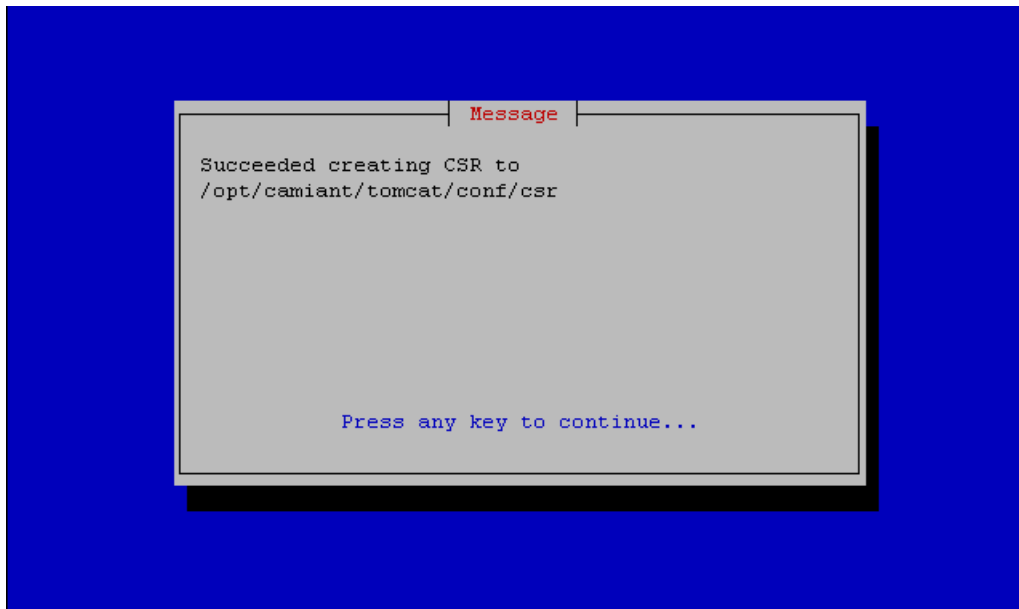


Figure 93: Message--CSR success

Export the Certificate Signature Request from the System

To export a locally generated certificate signature request, complete the following procedures:

1. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
2. Select **SSL Key Configuration** from the **Policy Configuration Menu** and press **Enter**.
3. Select **Configure keystore** from the **Configure SSL keys Menu** and press **Enter**.
4. From the **Policy Configuration Menu**, select **SSL Key Configuration** and press **Enter**.
5. Select **Export key** and from the **Operate keystore Menu** and press **Enter**.
6. Enter the **Keystore Password** (changeit), select **OK** and press **Enter**.
7. 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.

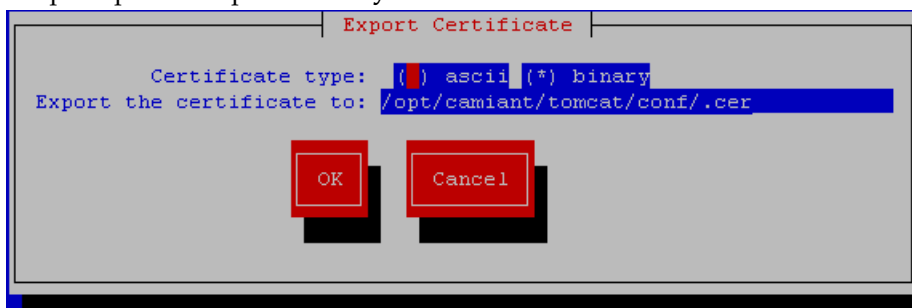


Figure 94: Export Certificate

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

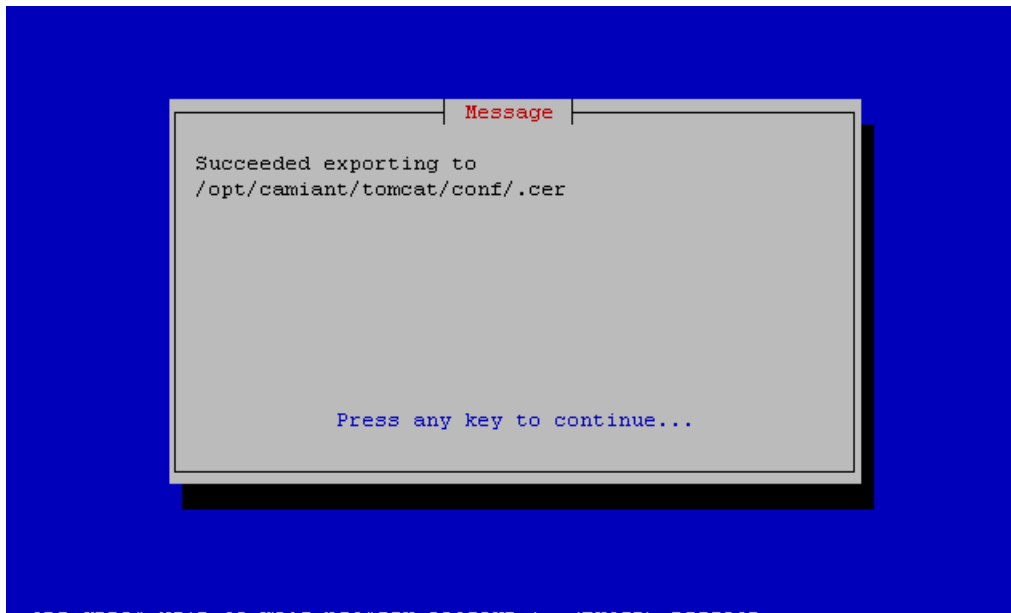


Figure 95: Export Success Message

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

Re-import the Third-party Signed Certificates

After the certificate has been signed by the third party, two certificate files are returned by them for importing into the Policy Management servers. One of these files is a signed local client certificate and the other is a certificate authority (CA), peer certificate. Both certificates must be imported into the system for proper SSL communication.

Note: It may necessary to edit the returned files to remove extraneous debugging information in the certificate. This must be accomplished using a 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.

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 Policy Management servers to be able to import the local certificate successfully, the CA certificate must be merged into this file as well. To do this, copy the BEGIN/END certificate text block from the CA certificate and then paste the blocks 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 cert that was provided by the third-party signer. An example of what this should look like is as follows:

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAligAwIBAgIBBTANBgkqhkiG9w0BAQUFADCBjDELMAkGA1UEBhMCMVMx
```

```
<text removed>
gJeTRnZwMJEXv71V85NGobVGqb1uR94kIQazFP5HC2b2C0Q=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDjTCCAvagAwIBAgIJAJCKgXrXbhQ/MA0GCSqGSIb3DQEEBQUAMIGMMQswCQYD
<text removed>
YVPOATiFnrt1B9Qb1P8kW8lwPmG88Gg6nqtto1hAnIi/1WBcp+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, complete the following procedures:

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

The certificate data displays for verification. To avoid confusion, though they may be different, ensure that the **Owner** and **Issuer** names used for the certificate match 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.

Note: The alias entered **MUST** match the alias originally used to Create the Certificate Request.

7. Next, import the CA signed certificate. Select **Import trusted key** from the **Operate cacerts Menu** and press **Enter**
8. Enter the **Keystore Password** (*changeit*), select **OK** and press **Enter**. You are prompted for the location of the certificate to be imported.
9. Select or enter the location where the certificate is located and the certificate alias name, then select **OK** and press **Enter**.

The certificate data displays for verification. To avoid confusion, though they may be different, ensure that the **Owner** and **Issuer** names used for the certificate match 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.

Note: The alias entered **MUST** match the alias originally used to Create the Certificate Request.

Import the Third-party Peer Certificates

In addition to the certificates that were imported in section [Re-import the Third-party Signed Certificates](#), you must also import a pair of peer certificates from the third party to connect to and communicate with their server (versus their client communicating with the Policy Management servers).

The third party will provide a set of new client and CA certificate files, both of which will be imported to the Policy Management servers as peer certificates.

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 Policy Management servers in advance, or store them somewhere on the network accessible via SCP. To import the certificate, complete the following procedures:

1. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
2. Select **SSL Key Configuration** from the **Policy Configuration Menu** and press **Enter**.
3. Select **Configure keystore** from the **Configure SSL keys Menu** and press **Enter**.
4. Select **Import trusted key** from the **Operate keystore Menu** 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 Request.

Synchronize and Reboot the Cluster

In order for the new certificates to take effect, all cluster servers must be synchronized and then rebooted for the certificates to take effect on the CMP system.

- To synchronize, refer to [Performing File Synchronization](#)
- To reboot, refer to the CMP user's guide corresponding to the system mode.

Chapter 5

Synchronizing Files

Topics:

- *Managing Cluster Sync Configurations.....80*
- *Showing Sync Configuration.....84*
- *Showing Sync Destination.....85*
- *Showing Sync Status.....86*
- *Performing File Synchronization.....87*

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

Files should be synchronized after any of the following are configured:

- Routes (Routing Config)
- Firewall (Firewall)

Managing Cluster Sync Configurations

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

- [Reading Destination from COMCOL](#)
- [Adding a Sync File](#)
- [Deleting a Sync File](#)

Reading Destination from COMCOL

To read the cluster sync destination from COMCOL, complete the following procedures:

1. Log in to your system as **root** if logging in from the system console. Otherwise, SSH into your system as **admusr**.
2. At the **root** prompt, enter the following command:
`su - platcfg`
3. Or, at the **admusr** prompt, enter the following command:
`sudo su - platcfg`
4. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **Cluster File Sync** from the **Policy Configuration Menu** and press **Enter**.

