Oracle® COMMUNICATIONS

Policy Management Feature Activation

Release 12.2

Generic Policy Notification Interface - Convert for Cable

E82618-01
February 2017

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

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

TABLE OF CONTENTS

1. CONTACTS AND CUSTOMER CARE 4

1.1 ORACLE CUSTOMER CARE 4
1.2 ACRONYMS 5

2. PURPOSE AND SCOPE 6

3. CMP GUI CHANGES 7

3.1 POLICY LIBRARY NEW ACTIONS 7
3.2 NEW MENUS 8
3.3 NEW LOGS 9
3.4 PERSISTENT NOTIFICATION SERVERS CONNECTION CONFIGURATIONS 9

4. PROCEDURE TO ENABLE THE FEATURE 11

5. BACK OUT PROCEDURE 20

1. Contacts and Customer Care

1.1 Oracle Customer Care

The Oracle Customer Care Center is your initial point of contact for all product support needs. A representative takes your call or email, creates a Customer Service Request (CSR) and directs your requests to the Oracle Technical Assistance Center (TAC). Each CSR includes an individual tracking number. Together with TAC Engineers, the representative will help you resolve your request. The Customer Care Center is available 24 hours a day, 7 days a week, 365 days a year, and is linked to TAC Engineers around the globe.

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

Oracle Technical Assistance Centers are located around the globe in the following locations:
Oracle – Global

CAUTION:
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*.

1.2 Acronyms

Acronym	Definition
AF	Application Function
BSS	Business Support System
CMP	Configuration Management Platform
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
JSON	JavaScript Object Notation
LDAP	Lightweight Directory Access Protocol
MPE-R/S	Multimedia Policy Engine – Routing/Serving
OSS	Operational Support System
PCRF	Policy and Charging Rules Function
P-CSCF	Proxy CSCF
SMPP	Short Message Peer-to-Peer
SMS	Short Message Service
URL	Uniform Resource Locator
XML	Extensible Markup Language

2. Purpose and Scope

This Work Instruction describes the steps needed to enable and configure the Policy Notifications interface feature in Cable mode of Oracle Communications Policy Management solution and the steps needed to disable it if required by customer.
The intent of this feature is to provide generic, highly configurable external event notification functions beyond the previously existing SMS, Email, and logging functions.
The existing methods in the current product to send either end-user notifications (SMS, Email) or operator notifications (logging, Syslog, LDAP Write) are specific to the interface on which they work and not flexible enough to provide generic notifications.

The eventual usage of these messages could be either end-user notifications (after processing by an external gateway), or event-specific messages as triggers to other operator systems (BSS/OSS).
The 'Generic Notifications from Policy System' feature provides necessary framework based on HTTP/web services interface to provide highly configurable/flexible notifications. The methods, destinations, and contents of the messages are flexible at the time of message generation by Policy Actions.

3. CMP GUI changes

The below new changes related to Policy Notification feature is only available in CMP GUI if mode settings has either SMPP or XML options under SMS enabled/checked. Refer to step 1 in section 4 for illustration

3.1 Policy Library New Actions

Policy Condition Group	Policy Condition or Action	Description
Action	**Send http POST notification to url URL with headers headers and content content**	Send a HTTP request to specified destination. The fields 'destination', 'headers', 'content' are all free-flowing text fields to be configured by operator.
Action	**Send http POST notification to select notification destination with headers headers and content content**	Send a HTTP request to pre-defined destination. The fields 'headers', 'content' are all free-flowing text fields to be configured by operator.

The **URL** field is free flowing text field – user can define the 'destination' URL directly into the policy. This allows for cases where the URL itself may be dynamic, based on policy variable substitution. For example: http://10.15.20.190:80/rs/quota/notify/{User.MSISDN}.

The **POST** is the default notification delivery technique, this field is a 'drop-down' having values 'GET', 'PUT', 'POST', 'DELETE'. Operator shall be able to choose one of the values in the action field.

The **headers** field is a pop-up box with 2 fields: 'Header' and 'Value'. Both fields shall be free-flowing text fields. There is no validation whether particular header type is a valid HTTP header. Similarly, there is no validation whether the 'value' corresponds to 'header type'. Operator shall be able to add up to 20 such rows of 'header' and 'value' in a single policy. Once the user clicks OK, header and value will be separated by a colon and multiple headers will come as a comma separated list of values. The content shown on the policy screen will display the escape characters as well, / in this case.

