Oracle® Communications
Diameter Signaling Router
DSR Security App Using Mediation Example Procedure
Release 8.1
E88989-01

July 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, 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.

**CAUTION:** Use only the Upgrade procedure included in the Upgrade Kit.

Before upgrading any system, please access My Oracle Support (MOS) (https://support.oracle.com) and review any Technical Service Bulletins (TSBs) that relate to this upgrade.

My Oracle Support (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.

See more information on My Oracle Support (MOS).

**Disclaimer:** This is just a reference to an example for creating security application using DSR Mediation functionality.
Table of Contents

1. Introduction .................................................................................................................. 5
   1.1 Purpose and Scope ................................................................................................. 5
   1.2 Overview of Security Application ......................................................................... 5

2. Example Procedure ...................................................................................................... 6
   2.1 Define Internal Variables .................................................................................. 6
   2.2 Define Measurements ......................................................................................... 7
   2.3 Add AVP to DSR Custom Dictionary ................................................................... 7
      2.3.1 OC-Supported-Features AVP ..................................................................... 7
      2.3.2 OC-OLR AVP ......................................................................................... 8
      2.3.3 DRMP AVP ........................................................................................... 8
   2.4 Ruleset Configuration ......................................................................................... 8
      2.4.1 Template 1: Roaming Scenario Identification .......................................... 9
      2.4.2 Template 2: Application ID and CC WhiteList for Inbound Roamers ........ 10
      2.4.3 Template 3: Application ID and CC Whitelist for Outbound Roamers ....... 12
      2.4.4 Template 4: OR Whitelist ....................................................................... 14
      2.4.5 Template 5: DR Whitelist ....................................................................... 16
      2.4.6 Template 6: OH Ends with OR ................................................................. 18
      2.4.7 Template 7: Handle Route Record AVP ................................................. 20
      2.4.8 Template 8: Handle Disallowed Requests .............................................. 22
      2.4.9 Template 9a: Remove DOIC AVP ............................................................ 23
      2.4.10 Template 9b: Remove DRMP AVP ......................................................... 25
      2.4.11 Template 10: Roaming Scenario Identification ...................................... 26
      2.4.12 Template 11: Destination-Realm Whitelist ........................................... 28
      2.4.13 Template 12a: Remove DOIC AVP ......................................................... 30
      2.4.14 Template 12b: Remove DRMP AVP ....................................................... 32
   2.5 Insert Rules within a Rule Set .............................................................................. 32
   2.6 State and Properties of Ruleset ......................................................................... 36
   2.7 Association of Ruleset to a Trigger Point ......................................................... 38

Appendix A. My Oracle Support (MOS) .......................................................................... 38
List of Tables

Table 1: Internal Variables ........................................................................................................... 6
Table 2: Measurements .................................................................................................................. 7
Table 3: Mediation Templates ...................................................................................................... 8
Table 4: Sample IMSIs .................................................................................................................. 9

List of Figures

Figure 1: Define Internal Variables ............................................................................................ 6
Figure 2: Screenshot of Measurements ......................................................................................... 7
Figure 3: Screenshot of DRMP AVP ............................................................................................. 8
Figure 4: Screenshot of Roaming Scenario Identification Template ............................................. 10
Figure 5: Screenshot of Application ID and CC Whitelist for Inbound Roamers Configured Template .................................... 11
Figure 6: Screenshot of Application ID and CC Whitelist for Outbound Roamers Configured Template .................................. 13
Figure 7: Screenshot of OR Whitelist Configured Template ....................................................... 15
Figure 8: Screenshot of DR Whitelist Configured Template ....................................................... 17
Figure 9: Screenshot of OH Ends with OR Configured Template ................................................. 19
Figure 10: Screenshot of Handle Route Record AVP Configured Template ................................ 21
Figure 11: Screenshot of Handle Disallowed Requests Configured Template ............................. 22
Figure 12: Screenshot of Remove DOIC AVP Configured Template ........................................... 24
Figure 13: Screenshot of Remove DRMP AVP Configured Template .......................................... 25
Figure 14: Screenshot of Roaming Scenario Identification Configured Template ........................ 27
Figure 15: Screenshot of Destination-Realm Whitelist Configured Template .............................. 29
Figure 16: Screenshot of Remove DOIC AVP Configured Template ........................................... 31
Figure 17: Screenshot of Configured Template ............................................................................. 32
Figure 18: Template 1: Roaming Scenario Identification .............................................................. 33
Figure 19: Template 2: Application ID and CC Whitelist for Inbound Roamers ............................ 33
Figure 20: Template 3: Application ID and CC Whitelist for Outbound Roamers ......................... 33
Figure 21: Template 4: OR Whitelist ........................................................................................... 34
Figure 22: Template 5: DR Whitelist ........................................................................................... 34
Figure 23: Template 6: OH Ends with OR .................................................................................... 34
Figure 24: Template 7: Handle RouteRecord AVP ...................................................................... 34
Figure 25: Template 8: Handle Disallowed Requests ................................................................... 35
Figure 26: Template 9a: Remove DOIC AVP .............................................................................. 35
Figure 27: Template 9b: Remove DRMP AVP ............................................................................ 35
Figure 28: Template 10: Roaming Scenario Identification ........................................................... 35
Figure 29: Template 11. Destination-Realm Whitelist ................................................................. 36
Figure 30: Template 12a. Remove DOIC AVP ............................................................................ 36
Figure 31: Template 12b. Remove DRMP AVP .......................................................................... 36
Figure 32: Active Templates Used as Reference ......................................................................... 37
Figure 33: Screenshot of Rule Set Attached to its Trigger Points ................................................. 38
1. Introduction

1.1 Purpose and Scope

This document provides a sample procedure required to build a security application using mediation. No additional software installation is required before executing this procedure. The standard DSR installation procedure loads all required software. You do need to activate the Mediation feature before implementing the security application.

