Diameter Signaling Router

Full Address Based Resolution (FABR) User's Guide

Release 8.2

E89003

January 2018

ORACLE

Diameter Signaling Router Full Address Based Resolution (FABR) User's Guide, Release 8.2

E89003

Contents

1 Introduction

Revision History 1-1
Overview 1-1
Scope and Audience 1-1
Manual Organization 1-1
Documentation Admonishments 1-2
Locate Product Documentation on the Oracle Help Center Site 1-2
Customer Training 1-3
My Oracle Support (MOS) 1-3
Emergency Response 1-3

2 User Interface Introduction

User Interface Organization 2-1
- User Interface Elements 2-2
- Main Menu Options 2-5

Missing Main Menu options 2-11
Common Graphical User Interface Widgets 2-11
- Supported Browsers 2-11
- System Login Page 2-12
- Main Menu Icons 2-13
- Work Area Displays 2-14
- Customizing the Splash Page Welcome Message 2-17
- Column Headers (Sorting) 2-17
- Page Controls 2-17
- Clear Field Control 2-18
- Optional Layout Element Toolbar 2-18
- Filters 2-20
- Pause Updates 2-22
- Max Records Per Page Controls 2-22

3 Full Address Based Resolution

Full Address Based Resolution overview 3-1

Application Chaining 3-2
Request Message Validation 3-4
Multiple DSR Application Invocation Prevention 3-11
Transaction Metadata Recording for Integrated DIH (IDIH) 3-12

4 Configuration of FABR

Pre-Configuration Activities 4-1
Verifying Server status 4-1
Diameter Common Configuration for FABR 4-1
Diameter Configuration for FABR 4-2
SDS DP Remote Server Configuration 4-3
FABR Configuration 4-4
Applications configuration 4-4
Exceptions configuration 4-6
Default Destinations configuration 4-8
Address Resolutions configuration 4-10
System Options configuration 4-14
Post-Configuration Activities 4-18
Enabling the FABR Application 4-18
Status Verification 4-18
Bulk Import and Export 4-18

5 Maintenance of FABR

Overview 5-1
FABR Administrative State and Operational Status 5-1

List of Figures

2-1 Oracle System Login 2-12
2-2 Paginated Table 2-15
2-3 Scrollable Table 2-15
2-4 Form Page 2-16
2-5 Tabbed Pages 2-16
2-6 Tabbed Pages 2-16
2-7 Report Output 2-17
2-8 Sorting a Table by Column Header 2-17
2-9 Clear Field Control X 2-18
2-10 Optional Layout Element Toolbar 2-19
2-11 Automatic Error Notification 2-19
2-12 Examples of Filter Styles 2-20

List of Tables

1-1 Admonishments 1-2
2-1 User Interface Elements 2-3
2-2 Main Menu Options 2-6
2-3 Main Menu Icons 2-13
2-4 Example Action Buttons 2-18
2-5 Submit Buttons 2-18
2-6 Filter Control Elements 2-20
3-1 FABR Supported AVPs 3-6
3-2 Combinations of User Identity Types and Associated AVPs 3-7
3-3 Relation between Configured User Identity Types and Data Formats 3-8
3-4 DSR Application-Invoked AVP 3-11
3-5 FABR Metadata-Generating Events 3-12
4-1 Applications Configuration Elements 4-5
4-2 Exceptions Configuration Elements 4-6
4-3 Destinations Configuration Elements 4-8
4-4 Address Resolutions Configuration Elements 4-10
4-5 System Options Elements 4-14
5-1 FABR Admin State and Operational Status 5-2

1

Introduction

The *Full Address Based Resolution (FABR) User's Guide* and Help provides an overview of the functions and procedures to configure FABR. The contents of this chapter include sections on the scope, audience, and organization of the documentation, and how to contact Oracle for assistance.

Revision History

Date	Description
June 2016	Accessibility changes throughout.
January 2017	Updates in the FABR supported AVPs table.

