# Oracle® Communications
# Diameter Signaling Router

Gateway Location Application (GLA) User Guide

**910-6924-001 Revision A**

May 2014

**ORACLE**®

# Table of Contents

# List of Tables

# Chapter

# 1

## Introduction

**Topics:**

This chapter contains a brief description of the Gateway Location Application (GLA) feature. The contents include sections about the document scope, audience, and organization; how to find related publications; and how to contact Customer Support for assistance.

## Purpose of this Documentation

This documentation:

- Gives a conceptual overview of the application's purpose, architecture, and functionality
- Describes the pages and fields on the application GUI (Graphical User Interface)
- Provides tasks for using the application interface
- Explains the organization of, and how to use, the documentation

### The Gateway Location Application (GLA)

The Gateway Location Application (GLA) is a DSR Application that provides a Diameter interface to subscriber data stored in the DSR's Policy Session Binding Repository (pSBR). Subscriber data concerning binding and session information is populated in the pSBR-B (Policy SBR - Binding) by the Policy Diameter Routing Agent (Policy DRA). GLA provides methods for a Diameter node to query binding information stored in the pSBR-B. The query can be by either IMSI or MSISDN.

GLA processes Diameter Requests and generates Diameter Answers. It does not route Diameter Requests to other Diameter nodes. A Diameter Peer Node can be a Gateway Query Client (GQC). GLA allows DSR to be a Gateway Query Server (GQS)

GLA provides the following capabilities:

- Ability to configure GLA exceptions
- Ability to configure GLA system options
- Ability to configure GLA alarm thresholds

## Manual Organization

This manual is organized into the following chapters:

- *Introduction* contains general information about the Gateway Location Application (GLA) documentation, the organization of this document, and how to get technical assistance.
- *The Gateway Location Application* describes the topology, architecture, components, and functions of the GLA.
- *Gateway Location Application Configuration* describes configuration of GLA application components.

## Scope and Audience

This document is intended for anyone responsible for configuring and using the EAGLE XG DSR Gateway Location Application functionality. Users of this manual must have a working knowledge of telecommunications and network installations.

## Documentation Admonishments

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

**Table 1: Admonishments**

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

## Related Publications

The Diameter Signaling Router (DSR) documentation set includes the following publications, which provide information for the configuration and use of DSR and related applications.

*Getting Started* includes a product overview, system architecture, and functions. It also explains the DSR GUI features including user interface elements, main menu options, supported browsers, and common user interface widgets.

*Feature Notice* describes new features in the current release, provides the hardware baseline for this release, and explains how to find customer documentation on the Oracle Customer Support Site.

*Roadmap to Hardware Documentation* provides links to access manufacturer online documentation for hardware related to the DSR.

*Operation, Administration, and Maintenance (OAM) Guide* provides information on system-level configuration and administration tasks for the advanced functions of the DSR, both for initial setup and maintenance.

*Communication Agent User's Guide* explains how to use the Communication Agent GUI pages to configure Remote Servers, Connection Groups, and Routed Servers, and to maintain configured connections.

*Diameter User's Guide* explains how to use the Diameter GUI pages to manage the configuration and maintenance of Diameter Configuration components, including Local and Peer Nodes, Connections, Configuration Sets, Peer Routing Rules, Application Route Tables, System Options, and DNS options; describes the functions of Diameter Message Copy; and describes DSR capacity and congestion controls.

*Diameter Mediation User's Guide* describes the functions of Diameter Mediation, and explains how to use the Diameter Mediation GUI pages (nested inside the Diameter GUI folder) to configure and test Rule Templates, how to use the Formatting Value Wizard, and how to configure Rule Sets.

*IP Front End (IPFE) User's Guide* explains how to the use the IPFE GUI pages to configure IPFE to distribute IPv4 and IPv6 connections from multiple clients to multiple nodes.

*Range-Based Address Resolution (RBAR) User's Guide* explains how to use the RBAR GUI pages to configure RBAR to route Diameter end-to-end transactions based on Diameter Application ID, Command Code, Routing Entity Type, and Routing Entity address ranges and individual addresses.