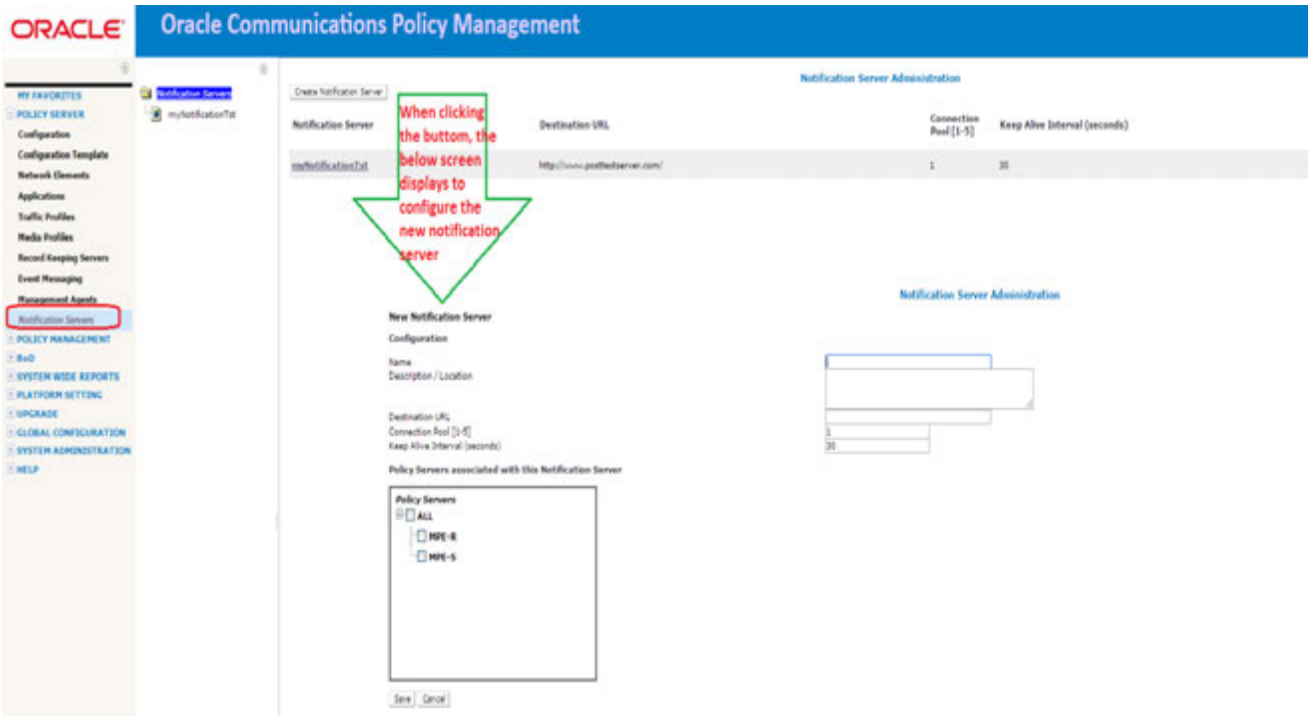
In order for MPE to read the headers correctly if there are colons and/or commas in the header or value they will be escaped with forward slash (/). Also, Forward slash is not allowed as the last character in either the header or value and header name cannot be empty.

The **content** field is also 'free-flowing' text field which allows for any type of notification like JSON/ XML/ Text message in the body of HTTP request. 'Content' field also allow for policy variable substitution. MPE shall not validate whether the 'header' value corresponds to particular 'content'.

For pre-defined destinations, the **select notification destination** field is a pop-up that will list the pre-defined static-destination servers already configured by operator and operator shall select one of them.

3.2 New Menus

New menu item “Notification Server” is added under “Policy Server” to configure static based Notification servers:



Mandatory Parameters:

Name – should be unique. The name will be used when a policy is configured using a notification server

Destination URL – should be unique and a valid http URL. Persistent connections will be created to this end point from SMSR. The URL cannot contain variables for substitution. The length of destination URL is limited to 255 characters.

Connection Pool – Defines the number of persistent connections to be created to the configured end point. Allowed values are from 1-5 and will be defaulted to 1.

Keep Alive Interval – Defines the interval for keeping the persistent connection active. The value entered is taken to be in seconds. Allowed values are from 0-300 and will be defaulted to 30.

Optional Parameters:

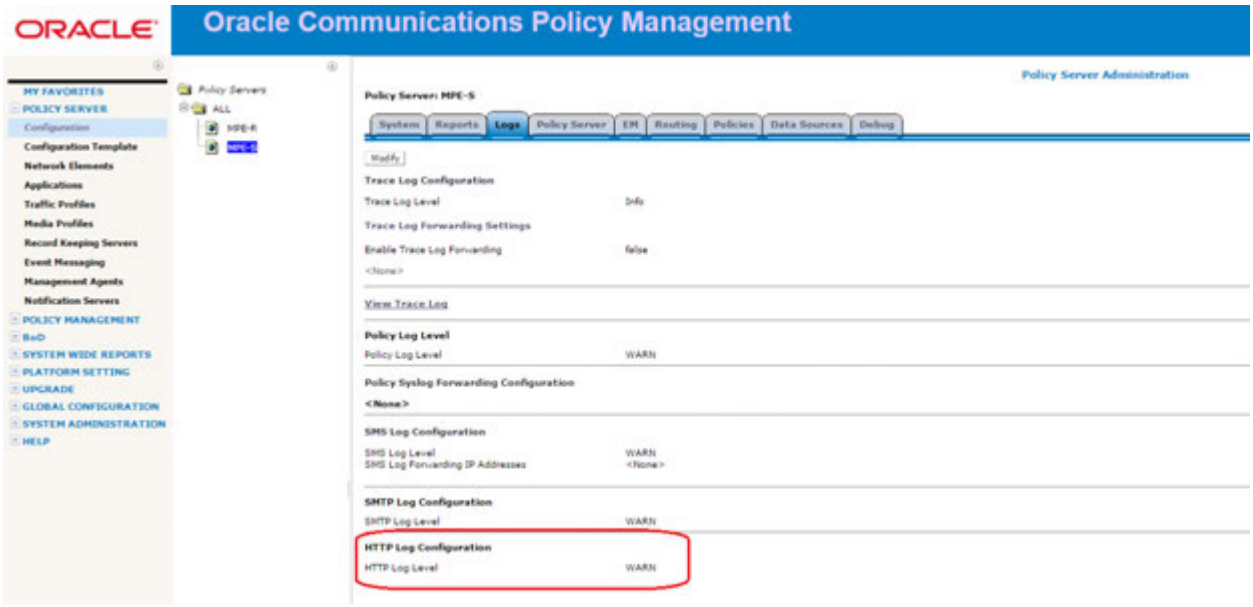
Description/Location – allows for any descriptive text to be entered for the notification server.

