

**Oracle® COMMUNICATIONS**

---

**Policy Management Feature Activation**

**Release 12.2**

**Generic Policy Notification Interface -  
Convert for Cable**

**E82618-01**

**February 2017**

Copyright © 2017 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, 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 on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services except as set forth in an applicable agreement between you and Oracle.

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**

<b>Acronym</b>	<b>Definition</b>
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 <b>POST</b> notification to url <b>URL</b> with headers <b>headers</b> and content <b>content</b>	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 <b>POST</b> notification to <b>select notification destination</b> with headers <b>headers</b> and content <b>content</b>	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.

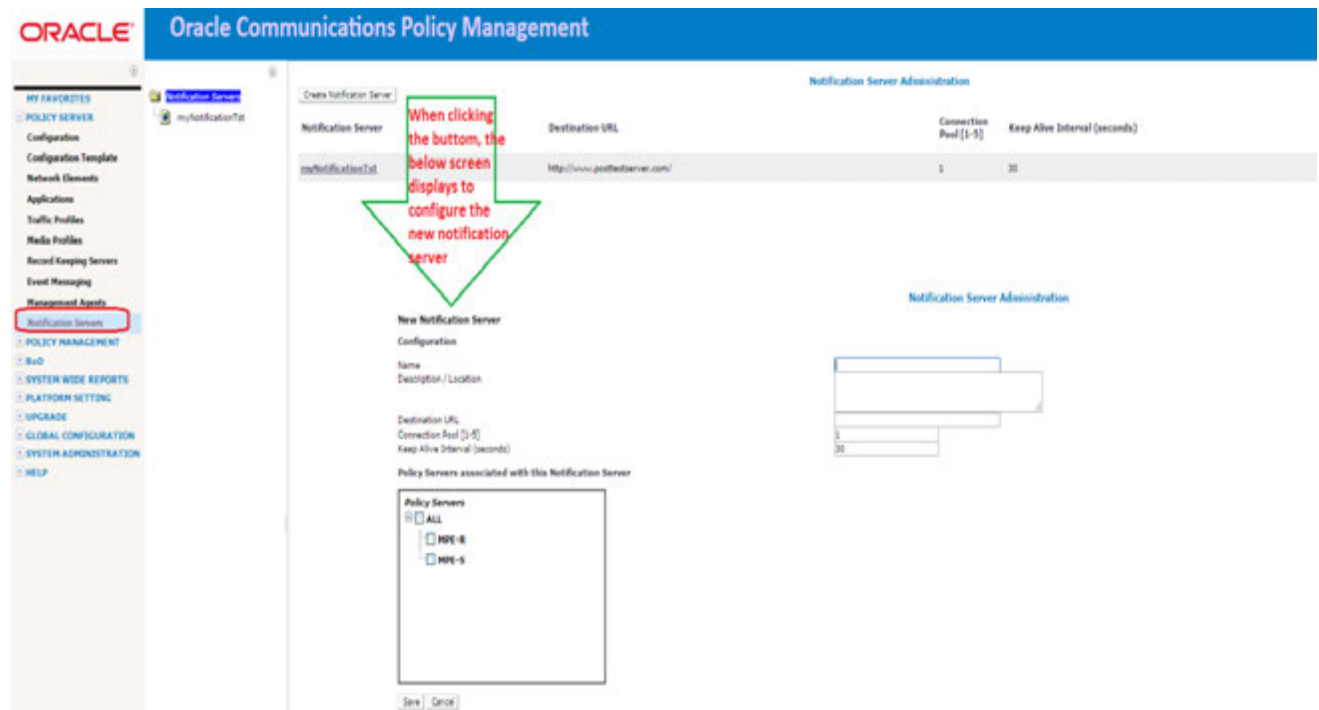
**In order for MPE to read the headers correctly if there are colons and/or commas in the header or value they will be escaped with forward slash (/). Also, Forward slash is not allowed as the last character in either the header or value and header name cannot be empty.**

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.

