Oracle® Communications Tekelec Platform

Gateway Location Application (GLA) User's Guide

E76932 Revision 01

March 2017

ORACLE®

Oracle Communications Tekelec Platform Gateway Location Application (GLA) User's Guide

Table of Contents

List of Figures

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.

Revision History

Date	Description
June 2016	Accessibility changes throughout.

Overview

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

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.

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.
- *User Interface Introduction* describes the organization and usage of the application user interface. In it you can find information about how the interface options are organized, how to use widgets and buttons, and how filtering and other page display options work.
- *The Gateway Location Application* describes the topology, architecture, components, and functions of the GLA.
- *Gateway Location Application Configuration* describes configuration of GLA application components.

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: (This icon and text indicate the possibility of *personal injury*.)
	Warning: (This icon and text indicate the possibility of *equipment damage*.)
	Caution: (This icon and text indicate the possibility of *service interruption*.)
	Topple: (This icon and text indicate the possibility of *personal injury* and *equipment damage*.)

Related Specifications

For information about additional publications related to this document, refer to the Oracle Help Center site. See *Locate Product Documentation on the Oracle Help Center Site* for more information on related product publications.

Locate Product Documentation on the Oracle Help Center Site

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*.

1. Access the Oracle Help Center site at *http://docs.oracle.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 will appear 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 appears.

5. 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.

Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training:

http://education.oracle.com/communication

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site:

www.oracle.com/education/contacts

My Oracle Support (MOS)

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

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

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

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

MOS is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at *http://www.oracle.com/us/support/contact/index.html*. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

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

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

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

Chapter 2

User Interface Introduction

Topics:

This section describes the organization and usage of the application's user interface. In it you can find information about how the interface options are organized, how to use widgets and buttons, and how filtering and other page display options work.

User Interface Organization

The user interface is the central point of user interaction within an application. It is a Web-based graphical user interface (GUI) that enables remote user access over the network to an application and its functions.

The core framework presents a common set of Main Menu options that serve various applications. The common Main Menu options are:

- Administration
- Configuration
- Alarms and Events
- Security Log
- Status and Manage
- Measurements
- Help
- Legal Notices
- Logout

Applications build upon this framework to present features and functions. Depending on your application, some or all of the following Main Menu options may appear on the Network Operation, Administration, and Maintenance (NOAM) GUI:

- Communication Agent
- Diameter Common
- Diameter
- UDR (User Data Repository)
- MAP-Diameter IWF
- RADIUS (Remote Authentication Dial-In User Service)
- SBR (Session Binding Repository)
- Policy and Charging
- DCA (DOIC Capabilities Announcement) Framework

The DSR System OAM GUI may present even more Main Menu options as listed below. The end result is a flexible menu structure that changes according to the application needs and features activated.

- Transport Manager
- SS7/Sigtran
- RBAR (Range Based Address Resolution)
- FABR (Full Address Based Resolution)
- GLA (Gateway Location Application)
- MAP-Diameter IWF
- RADIUS
- SBR
- Mediation
- Policy and Charging
- DCA Framework
- IPFE (IP Front End)

Note that the System OAM (SOAM) Main Menu options differ from the Network OAM (NOAM) options. Some Main Menu options are configurable from the NOAM server and view-only from the SOAM (SOAM) server. This remains true for other applications.

User Interface Elements

Table 2: User Interface Elements describes elements of the user interface.

Table 2: User Interface Elements

Element	Location	Function
Identification Banner	Top bar across the web page	The left side of the banner provides the following information: • Displays the company name, • product name and version, and • the alarm panel. The right side of the banner: • Allows you to pause any software updates. • Links to the online help for all software. • Shows the user name of the currently logged-in user. • Provides a link to log out of the GUI.
Main Menu	Left side of screen, under banners	A tree-structured menu of all operations that can be performed through the user interface. The plus character (+) indicates a menu item contains subfolders. • To display submenu items, click the plus character, the folder, or anywhere on the same line. • To select a menu item that does not have submenu items, click on the menu item text or its associated symbol.
Work Area	Right side of panel under status	Consists of three sections: Page Title Area, Page Control Area (optional), and Page Area. • Page Title Area: Occupies the top of the work area. It displays the title of the current page being displayed, date and time, and includes a link to context-sensitive help. • Page Control Area: Located below the Page Title Area, this area shows controls for the Page Area (this area is optional). When available as an option, filter controls display in this area. The Page Control Area contains the optional layout element toolbar, which displays different elements depending on which GUI page is selected. For more information, see *Optional Layout Element Toolbar*. • Page Area: Occupies the bottom of the work area. This area is used for all types of operations. It displays all options, status, data, file, and query screens. Information

Element	Location	Function
		or error messages are displayed in a message box at the top of this section. A horizontal and/or vertical scroll bar is provided when the displayed information exceeds the page area of the screen. When a user first logs in, this area displays the application user interface page. The page displays a user-defined welcome message. To customize the message, see *Customizing the Login Message*.
Session Banner	Across the bottom of the web page	The left side of the banner provides the following session information: • The name of the machine to which the user is connected, and whether the user is connected via the VIP or directly to the machine. • The HA state of the machine to which the user is connected. • The role of the machine to which the user is connected. The right side of the banner shows the alarm panel.

Main Menu Options

Table 3: Main Menu Options describes all main menu user interface options.

Note: The menu options can differ according to the permissions assigned to a user's log-in account. For example, the Administration menu options do not appear on the screen of a user who does not have administrative privileges.

Note: Some menu items are configurable only on the Network OAM and view-only on the System OAM; and some menu options are configurable only on the System OAM.

Note: Some features do not appear in the main menu until the features are activated.