The screen also allows the user to associate a Notification Server with the available Policy Servers.

On clicking Save, the Notification Server will be created in CMP database and the configuration for the same will be pushed to the selected Policy Server(s). In case the Policy server association is removed then the same would also be removed from the MPE with which it was previously associated.

3.3 New Logs

A new log called "HTTP log" is introduced to track the HTTP notification messages sent from Oracle Communications Policy Management to external Notification servers. Log level can be set from CMP GUI as follows:



The actual log file is located on MPE servers under /var/camiant/log:

```
[root@Cable-MPE-S-A log]# cd /var/camiant/log
[root@Cable-MPE-S-A log]# ls -ltr
total 1114468
drwx------ 2 root root    16384 Mar  9 18:56 lost+found
drwxr-x--- 2 root root     4096 Mar  9 19:11 firewall
-rw-r----- 1 root root        0 Mar  9 19:11 rc.stats.daily
-rw-r----- 1 root root        0 Mar  9 19:11 policy.log
-rw-r----- 1 root root        0 Mar  9 19:11 dynamic_quota.log
-rw-r----- 1 root root        0 Mar  9 19:11 quota_rollover.log
-rw-r--r-- 1 root root        0 Mar  9 19:12 huge_core.log
-rw-r----- 1 root root        0 Mar  9 19:12 smsr.log
-rw-r----- 1 root root        0 Mar  9 19:12 smsclient.log
-rw-r----- 1 root root        0 Mar  9 19:12 SMPP.log
-rw-r----- 1 root root        0 Mar  9 19:12 SMTP.log
-rw-r----- 1 root root        0 Mar  9 19:12 HTTP.log
-rw-r----- 1 root root      990 Mar  9 19:16 qpLayout.log
```

3.4 Persistent Notification servers Connection Configurations

A new configuration file "**NotificationCfg.properties**" is introduced to handle the settings of establishing persistent connection to the configured Notification Servers in CMP GUI.
The file would be in MPE server under the following path: /opt/camiant/smsr/smscfg/
Should a connection attempt fail Oracle Communications Policy Management will continuously retry at constant intervals as per the configured connection retry value in this properties file till the connection is restored.

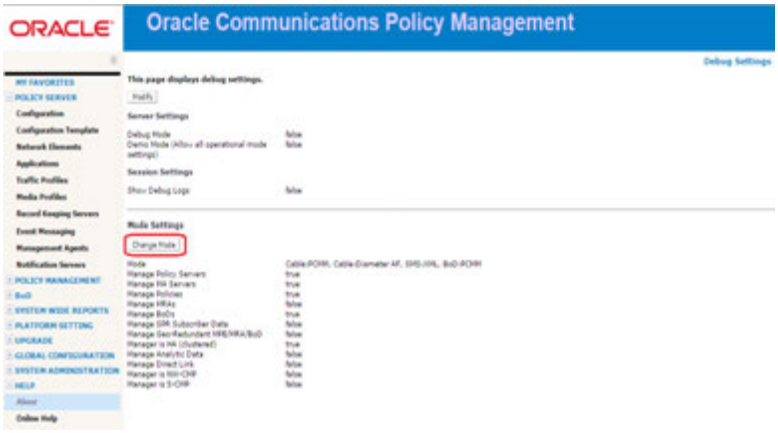
```
[admusr@Cable-MPE-S-A smscfg]$ more NotificationCfg.properties
#Generated at Tue Apr 12 17:42:27 EDT 2016
#Tue Apr 12 17:42:27 EDT 2016
http.cfg.connectionTimeout=3
http.cfg.enabled=true
http.cfg.numConnectionDynamic=1
http.cfg.requestTimeout=3
http.cfg.retry.enabled=true
http.cfg.retry.interval=60
http.queue.clearsize=1600
http.queue.size=2000
http.queue.threads=10
[admusr@Cable-MPE-S-A smscfg]$
```

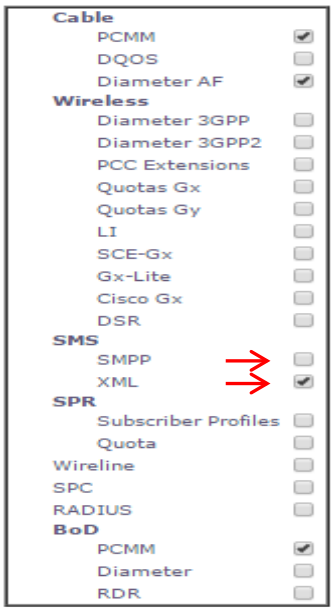
At the time of policy execution if a policy notification is triggered with a target destination for which a connection does not exist, the notification message shall be dropped generating a Warning Trace Log.