1.2 Overview of Security Application

- Most of the Diameter security vulnerabilities are for interconnect from roaming networks through IPX or directly from roaming partner networks.
- DEA is considered as the only point of contact into and out of an operator’s network at the Diameter application level.
- Attacks are induced in operator’s home network through Diameter messages passing through DEA.
- Security threats currently being discussed for SS7 are around below mentioned attacks:
  - Location tracking
  - Call intercept
  - Subscriber Denial of Service
  - Subscriber Account fraud
  - SMS SPAMS
- DSR based Diameter Security Countermeasures can be used to mitigate different diameter attacks.
- Diameter security countermeasures shall be implemented using ART or Mediation rules based screening.
- In this user guide, we use Mediation to configure and implement Diameter security countermeasures (Security Application).
- Diameter Security Countermeasures shall be applied on:
  - Ingress messages received from the peers of external foreign network
  - Egress messages sent from home network to external foreign network.
- For the purposes of applying countermeasures, subscribers are classified into one of following three types:
  - Inbound roaming subscribers: Security countermeasures are applicable for visited network subscribers roaming in home network
  - Outbound roaming subscribers: Security countermeasures are applicable for home network subscribers roaming in visited network
  - Non-Roaming home network subscribers: Security countermeasures are applicable for home network subscribers who are not roaming outside home network
2. **Example Procedure**

This section lists the steps followed to build the sample security application using mediation. The security application uses various countermeasure checks. User may vary the templates (add/delete/modify) as per their needs.

**Test Setup topology:** DSR Setup with 1 NO + 1 SO + 1 MP. In the example (sample testing), DSR 80.14.1 is used with 1 NO + 1 SO + 1 MP, and taken as reference in this user guide.

### 2.1 Define Internal Variables

The internal variable provides inputs (i.e., Peer Type, Roamer Type, etc.) to templates, which implements countermeasures, generates alarms, and drops the vulnerable message.

To configure Internal Variables:

1. Launch an active SO GUI.
2. Navigate to **Main Menu -> Diameter -> Mediation -> Internal Variables Screen.**
3. Click **Insert** to insert each internal variable individually.
4. Define the internal variables as shown in Table 1 and shown in Figure 1 as reference. The templates set and read these internal variables.

<table>
<thead>
<tr>
<th>Variable Name</th>
<th>Description</th>
<th>Type</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$msgDisallowed</td>
<td>If true, then message is not allowed further; false then message is allowed and it is still tracked by other templates.</td>
<td>Integer32</td>
<td>0</td>
</tr>
<tr>
<td>$foreignIngressPeer</td>
<td>If true, then message is from foreign network to home network.</td>
<td>Integer32</td>
<td>0</td>
</tr>
<tr>
<td>$foreignEgressPeer</td>
<td>If true, then message is from home network to foreign network.</td>
<td>Integer32</td>
<td>0</td>
</tr>
<tr>
<td>$inboundRoaming</td>
<td>If true, then subscriber is inbound subscriber.</td>
<td>Integer32</td>
<td>0</td>
</tr>
<tr>
<td>$outboundRoaming</td>
<td>If true, then subscriber is outbound subscriber.</td>
<td>Integer32</td>
<td>0</td>
</tr>
<tr>
<td>$index</td>
<td>Used as an index to delete the multiple occurrence of an AVP in one shot</td>
<td>Integer32</td>
<td>0</td>
</tr>
</tbody>
</table>

**Table 1: Internal Variables**

![Define Internal Variables](image_url)
2.2 Define Measurements

Measurements calculate the number of vulnerable messages dropped by the Security application. For each type of countermeasure, create an entry.

To configure Measurements,
1. Launch an active SO GUI.
3. Click Insert to insert each measurement individually.

Use the measurements from Table 2 and shown in Figure 2 as a reference for this example.

<table>
<thead>
<tr>
<th>Measurement Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>measurement_inbound_10</td>
<td>Application ID and CC whitelist for inbound roamers</td>
</tr>
<tr>
<td>measurement_outbound_20</td>
<td>Application ID and CC whitelist for outbound roamers</td>
</tr>
<tr>
<td>measurement_DRWhitelist_40</td>
<td>DR whitelist</td>
</tr>
<tr>
<td>measurement_DestRealm_ER_100</td>
<td>Destination Realm Egress Request</td>
</tr>
<tr>
<td>measurement_Handle_RRecordAVP_60</td>
<td>Handle Route Record AVP</td>
</tr>
<tr>
<td>measurement_OH_ends_with_OR_50</td>
<td>OH ends with OR</td>
</tr>
<tr>
<td>measurement_ORWhitelist_30</td>
<td>OR whitelist</td>
</tr>
</tbody>
</table>

Table 2: Measurements

2.3 Add AVP to DSR Custom Dictionary

Add the following AVPs to the DSR custom dictionary:

2.3.1 OC-Supported-Features AVP

OC-Supported-Features ::= AVP Header: 621 >
[ OC-Feature-Vector ]
* [ AVP ]
2.3.2 OC-OLR AVP

OC-OLR ::= < AVP Header: 623 >
  < OC-Sequence-Number >
  < OC-Report-Type >
  [ OC-Reduction-Percentage ]
  [ OC-Validity-Duration ]
  * [ AVP ]

2.3.3 DRMP AVP

The DRMP (AVP code 301) is an Enumerated type. Use Figure 3 as a reference.