Table 3: Main Menu Options

Menu Item	Function
Administration	The Administration menu allows the user to: • General Options. Configure options such as password history and expiration, login message, welcome message, and the number of failed login attempts before an account is disabled • Set up and manage user accounts • Configure group permissions • View session information • Manage sign-on certificates • Authorize IP addresses to access the user interface • Configure SFTP user information • View the software versions report • Upgrade management including backup and reporting

Menu Item	Function
	• Authenticate LDAP servers • Configure SNMP trapping services • Configure an export server • Configure DNS elements
Configuration	On the NOAM, allows the user to configure: • Network Elements • Network Devices • Network Routes • Services • Servers • Server Groups • Resource Domains • Places • Place Associations • Interface and Port DSCP
Alarms and Events	Allows the user to view: • Active alarms and events • Alarm and event history • Trap log
Security Log	Allows the user to view, export, and generate reports from security log history.
Status and Manage	Allows the user to monitor the individual and collective status of Network Elements, Servers, HA functions, Databases, KPIs, system Processes, and Tasks. The user can perform actions required for server maintenance, database management, data, and ISO file management.
Measurements	Allows the user to view and export measurement data.
Transport Manager (optional)	On the SOAM, allows the user to configure adjacent nodes, configuration sets, or transports. A maintenance option allows the user to perform enable, disable, and block actions on the transport entries. This option only appears with the DSR application.
Communication Agent (optional)	Allows the user to configure Remote Servers, Connection Groups, and Routed Services. The user can perform actions to enable, disable, and block connections. Also allows the user to monitor the status of Connections, Routed Services, and HA Services.
SS7/Sigtran (optional)	On the SOAM, allows the user to configure various users, groups, remote signaling points, links, and other items associated with SS7/Sigtran; perform maintenance and troubleshooting activities; and provides a command line interface for bulk loading SS7 configuration data. This option only appears with the DSR application.

Menu Item	Function
Diameter Common (optional)	Allows the user to view or configure: • Dashboard, configure on the NOAM; view on both OAMs • Network Identifiers on the SOAM - MCC Ranges • Network Identifiers on the NOAM - MCCMNC and MCCMNC Mapping • MPs (on the SOAM) - editable Profile parameters and Profile Assignments The DSR Bulk Import and Export functions are available on both OAMs for the data configured on that OAM.
Diameter (optional)	Allows the user to configure, modify, and monitor Diameter routing: • On the NOAMP, Diameter Topology Hiding and Egress Throttle List configuration • On the SOAM, Diameter Configuration, Maintenance, Reports, Troubleshooting with IDIH, AVP Dictionary, and Diameter Mediation configuration
UDR (User Data Repository) (optional)	Allows the user to add, edit, store, and manage subscriber and pool data. The user can also monitor the import, export, and subscribing client status. This option only appears with the UDR application.
RBAR (Range-Based Address Resolution) (optional)	Allows the user to configure the following Range-Based Address Resolution (RBAR) settings: • Applications • Exceptions • Destinations • Address Tables • Addresses • Address Resolutions • System Options This is accessible from the SOAM only. This option only appears with the DSR application.
FABR (Full Address Based Resolution) (optional)	Allows the user to configure the following Full Address Based Resolution (FABR) settings: • Applications • Exceptions • Default Destinations • Address Resolutions • System Options This is accessible from the SOAM only. This option is only available with the DSR application.
Gateway Location Application (optional)	On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for: • Exceptions

Menu Item	Function
	• Options GLA can deploy with Policy DRA (in the same DA-MP or a separate DA-MP). This option only appears with the DSR application.
MAP-Diameter Interworking (optional)	On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for the DM-IWF DSR Application: • DM-IWF Options • Diameter Exception On the NOAMP, allows the user to perform configuration tasks, edit options, and view elements for the MD-IWF SS7 Application: • MD-IWF Options • Diameter Realm • Diameter Identity GTA • GTA Range to PC • MAP Exception • CCNDC Mapping This option only appears with the DSR application.
RADIUS (Remote Authentication Dial-In User Service) (optional)	Allows the user to perform configuration tasks, edit system options, and view elements for: • Network Options • Message Authenticator Configuration Sets • Shared Secret Configuration Sets • Ingress Status Server Configuration Sets • Message Conversion Configuration Sets • NAS Node This option only appears with the DSR application.

SBR (Session Binding Repository) (optional)	Allows the user to perform configuration tasks, edit system options, and view elements for:
	• SBR Databases
	• SBR Database Resizing Plans
	• SBR Data Migration Plans
	• Database Options
	Additionally, on the NOAMP, users are allowed to perform maintenance tasks, edit options, and view elements for:
	• Maintenance
	  • SBR Database Status
	  • SBR Status
	  • SBR Database Reconfiguration Status
	This option only appears with the DSR application.

Menu Item	Function
Mediation	Allows the user to make routable decisions to end the reply, drop the message, or set the destination realm.

Policy and Charging (optional)	On the NOAMP, allows the user to perform configuration tasks, edit options, and view elements for:
	• General Options
	• Access Point Names
	• Policy DRA
	  • PCRF Pools
	  • PCRF Sub-Pool Selection Rules
	  • Network-Wide Options
	• Online Charging DRA
	  • OCS Session State
	  • Realms
	  • Network-Wide Options
	• Alarm Settings
	• Congestion Options
	Additionally on the NOAMP, users are allowed to perform maintenance tasks, edit options, and view elements for:
	• Maintenance
	  • SBR Database Status
	  • SBR Status
	  • SBR Database Reconfiguration Status
	  • Policy Database Query
	On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for:
	• General Options
	• Access Point Names
	• Policy DRA
	  • PCRFs
	  • Binding Key Priority
	  • PCRF Pools
	  • PCRF Pool to PRT Mapping
	  • PCRF Sub-Pool Selection Rules
	  • Policy Clients
	  • Suspect Binding Removal Rules
	  • Site Options
	• Online Charging DRA
	  • OCSs
	  • CTFs

Menu Item	Function
	• OCS Session State • Realms • Error Codes • Alarm Settings • Congestion Options This option only appears with the DSR application.
DCA Framework (optional)	Allows the user to perform configuration tasks, edit system options, and view elements for DCA applications: • Custom MEALs (Measurements, Events, Alarms, and Logs) • General Options • Trial MPs assignment • Application Control • System Options
IPFE (optional)	Allows the user to configure IP Front End (IPFE) options and IP List TSAs. This is accessible from the SOAM server only. This option only appears with the DSR application.
Help	Launches the Help system for the user interface
Legal Notices	Product Disclaimers and Notices
Logout	Allows the user to log out of the user interface

Missing Main Menu options

Permissions determine which Main Menu options are visible to users. Permissions are defined through the **Group Administration** page. The default group, **admin**, is permitted access to all GUI options and functionality. Additionally, members of the **admin** group set permissions for other users.