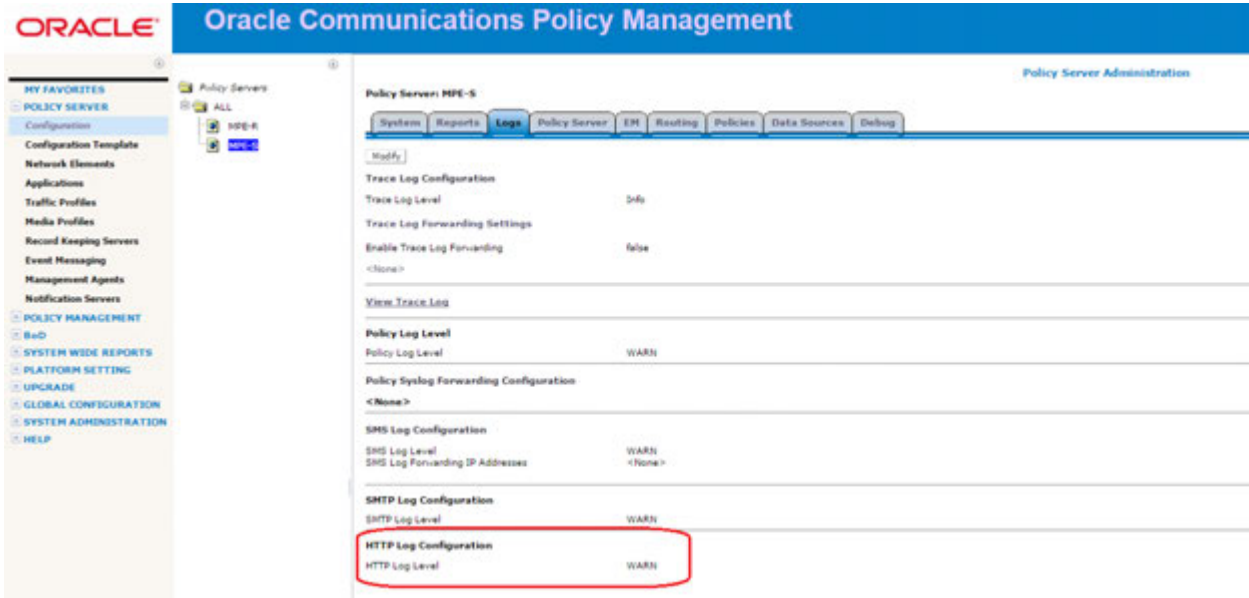
The screen also allows the user to associate a Notification Server with the available Policy Servers.

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.