*Full-Address Based Resolution (FABR) User's Guide* explains how to use the FABR GUI pages to configure FABR to resolve designated Diameter server addresses based on Diameter Application ID, Command Code, Routing Entity Type, and Routing Entity addresses.

*Charging Proxy Application (CPA) and Offline Charging Solution User's Guide* describes the Offline Charging Solution and explains how to use the CPA GUI pages to set System Options for CPA, configure the CPA's Message Copy capability, and configure the Session Binding Repository for CPA.

*Policy DRA User's Guide* describes the topology and functions of the Policy Diameter Routing Agent (Policy DRA) DSR Application and the Policy Session Binding Repository, and explains how to use the GUI pages to configure Policy DRA.

*Gateway Location Application (GLA) User's Guide* describes the functions of retrieving subscriber data stored in Policy Session Binding Repository (pSBR) provided by Policy DRA and explains how to use the GUI pages to configure GLA.

*DSR Alarms, KPIs, and Measurements Reference* provides detailed descriptions of alarms, events, Key Performance Indicators (KPIs), and measurements; indicates actions to take to resolve an alarm, event, or unusual Diameter measurement value; and explains how to generate reports containing current alarm, event, KPI, and measurement information.

*DSR Administration Guide* describes DSR architecture, functions, configuration, and tools and utilities (IPsec, Import/Export, DIH, and database backups); and provides references to other publications for more detailed information.

# Customer Care Center

Oracle's Tekelec Customer Care Center is your initial point of contact for all product support needs. A representative takes your call or email, creates a Customer Service Request (CSR) and directs your requests to the 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.

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.

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

**Related - Global**

Email (All Regions): support@tekelec.com

- **USA and Canada**

  Phone:

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

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

  TAC Regional Support Office Hours:

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

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

  Phone:

  +1-919-460-2150

  TAC Regional Support Office Hours (except Brazil):

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

  - **Argentina**

    Phone:

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

  - **Brazil**

    Phone:

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

    TAC Regional Support Office Hours:

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

  - **Chile**

    Phone:

    1230-020-555-5468

  - **Colombia**

    Phone:

    01-800-912-0537

  - **Dominican Republic**

    Phone:

1-888-367-8552

- **Mexico**

  Phone:

  001-888-367-8552

- **Peru**

  Phone:

  0800-53-087

- **Puerto Rico**

  Phone:

  1-888-367-8552

- **Venezuela**

  Phone:

  0800-176-6497

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

  Regional Office Hours:

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

  - **Signaling**

    Phone:

    +44 1784 467 804 (within UK)

  - **Software Solutions**

    Phone:

    +33 3 89 33 54 00

- **Asia**

  - **India**

    Phone:

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

    TAC Regional Support Office Hours:

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

  - **Singapore**

    Phone:

    +65 6796 2288

    TAC Regional Support Office Hours:

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

## Emergency Response

In the event of a critical service situation, emergency response is offered by Oracle's Tekelec Customer Care Center 24 hours a day, 7 days a week. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle's Tekelec Customer Care Center.

## Locate Product Documentation on the Customer Support Site

Oracle customer documentation is available on the web at the Oracle Technology Network (OTN) site, *http://docs.oracle.com*. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at *www.adobe.com*.

1. Log into the Oracle Customer Support site at *http://docs.oracle.com*.
2. Under **Applications**, click the link for **Communications**.
   The **Oracle Communications Documentation** window opens with Tekelec shown near the top.
3. Click **Oracle Communications Documentation for Tekelec Products**.
4. Navigate to your Product and then the Release Number, and click the **View** link (the **Download** link will retrieve the entire documentation set).
5. To download a file to your location, right-click the PDF link and select **Save Target As**.

# Chapter

# 2

# The Gateway Location Application

**Topics:**

* *Gateway Location Application (GLA)*
  *Description.....14*

The Gateway Location Application (GLA) is a
feature of the Diameter Signaling Router (DSR)
product. GLA runs as a DSR Application, to provide
a Diameter interface to subscriber data stored in the
DSR's Policy Session Binding Repository (pSBR).

# Gateway Location Application (GLA) Description

Gateway Location Application (GLA) is a DSR Application that retrieves subscriber data stored in Policy Session Binding Repository (pSBR) provided by Policy DRA. The GLA is deployed and must be in the same Resource Domain as DA-MPs activated with Policy DRA. No additional Resource Domain configuration is needed specifically for GLA in the DSR GUI.