Main Menu options vary according to the group permissions assigned to a user's account. Depending on your user permissions, some menu options may be missing from the Main Menu. For example, Administration menu options do not appear on your screen if you do not have administrative permissions. For more information about user permissions, see *Group Administration* in the OAM section of the online help, or contact your system administrator.

Common Graphical User Interface Widgets

Common controls allow you to easily navigate through the system. The location of the controls remains static for all pages that use the controls. For example, after you become familiar with the location of the display filter, you no longer need to search for the control on subsequent pages because the location is static.

Supported Browsers

This application supports the use of Microsoft® Internet Explorer 8.0, 9.0, or 10.0.

is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the *Oracle Software Web Browser Support Policy* for details

System Login Page

Access to the user interface begins at the System Login page. The System Login page allows users to log in with a username and password and provides the option of changing the password upon login. The System Login page also features a date and time stamp reflecting the time the page was last refreshed. Additionally, a customizable login message appears just below the **Log In** button.

The user interface is accessed via HTTPS, a secure form of the HTTP protocol. When accessing a server for the first time, HTTPS examines a web certificate to verify the identity of the server. The configuration of the user interface uses a self-signed web certificate to verify the identity of the server. When the server is first accessed, the supported browser warns the user that the server is using a self-signed certificate. The browser requests confirmation that the server can be trusted. The user is required to confirm the browser request to gain access.

Customizing the Login Message

Before logging in, the **System Login** page appears. You can create a login message that appears just below the **Log In** button on the **System Login** page.

Figure 1: Oracle System Login

1. From the **Main Menu**, click **Administration** > **General Options**.
   The **General Options Administration** page appears.
2. Locate **LoginMessage** in the **Variable** column.
3. Enter the login message text in the **Value** column.
4. Click **OK** or **Apply** to submit the information.
   A status message appears at the top of the Configuration Administration page to inform you if the operation was successful.

The next time you log in to the user interface, the login message text displays.

Accessing the DSR Graphical User Interface

In DSR, some configuration is done at the NOAM server, while some is done at the SOAM server. Because of this, you need to access the DSR graphical user interface (GUI) from two servers. Certificate Management (Single Sign-On) can be configured to simplify accessing the DSR GUI on the NOAM and the SOAM.

For information on configuring Single Sign-On certificates, see **OAM** > **Administration** > **Access Control** > **Certificate Management** in the DSR online help.

After the certificates have been configured, you can log into the DSR GUI on any NOAM or SOAM, and then access the DSR GUI on other servers (NOAM or other SOAMs) without having to re-enter your login credentials.

1. In the browser URL field, enter the fully qualified hostname of the NOAM server, for example https://dsr-no.yourcompany.com.

   When using Single Sign-On, you cannot use the IP address of the server.
2. When prompted by the browser, confirm that the server can be trusted.

   The System Login page appears.
3. Enter the Username and Password for your account.

   The DSR GUI for the NOAM appears.
4. To access the DSR GUI for the SOAM, open another browser window and enter the fully qualified hostname of the SOAM.

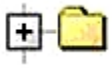
   The DSR GUI for the SOAM appears

You can toggle between the DSR GUI on the NOAM and the DSR GUI on the SOAM as you perform configuration tasks.

Main Menu Icons

This table describes the icons used in the **Main Menu**.

Table 4: Main Menu Icons

Icon	Name	Description
	Folder	Contains a group of operations. If the folder is expanded by clicking the plus (+) sign, all available operations and sub-folders are displayed. Clicking the minus (-) collapses the folder.
	Config File	Contains operations in an Options page.
	File with Magnifying Glass	Contains operations in a Status View page.
	File	Contains operations in a Data View page.
	Multiple Files	Contains operations in a File View page.
	File with Question Mark	Contains operations in a Query page.

Icon	Name	Description
	User	Contains operations related to users.
	Group	Contains operations related to groups.
	Task	Contains operations related to Tasks
	Help	Launches the Online Help.
	Logout	Logs the user out of the user interface.

Work Area Displays

In the user interface, tables, forms, tabbed pages, and reports are the most common formats.

Note: Screen shots are provided for reference only and may not exactly match a specific application's GUI.

Tables

Paginated tables describe the total number of records being displayed at the beginning and end of the table. They provide optional pagination with **First | Prev | Next | Last** links at both the beginning and end of this table type. Paginated tables also contain action links on the beginning and end of each row. For more information on action links and other page controls, see *Page Controls*.