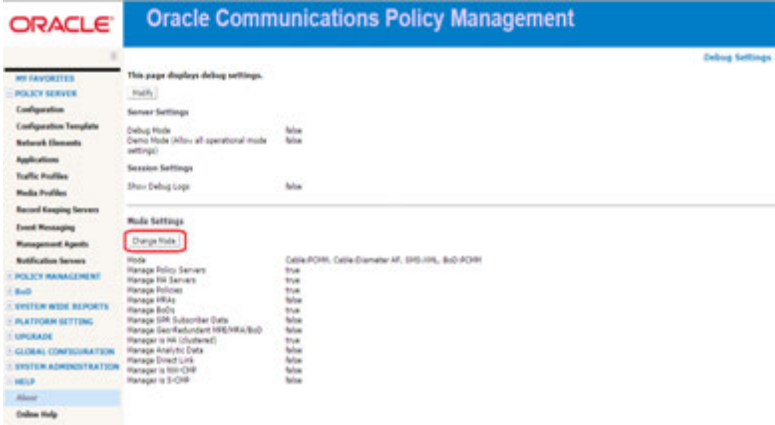
```
[admusr@Cable-MPE-S-A smscfg]$ more NotificationCfg.properties
#Generated at Tue Apr 12 17:42:27 EDT 2016
#Tue Apr 12 17:42:27 EDT 2016
http.cfg.connectionTimeout=3
http.cfg.enabled=true
http.cfg.numConnectionDynamic=1
http.cfg.requestTimeout=3
http.cfg.retry.enabled=true
http.cfg.retry.interval=60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

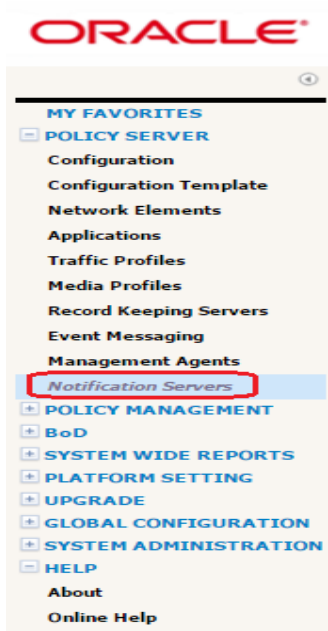
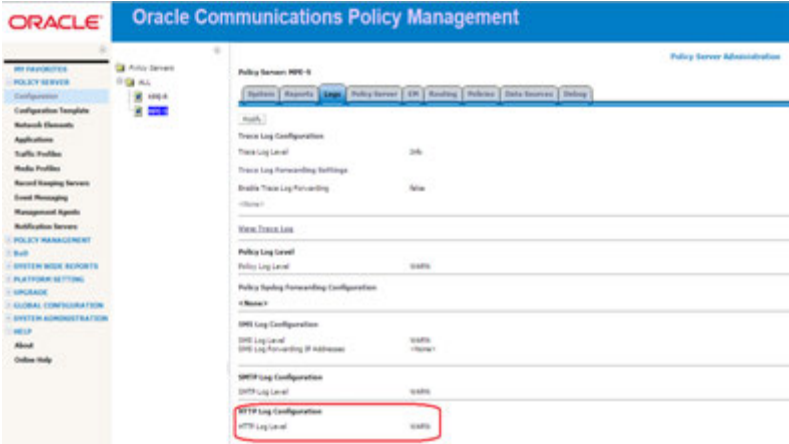
#### 4. Procedure To Enable The Feature

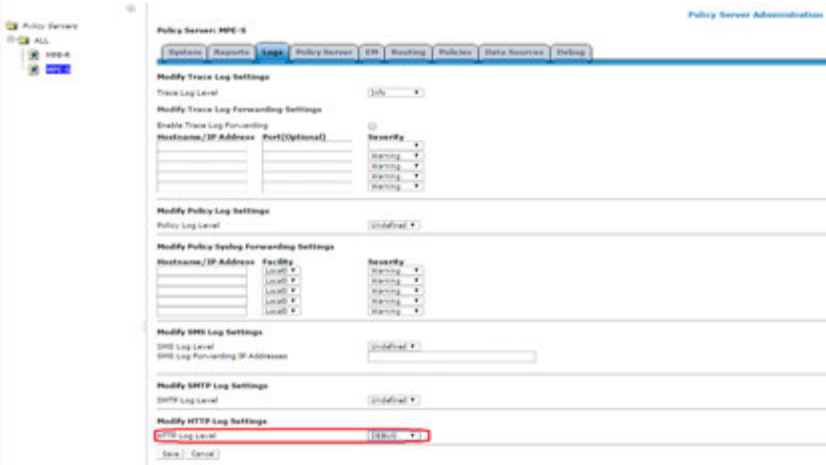
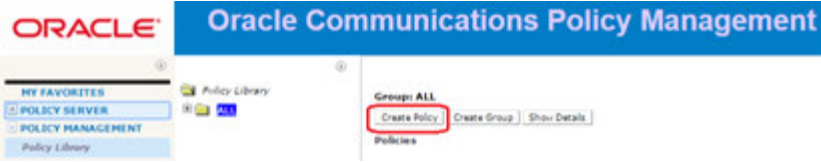
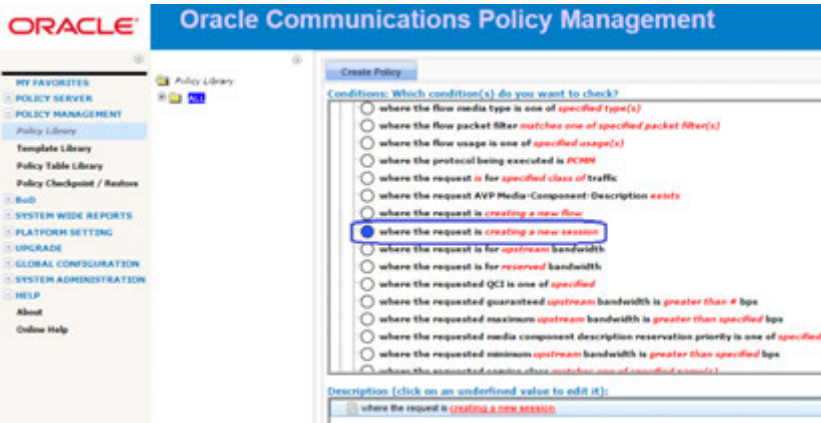
Pre-Enable Steps			
Step	Action	Expected Results	Pass   Fail
1	Validate CMP Mode settings	<p><b>CMP GUI: Help → About → Highlight the screen to reveal the small square (marked by the red circle below) then click it</b></p>  <ul style="list-style-type: none"> <li>Click the “Change Mode” button</li> </ul>  <ul style="list-style-type: none"> <li>Validate that either “SMPP” or “XML” options under “SMS” are enabled/checked</li> </ul>	

		<p>Mode</p> <div data-bbox="812 226 1136 823"><p><b>Cable</b></p><p>PCMM <input checked="" type="checkbox"/></p><p>DQOS <input type="checkbox"/></p><p>Diameter AF <input checked="" type="checkbox"/></p><p><b>Wireless</b></p><p>Diameter 3GPP <input type="checkbox"/></p><p>Diameter 3GPP2 <input type="checkbox"/></p><p>PCC Extensions <input type="checkbox"/></p><p>Quotas Gx <input type="checkbox"/></p><p>Quotas Gy <input type="checkbox"/></p><p>LI <input type="checkbox"/></p><p>SCE-Gx <input type="checkbox"/></p><p>Gx-Lite <input type="checkbox"/></p><p>Cisco Gx <input type="checkbox"/></p><p>DSR <input type="checkbox"/></p><p><b>SMS</b></p><p>SMPP <input type="checkbox"/></p><p>XML <input checked="" type="checkbox"/></p><p><b>SPR</b></p><p>Subscriber Profiles <input type="checkbox"/></p><p>Quota <input type="checkbox"/></p><p>Wireline <input type="checkbox"/></p><p>SPC <input type="checkbox"/></p><p>RADIUS <input type="checkbox"/></p><p><b>BoD</b></p><p>PCMM <input checked="" type="checkbox"/></p><p>Diameter <input type="checkbox"/></p><p>RDR <input type="checkbox"/></p></div> <ul style="list-style-type: none"><li>• If not enable one and then click "OK" to save</li></ul>	
--	--	---	--

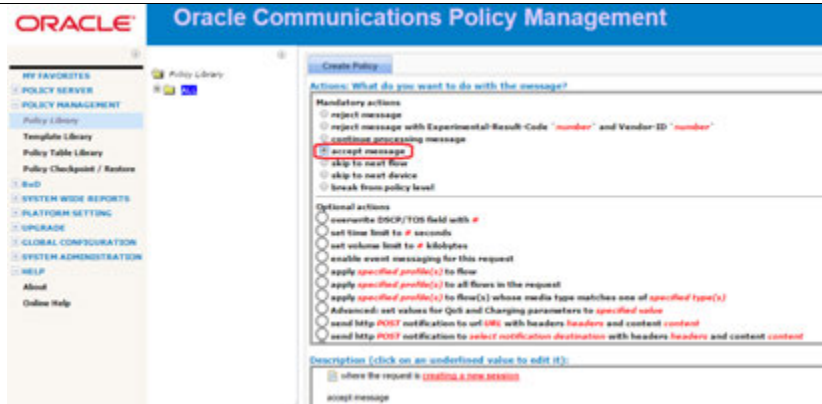
Enable Steps			
Step	Action	Expected Results	Pass   Fail