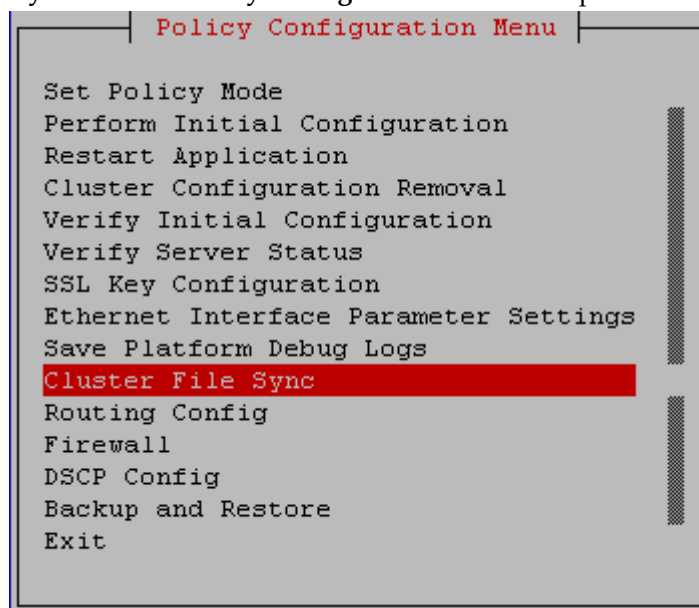


Figure 96: Policy Configuration Menu--Cluster File Sync

6. Select **Cluster Sync Config** from the **Cluster Configuration Sync Menu** and press **Enter**.

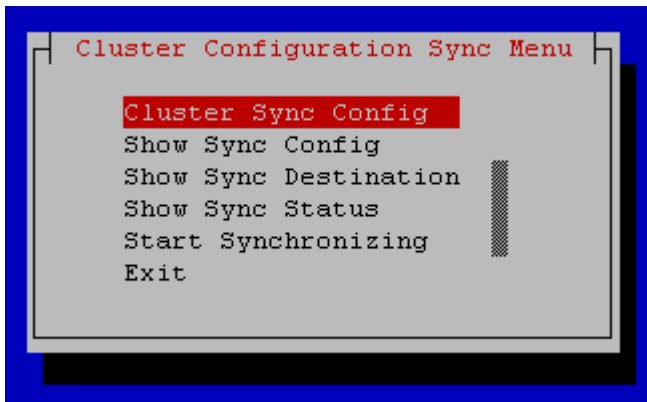


Figure 97: Cluster Configuration Sync Menu--Cluster Sync Config

7. Select Read Destination from Comcol from the Config the Destination of Cluster Sync Menu and press Enter.

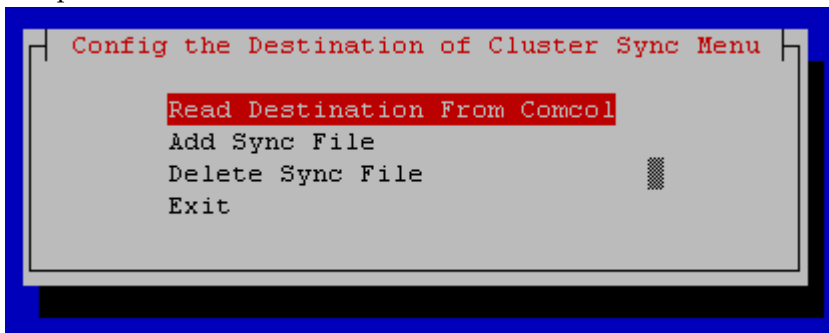


Figure 98: Config the Destination of Cluster Sync Menu--Read Destination from COMCOL

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

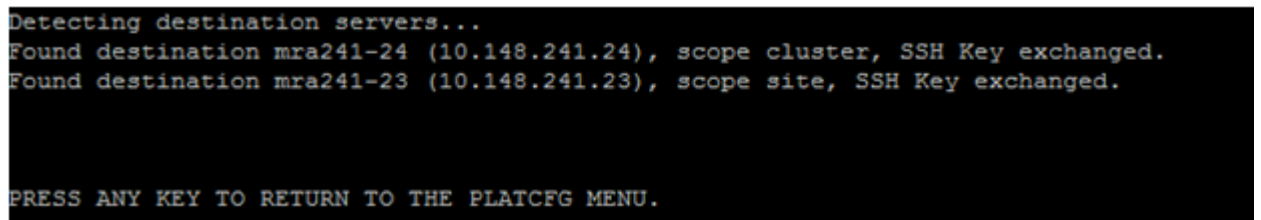


Figure 99: Detecting destination servers

Adding a Sync File

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

1. Log in to your system as root if logging in from the system console. Otherwise, SSH into your system as admusr.
2. At the **root** prompt, enter the following command:
`su - platcfg`

3. Or, at the **admusr** prompt, enter the following command:
`sudo su - platcfg`
4. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **Cluster File Sync** from the **Policy Configuration Menu** and press **Enter**.
6. Select **Cluster Sync Config** from the **Cluster Configuration Sync Menu** and press **Enter**.
7. Select **Add Sync File** from the **Config the Destination of Cluster Sync Menu** and press **Enter**.

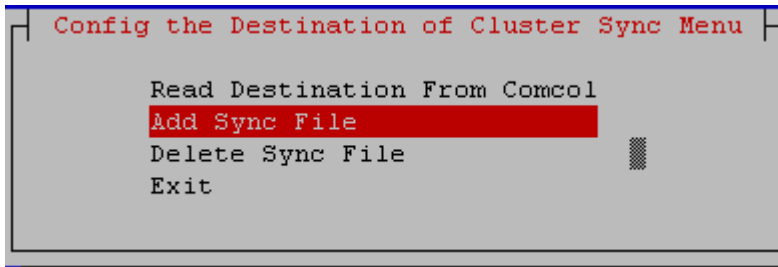


Figure 100: Config the Destination of Cluster Sync Menu--Add Sync File

8. The Add a Sync File screen is displayed.

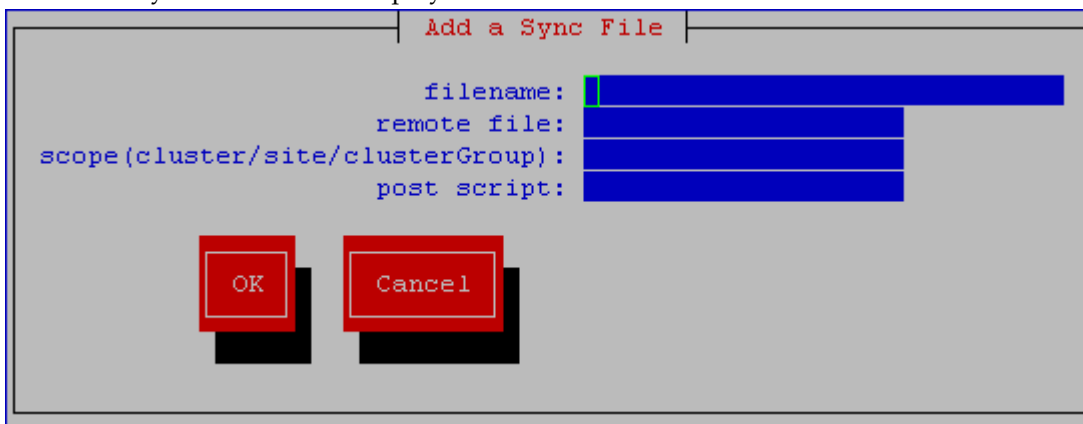


Figure 101: Add a Sync File

9. Enter data into the fields, where:
 1. **filename**--The name of the sync file.
 2. **remote file**--The name of the sync file if different at the remote site.
 3. **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.
 4. **post script**--
10. Select **OK** and press **Enter**
 The new cluster sync configuration is saved.

Deleting a Sync File

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

1. Log in to your system as `root` if logging in from the system console. Otherwise, SSH into your system as `admusr`.
2. At the `root` prompt, enter the following command:
`su - platcfg`
3. Or, at the `admusr` prompt, enter the following command:
`sudo su - platcfg`
4. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **Cluster File Sync** from the **Policy Configuration Menu** and press **Enter**.
6. Select **Cluster Sync Config** from the **Cluster Configuration Sync Menu** and press **Enter**.
7. Select **Delete Sync File** from the **Config the Destination of Cluster Sync Menu** and press **Enter**.

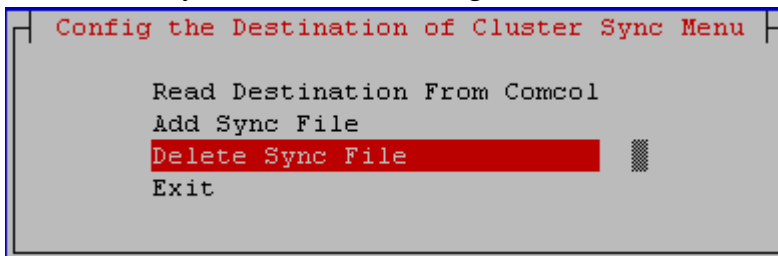
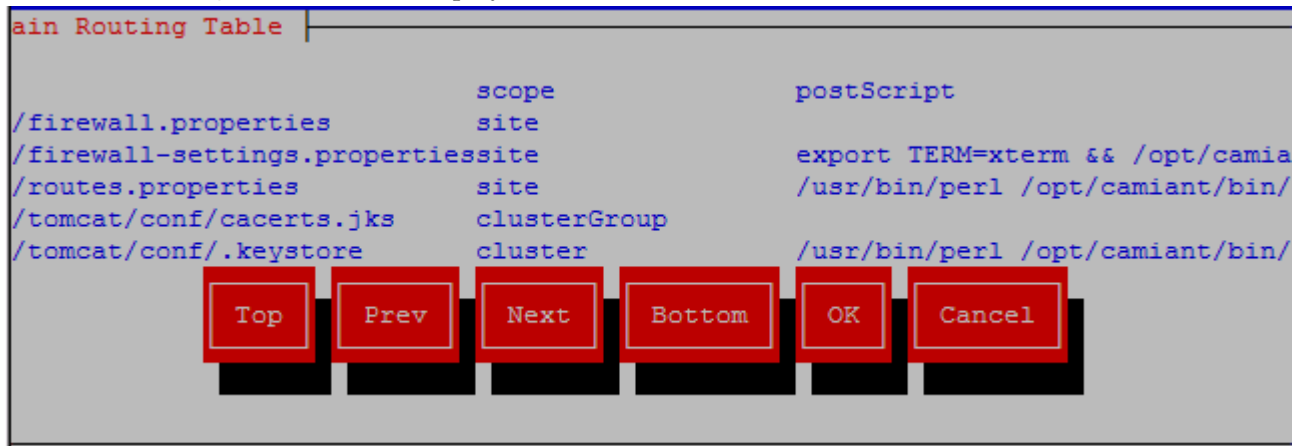


Figure 102: Config the Destination of Cluster Sync Menu--Delete Sync File

8. The **Main Routing Table** screen is displayed.



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

Figure 103: Main Routing Table

Showing Sync Configuration

Use this option to view the location of synced files; this is useful when georedundancy is implemented. 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. Files that must 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 procedure:

1. Log in to your system as `root` if logging in from the system console. Otherwise, SSH into your system as `admusr`.
2. At the `root` prompt, enter the following command:
`su - platcfg`
3. Or, at the `admusr` prompt, enter the following command:
`sudo su - platcfg`
4. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **Cluster File Sync** from the **Policy Configuration Menu** and press **Enter**.
6. Select **Show Sync Config** from the **Cluster Configuration Sync Menu** and press **Enter**.