Main Menu: Diameter -> AVP Dictionary -> Custom Dictionary

Filter

Table Description: Custom Dictionary Table

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>AVP Code</th>
<th>V</th>
<th>M</th>
<th>P</th>
<th>r3</th>
<th>r4</th>
<th>r5</th>
<th>r6</th>
<th>r7</th>
<th>Vendor ID</th>
<th>Data Type</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>DRMP</td>
<td>301</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>Participant-Access-Priority</td>
<td>3GPP</td>
<td></td>
</tr>
<tr>
<td>OC-Feature-Vector</td>
<td>622</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>Unsigned64</td>
<td>Grouped</td>
<td>RFC 7533</td>
</tr>
<tr>
<td>OC-OLR</td>
<td>623</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>Unsigned32</td>
<td>Grouped</td>
<td>RFC 7533</td>
</tr>
<tr>
<td>OC-Reduction-Percentage</td>
<td>627</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>Unsigned32</td>
<td>Grouped</td>
<td>RFC 7533</td>
</tr>
<tr>
<td>OC-Report-Type</td>
<td>626</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>CC-Unit-Type</td>
<td>Grouped</td>
<td>RFC 7533</td>
</tr>
<tr>
<td>OC-Sequence-Number</td>
<td>624</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>Unsigned64</td>
<td>Grouped</td>
<td>RFC 7533</td>
</tr>
<tr>
<td>OC-Supported-Features</td>
<td>621</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>Unsigned32</td>
<td>Grouped</td>
<td>RFC 7533</td>
</tr>
<tr>
<td>OC-Validity-Duration</td>
<td>625</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>Unsigned32</td>
<td>Grouped</td>
<td>RFC 7533</td>
</tr>
</tbody>
</table>

Figure 3: Screenshot of DRMP AVP

2.4 Ruleset Configuration

To implement all six counter measures, configure the 14 Mediation templates. A few of these templates are common (i.e., not related to any specific counter measure), which performs generic actions like computing Peer Type/Roamer Type, generating alarms, pegging corresponding counters, and dropping the vulnerable messages. The remaining templates implement the counter measure specific business logic.

Refer to Table 1 to see counter measures to template mapping.

Table 3: Mediation Templates

<table>
<thead>
<tr>
<th>Counter Measure Name</th>
<th>Used Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application-ID Whitelist Screening</td>
<td>Template 2 &amp; 3</td>
</tr>
<tr>
<td>Application-ID and Command Code Consistency Check</td>
<td>Template 2 &amp; 3</td>
</tr>
<tr>
<td>Origin Realm and Destination Realm Whitelist Screening</td>
<td>Template 4, 5 &amp; 11</td>
</tr>
<tr>
<td>Origin host and Origin Realm Consistency Check</td>
<td>Template 6</td>
</tr>
<tr>
<td>Route-Record Validation</td>
<td>Template 7</td>
</tr>
<tr>
<td>Removal of Blacklisted AVPs</td>
<td>Template 9a, 9b, 12a &amp; 12b</td>
</tr>
</tbody>
</table>
2.4.1 Template 1: Roaming Scenario Identification

This template computes Peer Type [Foreign or Home Peer], Roamer Type [Inbound or Outbound Roamer], which is used by remaining templates.

It is associated with trigger point RTP1.

Template Definition

If @dsr.ingress.peer equals list of foreign peers

Then

Set Internal Variable: $foreignIngressPeer = 1

Set Internal Variable $outboundRoaming = (@msg.avp["User-Name"])[1].imsi.mccmnc == <LOCAL MCCMNC>)

Set Internal Variable: $inboundRoaming = !$outboundRoaming

This template sets internal variables if ingress peer is listed in a foreign peer list.

If the peer is in the whitelist then, check IMSI (International Mobile Subscriber Identity) from User-Name AVP to find out the home network of this user.

If the MCCMNC (extracted from IMSI) is equal to the local MCCMNC, then this subscriber is an outbound roaming subscriber.

If the MCCMC (extracted from IMSI) is not equal to the local MCCMNC, then this subscriber is an inbound roaming subscriber.

How to Extract MCC and MNC from IMSI Stored in USIM

The value of MNC (two or three digits) depends on the value of MCC.

![Diagram of MCC, MNC, MSIN, IMSI]

In our sample testing, we used the following IMSIs:

<table>
<thead>
<tr>
<th>MCC</th>
<th>MNC</th>
<th>Country</th>
<th>IMSI</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>404</td>
<td>17</td>
<td>India</td>
<td>404179712345678</td>
<td>Home Network Subscriber</td>
</tr>
<tr>
<td>460</td>
<td>02</td>
<td>China</td>
<td>460022112345678</td>
<td>Foreign Network Subscriber</td>
</tr>
</tbody>
</table>

These IMSIs have been used for outbound and inbound subscriber in our sample testing and can be used as a reference.
2.4.2 Template 2: Application ID and CC WhiteList for Inbound Roamers

This template is applicable for the subscriber marked as Valid Inbound Subscriber by Template 1 “Roaming Scenario Identification.”

If the diameter message is for inbound subscriber, then this template is executed.

This template checks for $msgDisallowed (to allow this message or not), @msg.application_id (to check that application ID is in the whitelist or not) and @msg.command.code (to check that this command code is allowed or not).

If above conditions are satisfied, then it allows the message by setting $msgDisallowed = 0.

If not satisfied, then it abandons the message by setting $msgDisallowed = 10. 10 indicates “Application ID and CC whitelist for inbound roamers” template check fails for this message. Hence, every template sets a different msgDisallowed value in case of failure.

It is associated with trigger point RTP1.