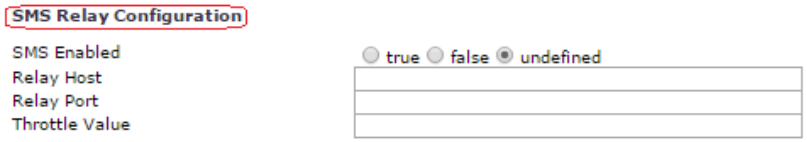
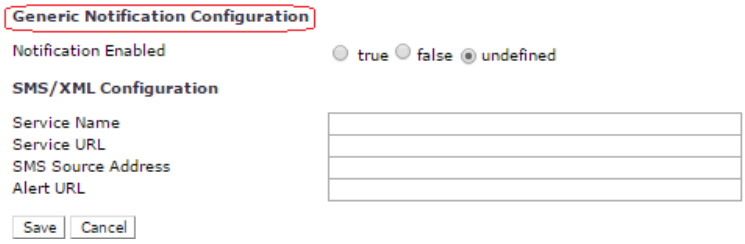
```
04/13/2016 19:54:04 EDT   2567   Warning   SMTP:Error attempting to establish a new connection to . Error: Could not connect to SMTP host: localhost, port: 25
04/13/2016 19:54:06 EDT   2565   Warning   SMTP:Connection to MTA was closed.
```

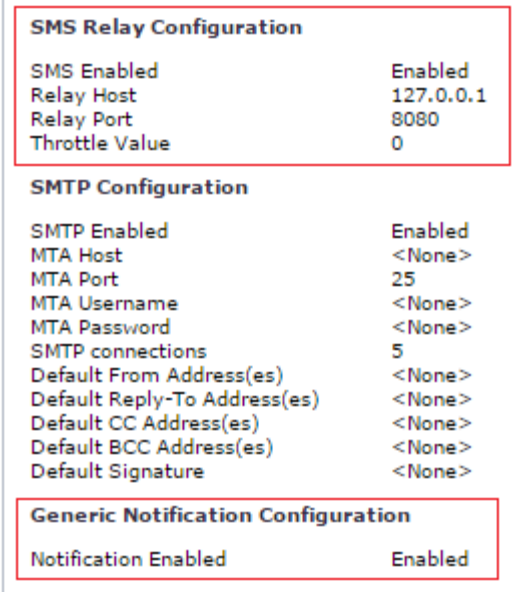
Additionally, the file "**HTTP.properties**" is also introduced under same path (/opt/camiant/smsr/smscfg/). This file shall contain all the data for persistent Notification Servers as configured from CMP. Any modifications made from CMP shall be reflected in this file

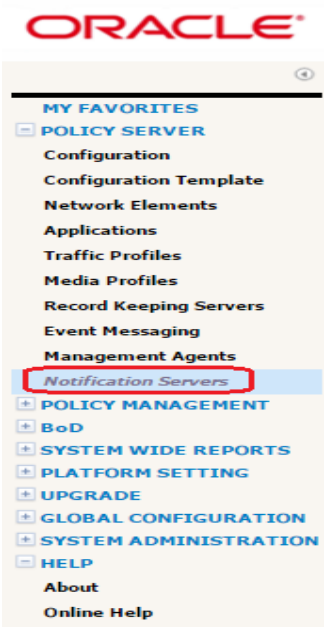
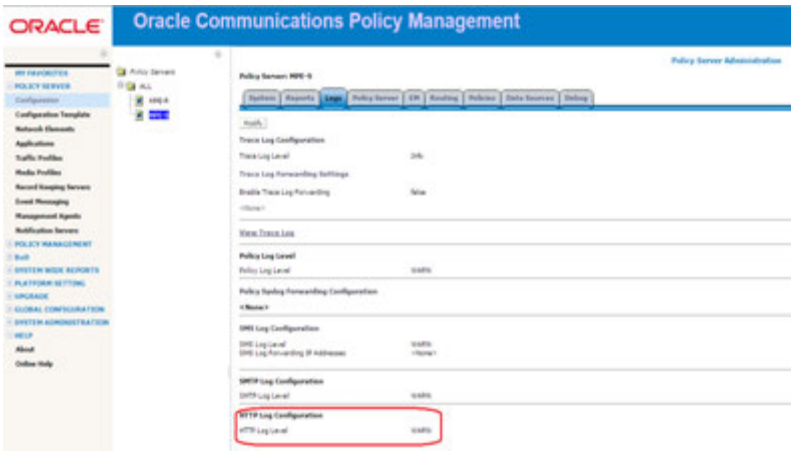
4. Procedure To Enable The Feature