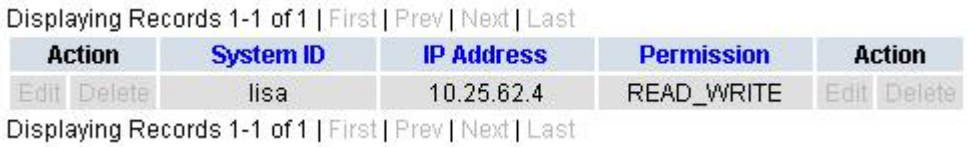
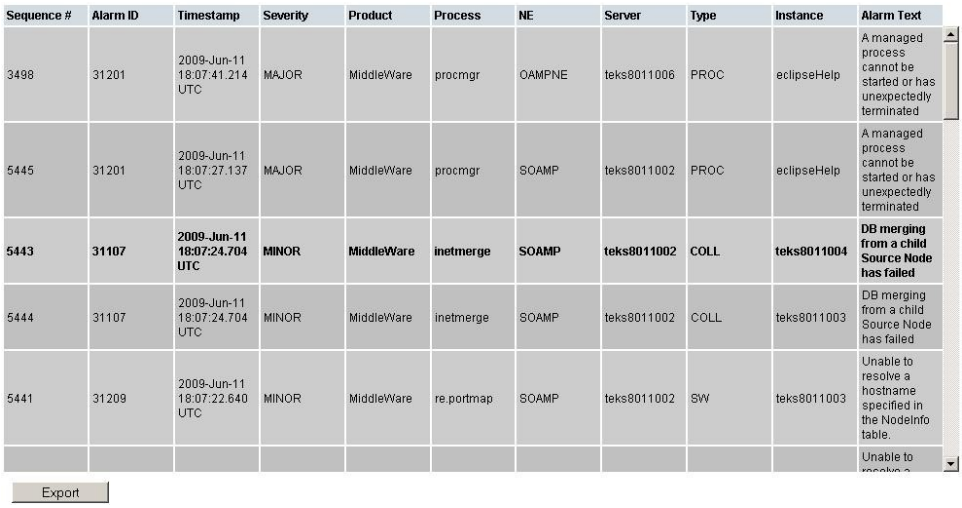


Figure 2: Paginated Table

Scrollable tables display all of the records on a single page. The scroll bar, located on the right side of the table, allows you to view all records in the table. Scrollable tables also provide action buttons that operate on selected rows. For more information on buttons and other page controls, see *Page Controls*.



Sequence #	Alarm ID	Timestamp	Severity	Product	Process	NE	Server	Type	Instance	Alarm Text
3498	31201	2009-Jun-11 18:07:41.214 UTC	MAJOR	MiddleWare	procmgr	OAMPNE	teks8011006	PROC	eclipseHelp	A managed process cannot be started or has unexpectedly terminated
5445	31201	2009-Jun-11 18:07:27.137 UTC	MAJOR	MiddleWare	procmgr	SOAMP	teks8011002	PROC	eclipseHelp	A managed process cannot be started or has unexpectedly terminated
5443	**31107**	**2009-Jun-11 18:07:24.704 UTC**	**MINOR**	**MiddleWare**	**inetmerge**	**SOAMP**	**teks8011002**	**COLL**	**teks8011004**	**DB merging from a child Source Node has failed**
5444	31107	2009-Jun-11 18:07:24.704 UTC	MINOR	MiddleWare	inetmerge	SOAMP	teks8011002	COLL	teks8011003	DB merging from a child Source Node has failed
5441	31209	2009-Jun-11 18:07:22.640 UTC	MINOR	MiddleWare	re.portmap	SOAMP	teks8011002	SW	teks8011003	Unable to resolve a hostname specified in the NodeInfo table.
										Unable to

Export

Figure 3: Scrollable Table

Note: Multiple rows can be selected in a scrollable table. Add rows one at a time using CTRL-click. Add a span of rows using SHIFT-click.

Forms

Forms are pages on which data can be entered. Forms are typically used for configuration. Forms contain fields and may also contain a combination of pulldown lists, buttons, and links.

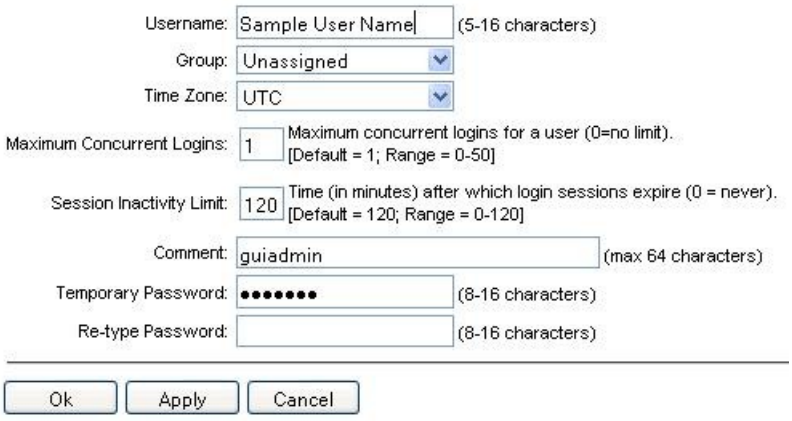
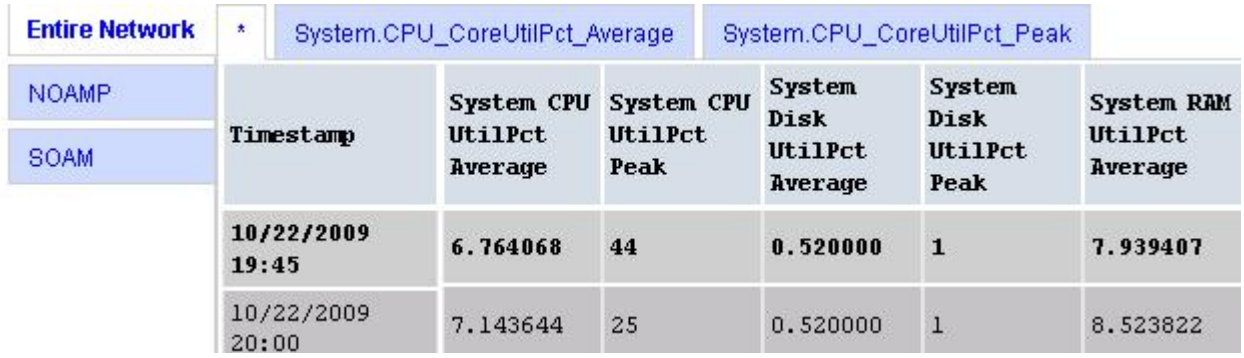


Figure 4: Form Page

Tabbed pages

Tabbed pages provide collections of data in selectable tabs. Click on a tab to see the relevant data on that tab. Tabbed pages also group Retrieve, Add, Update, and Delete options on one page. Click on the relevant tab for the task you want to perform and the appropriate fields populate on the page. Retrieve is always the default for tabbed pages.