Overview

The Full Address Based Resolution (FABR) documentation provides information about functions, and how to use the GUI and the following procedures to configure the application:

- Applications
- Exceptions
- Default Destinations
- Address Resolutions
- System Options

Scope and Audience

The FABR documentation is intended for anyone responsible for configuring and using the Full Address Based Resolution application. Users of this manual must have a working knowledge of telecommunications, of network installations, and of the product that is using the FABR functions.

Manual Organization

This manual is organized into the following chapters:

- Introduction contains general information about the FABR help documentation, the organization of this manual, 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.

- Full Address Based Resolution describes the function of the FABR application.
- Configuration of FABR describes how to configure the FABR application, including Applications, Exceptions, Default Destinations, Address Resolutions, and System Options.
- Maintenance of FABR describes maintenance functions and information that can be used with the FABR application.

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 1-1 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.)

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 displays. Most products covered by these documentation sets display under the headings "Network Session Delivery and Control Infrastructure" and "Platforms."
4. Click on your Product and then the Release Number.

   A list of the entire documentation set for the selected product and release displays.

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 at http://education.oracle.com/communication

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site at 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 are connected to a live agent who can assist you with MOS registration and opening a support ticket.

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

Emergency Response

In the event of a critical service situation, emergency response is offered by the 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.

2

User Interface Introduction

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 display 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 2-1 describes elements of the user interface.

Table 2-1 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.

Table 2-1 (Cont.) User Interface Elements

Element	Location	Function
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 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

Table 2-1 (Cont.) User Interface Elements

Element	Location	Function
		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 2-2 describes all main menu user interface options.

Note: The menu options can differ according to the permissions assigned to a user's login account. For example, the Administration menu options do not display 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 display in the main menu until the features are activated.

Table 2-2 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 • 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, **KPI**s, 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.

Table 2-2 (Cont.) Main Menu Options

Menu Item	Function
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 displays 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 displays with the DSR application.
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 displays with the UDR application.

Table 2-2 (Cont.) Main Menu Options

Menu Item	Function
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 displays 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 • Options GLA can deploy with Policy DRA (in the same DA-MP or a separate DA-MP). This option only displays 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 displays with the DSR application.

Table 2-2 (Cont.) Main Menu Options

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

Table 2-2 (Cont.) Main Menu Options

Menu Item	Function
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 – **CTF**s – **OCS** Session State – Realms • Error Codes • Alarm Settings • Congestion Options This option only displays with the DSR application.

Table 2-2 (Cont.) Main Menu Options

Menu Item	Function
DCA Framework (optional)	Allows the user to perform configuration tasks, edit system options, and view elements for DCA applications: • Custom **MEAL**s (Measurements, Events, Alarms, and Logs) • General Options • Trial **MP**s assignment • Application Control • System Options
IPFE (optional)	Allows the user to configure IP Front End (IPFE) options and **IP** List **TSA**s. This is accessible from the SOAM server only. This option only displays 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 display 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 displays 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 displays. You can create a login message that displays just below the **Log In** button on the System Login page.

Figure 2-1 Oracle System Login

1. From the **Main Menu**, click **Administration** > **General Options**.
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 displays at the top of the Configuration Administration page to inform you if the operation was successful.

The next time you log into 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 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 displays.

3. Enter the Username and Password for your account.

   The DSR GUI for the NOAM displays.

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 displays.

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 2-3 Main Menu Icons

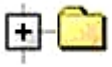
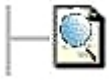
Icon	Name	Description
	Folder	Contains a group of operations. If the folder is expanded by clicking the plus (+) sign, all available operations and sub-folders are displayed. Clicking the minus (-) collapses the folder.

Table 2-3 (Cont.) Main Menu Icons

Icon	Name	Description
	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.
	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.

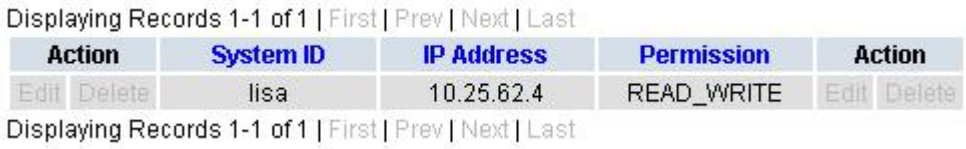
Note: Screen shots are provided for reference only and may not exactly match a specific application's GUI.