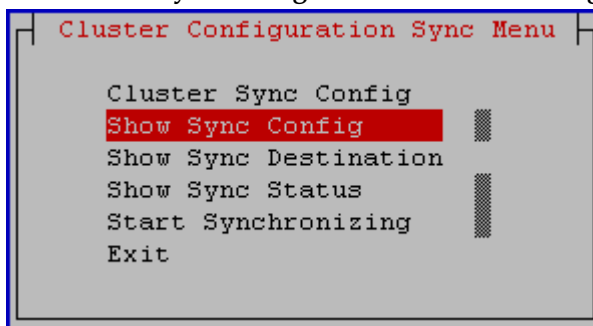


Figure 104: Cluster Configuration Sync Menu--Show Sync Config

7. The Sync File screen is displayed.

The Sync File		
Filename	Scope	PostScript
/etc/camiant/firewall.properties	site	
/etc/camiant/firewall-settings.properties	site	export TERM=xterm
&& /opt/camiant/bin/applyFirewall.py --all --custom-prefer		2>&l > /dev/null
/etc/camiant/routes.properties	site	/usr/bin/perl
/opt/camiant/bin/applyRoute.pl 2>&l > /dev/null		
/opt/camiant/tomcat/conf/cacerts.jks	clusterGroup	
/opt/camiant/tomcat/conf/.keystore	cluster	/usr/bin/perl
/opt/camiant/bin/qp_ssh_restart.pl 2>&l > /dev/null		

Forward Backward Top Bottom Exit

Figure 105: The Sync File

Showing Sync Destination

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

1. Log in to your system as **root** if logging in from the system console. Otherwise, SSH into your system as **admusr**.
2. At the **root** prompt, enter the following command:
`su - platcfg`
3. Or, at the **admusr** prompt, enter the following command:
`sudo su - platcfg`
4. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **Cluster File Sync** from the **Policy Configuration Menu** and press **Enter**.
6. Select **Show Sync Destination** from the **Cluster Configuration Sync Menu** and press **Enter**.

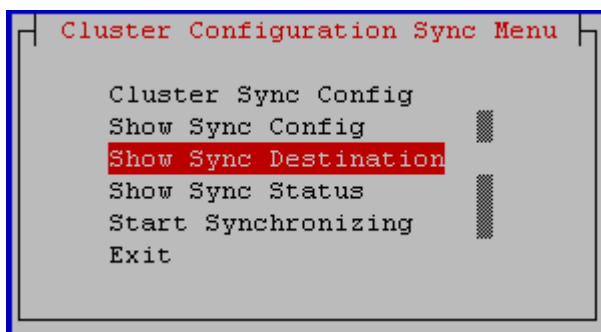


Figure 106: Cluster Configuration Sync Menu--Show Sync Destination

7. The Sync Destination screen is displayed.

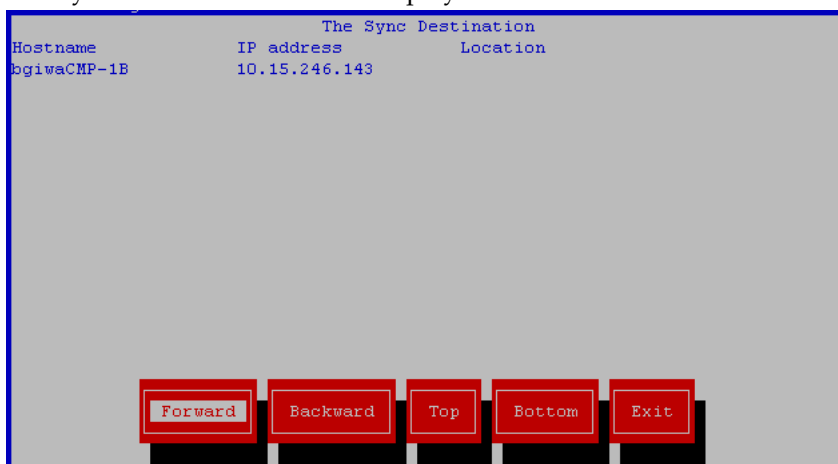


Figure 107: The Sync Destination

Showing Sync Status

To display cluster sync status, complete the following procedures:

1. Log in to your system as `root` if logging in from the system console. Otherwise, SSH into your system as `admusr`.
2. At the `root` prompt, enter the following command:
`su - platcfg`
3. Or, at the `admusr` prompt, enter the following command:
`sudo su - platcfg`
4. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **Cluster File Sync** from the **Policy Configuration Menu** and press **Enter**.
6. Select **Show Sync Status** from the **Cluster Configuration Sync Menu** and press **Enter**.

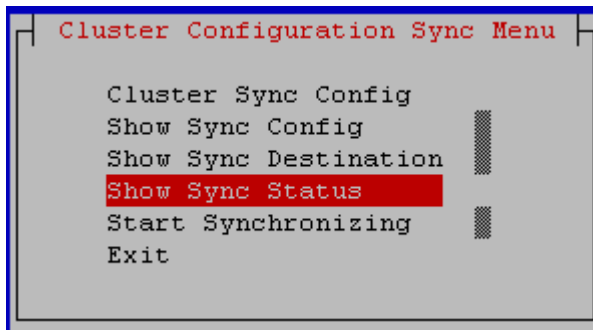


Figure 108: Cluster Configuration Sync Menu--Show Sync Status

7. The **Sync Status** screen is displayed.

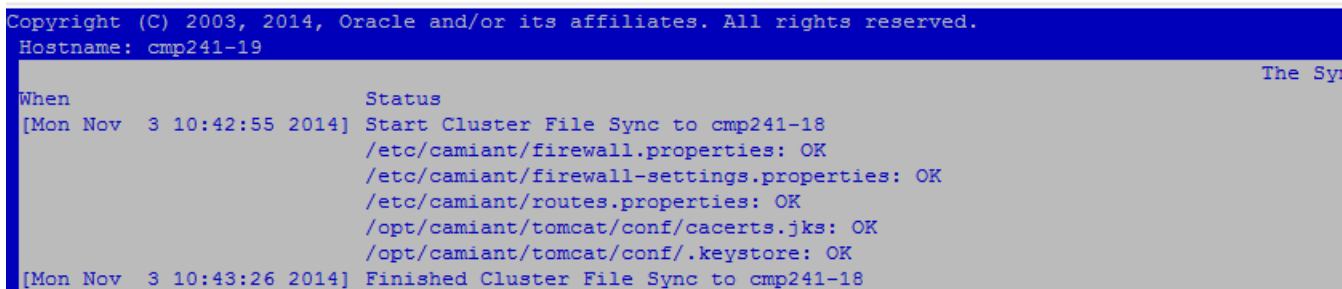


Figure 109: The Sync Status

Performing File Synchronization

Note: 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 servers, 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. There is a separate sync operation for DSCP configurations.

To perform the cluster sync, complete the following procedures:

1. Log in to your system as `root` if logging in from the system console. Otherwise, SSH into your system as `admusr`.
2. At the `root` prompt, enter the following command:
`su - platcfg`
3. Or, at the `admusr` prompt, enter the following command:
`sudo su - platcfg`
4. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **Cluster File Sync** from the **Policy Configuration Menu** and press **Enter**.
6. Select **Start Synchronizing** from the **Cluster Configuration Sync Menu** and press **Enter**.

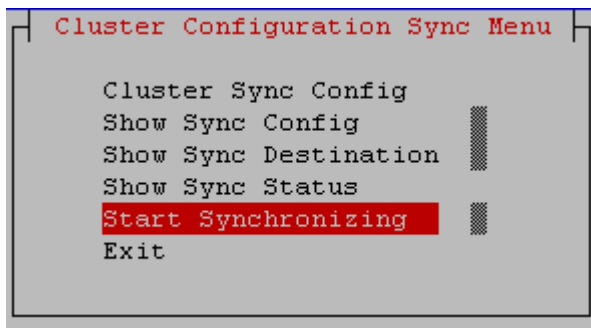


Figure 110: Cluster Configuration Sync Menu--Start Synchronizing

Note: A warning message is displayed, indicating that a cluster sync restarts `qp_procmgr` on the target servers.



WARNING

Warning: This action should only be performed from the Active server, otherwise a failover will occur.

7. Select **OK** and press **Enter** to continue.
Configuration files are synced to the other servers in the cluster, and `qp_procmgr` is restarted on the target servers.

Chapter 6

Custom Ethtool Options

Topics:

- [Edit Network Interface Ethernet Parameters \(Policy Configuration Method\).....90](#)
- [Edit Network Interface Ethernet Parameters \(TPD Method\).....92](#)

This chapter describes how to manually configure Ethtool options, including auto-negotiation, speed, and duplex transmission parameters, on the interface controller for a wireline network installation.

Configuration settings are persistent over system upgrades and reboots.

Edit Network Interface Ethernet Parameters (Policy Configuration Method)

This section describes how to edit Network Interface Ethernet parameter settings using the Policy Configuration method.

To edit network interface parameter settings, complete the following procedures:

1. Log in to your system as root if logging in from the system console. Otherwise, SSH into your system as admusr.
2. At the **root** prompt, enter the following command:
su - platcfg
3. Or, at the **admusr** prompt, enter the following command:
sudo su - platcfg
4. Select **Policy Configuration** from the **Main Menu** and press Enter.
5. Select **Ethernet Interface Parameter Settings** from the **Policy Configuration Menu** and press Enter.