1	Enable SMS Relay and Generic Notification Settings	<p><b>CMP GUI: Policy Server → Configuration → All → &lt;MPE cluster that is configured to execute policies on traffic &gt; → Policy Server Tab</b></p> <ul style="list-style-type: none"> <li>Click the “Modify” button</li> </ul>  <ul style="list-style-type: none"> <li>Scroll to the “SMS Relay Configuration” section</li> </ul> <div style="border: 1px solid red; padding: 5px; margin-bottom: 10px;"> <p><b>SMS Relay Configuration</b></p> <p>SMS Enabled <input type="radio"/> true <input type="radio"/> false <input checked="" type="radio"/> undefined</p> <p>Relay Host <input type="text"/></p> <p>Relay Port <input type="text"/></p> <p>Throttle Value <input type="text"/></p> </div> <ul style="list-style-type: none"> <li>Click on the “true” radio button and complete the host, port, throttle value configurations</li> <li>Scroll toward the end of the screen to the “Generic Notification Configuration” section</li> </ul> <div style="border: 1px solid red; padding: 5px; margin-bottom: 10px;"> <p><b>Generic Notification Configuration</b></p> <p>Notification Enabled <input type="radio"/> true <input type="radio"/> false <input checked="" type="radio"/> undefined</p> <p><b>SMS/XML Configuration</b></p> <p>Service Name <input type="text"/></p> <p>Service URL <input type="text"/></p> <p>SMS Source Address <input type="text"/></p> <p>Alert URL <input type="text"/></p> <p><input type="button" value="Save"/> <input type="button" value="Cancel"/></p> </div> <ul style="list-style-type: none"> <li>Click on the “true” radio button then “Save”</li> </ul>	

		<div style="border: 1px solid red; padding: 5px; margin-bottom: 10px;"> <p><b>SMS Relay Configuration</b></p> <p>SMS Enabled Enabled  Relay Host 127.0.0.1  Relay Port 8080  Throttle Value 0</p> </div> <div style="margin-bottom: 10px;"> <p><b>SMTP Configuration</b></p> <p>SMTP Enabled Enabled  MTA Host &lt;None&gt;  MTA Port 25  MTA Username &lt;None&gt;  MTA Password &lt;None&gt;  SMTP connections 5  Default From Address(es) &lt;None&gt;  Default Reply-To Address(es) &lt;None&gt;  Default CC Address(es) &lt;None&gt;  Default BCC Address(es) &lt;None&gt;  Default Signature &lt;None&gt;</p> </div> <div style="border: 1px solid red; padding: 5px;"> <p><b>Generic Notification Configuration</b></p> <p>Notification Enabled Enabled</p> </div> <p><b>Note:</b> 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.</p>	
--	--	---	--

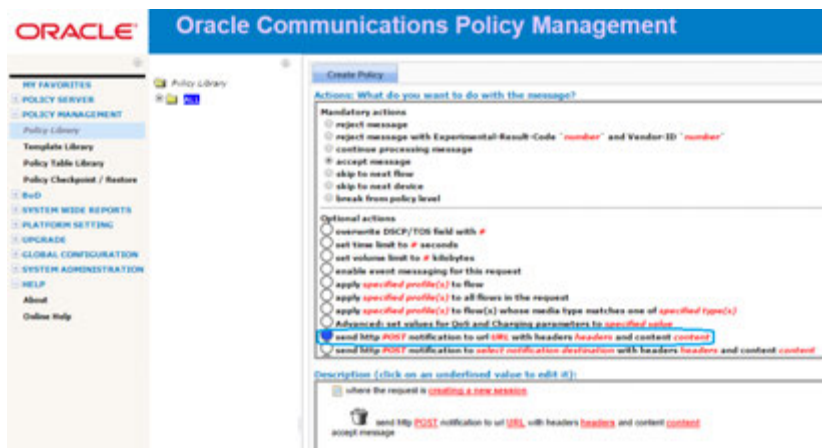
Post-Enable Verification Steps			
Step	Action	Expected Results	Pass   Fail