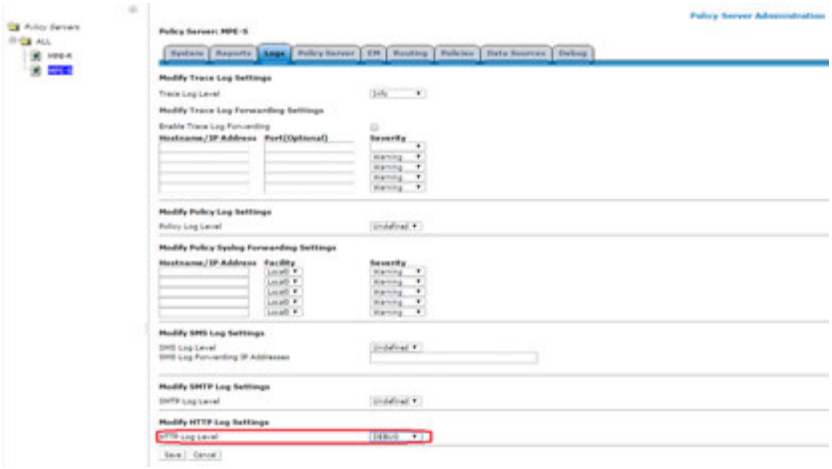
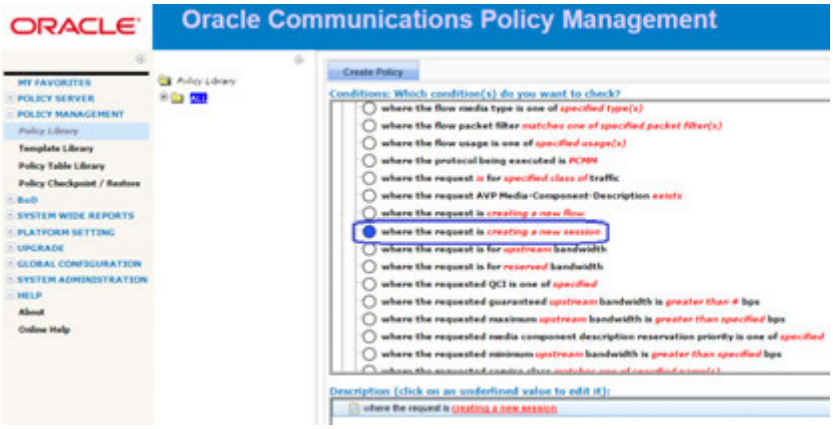
Pre-Enable Steps			
Step	Action	Expected Results	Pass | Fail
1	Validate CMP Mode settings	**CMP GUI: Help → About →Highlight the screen to reveal the small square (marked by the red circle below) then click it**  • Click the "Change Mode" button  • Validate that either "SMPP" or "XML" options under "SMS" are enabled/checked	

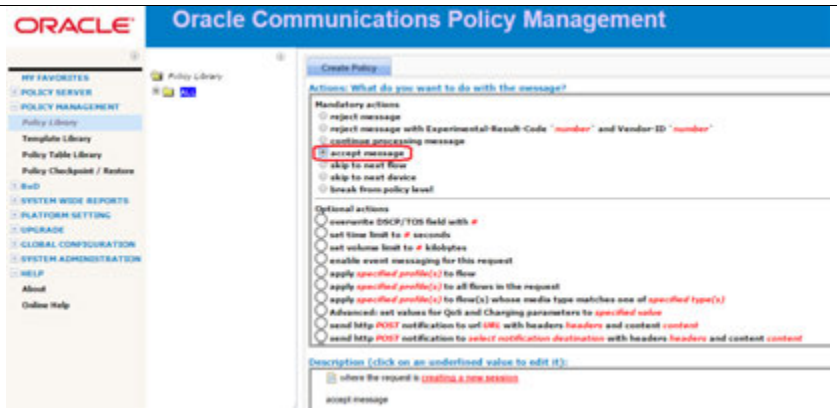
		Mode  • If not enable one and then click “OK” to save	

Enable Steps			
Step	Action	Expected Results	Pass | Fail
1	Enable SMS Relay and Generic Notification Settings	**CMP GUI: Policy Server → Configuration →All → <*MPE cluster that is configured to execute policies on traffic*> → Policy Server Tab** • Click the "Modify" button  • Scroll to the "**SMS Relay Configuration**" section  • Click on the "**true**" radio button and complete the host, port, throttle value configurations • Scroll toward the end of the screen to the "**Generic Notification Configuration**" section  • Click on the "**true**" radio button then "Save"	

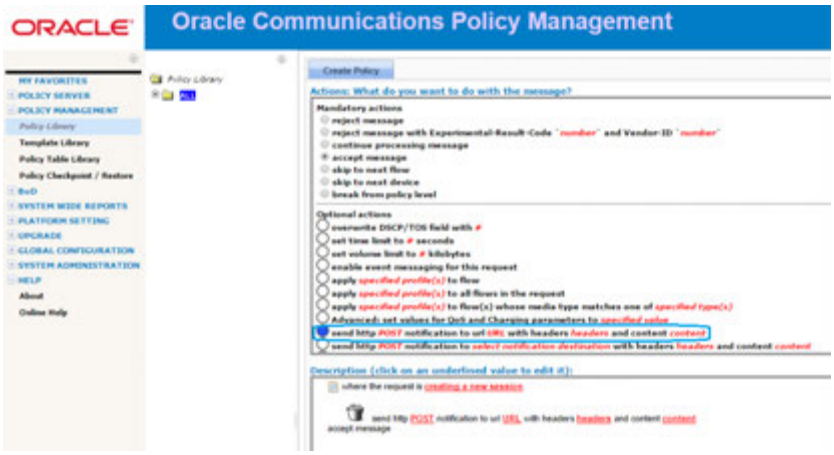
		 **SMS Relay Configuration** SMS Enabled: Enabled Relay Host: 127.0.0.1 Relay Port: 8080 Throttle Value: 0 **SMTP Configuration** SMTP Enabled: Enabled MTA Host: <None> MTA Port: 25 MTA Username: <None> MTA Password: <None> SMTP connections: 5 Default From Address(es): <None> Default Reply-To Address(es): <None> Default CC Address(es): <None> Default BCC Address(es): <None> Default Signature: <None> **Generic Notification Configuration** Notification Enabled: Enabled **Note:** Values above for SMS Relay Configuration (Relay Host, Port, Throttle value) are just an illustration example, these values need to change based on SMS relay of the customer.	