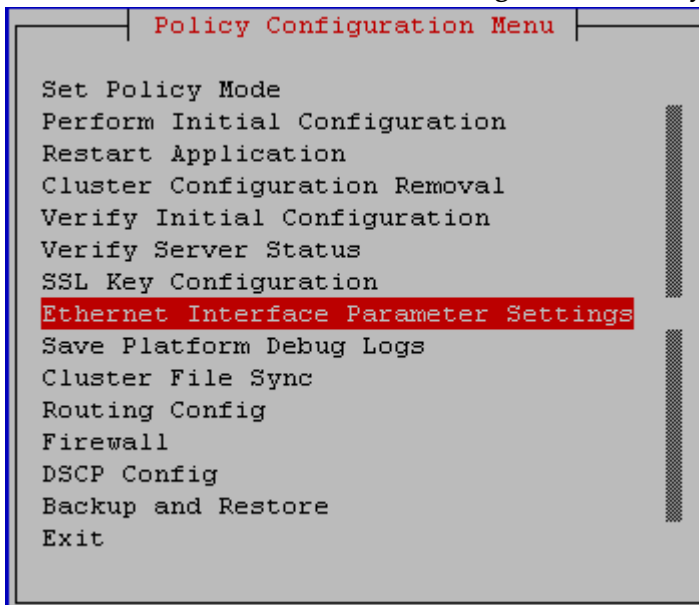


Figure 111: Policy Configuration Menu--Ethernet Interface Parameter Settings

6. Select a network from the list on the **Network Interfaces Menu**.

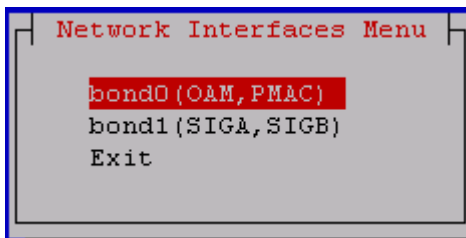


Figure 112: Network Interfaces Menu

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.

7. Select from the options on the **Edit <linkname> Link Options** screen, then select **OK** and press **Enter**. Selection changes are made on both devices of a bond interface at the same time.

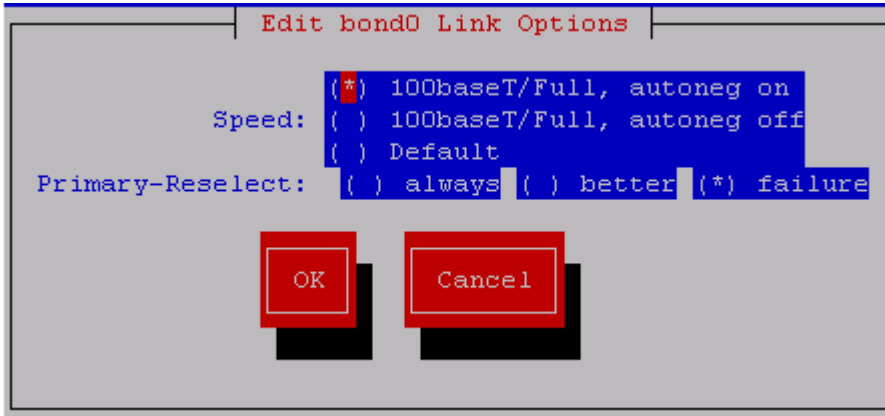


Figure 113: Edit <linkname> Link Options

Notes for setting link options:

1. The **Speed** is configurable only when the device supports **100baseT/Full**. HP ProLiant BL* (C-Class) eth01/eth02 does not support **100baseT/Full**, so the speed is not configurable for C-Class bond0.
2. The physical device might support several **Speed** modes, but **100baseT/Full** is the only candidate in the Platcfg gui.
3. 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 gui. If any secondary device of the bond interface is not linked, the bond interface is not configurable.
4. If the interface is a bond device, then primary_reselect is configurable.
5. If the two secondary devices in a bond device are running in different modes, a warning message is displayed before the window is updated.
6. 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.
7. The link behavior is undefined if one end has **autoneg on** while the other end has **autoneg off**.
8. 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.
9. If the applied mode is not compatible with the switch, it is possible that the link goes down. This utility does not try to detect or correct this case.

Table 5: 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

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

Edit 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 parameter settings, complete the following procedures:

1. Log in to your system as **root** if logging in from the system console. Otherwise, SSH into your system as **admusr**.
2. At the **root** prompt, enter the following command:
`su - platcfg`
3. Or, at the **admusr** prompt, enter the following command:
`sudo su - platcfg`
4. Select **Network Configuration** from the **Main Menu - Network Configuration** and press **Enter**.
5. Select **Network Interfaces** from the **Network Configuration Menu** and press **Enter**.
6. Select **Edit an Interface** from the **Network Interfaces Menu** and press **Enter**.

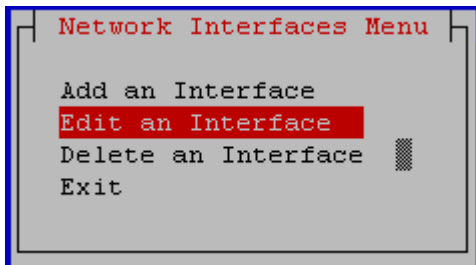


Figure 114: Network Interfaces Menu--Edit an Interface

Note: The following screens are for example only. Please contact [My Oracle Support \(MOS\)](#) for details needed to configure the network interfaces for your server type and system mode.

7. Select a Network Interface name from the **Connection to edit Menu** choices.

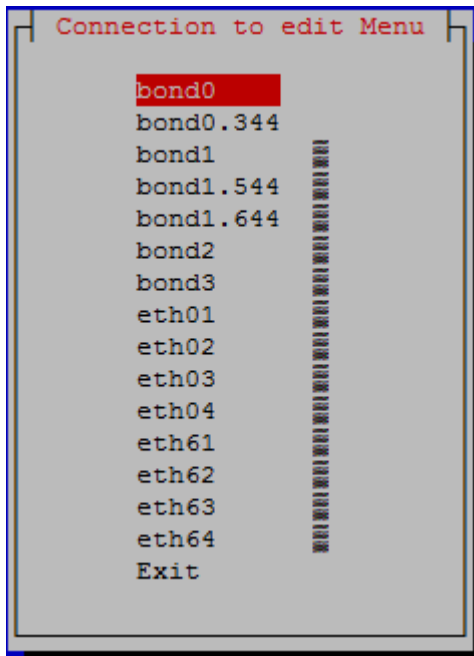


Figure 115: Example view of Connection to edit Menu

8. 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.

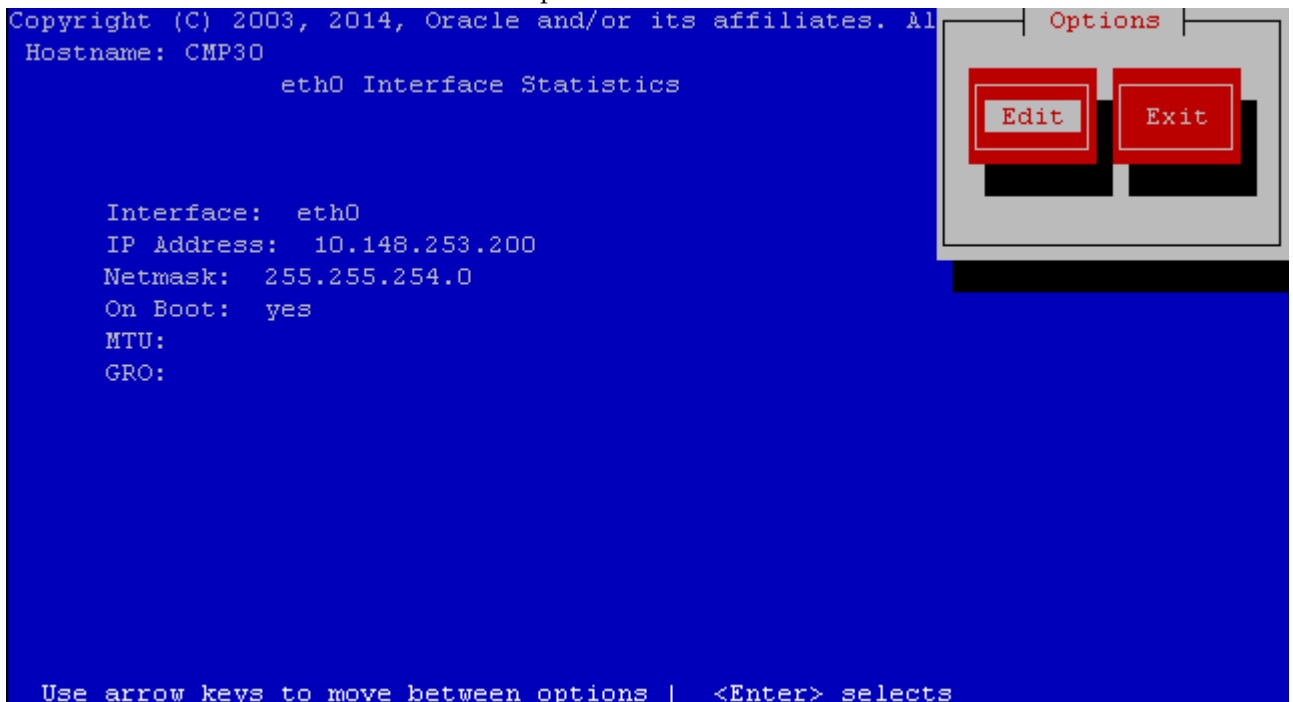


Figure 116: Example view of Interface Statistics

9. Select the required speed and duplex options from the **Interface Options** menu, select **OK** and press **Enter**.

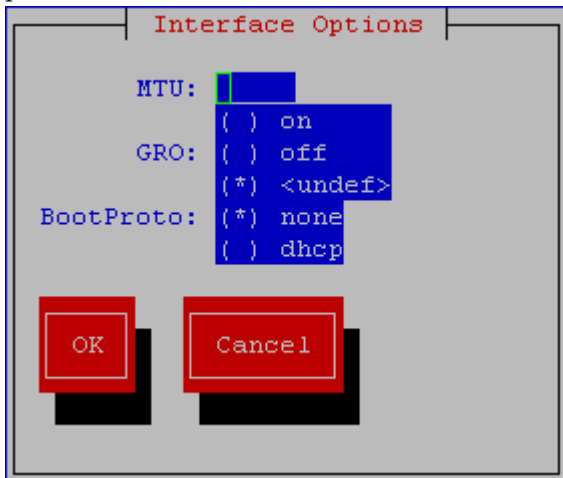


Figure 117: Example view of Interface Options

Performing System and Server Backups and Restores

Topics:

- *Performing a Server Backup.....96*
- *Performing a System Backup.....98*
- *Displaying Backup Files.....99*
- *Configuring Local Archive Settings.....102*
- *Configuring Remote Archive Settings.....103*
- *Scheduling Backups.....109*
- *Performing a System Restore.....113*
- *Performing a Server Restore.....114*

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

Performing a Server Backup

The server backup 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 your server settings, complete the following:

1. Log in to your system as `root` if logging in from the system console. Otherwise, SSH into your system as `admusr`.
2. At the `root` prompt, enter the following command:
`su - platcfg`
3. Or, at the `admusr` prompt, enter the following command:
`sudo su - platcfg`
4. Select the **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **Backup and Restore** from the **Policy Configuration Menu** and press **Enter**. Note that **System Backup** and **System Restore** are only allowed on a CMP or MA server, so these options do not appear on the menu for other types of servers.