1.	Validate the "Notification Server Menu" availability	<p><b>CMP GUI: Policy Server</b></p> <ul style="list-style-type: none"> <li>Validate the "Notification Servers" menu item exists</li> </ul> 	
2.	Validate the HTTP log level settings	<p><b>CMP GUI: Policy Server → Configuration → All → &lt;MPE cluster that is configured to execute policies on traffic &gt; → Logs Tab</b></p> <ul style="list-style-type: none"> <li>Verify "HTTP Log Configuration" section exists</li> </ul>  <p>Verify "HTTP Log Configuration" section exists</p> <ul style="list-style-type: none"> <li>Click "Modify" button and set the HTTP log level to "Debug" then</li> </ul>	

		<p>save</p> 	
<p>3.</p>	<p>Validate new Policy actions</p>	<p><b>CMP GUI: Policy Management → Policy Library → All</b></p> <ul style="list-style-type: none"> <li>Click “Create Policy”</li> </ul>  <ul style="list-style-type: none"> <li>Click Next to choose creating a “Blank” policy then click Next again for Table Associations</li> <li>Under conditions choose “<b>where the request is <i>creating a new session</i></b>”</li> </ul>  <ul style="list-style-type: none"> <li>Click Next then choose “accept message” from the mandatory actions section</li> </ul>	





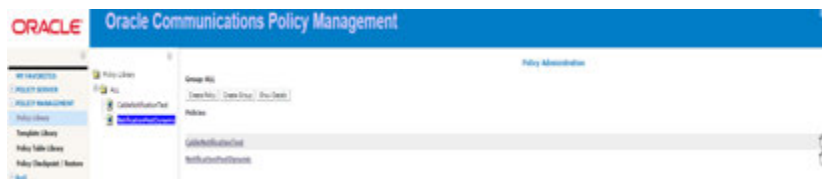
- From optional actions section, locate the 2 new HTTP Notification related actions and choose the dynamic action (the one where URL is set)



- 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

		<p><b>Deploying: NotificationPostDynamic</b></p> <p>Select the target Policy Server(s):</p> <div data-bbox="500 268 1040 646" style="border: 1px solid black; padding: 5px;"> <p><b>Policy Servers</b></p> <p><input checked="" type="checkbox"/> ALL</p> <p><input type="checkbox"/> MPE-R</p> <p><input checked="" type="checkbox"/> MPE-S</p> </div> <p><input type="button" value="Deploy"/> <input type="button" value="Cancel"/></p> <ul style="list-style-type: none"> <li>• Verify the deployment completes successfully</li> </ul> <p><b>Policy Servers - Deployment Succeeded</b></p> <p><b>MPE-S</b></p>	
<p>4.</p>	<p>Verify MPE send HTTP notification based on deployed Policy</p>	<ul style="list-style-type: none"> <li>• Start a new session so as AF/P-CSCF sends a new session request message to MPE</li> </ul> <p><b>CMP GUI: Policy Server → Configuration → All → &lt;MPE cluster that is configured to execute policies on traffic &gt; → Logs Tab → View Trace Log</b></p> <ul style="list-style-type: none"> <li>• Log message indicates Policy trigger and authorizing the operation after the successful