After a DA-MP is activated with the GLA, it receives a Request (Get Gateway Request (GGR)) generated by the Gateway Query Client (GQC), then decodes subscriber information (IMSI or MSISDN), then queries the pSBR (via ComAgent within the Gateway Query Server (GQS) or DSR). The GLA generates an Answer (Get Gateway Answer (GGA)) with subscriber information that includes the number of bindings for the subscriber, and the following information is included for each session:

- Access Point name
- PCEF FQDN
- Creation timestamp

The GLA is dependent on Policy DRA to populate data in pSBR and thus GLA will use Activation/Deactivation rules in the following conditions:

- The GLA is activated using the same mechanism as Policy DRA. It will be activated at the NOAM, and activation is performed so that it activates all SOAMs under a common NOAM.
- GLA cannot be activated unless Policy DRA is activated and PCRF-Pooling has been enabled.
- Policy DRA cannot be deactivated if GLA is activated.

To simplify deployment of GLA, it is piggybacked on Policy-DRA's configuration of DA-MPs within its Resource Domain and configuration of ComAgent connections between DA-MPs and pSBRs.

If PCRF pooling is enabled with GLA activated, Policy DRA stores all information required by GLA.

## GLA GUI Conventions

The GLA GUI uses the following conventions (this is not an all-inclusive list):

- The breadcrumb displays at the top of the GUI page reflects your position in the menu tree.
- Context sensitive online help is available via the help icon in the upper right side of the GUI page.
- Action buttons are available at the bottom of the GUI page.
- Edit and delete actions will be validated.
- Successful edit and delete actions generate a confirmation message.
- The items that are displayed on the GUI page differ from SOAM and NOAM views.
- The workspace grid is displayed in ascending order by the first field in the grid.
- All columns in the managed object View screen can be sorted by column headers.
- The column headers on all of the GLA view screens are sorted in ascending order by default.
- You can select only one row at a time in the work area grid of the managed object View screen, unless otherwise specified.
- **Edit** and **Delete** are not active until you select a row.
- **Apply** applies any updates and remains on the same GUI page. **OK** applies and updates and returns to the pervious GUI page.
- **OK**, **Apply**, and **Cancel** are enabled by default on all Insert and Edit screens where they appear.

## GLA Functions

The GLA application performs the following major functions:

- Provides a Diameter interface to subscriber data stored in the DSR's Policy Session Binding Repository (pSBR)
- Provides methods for a Diameter node to query binding information stored in the pSBR-B
- Processes Diameter Requests and generates Diameter Answers

## ComAgent Connectivity for GLA

GLA works with DA-MPs that require ComAgent connectivity to every pSBR-B server in a Policy Binding Resource Domain.

GLA does not configure its own ComAgent connections, but relies on the ComAgent connectivity setup already provided by Policy DRA. When a DA-MP initializes with GLA active, the DA-MP automatically creates ComAgent connections to each pSBR-B.

## Ingress Message Rate Alarming

GLA generates alarms based on the ingress message rate. The message processing rates required to generate an alarm are set by the user while configuring GLA, and should be significantly lower than a standard DA-MP's ingress message rate under any DA-MP profile.

The Ingress Message Rate Alarm is a notification that higher than 'expected' rates of traffic are being processed by the DSR Application.

Alarm trigger points differ based on whether the GLA is deployed as the sole DSR Application on a DA-MP or combined with Policy DRA on the same DA-MP. To satisfy the deployment variables, the Ingress Message Rate has the following settings:

| Field | Default | Configurable Range | Rules |
|---|---|---|---|
| Maximum | DA-MP Max Ingress Message Rate | N/A | Not configurable. This value is provided by the DA-MP Profile |
| CL 1 Abatement / Onset (% of Maximum) | 50 / 60 | 1-99 | CL1 Onset > CL1 Abatement |
| CL 2 Abatement / Onset (% of Maximum) | 70 / 80 | 1-99 | CL2 Abatement > CL1 Onset<br><br>CL2 Onset > CL2 Abatement |
| CL 3 Abatement / Onset (% of Maximum) | 90 / 95 | 1-99 | CL3 Abatement > CL2 Onset<br><br>CL3 Onset > CL3 Abatement |

## GLA Operational Status

The operational status determines when DRL delivers a request to GLA (for example, when GLA is the Available status) and when DRL uses the Unavailability Action for requests (for example, when GLA is in the Unavailable status).