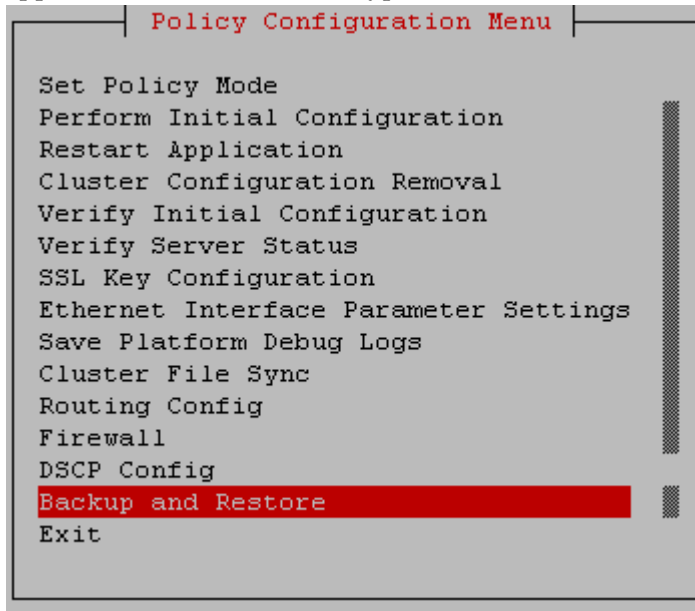


Figure 118: Policy Configuration Menu--Backup and Restore

6. Select **Server Backup** from the **Backup and Restore Menu** and press **Enter**.

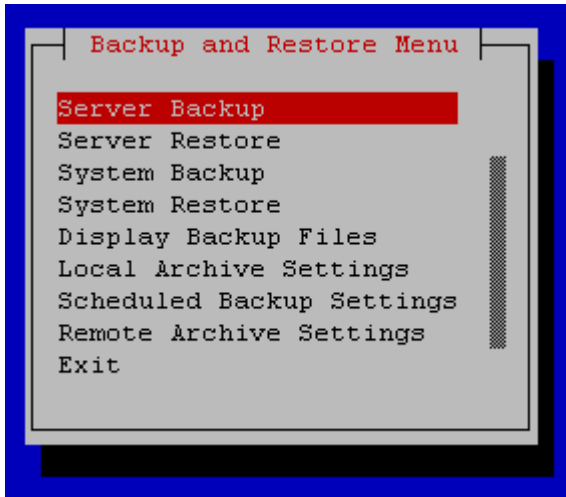


Figure 119: Backup and Restore Menu

7. You are prompted for the ISO path to save the backup file. For example:

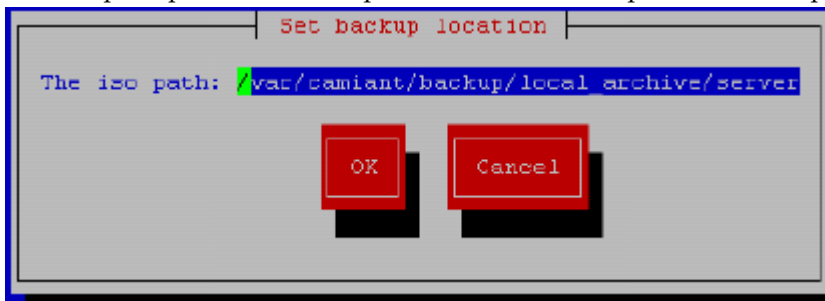


Figure 120: Set backup location

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

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

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

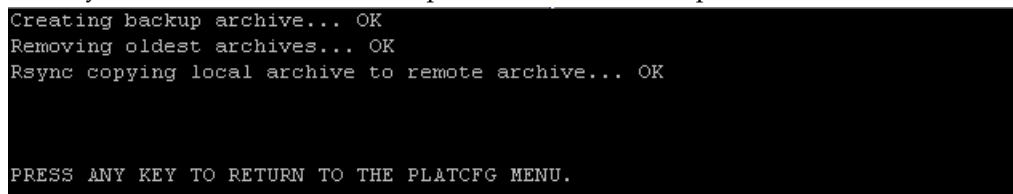


Figure 121: Backup creation message

Performing a System Backup

The system backup contains application-level information such as Topology, Network Element, and Policy Management configurations that are configured in the CMP system. This backup 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 and the PMAC server.

To back up your server settings, complete the following:

1. Log in to your system as `root` if logging in from the system console. Otherwise, SSH into your system as `admusr`.
2. At the `root` prompt, enter the following command:
`su - platcfg`
3. Or, at the `admusr` prompt, enter the following command:
`sudo su - platcfg`
4. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **Backup and Restore** from the **Policy Configuration Menu** and press **Enter**.
6. Select **System Backup** from the **Backup and Restore Menu** and press **Enter**.