Timestamp	System CPU UtilPct Average	System CPU UtilPct Peak	System Disk UtilPct Average	System Disk UtilPct Peak	System RAM UtilPct Average
10/22/2009 19:45	6.764068	44	0.520000	1	7.939407
10/22/2009 20:00	7.143644	25	0.520000	1	8.523822

Figure 5: Tabbed Pages

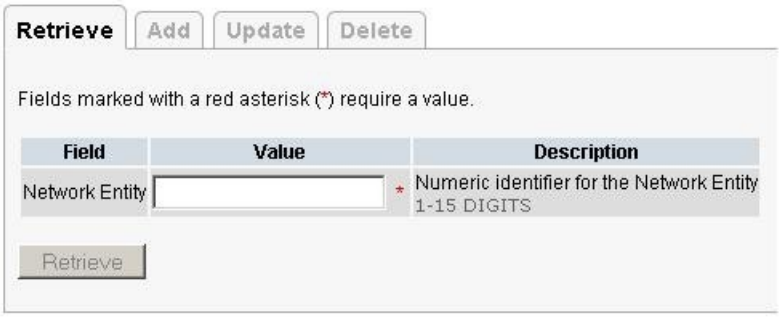


Figure 6: Tabbed Pages

Reports

Reports provide a formatted display of information. Reports are generated from data tables by clicking **Report**. Reports can be viewed directly on the user interface, or they can be printed. Reports can also be saved to a text file.

```
================================================================================

User Account Usage Report

================================================================================

Report Generated: Fri Jun 19 19:30:55 2009 UTC
From: Unknown Network OAM&P on host teks5001701
Report Version: 1.0
User: guiadmin

--------------------------------------------------------------------------------

Username          Date of Last Login    Days Since Last Login   Account Status
----------------  --------------------  ----------------------  ---------------
guiadmin          2009-06-19 19:00:17   0                       enabled

--------------------------------------------------------------------------------

End of User Account Usage Report

================================================================================
```

Figure 7: Report Output

Customizing the Splash Page Welcome Message

When you first log in to the user interface, the splash page appears. Located in the center of the main work area is a customizable welcome message. Use this procedure to create a message suitable for your needs.

1. From the **Main Menu**, click **Administration** > **General Options**.
2. Locate **Welcome Message** in the **Variable** column.
3. Enter the desired welcome message text in the **Value** column.
4. Click **OK** to save the change or **Cancel** to undo the change and return the field to the previously saved value.
   A status message appears at the top of the page to inform you if the operation was successful.

The next time you log in to the user interface, the new welcome message text is displayed.

Column Headers (Sorting)

You can sort a table by a column by clicking the column header. However, sorting is not necessarily available on every column. Sorting does not affect filtering.

When you click the header of a column that the table can be sorted by, an indicator appears in the column header showing the direction of the sort. See *Figure 8: Sorting a Table by Column Header*. Clicking the column header again reverses the direction of the sort.

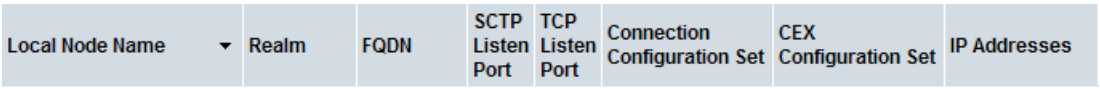


Figure 8: Sorting a Table by Column Header

Page Controls

User interface pages contain controls, such as buttons and links, that perform specified functions. The functions are described by the text of the links and buttons.

Note: Disabled buttons are grayed out. Buttons that are irrelevant to the selection or current system state, or which represent unauthorized actions as defined in **Group Administration**, are disabled. For example, **Delete** is disabled for users without Global Data Delete permission. Buttons are also disabled if, for example, multiple servers are selected for an action that can only be performed on a single server at a time.

Table 5: Example Action Buttons contains examples of Action buttons.

Table 5: Example Action Buttons

Action Button	Function
Insert	Inserts data into a table.
Edit	Edits data within a table.
Delete	Deletes data from table.

Action Button	Function
Change	Changes the status of a managed object.

Some Action buttons take you to another page.

Submit buttons, described in *Table 6: Submit Buttons*, are used to submit information to the server. The buttons are located in the page area and accompanied by a table in which you can enter information. The Submit buttons, except for **Cancel**, are disabled until you enter some data or select a value for all mandatory fields.

Table 6: Submit Buttons

Submit Button	Function
OK	Submits the information to the server, and if successful, returns to the View page for that table.
Apply	Submits the information to the server, and if successful, remains on the current page so that you can enter additional data.
Cancel	Returns to the View page for the table without submitting any information to the server.

Clear Field Control

The clear field control allows you to clear the value from a pulldown list. The clear field control is available only on some pulldown fields.

Click the **X** next to a pulldown list to clear the field.

Figure 9: Clear Field Control X

Optional Layout Element Toolbar

The optional layout element toolbar appears in the Page Control Area of the GUI.

Figure 10: Optional Layout Element Toolbar

The toolbar displays different elements depending on which GUI page is selected. The elements of the toolbar that can appear include:

- Filter – Allows you to filter data in a table.
- Errors – Displays errors associated with the work area.
- Info – Displays information messages associated with the work area.
- Status – Displays short status updates associated with the main work area.
- Warning – Displays warnings associated with the work area.

Notifications

Some messages require immediate attention, such as errors and status items. When new errors occur, the Errors element opens automatically with information about the error. Similarly, when new status items are added, the Status element opens. If you close an automatically opened element, the element stays closed until a new, unacknowledged item is added.