**Template Definition**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IF $inboundRoaming is true AND $msgDisallowed is false AND @msg.application_id equals list of application IDs AND @msg.command.code equals list of command-codes per application ID THEN Set Internal Variable: $msgDisallowed = 0 for all the rules except the default rule: $msgDisAllowed = 10</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** CC can be optional, i.e., App-ID can be put on the whitelist without setting any CC. If you decide not to put CC in the whitelist, then only the App-ID filters the messages irrespective of CC in messages.
Figure 5: Screenshot of Application ID and CC Whitelist for Inbound Roamers Configured Template
2.4.3 Template 3: Application ID and CC Whitelist for Outbound Roamers

This template is applicable for the subscriber marked as Valid Outbound Subscriber by Template 1 (i.e., roaming scenario identification).

If the diameter message is from outbound subscriber, then this template is executed.

This template checks for $msgDisallowed (to allow this message or not), @msg.application_id (to check that application ID is in the whitelist or not) and @msg.command.code (to check that this command code is allowed or not).

If above conditions satisfied, then it allows the message by setting $msgDisallowed = 0.

If not satisfied, then it abandons the message by setting $msgDisallowed = 20. 20 indicates "Application ID and CC whitelist for outbound roamers" template check fails for this message. Hence, every template sets a different msgDisallowed value in case of failure.

It is associated with trigger point RTP1.

Template Definition

IF $inboundRoaming is true
AND $msgDisallowed is false
AND @msg.application_id equals list of application IDs
AND @msg.command.code equals list of command-codes per application ID
THEN Set Internal Variable:
   $msgDisallowed = 0 for all the rules except the default rule:
   $msgDisallowed = 20

Note: CC can be optional, i.e., App-ID can be put on the whitelist without setting any CC. If you decide not to put CC in the whitelist, then only the App-ID filters the messages irrespective of CC in messages.
Figure 6: Screenshot of Application ID and CC Whitelist for Outbound Roamers Configured Template
2.4.4 Template 4: OR Whitelist

This template checks the Origin Realm of the incoming diameter message against the whitelist of Origin Realms. If the message’s Origin Realm is in the whitelist, then the diameter message is allowed for further processing, otherwise it is not.

This template checks for \$foreignIngressPeer (whitelisted foreign peer), \$msgDisallowed (to allow this message or not), and @msg.avp["Origin-Realm"] (to check that message’s Origin Realm is in the whitelist or not).

If above conditions are satisfied, then it allows the message by setting \$msgDisallowed = 0.

If not satisfied, then it abandons the message by setting \$msgDisallowed = 30. 30 indicates “OR whitelist” template check fails for this message. Hence, every template sets a different msgDisallowed value in case of failure.

It is associated with trigger point RTP1.

Template Definition

IF \$foreignIngressPeer is true
AND \$msgDisallowed is false
AND @msg.avp["Origin-Realm"] equals list of ORs
THEN Set Internal Variable: \$msgDisallowed = 0 for all the rules except the default rule:
\$msgDisallowed = 30

Note: The Origin-Realm is an optional condition. If you do not want to check origin realm, then use the empty value of origin realm or do not use this template.
Figure 7: Screenshot of OR Whitelist Configured Template
2.4.5 Template 5: DR Whitelist

After successful execution of Template 4 "OR Whitelist," if $msgDisallowed is 0 (message is still allowed for further processing), then Template 5 DR Whitelist is executed.

This template checks the Destination Realm of the incoming diameter message against the whitelist of Destination Realms. If the Destination Realm is in the whitelist, then the diameter message is allowed for further processing.

This template checks for $foreignIngressPeer (whitelisted foreign peer), $msgDisallowed (to allow this message or not), and @msg.avp["Destination-Realm"] (to check that Destination Realm is in the whitelist or not).

If above conditions are satisfied, then it allows the message by setting $msgDisallowed = 0.

If not satisfied, then it abandons the message by setting $msgDisallowed = 40. 40 indicates “DR whitelist" template check fails for this message. Hence, every template sets different msgDisallowed value in case of failure.

It is associated with trigger point RTP1.

**Template Definition**

IF $foreignIngressPeer is true AND $msgDisallowed is false AND @msg.avp["Destination-Realm"] equals list of DRs THEN Set Internal Variable: $msgDisallowed = 0 for all the rules except the default rule: $msgDisallowed = 40

**Note:** The Destination-Realm is an optional condition. If you do not want to check the destination realm, then use the empty value of destination realm or do not use this template.
<table>
<thead>
<tr>
<th>Rule Template Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DR whitelisted-RTP1</td>
<td>Name used to label this Rule Template in the system. The name is not case sensitive.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Message type support</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request/Question/Answer/Other</td>
<td>Indicates what type of message processing is supported by the Rule Template, i.e., Request, Answer, or both. The message type depends on the selected conditions and actions.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Conditions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fast search</td>
<td>A</td>
</tr>
<tr>
<td>Name</td>
<td>Check for Foreign Ingress Peer</td>
</tr>
<tr>
<td>Description</td>
<td>Check for Foreign Ingress Peer</td>
</tr>
<tr>
<td>Left value</td>
<td>DestinationRealm AVP</td>
</tr>
<tr>
<td>Right value</td>
<td>Integer32</td>
</tr>
</tbody>
</table>

| Fast search | B |
| Name | Check for mgdDisallowed |
| Description | Check for mgdDisallowed |
| Left value | DiameterIdentity |
| Right value | DiameterIdentity |

| Fast search | C |
| Name | Check for Destination-Realm AVP |
| Description | Check for Destination-Realm AVP |
| Left value | DiameterIdentity |
| Right value | DiameterIdentity |