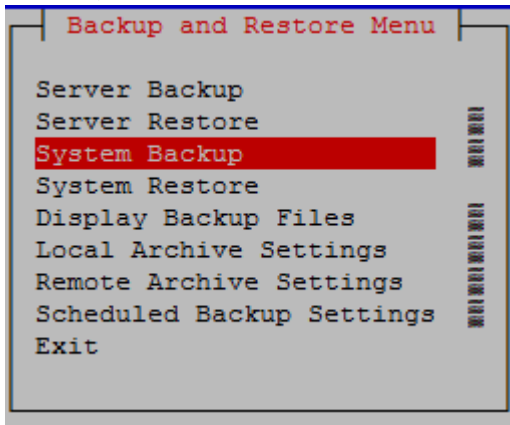


Figure 122: Backup and Restore Menu

7. You are prompted for the ISO path. For example:

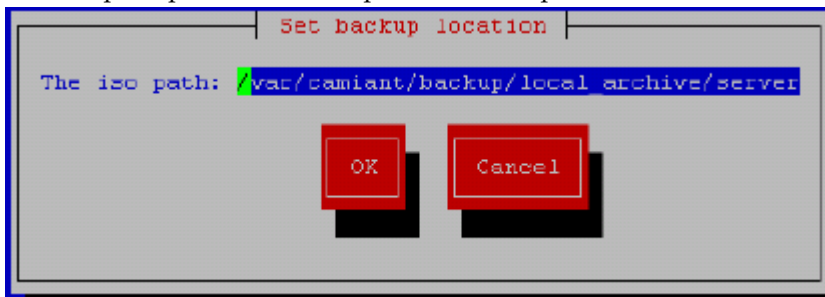


Figure 123: Set system backup location

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
```

8. 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... no remote mate server to rsync
to

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

Figure 124: Creating backup archive

Displaying Backup Files

To display current local archive and remote archive backup files, complete the following:

1. Log in to your system as **root** if logging in from the system console. Otherwise, SSH into your system as **admusr**.
2. At the **root** prompt, enter the following command:
`su - platcfg`
3. Or, at the **admusr** prompt, enter the following command:
`sudo su - platcfg`
4. Select the **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **Backup and Restore** from the **Policy Configuration Menu** and press **Enter**.
6. Select **Display Backup Files** from the **Backup and Restore Menu** and press **Enter**.

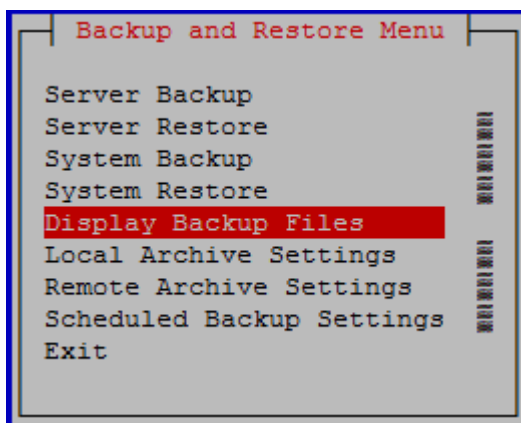


Figure 125: Backup and Restore Menu--Display Backup Files

7. Make a selection from the **Display Backup Files Menu** to display either the local archive or the remote archive:
 - a) Select **Display Local Archive** and press **Enter**.

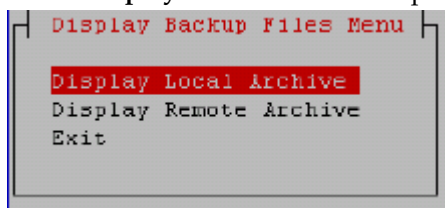


Figure 126: Display Backup Files Menu--Display Local Archive

The **Local Archives** screen is displayed. For example:



Figure 127: Local Archives

- b) Select **Display Remote Archive** and press **Enter**.

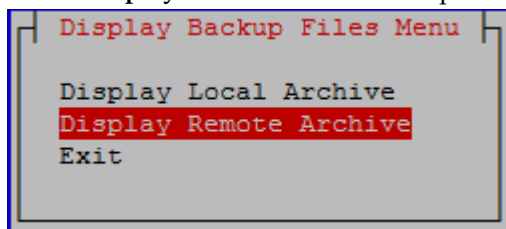


Figure 128: Display Backup Files Menu--Display Remote Archive

The **Remote Archives** screen is displayed. For example:

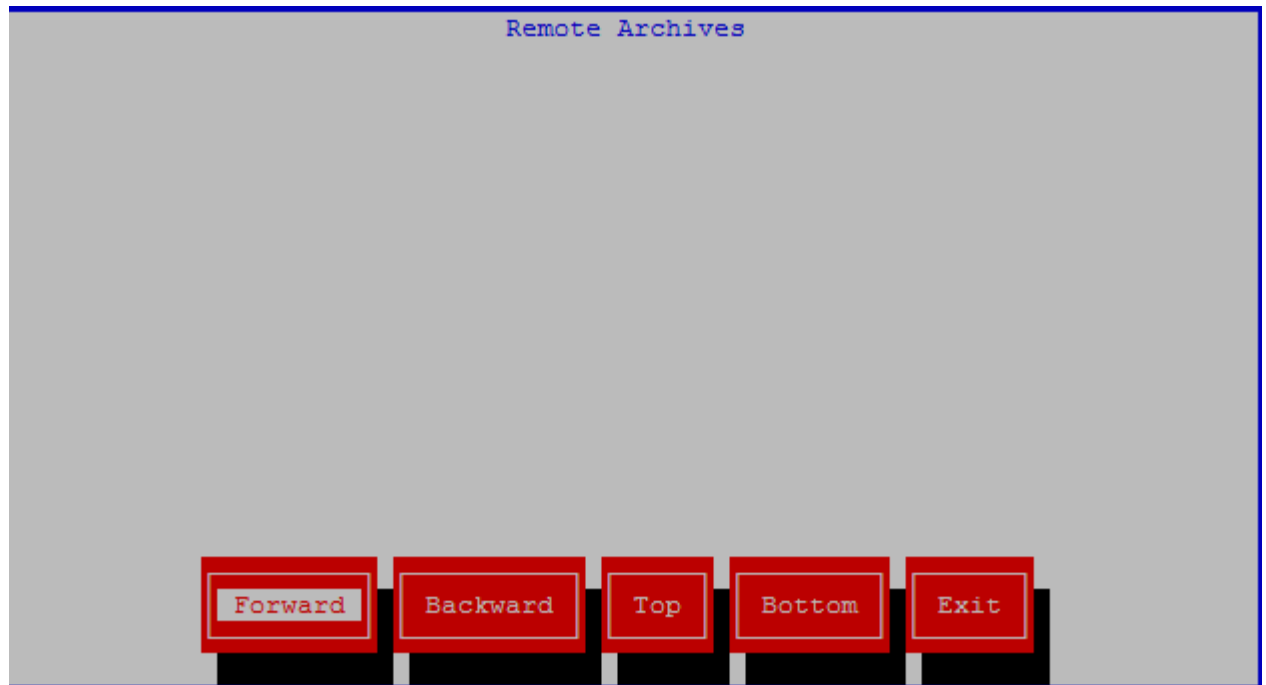


Figure 129: Remote Archives

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 procedure:

1. Log in to your system as `root` if logging in from the system console. Otherwise, SSH into your system as `admusr`.
2. At the `root` prompt, enter the following command:
`su - platcfg`
3. Or, at the `admusr` prompt, enter the following command:
`sudo su - platcfg`
4. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **Backup and Restore** from the **Policy Configuration Menu** and press **Enter**.
6. Select **Local Archive Settings** from the **Backup and Restore Menu** and press **Enter**.

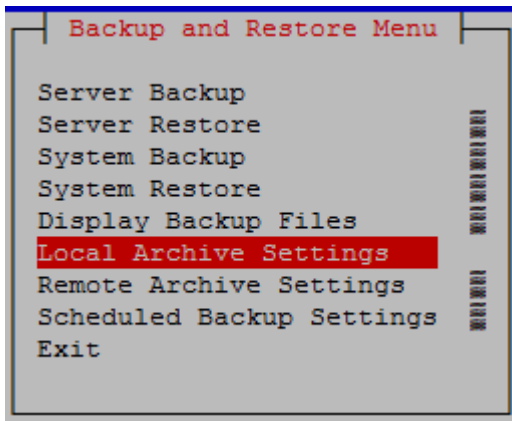


Figure 130: Backup and Restore Menu

7. You are prompted to specify the number of archives for both the server and system backups. Note that the following example shows both the number of server and system backups to keep; the server backup option will only appear on a CMP or MA system.

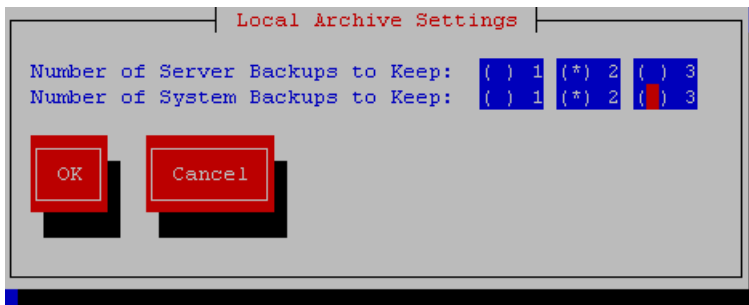


Figure 131: Local Archive Settings

8. Select the number of backups to keep for each archive. When finished, 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 remotely stored systems and server archives.

Configuring a Remote Archive

To configure this setting, complete the following:

1. Log in to your system as `root` if logging in from the system console. Otherwise, SSH into your system as `admusr`.
2. At the `root` prompt, enter the following command:
`su - platcfg`

3. Or, at the **admusr** prompt, enter the following command:
`sudo su - platcfg`
4. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **Backup and Restore** from the **Policy Configuration Menu** and press **Enter**.
6. Select **Remote Archive Settings** from the **Backup and Restore Menu** and press **Enter**.
7. You are prompted for the archive type (server or system) to configure. Note that the server backups option only appears on a CMP or MA system. Select **Remote Archive for Server Backups** or **Remote Archive for System Backups** from the **Remote Archive Settings Menu** and press **Enter**.

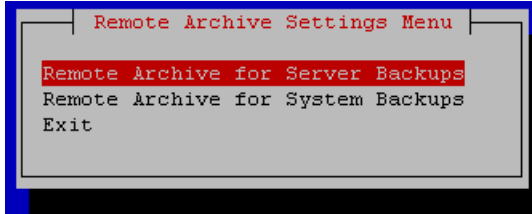


Figure 132: Remote Archive Settings Menu

8. Select **Add Remote Archive** or **Remote Archive Settings Menu** from the 2nd **Remote Archive Settings Menu** and press **Enter**.

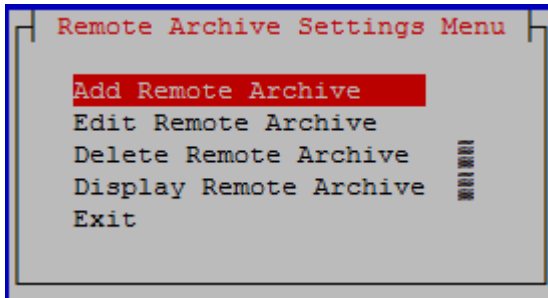


Figure 133: Remote Archive Settings Menu

9. Enter remote access information in the screen that displays:

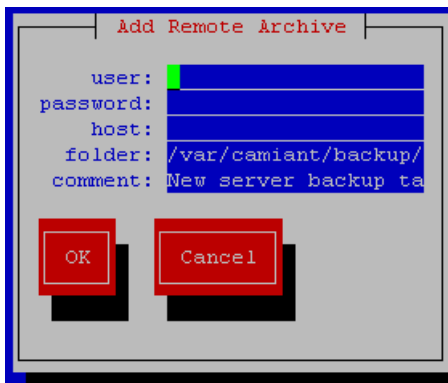


Figure 134: Add Remote Archive

- 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 the platcfg utility.

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

Editing a Remote Archive Configuration

To edit an archive configuration, complete the following:

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

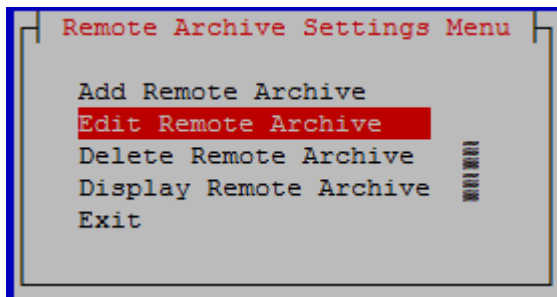


Figure 135: Remote Archive Settings Menu--Edit Remote Archive

6. Select the remote archive to edit from the **Remote Archives Menu** and press **Enter**.

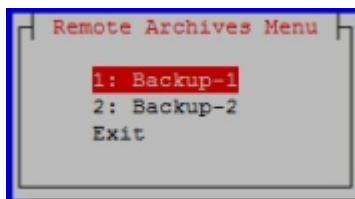


Figure 136: Remote Archives Menu

7. Enter all remote archive information and when finished, select **OK** and press **Enter**.

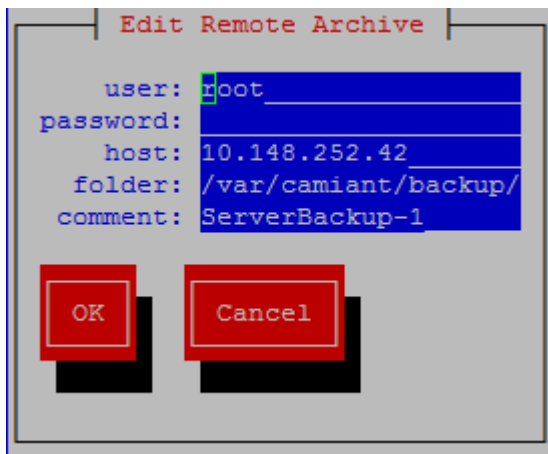


Figure 137: Edit Remote Archive

Deleting a Remote Archive Configuration

To delete a remote archive configuration, complete the following procedure:

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

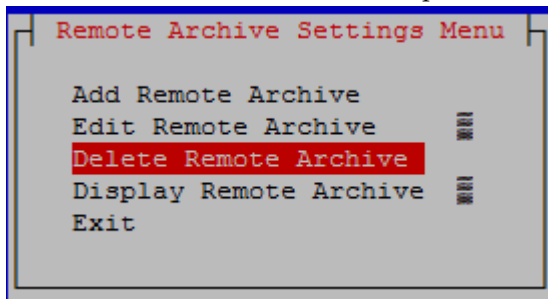


Figure 138: Remote Archive Settings Menu

6. Select the remote archive to edit from the **Remote Archives Menu** and press **Enter**.

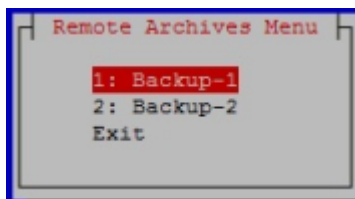


Figure 139: Remote Archives Menu

7. Select **Yes** or **No** from the **Confirm deletion** dialog box and press **Enter**. If **Yes** is selected, the remote archive is deleted; if **No** is selected, the **Remote Archive Settings Menu** is redisplayed.

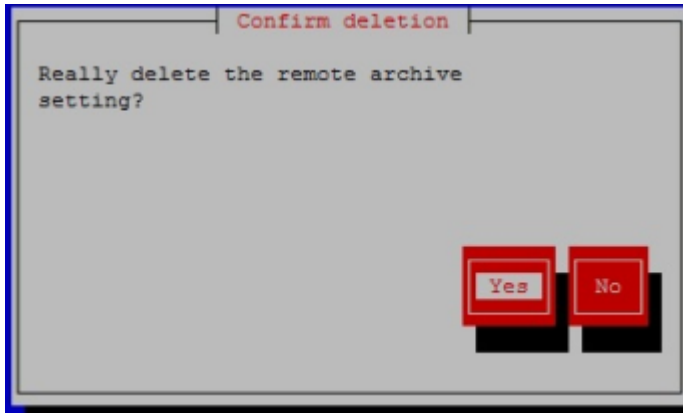


Figure 140: Confirm deletion

Displaying a Remote Archive Configuration

To delete a remote archive configuration, complete the following procedure:

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

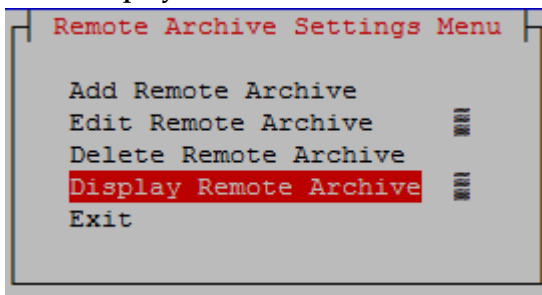


Figure 141: Remote Archive Settings Menu

6. One of the following screens is displayed: the first one for server backup and the second one for system backups.

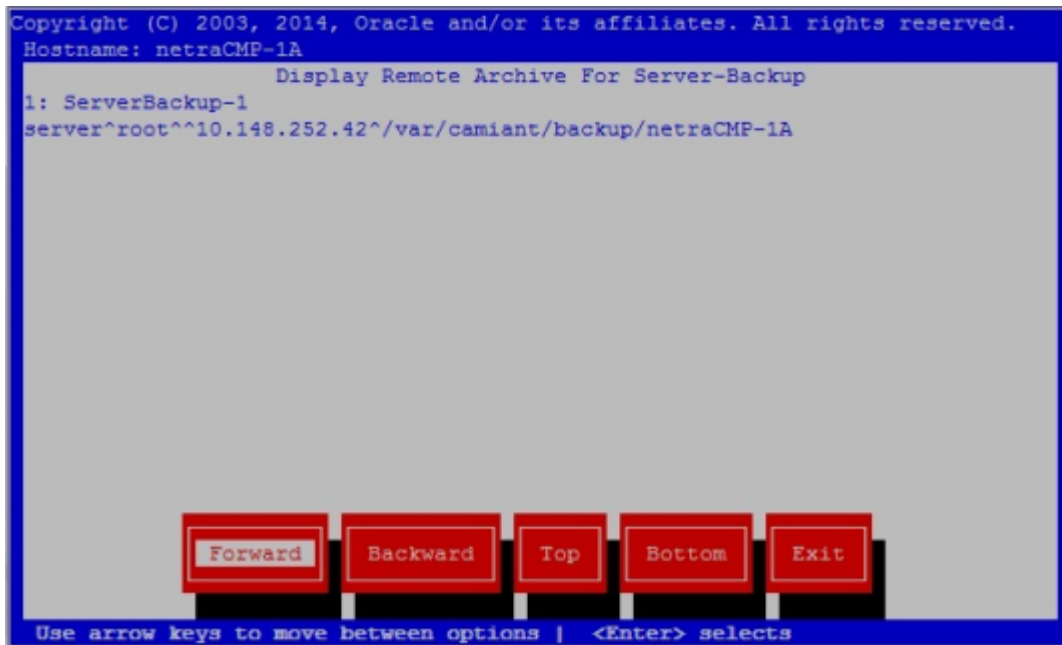


Figure 142: Display Remote Archive For Server-Backup

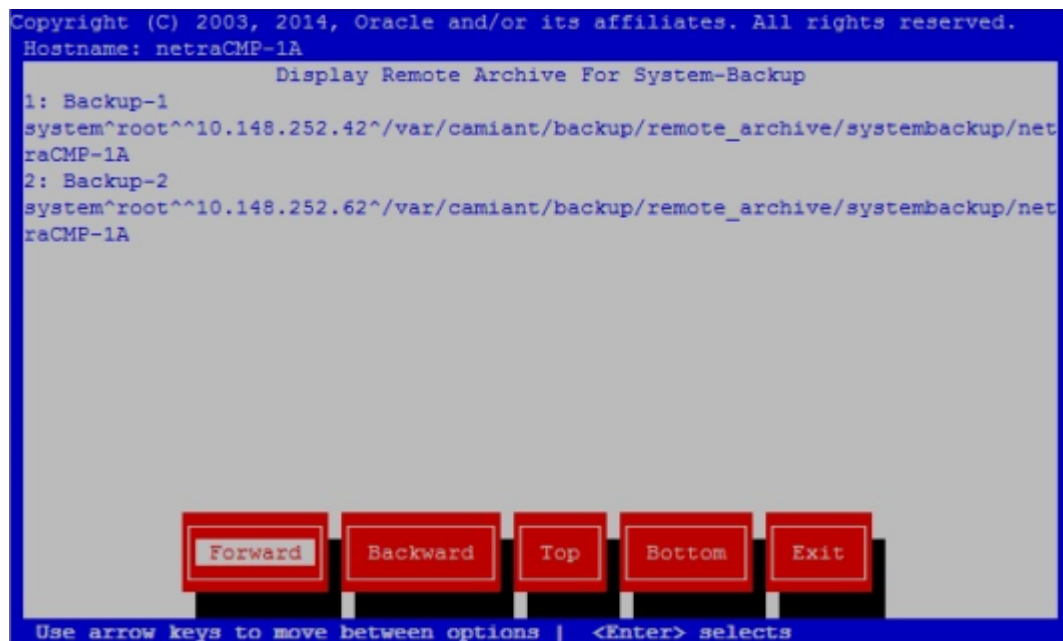


Figure 143: Display Remote Archive For System-Backup

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 **Weekly** 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 procedure:

1. Log in to your system as `root` if logging in from the system console. Otherwise, SSH into your system as `admusr`.
2. At the `root` prompt, enter the following command:
`su - platcfg`
3. Or, at the `admusr` prompt, enter the following command:
`sudo su - platcfg`
4. Select the **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **Backup and Restore** from the **Policy Configuration Menu** and press **Enter**.
6. Select **Scheduled Backup Settings** from the **Backup and Restore Menu** and press **Enter**.

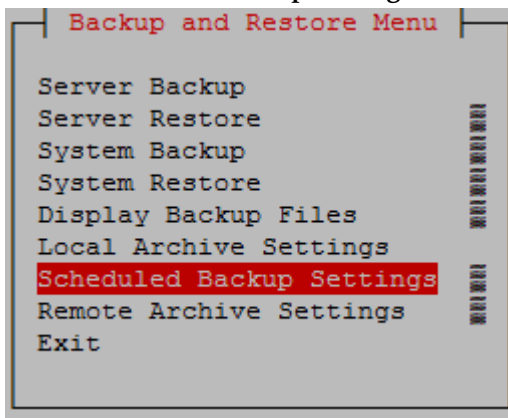


Figure 144: Backup and Restore Menu--Scheduled Backup Settings

7. You are prompted for the backup type (server or system) to be scheduled. Select either **Scheduled Backup for Server Backups** or **Scheduled Backup for System Backups** from the **Scheduled Backup Settings Menu** and press **Enter**.

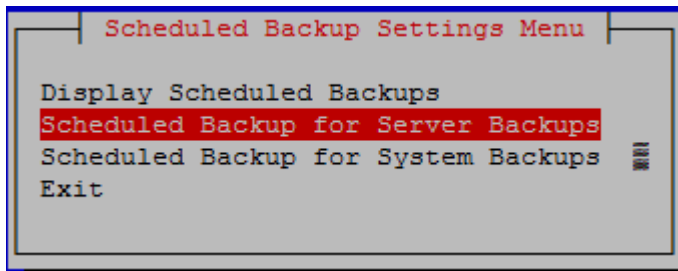


Figure 145: Scheduled Backup Settings Menu

8. Select **Add Schedule** from the **Scheduled Backup for server backups** Menu and press **Enter**.

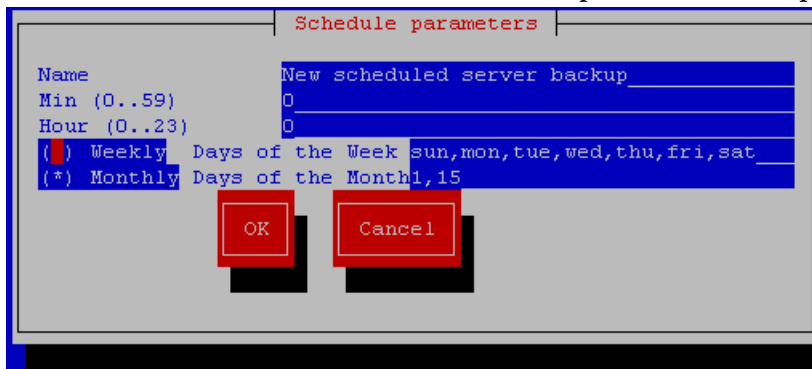


Figure 146: Schedule parameters

9. 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.
10. When you have finished, select **OK** and press **Enter**.

Editing a Scheduled Backup

To edit an existing scheduled backup, complete the following:

1. Log in to your system as `root` if logging in from the system console. Otherwise, SSH into your system as `admusr`.
2. At the `root` prompt, enter the following command:
`su - platcfg`
3. Or, at the `admusr` prompt, enter the following command:

```
sudo su - platcfg
```

4. Select the **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **Backup and Restore** from the **Policy Configuration Menu** and press **Enter**.
6. Select **Scheduled Backup Settings** from the **Backup and Restore Menu** and press **Enter**.

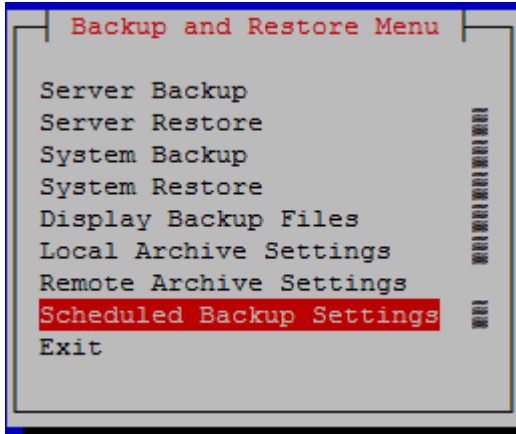


Figure 147: Backup and Restore Menu--Scheduled Backup Settings

7. Select either **Scheduled Backup for Server Backups** or **Scheduled Backup for System Backups** from the **Scheduled Backup Settings Menu** and press **Enter**.

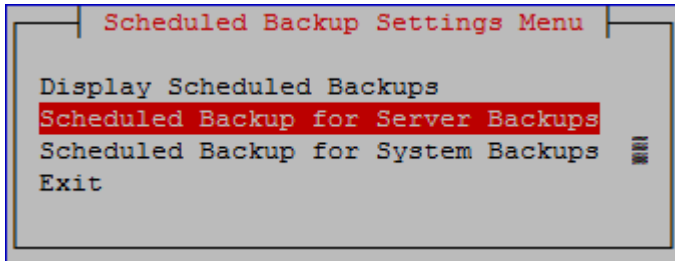


Figure 148: Scheduled Backup Settings Menu

8. Select **Edit Schedule** from the **Scheduled Backup for server backups Menu** or from the **Scheduled Backup for system backups Menu** (not shown) and press **Enter**.

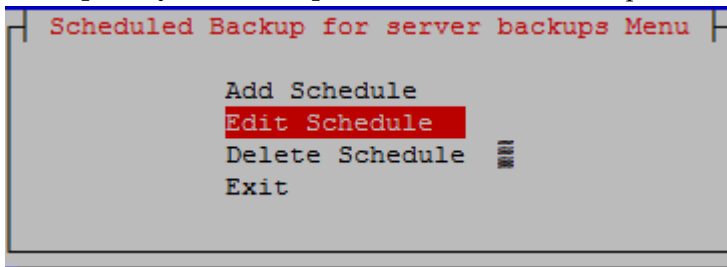


Figure 149: Scheduled Backup for server backups Menu

9. 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.
10. When you have finished, select **OK** and press **Enter**.

Deleting a Scheduled Backup

To delete an existing scheduled backup, complete the following procedure:

1. Log in to your system as `root` if logging in from the system console. Otherwise, SSH into your system as `admusr`.
2. At the `root` prompt, enter the following command:
`su - platcfg`
3. Or, at the `admusr` prompt, enter the following command:
`sudo su - platcfg`
4. Select the **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **Backup and Restore** from the **Policy Configuration Menu** and press **Enter**.
6. Select **Backup and Restore** from the **Policy Configuration Menu** and press **Enter**.
7. Select **Scheduled Backup Settings** from the **Backup and Restore Menu** and press **Enter**.
8. Select either **Scheduled Backup for Server Backups** or **Scheduled Backup for System Backups** from the **Scheduled Backup Settings Menu** and press **Enter**.
9. Select **Delete Schedule** from the **Scheduled Backup for server backups Menu** or from the **Scheduled Backup for system backups Menu** (not shown) and press **Enter**.

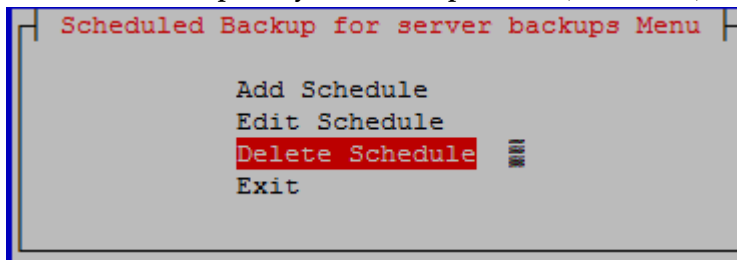


Figure 150: Scheduled Backup for server backups Menu

10. When you have finished, select **OK** and press **Enter**. The scheduled backup is deleted.

Displaying Scheduled Backups

To display the scheduled backups, complete the following:

1. Log in to your system as `root` if logging in from the system console. Otherwise, SSH into your system as `admusr`.

2. At the **root** prompt, enter the following command:
`su - platcfg`
3. Or, at the **admusr** prompt, enter the following command:
`sudo su - platcfg`
4. Select the **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **Backup and Restore** from the **Policy Configuration Menu** and press **Enter**.
6. Select **Backup and Restore** from the **Policy Configuration Menu** and press **Enter**.
7. Select **Scheduled Backup Settings** from the **Backup and Restore Menu** and press **Enter**.
8. Select **Display Scheduled Backups** from the **Scheduled Backup Settings Menu** and press **Enter**.
 The scheduled backups are displayed.