GLA's Operational Status is dependent on the following items:

- Admin State
- GLA Congestion Level
- pSBR-B SubResource Availability
- Previous Operational Status

When the GLA initializes with the Admin State set to 'Disabled', the Operational Status is set to Unavailable. When the Admin State changes from 'Enabled' to 'Disabled', the Operational Status is transitioned to Unavailable.

When the GLA initializes with the Admin State set to 'Enabled', or if the Admin State is changed from 'Disabled' to 'Enabled', the system begins to monitor resources to determine if it can change its Operational Status.

Once GLA moves into the Available state, the system attempts to answer as many queries as possible and remains available as long as any of the pSBR-B SubResources are also available.

**Chapter**

# 3

# Gateway Location Application Configuration

**Topics:**

The **GLA > Configuration** GUI pages for GLA components provide fields for entering the information needed to manage Gateway Location Application configuration in the DSR.

# GLA Configuration Overview

The **GLA > Configuration** GUI pages for Gateway Location Application components provide fields for entering the information needed to manage GLA configuration in the DSR.

Before configuring information in GLA the following characteristics need to be met:

- Since GLA retrieves subscriber information stored in pSBR-B by Policy DRA, Policy DRA must be active for data to be retrieved.
- GLA is activated at the NOAM, and also activates all SOAMs under a common NOAM.
- GLA cannot be active unless Policy DRA is active and PCRF-Pooling is enabled.

The GLA > Configuration GUI pages allow you to configure:

- Exceptions - direct the actions that are taken when specific requests cannot be processed correctly by the system
- System Options - determines actions taken when GLA is unavailable, as well as how the Realm and Fully Qualified Domain Name are applied to the answer message
- Alarm Settings - set alarm thresholds

# GLA Exceptions

GLA allows the configuration of exceptions to manage object attributes for error handling. This enables the configuration of error answers, which provide information on the result code, vendor ID, and the appropriate error message for each condition.

The following exception types are supported:

- Decode Error
- Unknown Application ID
- Unknown Command Code
- IMSI and MSISDN Present
- IMSI and MSISDN Absent
- pSBR-B Query Failure
- pSBR-B Query Timeout
- Resource Exhausted
- Unable to Process

## Configure GLA Exceptions elements

This table describes the elements for configuring GLA error exceptions:

**Table 2: Configure GLA Exception Elements**

| Element | Description | Data Input Notes |
|---|---|---|
| Action | The action to be taken when encountering the specific error. | Format: Radio buttons<br><br>Range:<br><br>• Discard - Request is discarded and no answer is sent<br>• Answer with Result Code - a Diameter Answer message with the Result-Code AVP is sent to Request's Origin-Host.<br>• Answer with Experimental Result Code - Diameter Answer message with an Experimental-Result AVP is sent to Request's Origin-Host Answer with Experimental Result Code |
| Result Code | The value displayed in the message if the Action is Answer with Result Code or Answer with Experimental Result Code.<br><br>Select a Result Code from the listing provided or enter a specific code. | Format: Pulldown list<br><br>Range: 1000-5999 |
| Vendor ID | The vendor ID displayed in the Experimental-Result pair if the Action is Answer with Experimental Result Code. | Format: Text box<br><br>Range: 1 - 4294967295 |
| Error String | The text string appended to the Error-Message AVP. | Format: Text box<br><br>Range: 0 to 64 characters |

## Configuring GLA Exceptions

Use this task to configure exceptions for GLA. Exceptions direct the actions that are taken when specific requests cannot be processed correctly by the system.

The steps below apply to any exception code listed on the GLA Exceptions page. All individual exception codes can be updated independently using these steps.

1. Select **GLA** > **Configuration** > **Exceptions**.

    The **GLA > Configuration > Exceptions** page appears with a list of configured exception attributes.

    The fields are described in *Configure GLA Exceptions elements*.