<table>
<thead>
<tr>
<th>Condition Set</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>In-Order</td>
<td>Specify whether the conditions are logically ANDed, ORed, or form a complex logical expression like A OR B AND C. Use parentheses for the condition set that contains both AND and OR. Try to optimize the complex expression to achieve the fastest lookup.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-terminate</td>
<td>Internal variable</td>
</tr>
<tr>
<td>magDnsAllowed</td>
<td>The action allows setting the value for an internal variable that is valid for the entire duration of a transaction.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>New action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify Diameter Header Part</td>
<td>Add a new action to the action list that is applied when the conditions of the Rule Template match on the message.</td>
</tr>
</tbody>
</table>

**Figure 8: Screenshot of DR Whitelist Configured Template**
2.4.6 Template 6: OH Ends with OR

After successful screening of the diameter message with Template 5 “DR whitelist,” if the internal variable $msgDisallowed is still false, then it means the diameter message is allowed for further processing and Template 6 “Origin Host Ends with Origin Realm” is executed.

This template picks the Origin-Host and Origin-Realm AVP from the diameter message and it checks that the Origin-Host is ending with Origin-Realm or not.

If not, then it abandons the diameter message and sets $msgDisallowed = 50.

It also checks for $foreignIngressPeer and $msgDisallowed in the same way as it has been tested by the previous template.

It is associated with trigger point RTP1.

Template Definition

IF $foreignIngressPeer is true
AND $msgDisallowed is false
AND @msg.avp["Origin-Host"] does not end with "." + @msg.avp["Origin-Realm"]
THEN Set Internal Variable: $msgDisallowed = 50

Below is the screen shot of configured template “OH ends with OR”:
Figure 9: Screenshot of OH Ends with OR Configured Template
### 2.4.7 Template 7: Handle Route Record AVP

After successful screening of diameter message with Template 6 “OH Ends with OR,” if the internal variable $msgDisallowed is still false, it means the diameter message is allowed for further processing and Template 7 “Handle Route Record AVP” is executed.

This template basically iterated through all the route record AVPs which are present in the diameter message and will compare each rout record AVP with blacklist of Realms. If any Rout Record AVP from diameter message match with ANY realm from blacklisted realms then it will abandoned the message by setting $msgDisallowed = 60.

It is associated with trigger point RTP1.

**Template Definition**

```
IF $foreignIngressPeer is true
AND $msgDisallowed is false
AND `@msg.avp"Route-Record"}[any].data ends with list of realms
THEN Set Internal Variable: $msgDisallowed = 60
```

**Note:** In this template, we are using ANY keyword, which acts as a loop and iterates through all the route record AVPs to find out blacklisted realms present in any of the route record AVPs. Create one rule for each blacklisted realm.

The right hand side type is set to xl-value to a force slow-search.
### Figure 10: Screenshot of Handle Route Record AVP Configured Template
2.4.8 Template 8: Handle Disallowed Requests

Template 8 picks certain AVPs from the diameter message, and tests them again with certain countermeasure, which you configure.

If the diameter message fails at any countermeasure, then $msgDisallowed is set to a non-zero integer. This template acts on the $msgDisallowed value.

Template 8 takes three types of action, but you can be modify the requirements.

- **Peg Counter**: Count the number of disallowed request.
- **Raise Alarm**: Include the value of $msgDisallowed in the alarm description.
- **Abandon** the diameter message.

It is associated with trigger point RTP1.

**Template Definition**

IF $msgDisallowed is true
THEN Peg counter Count the number of disallowed ingress requests
Raise alarm Include the value of $msgDisallowed in the alarm description
Abandon message

**Main Menu: Diameter -> Mediation -> Rule Templates [Edit]**

---

**Figure 11: Screenshot of Handle Disallowed Requests Configured Template**
2.4.9 Template 9a: Remove DOIC AVP

After successful execution of Template 8 "Handle Disallowed Requests," if the message has failed at any countermeasure check, then the "Handle Disallowed Requests" template abandons the message (As per current configuration).

Once the diameter message passes all the above countermeasure checks ($msgDisallowed is still 0), then Template 9a "Remove DOIC AVP" is executed.

It checks for DOIC AVP (OC-Supported-Features and OC-OLR AVPs). If it is present in the diameter message, then it deletes the DOIC AVPs and forwards the message for further processing.

It is associated with trigger point RTP1.

**Template Definition**

```plaintext
IF $foreignIngressPeer is true
AND @msg.avp["OC-Supported-Features"] exists
OR @msg.avp["OC-OLR"] exists
THEN Delete AVP OC-Supported-Features
    Delete AVP OC-OLR
```
Main Menu: Diameter -> Mediation -> Rule Templates [Edit]

Figure 12: Screenshot of Remove DOIC AVP Configured Template
2.4.10 Template 9b: Remove DRMP AVP

After successful execution of Template 8 “Handle Disallowed Requests,” if the message has failed at any countermeasure check, then the “Handle Disallowed Requests” template abandons the message (As per current configuration).

Once the diameter message passes all the above countermeasure checks ($msgDisallowed is still 0), then Template 9b “Remove DRMP AVP” is executed.

It checks for DRMP AVP. If it is present in the diameter message, then it deletes the DRMP AVP and forwards the message for further processing.

It is associated with trigger point RTP1.

**Template Definition**

IF $foreignIngressPeer is true AND @msg.avp["DRMP"] exists THEN Delete AVP DRMP

---

**Figure 13: Screenshot of Remove DRMP AVP Configured Template**
2.4.11 Template 10: Roaming Scenario Identification

Template 10 checks for an egress peer before sending the diameter message to the connection.