Figure 11: Automatic Error Notification

Note: Viewing and closing an error does not clear the Errors element. If you reopen the Errors element, previously viewed errors are still in the list.

When new messages are added to Warning or Info, the styling of the element changes to indicate new messages are available. The styling of the Task element changes when a task changes state (such as, a task begins or ends).

Opening an Element in the Toolbar

Use this procedure to open an element in the optional layout element toolbar.

1. Click the text of the element or the triangle icon to open an element.
   The selected element opens and overlays the work area.
2. Click **X** to close the element display.

Filters

Filters are part of the optional layout element toolbar and appear throughout the GUI in the Page Control Area. For more information about optional layout element toolbar functionality, see *Optional Layout Element Toolbar*.

Filters allow you to limit the data presented in a table and can specify multiple filter criteria. By default, table rows appear unfiltered. Three types of filters are supported, however, not all filtering options are available on every page. The types of filters supported include:

- Network Element – When enabled, the Network Element filter limits the data viewed to a single Network Element.

  Note: Once enabled, the Network Element filter affect all pages that list or display data relating to the Network Element.

- Collection Interval – When enabled, the collection interval filter limits the data to entries collected in a specified time range.
- Display Filter – The display filter limits the data viewed to data matching the specified criteria.

Once a field is selected, it cannot be selected again. All specified criteria must be met in order for a row to be displayed.

The style or format of filters may vary depending on which GUI pages the filters are displayed. Regardless of appearance, filters of the same type function the same.

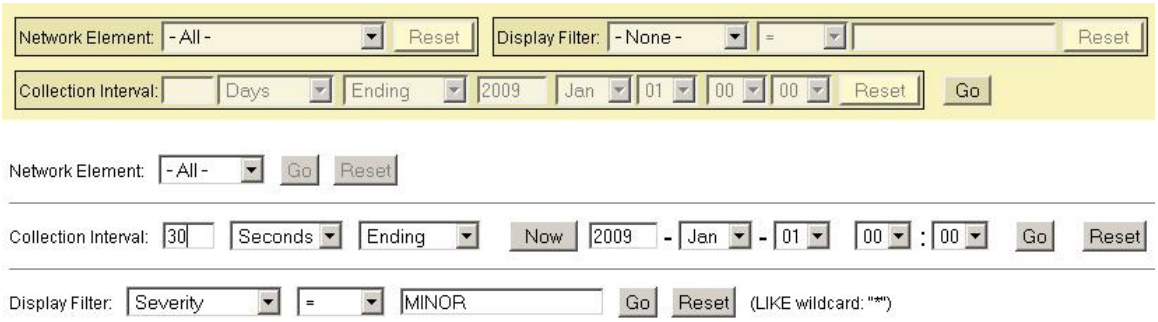


Figure 12: Examples of Filter Styles

Filter Control Elements

This table describes filter control elements of the user interface.

Table 7: Filter Control Elements

Operator	Description
=	Displays an exact match.
!=	Displays all records that do not match the specified filter parameter value.
>	Displays all records with a parameter value that is greater than the specified value.
>=	Displays all records with a parameter value that is greater than or equal to the specified value.
<	Displays all records with a parameter value that is less than the specified value.
<=	Displays all records with a parameter value that is less than or equal to the specified value.
Like	Enables you to use an asterisk (*) as a wildcard as part of the filter parameter value.
Is Null	Displays all records that have a value of **Is Null** in the specified field.

Note: Not all filterable fields support all operators. Only the supported operators are available for you to select.

Filtering on the Network Element

The global Network Element filter is a special filter that is enabled on a per-user basis. The global Network Element filter allows a user to limit the data viewed to a single Network Element. Once enabled, the global Network Element filter affects all sub-screens that display data related to Network Elements. This filtering option may not be available on all pages.

1. Click **Filter** in the optional layout element toolbar.
2. Select a Network Element from the **Network Element** pulldown menu.
3. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

Records are displayed according to the specified criteria.

Filtering on Collection Interval

The Collection Interval filter allows a user to limit the data viewed to a specified time interval. This filtering option may not be available on all pages.

1. Click **Filter** in the optional layout element toolbar.
2. Enter a duration for the **Collection Interval** filter.

   The duration must be a numeric value.
3. Select a unit of time from the pulldown menu.

   The unit of time can be seconds, minutes, hours, or days.
4. Select **Beginning** or **Ending** from the pulldown menu.
5. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

Records are displayed according to the specified criteria.

Filtering Using the Display Filter

Use this procedure to perform a filtering operation. This procedure assumes you have a data table displayed on your screen. This process is the same for all data tables. However, all filtering operations are not available for all tables.

1. Click **Filter** in the optional layout element toolbar.
2. Select a field name from the **Display Filter** pulldown menu.

   This selection specifies the field in the table that you want to filter on. The default is **None**, which indicates that you want all available data displayed.

   The selected field name displays in the **Display Filter** field.
3. Select an operator from the operation selector pulldown menu.
4. Enter a value in the value field.

   This value specifies the data that you want to filter on. For example, if you specify Filter=Severity with the equals (=) operator and a value of MINOR, the table would show only records where Severity=MINOR.
5. For data tables that support compound filtering, click **Add** to add another filter condition. Then repeat steps 2 through 4.

   Multiple filter conditions are joined by an AND operator.
6. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

Records are displayed according to the specified criteria.

Pause Updates

Some pages refresh automatically. Updates to these pages can be paused by selecting the **Pause updates** checkbox. Uncheck the **Pause updates** checkbox to resume automatic updates. The **Pause updates** checkbox is available only on some pages.

Max Records Per Page Controls

Max Records Per Page is used to control the maximum number of records displayed in the page area. If a page uses pagination, the value of Max Records Per Page is used. Use this procedure to change the Max Records Per Page.