2. Select an Action from the available options. Valid options are:

- Discard - the request is discarded and no answer is sent
- Answer with Result Code - an answer message with the Result Code AVP is sent to the request originator
- Answer with Experimental Result Code - an answer message with an Experimental Result Code AVP is sent to the request originator

3. Enter a Result Code or select one from the listing. If Discard is selected for the Action, this field is grayed out. If the Action is other than Discard, the result code is sent with the exception answer.

4. Enter a Vendor ID. This field is activated only if you selected Answer with Experimental Result Code for the Action. This value will be sent with the experimental/result pairing.

5. Enter an Error String to be appended to the error/message pairing sent with the answer message.

6. Click:

- **Apply** to save the Exception changes and refresh the page to show the changes.
- **Cancel** to discard the changes and refresh the page.

If **Apply** is clicked and any of the following conditions exist, an error message appears:

- Any fields contain a value that contains invalid characters or is out of the allowed range.
- Any required field is empty (not entered).
- A **Result Code** value is not set when **Answer With Result Code** or **Answer With Experimental Result Code** is selected.
- An **Vendor ID** value is not set when **Answer With Experimental Result Code** is selected.

# GLA System Options

GLA allows the configuration of system options. Setting options allows you to determine actions taken when GLA is unavailable, as well as how the Realm and Fully Qualified Domain Name are applied to the answer message.

The system options set include:

- Realm
- Fully Qualified Domain Name
- Application Unavailable Action
- Application Unavailable Route List
- Application Unavailable Result-Code
- Application Unavailable Error Message
- Application Unavailable Vendor-Id

## Configure GLA System Options elements

This table describes the elements for configuring GLA system options:

**Table 3: Configure GLA System Options Elements**

| Element | Description | Data Input Notes |
|---|---|---|
| Realm | A list of alphanumeric labels (a label is 1-63 characters, and may contain letters, digits, dashes and underscore) separated by dots (.). A label must start with a letter, digit or underscore and must end with a letter or digit.<br><br>This value is placed in the Origin-Realm AVP of the Answer message generated by GLA.<br><br>A Fully Qualified Domain Name is required to configure the Realm. | Format: Alphanumeric (A-Z, a-z, 0-9), dash (-) and underscore (_) characters. Not case-sensitive.<br><br>Range: Maximum of 255 characters. |
| Fully Qualified Domain Name | A list of alphanumeric labels (a label is 1-63 characters, and may contain letters, digits, dashes and underscore) separated by dots (.). A label must start with a letter, digit or underscore and must end with a letter or digit.<br><br>This value is placed in the Origin-Realm AVP of the Answer message generated by GLA.<br><br>A Realm is required to configure Fully Qualified Domain Name. | Format: Alphanumeric (A-Z, a-z, 0-9), dash (-) and underscore (_) characters.  Maximum of 255 characters. Not case-sensitive.<br><br>Range: Maximum of 255 characters. |
| Application Unavailable Action | Action to be taken when GLA application is unavailable to process messages. | Format: Radio button<br><br>Range: Valid responses<br><br>• Continue Routing<br>• Default Route<br>• Send Answer with Result-Code pair<br>• Send Answer with Experimental-Result AVP<br>• Discard |
| Application Unavailable Route List | Route List used to route requests when Unavailability Action is 'Default Route' and GLA application is not available. Using a route list bypasses the Peer Routing Rules. | Format: Drop down list<br><br>Range: Available Route Lists |

| Element | Description | Data Input Notes |
|---|---|---|
| Application Unavailable Result-Code | The Result-Code or Experimental-Result-Code value returned in an Answer message when a message is not successfully routed because the GLA application is unavailable.<br><br>If Vendor-Id is configured, this value would be included with the Experimental-Result Code AVP in the Answer message. | Format: Radio Button/Drop down list<br><br>Default: 3002<br><br>Range: 1000 - 5999 |
| Application Unavailable Error Message | The Error-Message AVP value returned in an Answer message when a message is not successfully routed because the GLA application is not unavailable. | Format: Text box<br><br>Default: GLA Unavailable<br><br>Range: 0 to 64 characters |
| Application Unavailable Vendor-Id | The Vendor-Id AVP value returned in an Answer message when a message is not successfully routed because the GLA application is unavailable.<br><br>If Vendor-Id is configured, this value would be included with the Experimental-Result Code AVP in the Answer message. | Format: Text box<br><br>Default: N/A<br><br>Range: 1 to 4294967295 |

## Configuring GLA System Options

Use this task to configure system options for GLA.