It checks for application ID s6a, which is fixed in the current configuration; egress peer (check for egress foreign peer); and command code. In the sample configuration, only two commands are allowed: AIR and ULR.

If the condition is satisfied, then the diameter message is marked for keeping track by setting $foreignEgressPeer = 1.

It is associated with trigger point RTP10.

Template Definition

<table>
<thead>
<tr>
<th>Condition</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>@msg.application_id</td>
<td>equals S6a</td>
</tr>
<tr>
<td>@dsr.egress.peer</td>
<td>equals list of foreign peers</td>
</tr>
<tr>
<td>@msg.command.code</td>
<td>equals AIR</td>
</tr>
<tr>
<td>OR</td>
<td>equals ULR</td>
</tr>
<tr>
<td>THEN</td>
<td>Set Internal Variable: $foreignEgressPeer = 1</td>
</tr>
</tbody>
</table>
Figure 14: Screenshot of Roaming Scenario Identification Configured Template
2.4.12 Template 11: Destination-Realm Whitelist

Once the Template 10 “Roaming Scenario Identification” successfully executes, and $foreignEgressPeer is set to 1, Template 11 checks for Destination Realm AVP.

If the Destination Realm of the current diameter message is in the Destination Realm whitelist, then the $msgDisallowed is set to 0; otherwise, $msgDisallowed is 100, where 100 indicates the “Destination-Realm Whitelist” template check failed.

It is associated with trigger point RTP10.

Template Definition

IF $foreignEgressPeer is true
AND $msgDisallowed is false
AND @msg.avp["Destination-Realm"] equals list of DRs
THEN Set Internal Variable: $msgDisallowed = 0 for all the rules except the default rule: $msgDisallowed = 100
<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Template Name</td>
<td>Destination-Realm whitelisted-RTPL0</td>
</tr>
<tr>
<td>Message type support</td>
<td>Request, Answer</td>
</tr>
</tbody>
</table>

**Conditions**

<table>
<thead>
<tr>
<th>Fast search</th>
<th>Description</th>
<th>Optional</th>
<th>Fixed</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Check for Foreign Egress Peer</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>B</td>
<td>Check for mgwDisallowed</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>C</td>
<td>Check for Destination-Realm AVP</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Actions**

<table>
<thead>
<tr>
<th>Fast search</th>
<th>Description</th>
<th>Optional</th>
<th>Fixed</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Check for Foreign Egress Peer</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Figure 15: Screenshot of Destination-Realm Whitelist Configured Template**
2.4.13 Template 12a: Remove DOIC AVP

This template’s behavior is same as Template 9a, but association to trigger point is different and this works for egress peer.

It checks for DOIC AVP (OC-Supported-Features and OC-OLR AVPs). If it is present in the diameter message, then it deletes the AVPs and forwards the message for further processing.

It is associated with trigger point RTP10.

Template Definition

IF $foreignEgressPeer is true
AND @msg.avp["OC-Supported-Features"] exists
OR @msg.avp["OC-OLR"] exists
THEN Delete AVP OC-Supported-Features
    Delete AVP OC-OLR
**Figure 16: Screenshot of Remove DOIC AVP Configured Template**
2.4.14 Template 12b: Remove DRMP AVP

This template behavior is same as template 9b but association to trigger point is different and this will work for egress peer.

It checks for DRMP AVP. If it is present in the diameter message, then it deletes the DFRMP AVP and forwards the message for further processing.

It is associated with trigger point RTP10.

**Template Definition**

```plaintext
IF $foreignEgressPeer is true
AND @msg.avp["DRMP"] exists
THEN Delete AVP DRMP
```

![Figure 17: Screenshot of Configured Template](image)

**2.5 Insert Rules within a Rule Set**

Insert rules within each rule set according to configuration. The condition value within each rule can be customized according to requirements.

In this sample application testing, templates are created (see screenshots of each of the Templates in Figure 4 though Figure 17) and rules are added accordingly in each template.

To insert a rule into the rule set:

1. Navigate to **Main Menu -> Diameter -> Mediation -> Rule Sets.**
2. Select a rule set and click Insert.

The following screenshots display each rule set with rules that can be used as a reference.
### Figure 18: Template 1: Roaming Scenario Identification

<table>
<thead>
<tr>
<th>Rule Id</th>
<th>Identifying the Imperson peer</th>
<th>Set internal variable</th>
<th>Set Value</th>
<th>Internal variable</th>
<th>Set internal variable</th>
<th>Set Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>48</td>
<td>FN_HSS1</td>
<td>foreignprogressPeer 1</td>
<td>outboundRoaming</td>
<td>[msg asg[&quot;User-Name&quot;]][imsi.mccmnc==44417]</td>
<td>inboundRoaming</td>
<td>[outboundRoaming==0]</td>
</tr>
<tr>
<td>49</td>
<td>FN_HSS2</td>
<td>foreignprogressPeer 1</td>
<td>outboundRoaming</td>
<td>[msg asg[&quot;User-Name&quot;]][imsi.mccmnc==44417]</td>
<td>inboundRoaming</td>
<td>[outboundRoaming==0]</td>
</tr>
<tr>
<td>47</td>
<td>FN_HME1</td>
<td>foreignprogressPeer 1</td>
<td>outboundRoaming</td>
<td>[msg asg[&quot;User-Name&quot;]][imsi.mccmnc==44417]</td>
<td>inboundRoaming</td>
<td>[outboundRoaming==0]</td>
</tr>
</tbody>
</table>