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

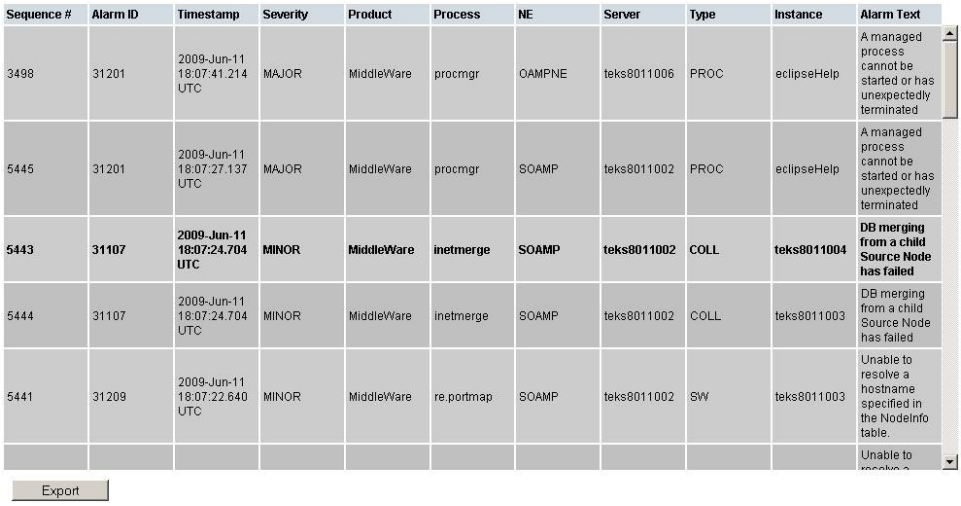
action links on the beginning and end of each row. For more information on action links and other page controls, see Page Controls.

Figure 2-2 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.

Figure 2-3 Scrollable Table

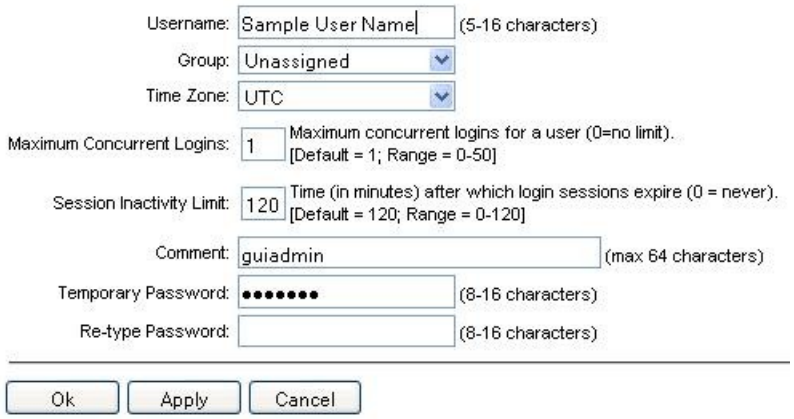


Note: Multiple rows can be selected in a scrollable table. Add rows one at a time using CTRL-click. Add a span of rows using SHIFT-click.

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 lists, buttons, and links.

Figure 2-4 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.