Post-Enable Verification Steps			
Step	Action	Expected Results	Pass | Fail
1.	Validate the "Notification Server Menu" availability	**CMP GUI: Policy Server** • Validate the "Notification Servers" menu item exists 	
2.	Validate the HTTP log level settings	**CMP GUI: Policy Server → Configuration →All → <*MPE cluster that is configured to execute policies on traffic*> → Logs Tab** • Verify "HTTP Log Configuration" section exists  Verify "HTTP Log Configuration" section exists • Click "Modify" button and set the HTTP log level to "Debug" then	

		save 	
3.	Validate new Policy actions	**CMP GUI: Policy Management → Policy Library → All** • Click "Create Policy"  • Click Next to choose creating a "Blank" policy then click Next again for Table Associations • Under conditions choose "**where the request is *creating a new session***"  • Click Next then choose "accept message" from the mandatory actions section	

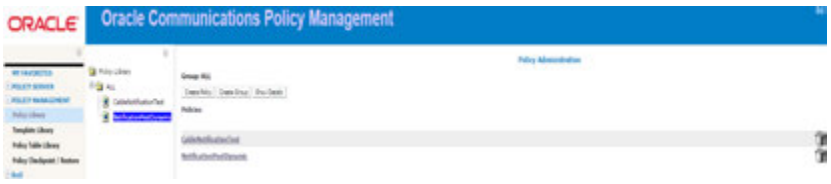


- From optional actions section, locate the 2 new HTTP Notification related actions and choose the dynamic action (the one where URL is set)



- Click on "***POST***" , "***URL***", "***headers***", "***content***" to set the method to deliver the notification, the destination URL of the notification server , and the message header and content.

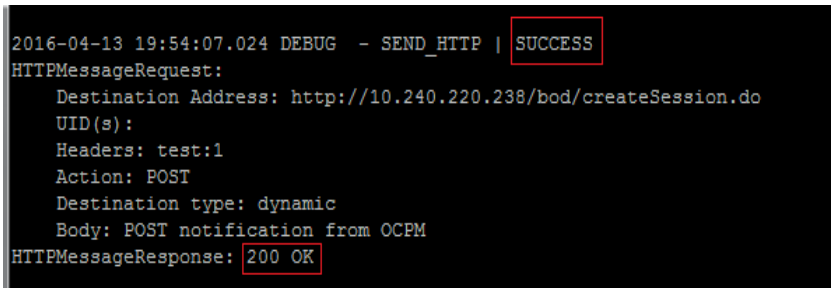
- Click Next, name the policy then click "Finish"



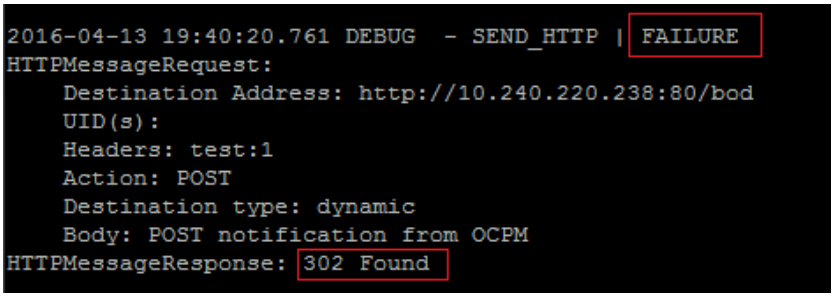
- Click on the Policy created then click "Deploy", choose the MPE configured to execute policies and push "Deploy" button

		Deploying: NotificationPostDynamic Select the target Policy Server(s): *Policy Servers* ALL MPE-R MPE-S Deploy Cancel • Verify the deployment completes successfully **Policy Servers - Deployment Succeeded** **MPE-S**	
4.	Verify MPE send HTTP notification based on deployed Policy	• Start a new session so as AF/P-CSCF sends a new session request message to MPE **CMP GUI: Policy Server → Configuration →All → <*MPE cluster that is configured to execute policies on traffic*> → Logs Tab → View Trace Log** • Log message indicates Policy trigger and authorizing the operation after the successful creation of the session  • SSH to MPE and navigate to logs directory (/var/camiant/log) • Display the content of the HTTP.log • Following an example of a successfully delivered HTTP	

notification log message:



- And following an example of failure delivery of an HTTP notification log message:



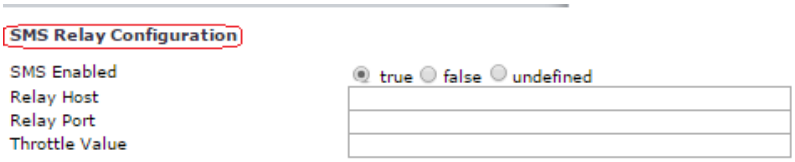
Note: The Policy Notification functionality is not intended as a fully "reliable" delivery mechanism and **is not subject to requirements for message queuing, retry, etc…** in the case of unreachable or malfunctioning destination peers at the time of notification delivery or indications of failure from the receiving system.