### Figure 19: Template 2: Application ID and CC Whitelist for Inbound Roamers

<table>
<thead>
<tr>
<th>Rule Id</th>
<th>Check for Inbound Roamers</th>
<th>Check for msgDisallowed</th>
<th>Check for ApplicationId</th>
<th>Check for CommandCode</th>
<th>Set internal variable</th>
<th>Set Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>169</td>
<td>IS TRUE</td>
<td>IS FALSE</td>
<td>16777251</td>
<td>317</td>
<td>msgDisallowed</td>
<td>0</td>
</tr>
<tr>
<td>170</td>
<td>IS TRUE</td>
<td>IS FALSE</td>
<td>16777251</td>
<td>319</td>
<td>msgDisallowed</td>
<td>0</td>
</tr>
<tr>
<td>171</td>
<td>IS TRUE</td>
<td>IS FALSE</td>
<td>16777251</td>
<td>320</td>
<td>msgDisallowed</td>
<td>0</td>
</tr>
<tr>
<td>172</td>
<td>IS TRUE</td>
<td>IS FALSE</td>
<td>16777251</td>
<td>322</td>
<td>msgDisallowed</td>
<td>0</td>
</tr>
<tr>
<td>173</td>
<td>IS TRUE</td>
<td>IS FALSE</td>
<td>16777252</td>
<td></td>
<td>msgDisallowed</td>
<td>10</td>
</tr>
<tr>
<td>174</td>
<td>IS TRUE</td>
<td>IS FALSE</td>
<td>16777252</td>
<td></td>
<td>msgDisallowed</td>
<td>10</td>
</tr>
</tbody>
</table>

### Figure 20: Template 3: Application ID and CC Whitelist for Outbound Roamers

<table>
<thead>
<tr>
<th>Rule Id</th>
<th>Check for Outbound Roamers</th>
<th>Check for msgDisallowed</th>
<th>Check for ApplicationId</th>
<th>Check for CommandCode</th>
<th>Set internal variable</th>
<th>Set Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>175</td>
<td>IS TRUE</td>
<td>IS FALSE</td>
<td>16777251</td>
<td>316</td>
<td>msgDisallowed</td>
<td>0</td>
</tr>
<tr>
<td>176</td>
<td>IS TRUE</td>
<td>IS FALSE</td>
<td>16777251</td>
<td>318</td>
<td>msgDisallowed</td>
<td>0</td>
</tr>
<tr>
<td>177</td>
<td>IS TRUE</td>
<td>IS FALSE</td>
<td>16777251</td>
<td>321</td>
<td>msgDisallowed</td>
<td>0</td>
</tr>
<tr>
<td>178</td>
<td>IS TRUE</td>
<td>IS FALSE</td>
<td>16777251</td>
<td>323</td>
<td>msgDisallowed</td>
<td>0</td>
</tr>
<tr>
<td>179</td>
<td>IS TRUE</td>
<td>IS FALSE</td>
<td>16777252</td>
<td></td>
<td>msgDisallowed</td>
<td>0</td>
</tr>
<tr>
<td>180</td>
<td>IS TRUE</td>
<td>IS FALSE</td>
<td>16777252</td>
<td></td>
<td>msgDisallowed</td>
<td>20</td>
</tr>
</tbody>
</table>
Figure 21: Template 4: OR Whitelist

Figure 22: Template 5: DR Whitelist

Figure 23: Template 6: OH Ends with OR

Figure 24: Template 7: Handle RouteRecord AVP
### Figure 25: Template 8: Handle Disallowed Requests

<table>
<thead>
<tr>
<th>Rule Id</th>
<th>A</th>
<th>Assent Alarm/Event</th>
<th>Additional Info</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>213</td>
<td>10</td>
<td>Mediation Generic Alarm Major</td>
<td>&quot;<strong>Error Code:</strong> &quot;String(SmsDisallowed)&quot; + &quot;<strong>Error Description:</strong> Application id and CI/white list for inbound carriers check failed. Abandoned the message&quot;</td>
<td>measurement_inbound_10</td>
</tr>
<tr>
<td>219</td>
<td>100</td>
<td>Mediation Generic Alarm Major</td>
<td>&quot;<strong>Error Code:</strong> &quot;String(SmsDisallowed)&quot; + &quot;<strong>Error Description:</strong> &quot;Destination-Realm whilst check failed. Abandoned the message&quot;</td>
<td>measurement_DestRealm_ER_100</td>
</tr>
<tr>
<td>214</td>
<td>20</td>
<td>Mediation Generic Alarm Major</td>
<td>&quot;<strong>Error Code:</strong> &quot;String(SmsDisallowed)&quot; + &quot;<strong>Error Description:</strong> &quot;Application id and CI/white list for outbound carriers check failed. Abandoned the message&quot;</td>
<td>measurement_outbound_20</td>
</tr>
<tr>
<td>215</td>
<td>30</td>
<td>Mediation Generic Alarm Major</td>
<td>&quot;<strong>Error Code:</strong> &quot;String(SmsDisallowed)&quot; + &quot;<strong>Error Description:</strong> &quot;OR whilst check failed. Abandoned the message&quot;</td>
<td>measurement_ORwhilelist_30</td>
</tr>
<tr>
<td>216</td>
<td>40</td>
<td>Mediation Generic Alarm Major</td>
<td>&quot;<strong>Error Code:</strong> &quot;String(SmsDisallowed)&quot; + &quot;<strong>Error Description:</strong> &quot;OR whilst check failed. Abandoned the message&quot;</td>
<td>measurement_ORwhilelist_40</td>
</tr>
<tr>
<td>217</td>
<td>50</td>
<td>Mediation Generic Alarm Major</td>
<td>&quot;<strong>Error Code:</strong> &quot;String(SmsDisallowed)&quot; + &quot;<strong>Error Description:</strong> &quot;OR whilst check failed. Abandoned the message&quot;</td>
<td>measurement_ORwhilelist_50</td>
</tr>
<tr>
<td>218</td>
<td>60</td>
<td>Mediation Generic Alarm Major</td>
<td>&quot;<strong>Error Code:</strong> &quot;String(SmsDisallowed)&quot; + &quot;<strong>Error Description:</strong> &quot;Handle RO list  Record AVP check failed. Abandoned the message&quot;</td>
<td>measurement_Handle_ROlistAVP_60</td>
</tr>
</tbody>
</table>