creation of the session</li> </ul> <pre> 04/13/2016 19:54:07 EDT 1408 Info DiameterReceived AAA [1409922863-3041245245 / rx1] from dnameN10.240.220.240:366291 04/13/2016 19:54:07 EDT 4890 Info Policy Trace CallDataApplicationTest: authorizing operation 04/13/2016 19:54:07 EDT 4890 Info Policy Trace CallDataApplicationTest: authorizing operation 04/13/2016 19:54:07 EDT 1021 Info PSMMReceived GateSet [3472,33] in Context-MPE-R [10.240.220.241:30418] 04/13/2016 19:54:07 EDT 0820 Info PSMMReceived GateSetAuth [3472,33] from Context-MPE-R [10.240.220.241:30418] 04/13/2016 19:54:07 EDT 1412 Info DiameterReed AAA [1409922863-3041245245 / rx1] DIAMETER SUCCESS [2001] to dnameN10.240.220.240:366291 in 21 ms     </pre> <p><b>Trace Log Details</b></p> <pre> DiameterReceived AAA [1409922863-3041245245 / rx1] from dnameN10.240.220.240:366291 Diameter Message: AAA Version: 1 Msg Length: 824 Cmd Flags: 000,Perf Cmd Code: 200 App-ID: 10777206 Msg-Req-ID: 140001040 Cmd-To-Node-ID: 3861300104 Session-ID (387,M,1) = 191 Origin-Realm (386,M,1) = dname1 Origin-Realm (386,M,1) = oracle.com Auth-Application-ID (386,M,1) = 10777206 DestINATION-Realm (387,M,1) = oracle.com Media-Component-Description (387,M,1) = 3861300104 Media-Component-Number (387,M,1) = 3861300104 Media-Component-Number (387,M,1) = 3861300104 Media-Sub-Component (387,M,1) = 3861300104 FQDN-Number (387,M,1) = 0 FQDN-Description (387,M,1) = 3861300104 FQDN-Start (387,M,1) = 3861300104 Req-Request-Header-Set (387,M,1) = 3861300104 AF-Application-Description (387,M,1) = 3861300104 Media-Type (387,M,1) = 3861300104 Req-Request-Header-Set (387,M,1) = 3861300104 FQDN-Start (387,M,1) = 3861300104 M-Header-Set (387,M,1) = 3861300104 M-Header-Set (387,M,1) = 3861300104 Subscription-ID (387,M,1) = 3861300104 Subscription-ID (387,M,1) = 3861300104 Reservation-Priority (387,M,1) = 3861300104     </pre> <ul style="list-style-type: none"> <li>• SSH to MPE and navigate to logs directory (/var/camiant/log)</li> <li>• Display the content of the HTTP.log</li> <li>• Following an example of a successfully delivered HTTP</li> </ul>	

notification log message:



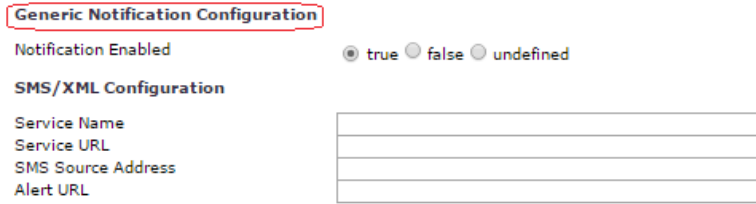
```
2016-04-13 19:54:07.024 DEBUG - SEND_HTTP | SUCCESS
HTTPMessageRequest:
  Destination Address: http://10.240.220.238/bod/createSession.do
  UID(s):
  Headers: test:1
  Action: POST
  Destination type: dynamic
  Body: POST notification from OCPM
HTTPMessageResponse: 200 OK
```


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