1. Select **GLA** > **Configuration** > **System Options**.

   The **GLA > Configuration > System Options** page appears with a list of system attributes.

   The fields are described in *Configure GLA System Options elements* .

2. Enter a Realm (optional). A Fully Qualified Domain Name is required for this value to be configured, and this value becomes part of the origin/realm pairing in the Answer message. If a realm is not configured, DSR uses the local node information for Answers.

3. Enter a Fully Qualified Domain Name (optional). A Realm is required for this value to be configured. If a FQDN is not configured, DSR uses the local node information for Answers.

4. Select an Application Unavailable Action from the available choices. This determines the action to be taken by the system is the application is unavailable. Valid options are:

   - Continue Routing
   - Default Route
   - Send Answer with Result-Code AVP

- Send Answer with Experimental-Result AVP
- Discard

5. Select the Application Unavailable Route List. This option is only available if Default Route is selected as the Unavailable Action, enabling the selected route list to be used when the application is unavailable.

6. Select the Application Unavailable Result-Code. This option is only available if Send Answer with Result-Code AVP or Send Answer with Experimental-Result AVP are selected as the Unavailable Action. This option determines the message returned in an Answer message when the application is unavailable.

7. Select the Application Unavailable Error Message. This option is only available if Send Answer with Result-Code AVP or Send Answer with Experimental-Result AVP are selected as the Unavailable Action. This option determines the error/message pair returned in an Answer message when the application is unavailable.

8. Select the Application Unavailable Vendor ID. This option is only available if Send Answer with Experimental-Result AVP is selected as the Unavailable Action. This option determines the vendor/ID pair returned in an Answer message when the application is unavailable.

9. Click:

- **Apply** to save the System Options changes and refresh the page to show the changes.
- **Cancel** to discard the changes and refresh the page.

If **Apply** is clicked and any of the following conditions exist, an error message appears:

- Any fields contain a value that contains invalid characters or is out of the allowed range.
- Any required field is empty (not entered).
- An **Application Unavailable Route List** value is not set when **Default Route** is selected.
- An **Application Unavailable Result-Code** value is not set when **Send Answer with Result-Code AVP** or **Send Answer with Experimental-Result AVP** is selected.
- An **Application Unavailable Vendor ID** value is not set when **Send Answer with Experimental-Result AVP** is selected.

# GLA Alarm Settings

GLA allows the configuration of alarm thresholds. These thresholds are used to generate notifications concerning the ingress message rates for the application.

Alarm thresholds may be set for the following limits:

- Critical Alarm Clear
- Critical Alarm Threshold
- Major Alarm Clear
- Major Alarm Threshold
- Minor Alarm Clear
- Minor Alarm Threshold

## Configure GLA Alarm Settings elements

This table describes the elements for configuring a GLA Alarm Setting:

**Table 4: Configure GLA Alarm Settings Elements**

| Element | Description | Data Input Notes |
|---------|-------------|------------------|
| Critical Alarm Threshold (Percent) | GLA ingress message rate threshold for this alarm to be raised as a severity Critical. The threshold is expressed as a percentage of the Ingress Message Capacity. | Default: 95<br><br>Range: 1 to 99 |
| Critical Alarm Clear (Percent) | GLA ingress message rate clear for this alarm to be raised as a severity Critical. The threshold is expressed as a percentage of the Ingress Message Capacity. | Default: 90<br><br>Range: 1 to 99 |
| Major Alarm Threshold (Percent) | GLA ingress message rate threshold for this alarm to be raised as a severity Major. The threshold is expressed as a percentage of the Ingress Message Capacity. | Default: 80<br><br>Range: 1 to 99 |
| Major Alarm Clear (Percent) | GLA ingress message rate clear for this alarm to be raised as a severity Major. The threshold is expressed as a percentage of the Ingress Message Capacity. | Default: 70<br><br>Range: 1 to 99 |
| Minor Alarm Threshold (Percent) | GLA ingress message rate threshold for this alarm to be raised as a severity Minor. The threshold is expressed as a percentage of the Ingress Message Capacity. | Default: 60<br><br>Range: 1 to 99 |
| Minor Alarm Clear (Percent) | GLA ingress message rate clear for this alarm to be raised as a severity Minor. The threshold is expressed as a percentage of the Ingress Message Capacity. | Default: 50<br><br>Range: 1 to 99 |

## Configuring GLA Alarm Settings

Use this task to configure alarm settings for GLA.