Figure 2-5 Tabbed Pages

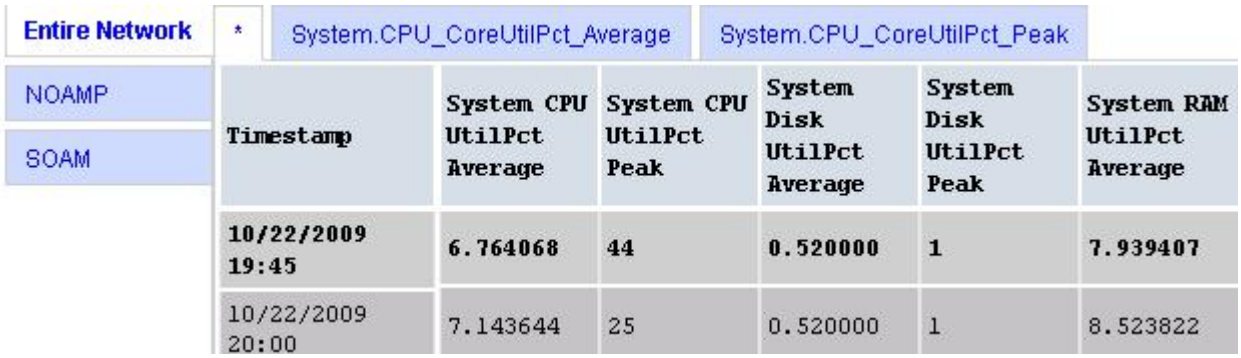
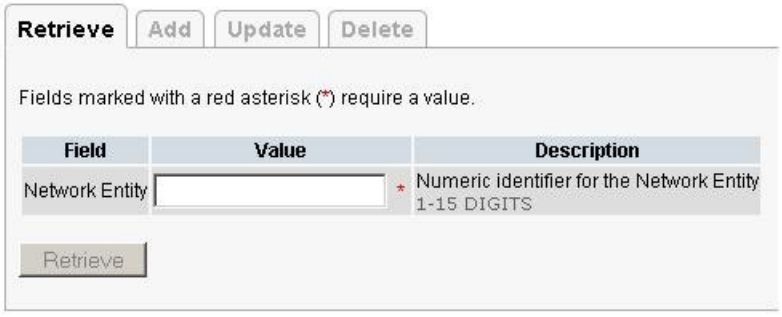


Figure 2-6 Tabbed Pages



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.

Figure 2-7 Report Output

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

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

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

Customizing the Splash Page Welcome Message

When you first log into the user interface, the splash page displays. 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 displays at the top of the page to inform you if the operation was successful.

The next time you log into the user interface, the new welcome message text displays.

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 in a table that can be sorted, an indicator displays in the column header showing the direction of the sort. See Figure 2-8. Clicking the column header again reverses the direction of the sort.

Figure 2-8 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 2-4 contains examples of Action buttons.

Table 2-4 Example Action Buttons

Action Button	Function
Insert	Inserts data into a table.
Edit	Edits data within a table.
Delete	Deletes data from table.
Change	Changes the status of a managed object.

Some Action buttons take you to another page.

Submit buttons, described in Table 2-5, 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 2-5 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 list. The clear field control is available only on some lists.

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

Figure 2-9 Clear Field Control X

Optional Layout Element Toolbar

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

Figure 2-10 Optional Layout Element Toolbar

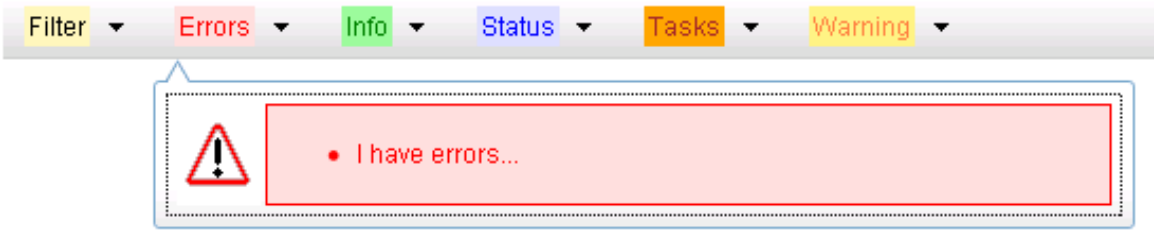
The toolbar displays different elements depending on which GUI page is selected. The elements of the toolbar that can display include:

- 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 2-11 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.