1. From the **Main Menu**, click **Administration** > **General Options**.
2. Change the value of the **MaxRecordsPerPage** variable.

   Note: Maximum Records Per Page has a range of values from 10 to 100 records. The default value is 20.

3. Click **OK** or **Apply**.

   OK saves the change and returns to the previous page.

   Apply saves the change and remains on the same page.

The maximum number of records displayed is changed.

Chapter 3

The Gateway Location Application

Topics:

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

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 (SBR). Subscriber data concerning binding and session information is populated in the SBR-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 SBR-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

Gateway Location Application (GLA) Description

Gateway Location Application (GLA) is a DSR Application that retrieves subscriber data stored in Policy Session Binding Repository (SBR) 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), decodes subscriber information (IMSI or MSISDN), and queries the SBR (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 SBR and thus GLA uses Activation/Deactivation rules in the following conditions:

- The GLA is activated using the same mechanism as Policy DRA. It is 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 SBRs.

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 are 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 (SBR)
- Provides methods for a Diameter node to query binding information stored in the SBR-B
- Processes Diameter Requests and generates Diameter Answers

ComAgent Connectivity for GLA

GLA works with DA-MPs that require ComAgent connectivity to every SBR-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 SBR-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:

Table 8: Ingress Message Rate 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 CL2 Onset > CL2 Abatement
CL 3 Abatement/Onset (% of Maximum)	90/95	1-99	CL3 Abatement > CL2 Onset 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
- SBR-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 SBR-B SubResources are also available.

Chapter 4

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 SBR-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
- SBR-B Query Failure
- SBR-B Query Timeout
- Resource Exhausted
- Unable to Process

Configure GLA Exceptions elements

This table describes the elements for configuring GLA error exceptions:

Table 9: Configure GLA Exception Elements

Element	Description	Data Input Notes
Action	The action to be taken when encountering the specific error.	Format: Radio buttons Range: • Discard - Request is discarded and no answer is sent • Answer with Result Code - a Diameter Answer message with the Result-Code AVP is sent to Request's Origin-Host. • 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. Select a Result Code from the listing provided or enter a specific code.	Format: Pulldown list 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 Range: 1 - 4294967295
Error String	The text string appended to the Error-Message AVP.	Format: Text box 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 is 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 10: 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 (.).	Format: Alphanumeric (A-Z, a-z, 0-9), dash (-) and underscore (_) characters. Not case-sensitive.

Element	Description	Data Input Notes
	A label must start with a letter, digit or underscore and must end with a letter or digit. This value is placed in the Origin-Realm AVP of the Answer message generated by GLA. A Fully Qualified Domain Name is required to configure the Realm.	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. This value is placed in the Origin-Realm AVP of the Answer message generated by GLA. 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. Range: Maximum of 255 characters.
Application Unavailable Action	Action to be taken when GLA application is unavailable to process messages.	Format: Radio button Range: Valid responses • Continue Routing • Default Route • Send Answer with Result-Code pair • Send Answer with Experimental-Result AVP • 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 Range: Available Route Lists
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. 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 Default: 3002 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 Default: GLA Unavailable Range: 0 to 64 characters

Element	Description	Data Input Notes
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. If Vendor-ID is configured, this value would be included with the Experimental-Result Code AVP in the Answer message.	Format: Text box Default: N/A 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 11: 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 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 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 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 Range: 1 to 99

Element	Description	Data Input Notes
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 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 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 process traffic
- Verify GLA comes into service in the Normal state
- Verify the Application Routing Table that has GLA rules is used for traffic arriving from Gateway Query Clients
- Enable any connections that 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**.
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 SBR Status Verification

Use the following task to verify ComAgent and SBR 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 **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 **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 the **Resource HA Role** server 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 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**.
2. Verify 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**.
4. Select the available rules from the table and select **Edit**.
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**.

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**.
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).

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

Bulk Import and Export

The *Diameter Common User's Guide* describes the use and operation of Bulk Import and Export functions:

- **Help** > **Diameter Common** > **Bulk Import**
- **Help** > **Diameter Common** > **Bulk Export**

The Bulk Import and Export functions can be used to export Diameter, IPFE, and Application configuration data in CSV files to a location outside the system, and to import the files (usually edited) into the system where the Import function is executed.

Bulk Import

The Bulk Import operations use configuration data in ASCII Comma-Separated Values (CSV) files (.csv), to insert new data into, update existing data in, or delete existing data from the configuration data in the system.

Note: Some configuration data can be imported only with the Update operation, and other data can be imported with Insert and Delete operations but not Update. Refer to the *Diameter Common User's Guide* or the **Diameter Common** > **Import** Help for valid Import operations.

Import CSV files can be created by using a Bulk Export operation, or can be manually created using a text editor.

Note: The format of each Import CSV file record must be compatible with the configuration data in the release used to import the file. Across different release versions, column counts may not be compatible, and the import fails.

Files that are created using the Bulk Export operation can be exported either to the local Status & Manage File Management Directory (**Status & Manage** > **Files** page), or to the local Export Server Directory.

CSV files that are in the local File Management area can be used for Bulk Import operations on the local system.

Files can be created manually using a text editor; the files must be uploaded to the File Management area of the local system before they can be used for Import operations on the local system.

Multiple Import operations can be performed:

- Insert new configuration data records that do not currently exist in the system
- Update existing configuration data in the system
- Delete existing configuration data from the system

Each Import operation creates a log file. If errors occur, a Failures CSV file is created that appears in the File Management area. Failures files can be downloaded, edited to correct the errors, and imported to successfully process the records that failed. Failures files that are unchanged for more than 14 days and log files that are older than 14 days are automatically deleted from the File Management area.

Bulk Export

The Bulk Export operation creates ASCII Comma-Separated Values (CSV) files (.csv) containing Diameter, IPFE, and Application configuration data. Exported configuration data can be edited and used with the Bulk Import operations to change the configuration data in the local system without the use of GUI pages. The exported files can be transferred to and used to configure another system.