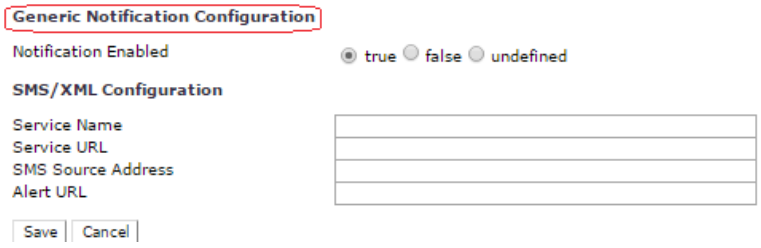
5. Back out Procedure

<table>
<tr><th colspan="4">Disable the Feature</th></tr>
<tr><th>Step</th><th>Action</th><th>Expected Results</th><th>Pass | Fail</th></tr>
<tr><td>1.</td><td>Disable SMS Relay and Generic Notification settings</td><td>
Disable SMS relay only if it is not needed by other feature/functionality.

CMP GUI: Policy Server → Configuration →All → <i><MPE cluster that is configured to execute policies on traffic</i> > → Policy Server Tab

• Click the “Modify” button

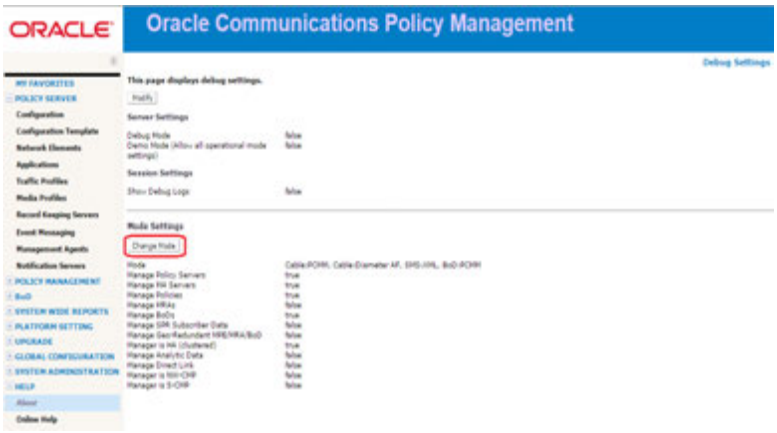

• Scroll to the “SMS Relay Configuration” section


• Click on the “false” radio button
• Scroll toward the end of the screen to the “Generic Notification Configuration” section


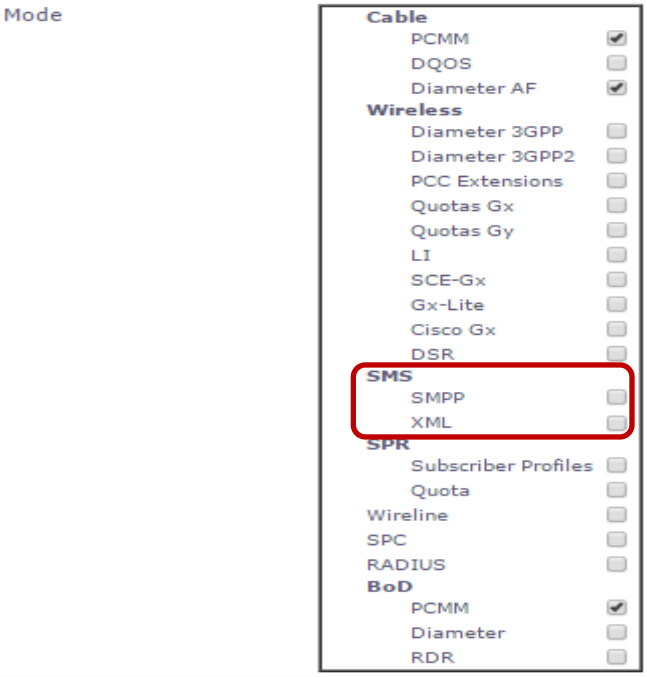
• Click on the “false” radio button then “Save”
</td><td></td></tr>
</table>

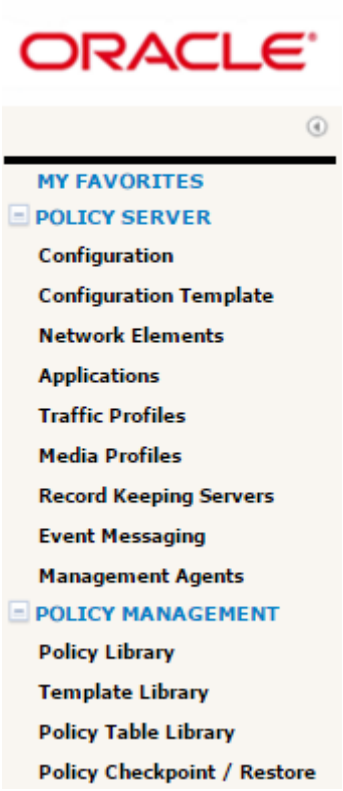
		Diameter AF Default Profiles: Default <None> Audio <None> Video <None> Data <None> Application <None> Control <None> Text <None> Message <None> Other <None> **SMS Relay Configuration** SMS Enabled Disabled Relay Host 127.0.0.1 Relay Port 8080 Throttle Value 0 **SMTP Configuration** SMTP Enabled Enabled MTA Host <None> MTA Port 25 MTA Username <None> MTA Password <None> SMTP connections 5 Default From Address(es) <None> Default Reply-To Address(es) <None> Default CC Address(es) <None> Default BCC Address(es) <None> Default Signature <None> **Generic Notification Configuration** Notification Enabled Disabled **SMS/XML Configuration** Service Name <None> Service URL <None> SMS Source Address 614 Alert URL <None>	
2.	Disable SMS related CMP Mode settings	**Disable SMS related mode settings only if it is not needed by other SMS delivery feature/functionality** **CMP GUI: Help → About →Highlight the screen to reveal the small square (marked by the red circle below) then click it** 	