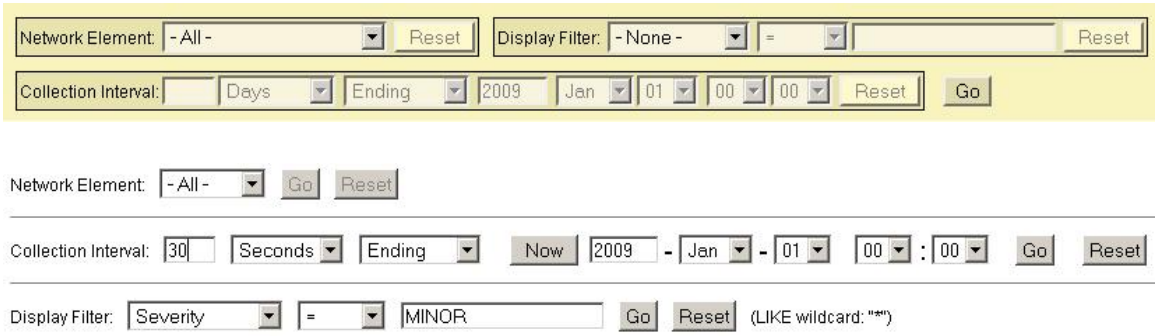
  Note: Once enabled, the Network Element filter affect all pages that list or display data relating to the Network Element.

- 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 2-12 Examples of Filter Styles



Filter Control Elements

This table describes filter control elements of the user interface.

Table 2-6 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.

Table 2-6 (Cont.) Filter Control Elements

Operator	Description
>=	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** list.
3. Click **Go** to filter on the selection or click **Reset** to clear the selection.
4. For data tables that support compound filtering, click **Add** to add another filter condition and repeat steps 2 through 4.

   Multiple filter conditions are joined by an AND operator.

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 list.

   The unit of time can be seconds, minutes, hours, or days.

4. Select **Beginning** or **Ending** from the list.

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 with the Display Filter field. This process is the same for all data tables. However, all filtering operations are not available for all tables.

> **Note:** Display Filter does not support compound filtering. For example, you cannot filter on both severity and a server name. Try to filter on a single filter criteria, such as the server hostname for server-scoped metric cells; or the application name for St- and NE-scoped metric cells. You can also sort by congestion level (descending) to help improve your filter.

1. Click **Filter** in the optional layout element toolbar.

2. Select a field name from the **Display Filter** list.

   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.

3. Select an operator from the operation selector list.

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. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

Records are displayed according to the specified criteria.

> **Note:** PCA was known as PDRA and may still be seen in some filtering.

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.

3

Full Address Based Resolution

This section provides an overview of the functions for the **Full Address Based Resolution** (**FABR**) application.

Full Address Based Resolution overview

Full Address Based Resolution (FABR) is a routing application that enables network operators to resolve the designated Diameter server (IMS HSS, LTE HSS, MTC HSS, PCRF, OCS, OFCS, AAA) addresses based on Diameter Application ID, Command Code, Routing Entity Type, and Routing Entity Addresses, and then routes the Diameter Request to the resolved destination.

The FABR application validates the ingress Diameter Request message, retrieves the Application ID and Command Code from it, and determines the desired Routing Entity Type to decode from the message based on the configuration. The FABR application extracts the Routing Entity Address from user-configured Attribute-Value Pairs (AVPs) in the ingress message and sends the Routing Entity Address, if extracted successfully, to an off-board DP running the Subscriber Database Server (SDS) for destination address resolution.

The resolved Destination address can be any combination of a Realm and Fully Qualified Domain Name (FQDN); Realm-only, FQDN-only, or Realm and FQDN.

FABR replaces the Destination-Host and/or Destination-Realm AVP in the ingress Request message with the corresponding values of the resolved Destination, and forwards the message to the Diameter Relay Agent for egress routing into the network.

A Routing Entity can be any of the following:

- International Mobile Subscriber Identity (IMSI)
- Mobile Subscriber Integrated Services Digital Network (Number) (MSISDN)
- IP Multimedia Private Identity (IMPI)
- IP Multimedia Public Identity (IMPU)
- External Identifier

FABR Functions

FABR provides the following functions:

- Routing based on IMSI/MSISDN Prefix Lookup performs prefix-based lookups after completion of the full address lookup. The prefix and range based lookup are only performed if the full address lookup does not find a match and can be enabled by the operator for a combination of Application-ID, Command-Code, and Routing Entity Type.