1. Select **GLA** > **Configuration** > **Alarm Settings**.

The **GLA > Configuration > Alarm Settings** page appears with a list of alarm attribute percentages.

The fields are described in *Configure GLA Alarm Settings elements* .

2. Select a value for the Critical Alarm Threshold percent. This determines the ingress message rate threshold for this alarm to be raised as Critical. The default is 95 percent.

3. Select a value for the Critical Alarm Clear percent. This determines the ingress message rate clear for this alarm to be raised as Critical. The default is 90 percent.

4. Select a value for the Major Alarm Threshold percent. This determines the ingress message rate threshold for this alarm to be raised as Major. The default is 80 percent.

5. Select a value for the Major Alarm Clear percent. This determines the ingress message rate clear for this alarm to be raised as Major. The default is 70 percent.

6. Select a value for the Minor Alarm Threshold percent. This determines the ingress message rate threshold for this alarm to be raised as Minor. The default is 60 percent.

7. Select a value for the Minor Alarm Clear percent. This determines the ingress message rate clear for this alarm to be raised as Minor. The default is 50 percent.

8. Click:

   - **Apply** to save the Alarm Settings changes and refresh the page to show the changes.
   - **Cancel** to discard the changes and refresh the page.

   If **Apply** is clicked and any of the following conditions exist, an error message appears:

   - Any fields contain a value that contains invalid characters or is out of the allowed range.
   - A **Critical Alarm Clear** value is greater than the **Critical Alarm Threshold.**
   - A **Major Alarm Clear** value is greater than the **Major Alarm Threshold.**
   - A **Minor Alarm Clear** value is greater than the **Minor Alarm Threshold.**
   - A **Major Alarm Threshold** value is greater than the **Critical Alarm Clear** or **Critical Alarm Threshold.**
   - A **Minor Alarm Threshold** value is greater than the **Major Alarm Clear** or **Major Alarm Threshold.**

# Post-Configuration Activities

After GLA configuration is complete, the following activities need to be performed to make the GLA application fully operational in the system:

- Enable GLA on the DA-MPs that will be processing traffic.
- Verify that GLA comes into service in the Normal state
- Verify that the Application Routing Table that has GLA rules will be used for traffic arriving from Gateway Query Clients
- Enable any connections that will carry GL traffic and verify they are in-service.

## Enable the GLA

Use this task to enable GLA. For each Active SOAM,

1. Select **Diameter** > **Maintenance** > **Applications**.

The **Diameter > Maintenance > Applications** page appears.

2. Under **DSR Application Name**, select each **GLA** row.

   To select more than one row, press and hold **Ctrl** while you click each row.

3. Click **Enable**.

4. Verify the application status on the page.

   The **Admin State**, **Operational Status**, **Operational Reason**, and **Congestion Level** in each of the selected rows should change respectively to **Enabled**, **Available**, **Normal**, **Normal**.

## ComAgent and PSBR Status Verification

Use the following task to verify ComAgent and PSBR status after configuration is complete.

1. Verify Communication Agent (ComAgent) HA Services Status.
   a) At the Active NOAM, select **Communication Agent** > **Maintenance** > **Connection Status**.
   b) Verify that **Resource Routing Status** is **Available** for all listed **User/Provider** entries.

2. Verify the ComAgent Automatic Connection Status.
   a) At the Active NOAM, select **Communication Agent** > **Maintenance** > **Ha Services Status**
   b) Verify that **Automatic Connection Count** is **X of Y In Service**, where Y >= X and X = Y indicate successful Automatic Connection setup.