```
Copyright (C) 2003, 2014, Oracle and/or its affiliates. All rights reserved.
Hostname: cmp241-19
Name
BackupType Minute Hour SchedType When
-----
New scheduled server backup
server 0 0 Monthly 1,15
-----
New scheduled system backup
system 0 0 Weekly sun,mon,tue,wed,thu,fri,sat
-----
```

Figure 151: Scheduled Backups

Performing a System Restore

The system restore option restores the Policy Management information that is unique to this system, including topology, policies, and feature configuration.

Note: If a failover occurs during a system restore on the active server, the restored data will be replaced by replication. To avoid this unintended overwriting, before conducting the restore on the active server, stop QP and COMCOL on the standby server using the CMP interface, then perform the system restore using the Platcfg Utility, and finally, restart QP and COMCOL on the standby server using the CMP interface. The following commands from the CMP interface stop QP and COMCOL on the standby server:

Note: The following commands from the CMP interface stop QP and COMCOL on the standby server:

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

Note: The following commands from the CMP interface start COMCOL and QP on the standby server:

```
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.

To perform a system restore, complete the following:

1. Log in to your system as `root` if logging in from the system console. Otherwise, SSH into your system as `admusr`.
2. At the `root` prompt, enter the following command:
`su - platcfg`
3. Or, at the `admusr` prompt, enter the following command:
`sudo su - platcfg`
4. Select the **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **Backup and Restore** from the **Policy Configuration Menu** and press **Enter**.
6. Select **System Restore** from the **Backup and Restore Menu** and press **Enter**.
7. Enter the path that contains the backup and select either **Application** or **Full** for the type of restore.

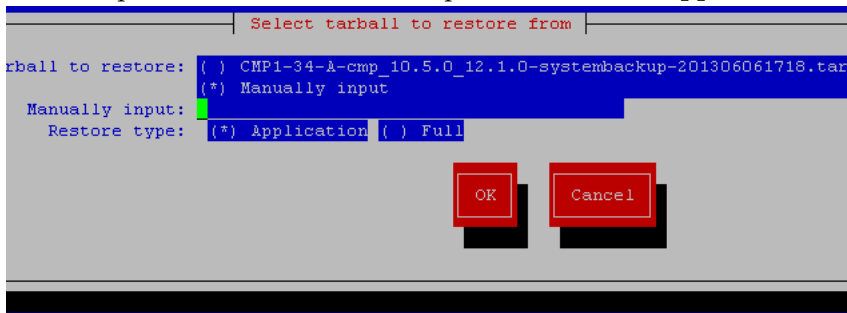


Figure 152: Select tarball to restore from

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 procedures:

1. Log in to your system as `root` if logging in from the system console. Otherwise, SSH into your system as `admusr`.
2. At the `root` prompt, enter the following command:
`su - platcfg`
3. Or, at the `admusr` prompt, enter the following command:
`sudo su - platcfg`
4. Select the **Policy Configuration** from the **Main Menu** and press **Enter**.
5. Select **Backup and Restore** from the **Policy Configuration Menu** and press **Enter**.
6. Select **Server Restore** from the **Backup and Restore Menu** and press **Enter**.

7. Enter the path that contains the backup, select **OK**, and press **Enter**. The system restores to the backup version specified.

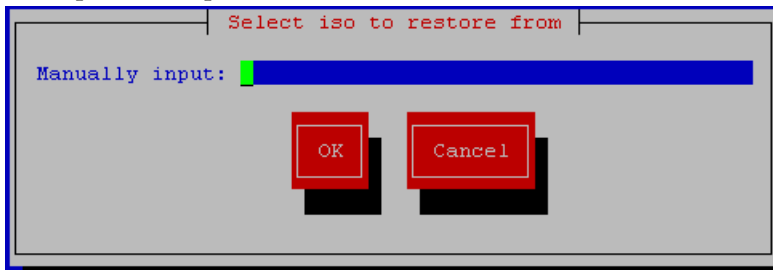


Figure 153: Select iso to restore from screen

B

Bandwidth on Demand

See BoD.

BoD

Bandwidth on Demand

An application that provides dynamic allocation of bandwidth; for example, a broadband speed promotion.

C

CA

Canada (NPAC Region)

Conditioning Action

NPP CAs indicate what digit conditioning actions to execute when processing a digit string.

Certificate Authority: An entity that issues digital certificates

CMP

Configuration Management Platform

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.

D

DNS

Domain Name Services

Domain Name System

A system for converting Internet host and domain names into IP addresses.

D

DSCP

Differentiated Service Code Point

Differentiated Services Code Point

Provides a framework and building blocks to enable deployment of scalable service discrimination in the internet. The differentiated services are realized by mapping the code point contained in a field in the IP packet header to a particular forwarding treatment or per-hop behavior (PHB).

Differentiated services or DiffServ is a computer networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying and managing network traffic and providing quality of service (QoS) on modern IP networks.

H

HA

High Availability

High Availability refers to a system or component that operates on a continuous basis by utilizing redundant connectivity, thereby circumventing unplanned outages.

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

I

re-assembly through the data link layer.

ISO

International Standards Organization

M

MA

Management Agent

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 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.

Multimedia Policy Engine

See MPE.

N

N

NTP Network Time Protocol

P

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

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

V

VIP Virtual IP Address

Virtual IP is a layer-3 concept employed to provide HA at a host level. A VIP enables two or more IP hosts to operate in an active/standby HA manner. From the perspective of the IP network, these IP hosts appear as a single host.

VLAN Virtual Local Area Network

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.