```
2016-04-13 19:40:20.761 DEBUG - SEND_HTTP | FAILURE
HTTPMessageRequest:
  Destination Address: http://10.240.220.238:80/bod
  UID(s):
  Headers: test:1
  Action: POST
  Destination type: dynamic
  Body: POST notification from OCPM
HTTPMessageResponse: 302 Found
```

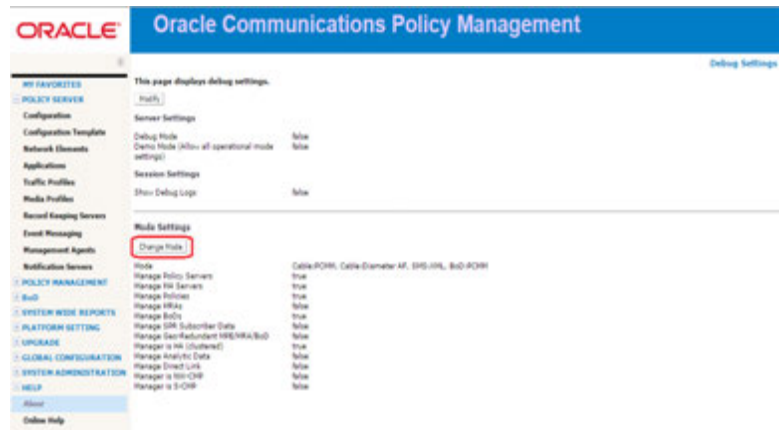
**Note:** The Policy Notification functionality is not intended as a fully “reliable” delivery mechanism and **is not subject to requirements for message queuing, retry, etc...** in the case of unreachable or malfunctioning destination peers at the time of notification delivery or indications of failure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

## 5. Back out Procedure

Disable the Feature			
Step	Action	Expected Results	Pass   Fail
1.	Disable SMS Relay and Generic Notification settings	<p><b>Disable SMS relay only if it is not needed by other feature/functionality.</b></p> <p><b>CMP GUI: Policy Server → Configuration → All → &lt;MPE cluster that is configured to execute policies on traffic &gt; → Policy Server Tab</b></p> <ul style="list-style-type: none"> <li>Click the “Modify” button</li> </ul>  <ul style="list-style-type: none"> <li>Scroll to the “SMS Relay Configuration” section</li> </ul>  <ul style="list-style-type: none"> <li>Click on the “false” radio button</li> <li>Scroll toward the end of the screen to the “Generic Notification Configuration” section</li> </ul>  <ul style="list-style-type: none"> <li>Click on the “false” radio button then “Save”</li> </ul>	

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

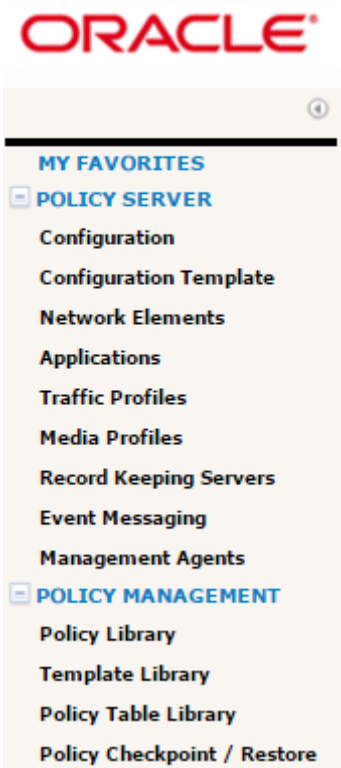
- Click the "Change Mode" button

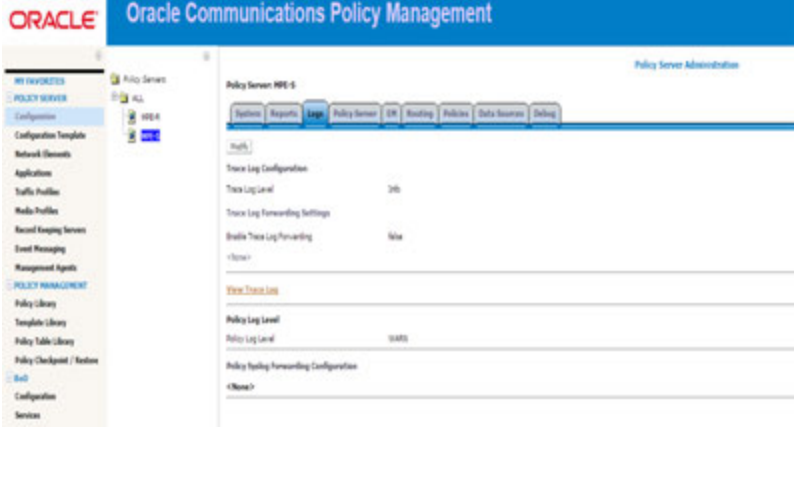

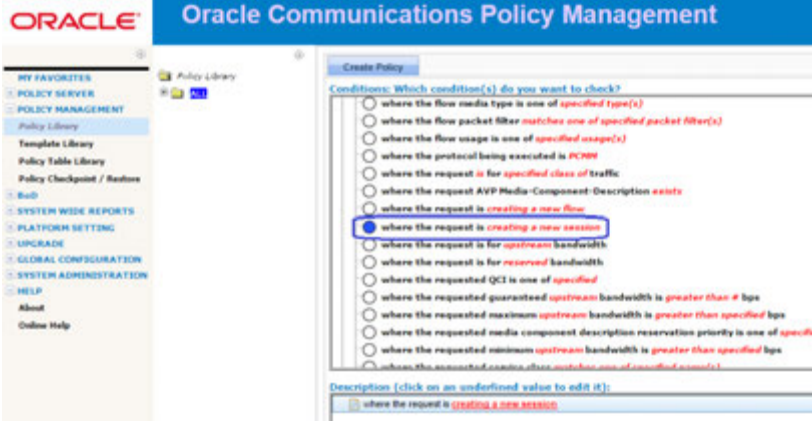


- Uncheck "SMPP" or "XML" options under "SMS" section then click "OK" to save

Mode

<b>Cable</b>	
PCMM	<input checked="" type="checkbox"/>
DQOS	<input type="checkbox"/>
Diameter AF	<input checked="" type="checkbox"/>
<b>Wireless</b>	
Diameter 3GPP	<input type="checkbox"/>
Diameter 3GPP2	<input type="checkbox"/>
PCC Extensions	<input type="checkbox"/>
Quotas Gx	<input type="checkbox"/>
Quotas Gy	<input type="checkbox"/>
LI	<input type="checkbox"/>
SCE-Gx	<input type="checkbox"/>
Gx-Lite	<input type="checkbox"/>
Cisco Gx	<input type="checkbox"/>
DSR	<input type="checkbox"/>
<b>SMS</b>	
SMPP	<input type="checkbox"/>
XML	<input type="checkbox"/>
<b>SPR</b>	
Subscriber Profiles	<input type="checkbox"/>
Quota	<input type="checkbox"/>
Wireline	<input type="checkbox"/>
SPC	<input type="checkbox"/>
RADIUS	<input type="checkbox"/>
<b>BoD</b>	
PCMM	<input checked="" type="checkbox"/>
Diameter	<input type="checkbox"/>
RDR	<input type="checkbox"/>

Disable Verification Steps			
Step	Action	Expected Results	Pass   Fail