### Figure 26: Template 9a: Remove DOIC AVP

```
IF A
   THEN Delete AVP
```

### Figure 27: Template 9b: Remove DRMP AVP

```
IF A
   THEN Delete AVP
```

### Figure 28: Template 10. Roaming Scenario Identification
2.6 State and Properties of Ruleset

After injecting rules within a rule set, change the state of the template to Active.

1. Navigate to **Main Menu -> Diameter -> Mediation -> State & Properties**.
2. Select a template and click **Edit**.
3. Change the State to **Active**.
4. You can change the Action Error Handling: Ignore the error depending on your requirements.
5. You can change the Status of Rule Counters: Checked. If checked, then you can see the peg counter for each rule.
### Active Templates Used as Reference

<table>
<thead>
<tr>
<th>Rule Template Name</th>
<th>State</th>
<th>Action Error Handling</th>
<th>Status of Rule Counters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Id and CC white list for inbound roamers-RTP1</td>
<td>Test</td>
<td>Ignore the error</td>
<td>Stopped</td>
</tr>
<tr>
<td>Application Id and CC white list for inbound roamers-RTP1-First Ver</td>
<td>Active</td>
<td>Ignore the error</td>
<td>Active</td>
</tr>
<tr>
<td>Application Id and CC white list for outbound roamers-RTP1</td>
<td>Test</td>
<td>Ignore the error</td>
<td>Stopped</td>
</tr>
<tr>
<td>Application Id and CC white list for outbound roamers-RTP1-First Ver</td>
<td>Active</td>
<td>Ignore the error</td>
<td>Active</td>
</tr>
<tr>
<td>CR whitelist RTP1</td>
<td>Test</td>
<td>Ignore the error</td>
<td>Stopped</td>
</tr>
<tr>
<td>CR whitelist RTP1-First Ver</td>
<td>Active</td>
<td>Ignore the error</td>
<td>Active</td>
</tr>
<tr>
<td>Destination-Realm whitelist-RTP1</td>
<td>Test</td>
<td>Ignore the error</td>
<td>Stopped</td>
</tr>
<tr>
<td>Destination-Realm whitelist-RTP1-First Ver</td>
<td>Active</td>
<td>Ignore the error</td>
<td>Active</td>
</tr>
<tr>
<td>Handle RouteRecord MAP</td>
<td>Test</td>
<td>Ignore the error</td>
<td>Stopped</td>
</tr>
<tr>
<td>Handle RouteRecord MAP-First Ver</td>
<td>Active</td>
<td>Ignore the error</td>
<td>Active</td>
</tr>
<tr>
<td>Handle disallowed requests</td>
<td>Test</td>
<td>Ignore the error</td>
<td>Stopped</td>
</tr>
<tr>
<td>Handle disallowed requests-First Ver</td>
<td>Active</td>
<td>Ignore the error</td>
<td>Active</td>
</tr>
<tr>
<td>Handle disallowed requests-RTP1-copy</td>
<td>Test</td>
<td>Ignore the error</td>
<td>Stopped</td>
</tr>
<tr>
<td>MlsesseTest</td>
<td>Development</td>
<td>Ignore the error</td>
<td>Stopped</td>
</tr>
<tr>
<td>MlsesseTest-copy</td>
<td>Development</td>
<td>Ignore the error</td>
<td>Stopped</td>
</tr>
<tr>
<td>MlsesseTest1</td>
<td>Development</td>
<td>Ignore the error</td>
<td>Stopped</td>
</tr>
<tr>
<td>CR ends with CR-RTP1</td>
<td>Test</td>
<td>Ignore the error</td>
<td>Stopped</td>
</tr>
<tr>
<td>CR ends with CR-RTP1-First Ver</td>
<td>Active</td>
<td>Ignore the error</td>
<td>Active</td>
</tr>
<tr>
<td>CR whitelist RTP1</td>
<td>Test</td>
<td>Ignore the error</td>
<td>Stopped</td>
</tr>
<tr>
<td>CR whitelist RTP1-First Ver</td>
<td>Active</td>
<td>Ignore the error</td>
<td>Active</td>
</tr>
</tbody>
</table>

Figure 32: Active Templates Used as Reference
2.7 Association of Ruleset to a Trigger Point

This procedure associates the templates to a trigger point.

Associate Template 1 to Template 9b on trigger point RTP1 in increasing order. Associate Template 10, Template 11, Template 8, Template 12a, and Template 12b on trigger point RTP 10 in given sequence. Associate Template 12a and 12b for the answer message on trigger point ATP10.

Figure 33: Screenshot of Rule Set Attached to its Trigger Points

Appendix A. My Oracle Support (MOS)

My Oracle Support

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 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 are 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 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.

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

2. Click Industries.
3. Under the Oracle Communications subheading, click the Oracle Communications documentation link. The Communications Documentation page appears. Most products covered by these documentation sets display under the headings Network Session Delivery and Control Infrastructure or “Platforms.”
4. Click on your Product and then the Release Number. A list of the entire documentation set for the selected product and release displays. To download a file to your location, right-click the PDF link, select Save target as (or similar command based on your browser), and save to a local folder.