Each exported CSV file contains one or more records for the configuration data that was selected for the Export operation. The selected configuration data can be exported once immediately, or exports can be scheduled to periodically occur automatically at configured times.

Configuration data can be exported in one Export operation:

- All exportable configuration data in the system
- All exportable configuration data from the selected Application, IPFE, or Diameter (each component's data is in a separate file)
- Exportable configuration data from a selected configuration component for the selected Application, IPFE, or Diameter

Exported files can be written to the File Management Directory in the local File Management area (**Status & Manage** > **Files** page), or to the Export Server Directory for transfer to a configured remote Export server.

CSV files that are in the local File Management area can be used for Bulk Import operations on the local system.

If the export has any failures or is unsuccessful, the results of the export operation are logged to a log file with the same name as the exported file but with a .log extension. Successful export operations are not logged.

Glossary

A

AVP	Attribute-Value Pair The Diameter protocol consists of a header followed by one or more attribute-value pairs (AVPs). An AVP includes a header and is used to encapsulate protocol-specific data (for example, routing information) as well as authentication, authorization or accounting information.

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.
CTF	Charging Trigger Function

D

DA-MP	Diameter Agent Message Processor A DSR MP (Server Role = MP, Server Group Function = Diameter Signaling Router). A local application that can optionally be activated on the DA-MP. A computer or blade that is hosting a Diameter Signaling Router Application.
DCA	DOIC Capabilities Announcement

D

DNS	Domain Name Services Domain Name System A system for converting Internet host and domain names into IP addresses.
DRA	Destination Routing Address Diameter Relay Agent Diameter Routing Agent A functional element in a 3G or 4G (such as LTE) wireless network that provides real-time routing capabilities to ensure that messages are routed among the correct elements in a network.
DSCP	Differentiated Service Code Point Differentiated Services Code Point Provides a framework and building blocks to enable deployment of scalable service discrimination in the internet. The differentiated services are realized by mapping the code point contained in a field in the IP packet header to a particular forwarding treatment or per-hop behavior (PHB). Differentiated services or DiffServ is a computer networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying and managing network traffic and providing quality of service (QoS) on modern IP networks.

G

GGA	Get-Gateway-Answer A reply to a GGR. It contains session information for the

G

	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 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.
GLA	Gateway Location Application 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 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.
GQC	Gateway Query Client also known as Diameter Node
GQS	Gateway Query Server also known as DSR
GTA	Global Title Address
GUI	Graphical User Interface

G

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

H

HA

High Availability

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

I

IDIH

Integrated Diameter Intelligence Hub

IP

Intelligent Peripheral

Internet Protocol - IP specifies the format of packets, also called datagrams, and the addressing scheme. The network layer for the TCP/IP protocol suite widely used on Ethernet networks, defined in STD 5, RFC 791. IP is a connectionless, best-effort packet switching protocol. It provides packet routing, fragmentation and re-assembly through the data link layer.

K

KPI

Key Performance Indicator

L

LDAP

Lightweight Directory Access Protocol

A protocol for providing and receiving directory information in a TCP/IP network.

M

MAP	Mated Application Part Mobile Application Part An application part in SS7 signaling for mobile communications systems.
MD-IWF	MAP-Diameter Interworking SS7 Application, which translates MAP messages into Diameter messages
MEAL	Measurements, Events, Alarms, and Logs
MP	Measurement Platform Message Processor - The role of the Message Processor is to provide the application messaging protocol interfaces and processing. However, these servers also have OAM components. All Message Processors replicate from their Signaling OAM's database and generate faults to a Fault Management System.

N

NAS	Network Access Server A single point of access or gateway to a remote resource. NAS systems are usually associated with AAA servers.
NOAM	Network Operations, Administration, and Maintenance
NOAMP	Network Operations, Administration, Maintenance, and Provisioning

O

O

OCS	Online Charging System A system allowing a Communications Service Provider to charge customers in real time based on service usage.

P

PCRF	Policy and Charging Rules Function The ability to dynamically control access, services, network capacity, and charges in a network. Maintains rules regarding a subscriber's use of network resources. Responds to CCR and AAR messages. Periodically sends RAR messages. All policy sessions for a given subscriber, originating anywhere in the network, must be processed by the same PCRF. In the Policy Management system, PCRF is located in the MPE device. Software node designated in real-time to determine policy rules in a multimedia network.
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.
PRT	Peer Route Table or Peer Routing Table

R

R

RADIUS	Remote Authentication Dial-In User Service A client/server protocol and associated software that enables remote access servers to communicate with a central server to authorize their access to the requested service. The MPE device functions with RADIUS servers to authenticate messages received from remote gateways. See also Diameter.

S

SBR	Subsystem Backup Routing
SFTP	SSH File Transfer Protocol (sometimes also called Secure File Transfer Protocol) A client-server protocol that allows a user on one computer to transfer files to and from another computer over a TCP/IP network over any reliable data stream. It is typically used over typically used with version two of the SSH protocol.
SNMP	Simple Network Management Protocol. An industry-wide standard protocol used for network management. The SNMP agent maintains data variables that represent aspects of the network. These variables are called managed objects and are stored in a management information base (MIB). The SNMP protocol arranges managed objects into groups.

S

SOAM	System Operations, Administration, and Maintenance
SS7	Signaling System #7 A communications protocol that allows signaling points in a network to send messages to each other so that voice and data connections can be set up between these signaling points. These messages are sent over its own network and not over the revenue producing voice and data paths. The EAGLE is an STP, which is a device that routes these messages through the network.

T

TSA	Target Set Address An externally routable IP address that the IPFE presents to application clients. The IPFE distributes traffic sent to a target set address across a set of application servers.

U

UDR	User Data Repository A logical entity containing user data. User-Data-Request A user-identity and service indication sent by a Diameter client to a Diameter server in order to request user data.