3. Verify Policy SBR Status.
   a) At the Active NOAM, select **Policy DRA** > **Maintenance** > **Policy SBR Status**.
   b) Verify that the server **Resource HA Role** is **Active/Standby/Spare** and **Congestion Level** is **Normal** for all Servers in each Server Group in the Binding Region and Mated Site tab entries.

## Verify Application Route Table

Use the following task to verify that the Application Routing Table that includes GLA rules is used for traffic arriving from Gateway Query Clients.

1. At the Active SOAM, select **Diameter** > **Configuration** > **Application Route Tables**.
   The **Diameter > Configuration > Application Route Tables** page appears.

2. Verify that there is an Application Route Table and Rules set up for GLA. If no table and rules exist, refer to the *DSR Administration Guide.*

3. Select GLA from the Application Route Table and select **View/Edit Rules**.
   The Viewing Rules for Application Route Table: GLA page appears.

4. Select the available rules from the table and select **Edit**.
   The Viewing Rules for Application Route Table: GLA page appears.

5. Examine the Application Routing Rules that direct traffic to GLA and verify that the Application-Id is configured as GL (16777321) and the Command-Code is configured as GGR (8388655) for all Application Routing Rules referring to GLA.
   Once all information is verified, select OK or Cancel to navigate away from the Viewing Rules for Application Route Table: GLA page.

## Enable GLA Query Client Connections

Use the following task to enable one or more GLA Query Client connections to Peer Nodes.

1. At the Active SOAM, select **Diameter** > **Maintenance** > **Connections**.
   The **Diameter > Maintenance > Connections** page appears.

2. Select 1 - 20 connections to enable.

   To select multiple connections, press and hold the Ctrl key while you select each connection.

   To select multiple contiguous connections, click the first connection you want, press and hold the Shift key, and select the last connection you want. All the connections between are also selected.

3. Click **Enable**.
   A confirmation box appears.

4. Click **OK**.
   The selected connections are enabled.

   If any of the selected connections no longer exist (they have been deleted by another user), an error message is displayed, but any selected connections that do exist are enabled.

5. Verify Connection status on the page.

   Verify that the **Admin State** of all connections changes to Enabled and the Operational Reason shows Connecting for connections to PCRF nodes and Listening for connections to other nodes (such as policy clients - PCEF, AF, and others). nodes.

   For connections of type Responder Only (Policy Client nodes), the **Operational Status** and **Operational Reason** will be "Unk" if IPFE TSA connections are used.

# Glossary

**C**

ComAgent

Communication Agent

A common infrastructure component delivered as part of a common plug-in, which provides services to enable communication of message between application processes on different servers.

**D**

DA-MP

Diameter Agent Message Processor

A DSR MP (Server Role = MP, Server Group Function = Diameter Signaling Router). A local application such as CPA can optionally be activated on the DA-MP. A computer or blade that is hosting a Diameter Signaling Router Application.

DSR

Diameter Signaling Router

A set of co-located Message Processors which share common Diameter routing tables and are supported by a pair of OAM servers. A DSR Network Element may consist of one or more Diameter nodes.

**G**

GGA

Get-Gateway-Answer A reply to a GGR. It contains session information for the subscriber present in the GGR. GGA includes the bindings for the subscriber such as, Access Point Name, PCEF FQDN and Creation timestamp. The session information is

**G**

aggregated in the GGA based on the PCRF to which is it assigned.

GGR

Get-Gateway-Request A request for information for either an IMSI or an MSISDN. Only one subscriber (IMSI or MSISDN) is allowed to be queried per GGR. The GGR is generated by the GQC.

GQC

Gateway Query Client also known as Diameter Node

GQS

Gateway Query Server also known as DSR

GUI

Graphical User Interface

The term given to that set of items and facilities which provide the user with a graphic means for manipulating screen data rather than being limited to character based commands.

**N**

NOAM

Network Operations, Administration, and Maintenance

**P**

Policy DRA

Policy Diameter Relay Agent. A scalable, geo-diverse DSR application that creates a binding between a subscriber and a PCRF, and routes all policy messages for a given subscriber to the PCRF that currently hosts that subscriber's policy rules. Policy DRA is capable of performing Topology Hiding to hide the PCRF from the Policy Client.

**P**

pSBR                                    Policy SBR

**S**

SOAM                                    System Operations,
                                        Administration, and Maintenance