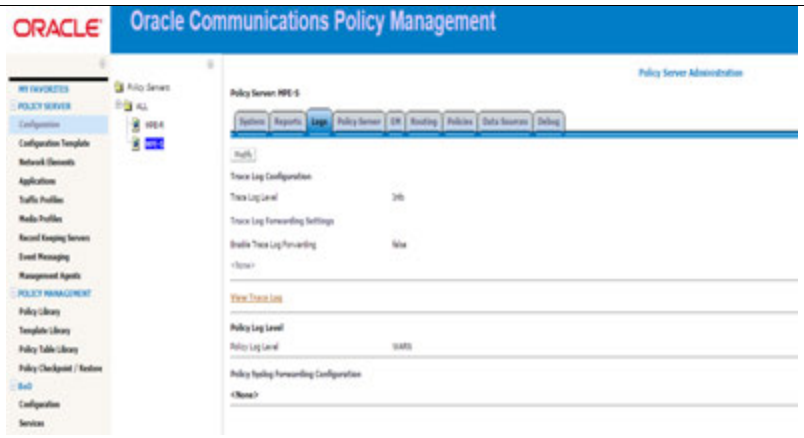
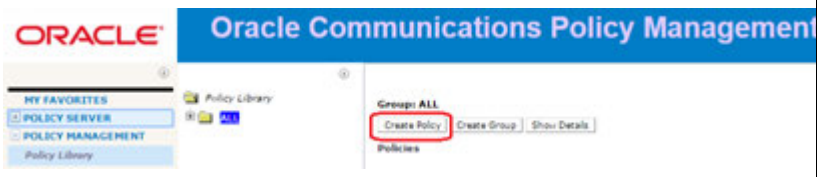
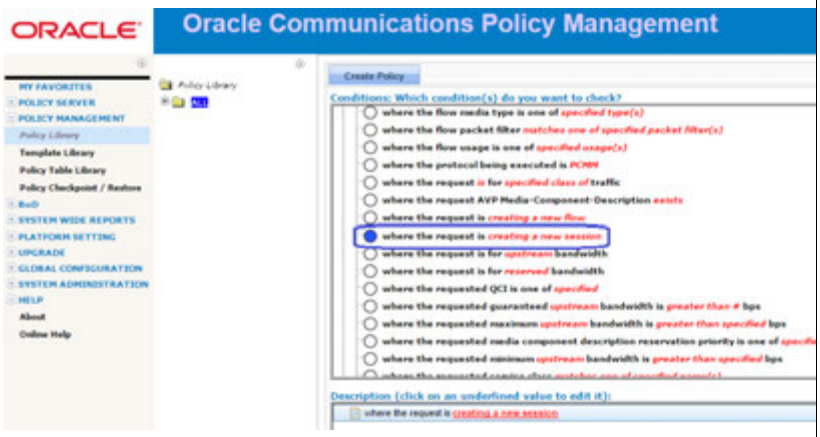
- Click the “Change Mode” button



- Uncheck “SMPP” or “XML” options under “SMS” section then click “OK” to save



Disable Verification Steps			
Step	Action	Expected Results	Pass | Fail
1.	Validate the "Notification Server Menu" does not exist	**CMP GUI: Policy Server** • Validate the "Notification Servers" menu item does not exist anymore 	
2.	Validate the HTTP log level settings does not exist	**CMP GUI: Policy Server → Configuration →All → <** ***MPE cluster that is configured to execute policies on traffic*** **> → Logs Tab** • Verify "HTTP Log Configuration" section does not exist anymore	

			
3.	Validate new Policy actions do not exist	**CMP GUI: Policy Management → Policy Library → All** • Click "Create Policy"  • Click Next to choose creating a "Blank" policy then click Next again for Table Associations • Under conditions choose "**where the request is *creating a new session***" for example to get to the next step for configuring actions  • Click Next and inspect actions section the optional actions section, ensure that the 2 new HTTP Notifications related actions do not exist anymore	

		Actions: What do you want to do with the message? **Mandatory actions** (•) reject message ( ) reject message with Experimental-Result-Code `*number*` and Vendor-ID `*number*` ( ) continue processing message ( ) accept message ( ) skip to next flow ( ) skip to next device ( ) break from policy level **Optional actions** ( ) overwrite DSCP/TOS field with *#* ( ) set time limit to *#* seconds ( ) set volume limit to *#* kilobytes ( ) enable event messaging for this request ( ) apply *specified profile(s)* to flow ( ) apply *specified profile(s)* to all flows in the request ( ) apply *specified profile(s)* to flow(s) whose media type matches one of *specified type(s)* ( ) Advanced: set values for QoS and Charging parameters to *specified value* ( ) send notification to syslog with `*message text*` and severity `*severity level*` ( ) send notification to trace log with `*message text*` and severity `*severity level*`	