1.	Validate the "Notification Server Menu" does not exist	<p><b>CMP GUI: Policy Server</b></p> <ul style="list-style-type: none"> <li>Validate the "Notification Servers" menu item does not exist anymore</li> </ul> 	
2.	Validate the HTTP log level settings does not exist	<p><b>CMP GUI: Policy Server → Configuration → All → &lt;MPE cluster that is configured to execute policies on traffic &gt; → Logs Tab</b></p> <ul style="list-style-type: none"> <li>Verify "HTTP Log Configuration" section does not exist anymore</li> </ul>	

			
<p>3.</p>	<p>Validate new Policy actions do not exist</p>	<p><b>CMP GUI: Policy Management → Policy Library → All</b></p> <ul style="list-style-type: none"> <li>Click “Create Policy”</li> </ul>  <ul style="list-style-type: none"> <li>Click Next to choose creating a “Blank” policy then click Next again for Table Associations</li> <li>Under conditions choose “<b>where the request is <i>creating a new session</i></b>” for example to get to the next step for configuring actions</li> </ul>  <ul style="list-style-type: none"> <li>Click Next and inspect actions section the optional actions section, ensure that the 2 new HTTP Notifications related actions do not exist anymore</li> </ul>	



		<p><b>Actions: What do you want to do with the message?</b></p> <hr/> <p><b>Mandatory actions</b></p> <ul style="list-style-type: none"> <li><input checked="" type="radio"/> reject message</li> <li><input type="radio"/> reject message with Experimental-Result-Code <code>`number`</code> and Vendor-ID <code>`number`</code></li> <li><input type="radio"/> continue processing message</li> <li><input type="radio"/> accept message</li> <li><input type="radio"/> skip to next flow</li> <li><input type="radio"/> skip to next device</li> <li><input type="radio"/> break from policy level</li> </ul> <hr/> <p><b>Optional actions</b></p> <ul style="list-style-type: none"> <li><input type="radio"/> overwrite DSCP/TOS field with <code>#</code></li> <li><input type="radio"/> set time limit to <code>#</code> seconds</li> <li><input type="radio"/> set volume limit to <code>#</code> kilobytes</li> <li><input type="radio"/> enable event messaging for this request</li> <li><input type="radio"/> apply <i>specified profile(s)</i> to flow</li> <li><input type="radio"/> apply <i>specified profile(s)</i> to all flows in the request</li> <li><input type="radio"/> apply <i>specified profile(s)</i> to flow(s) whose media type matches one of <i>specified type(s)</i></li> <li><input type="radio"/> Advanced: set values for QoS and Charging parameters to <i>specified value</i></li> <li><input type="radio"/> send notification to syslog with <code>`message text`</code> and severity <code>`severity level`</code></li> <li><input type="radio"/> send notification to trace log with <code>`message text`</code> and severity <code>`severity level`</code></li> </ul>	
--	--	--	--