Populates the Destination-Host AVP and/or the Destination-Realm AVP based on the resolved destination if a match is found in the prefix database.

Performs the No Address Match Found routing exception handling procedure if there is not a match in the prefix database.

The IMSI/MSISDN Prefix and Range lookup can be enabled or disabled on system wide.

- DP Query Bundling enhances the FABR-to-DP interface by supporting the bundling of multiple queries into a single bundled query stack event when enabled.

  When the DP receives a bundled query, the corresponding bundled response have responses to all the queries that constitute the bundled query.

- Reserved MCC Ranges are reserved for future Mobile Country Code (MCC) ranges and are defined in a system-wide MCC Ranges table. If the MCC digits portion of decoded IMSI digits fall within one of the ranges designated in the MCC Ranges table, the IMSI digits are NOT used for further address resolution. FABR continues decoding the digits using other AVP instances or next Priority AVP (if provisioned), or next Routing Entity (if provisioned).

- Identifying IMSI, MSISDN, and External Identifier address resolution applications like Full Address Based Resolution (FABR) and Range Based Address Resolution (RBAR) need to categorize User Identities (digit strings) decoded from the Diameter Request AVPs as either MSISDN or IMSI to allow looking up the User Identity in the appropriate lookup table.

  If there is no plus sign before the digits, the Routing Entity Type is IMPU, and decoded digits fall within MSISDN and IMSI overlap range. Configured MCC +MNC combinations can be compared to the first 5 or 6 digits of the User Identity. The User Identity is considered as an IMSI and used for IMSI lookup if a match occurs. The User Identity considered as a MSISDN and used for MSISDN lookup if a match does not occur.

  Identifying IMSIs and MSISDNs provides more information about identifying IMSIs and MSISDNs using digit string lengths and MCC+MNC combinations.

- Application Chaining allows FABR and the DM-IWF applications to process the same Diameter Request message by configuring application routing rules.

Application Chaining

Application Chaining is a method for invoking multiple DSR applications in sequence on the same DSR.

To process a Request for two DSR applications executing in sequence, the Application Route Table execution is:

1. When the Request enters the system at the Application Routing Table (ART).
2. When DSR Application 1 sends the Request back to the Diameter Routing Function at the Application Routing Table (ART).
3. When DSR Application 2 sends the Request back to the Diameter Routing Function at the Application Routing Table (ART).

At the Application Routing Table (ART) if there is no matching Application Routing Rule for the Request, the Request routes to Peer Route Table for processing.

- Application Route Table (ART)

  Application Route Tables are used for routing Request messages to DSR applications. An ART contains a prioritized list of user-configurable Application Routing Rules. Each Application Routing Rule associates Request message content with a DSR application.

  An ART is searched, when a received Request message from a Peer Node or a DSR application. Searching an ART when a Request message is received from a DSR application allows the operator to route the ingress Diameter transaction to multiple DSR applications in sequence. The operator can create multiple ARTs to assign an ART to a Request message based upon a set of user-defined criteria.

- Application Routing Rules

  An ART consists of a set of prioritized Application Routing Rules that the Diameter Routing Function searches with the content of a Request message, to determine whether to forward the message to a DSR application for processing.

  One ART is searched each time a Request message received from a Peer Node or a DSR application. This method allows forwarding a Diameter transaction to one or more DSR applications for processing.

  However, the Diameter Routing Function does not allow a DSR application to process a Diameter transaction more than once. The Diameter Routing Function internally keeps track of which DSR applications have already processed the message. When the Diameter Routing Function searches an ART and encounters an Application Routing Rule associated with a DSR application that processed the transaction, the Diameter Routing Function bypasses the Application Routing Rule.

The system default ART is not removable using the configuration GUI. The user can create additional ARTs and then define, through configuration, which ART is searched based on ART precedence selection rules.

Each time a Request message is received from a Peer Node or DSR application, the Diameter Routing Function selects an ART to search based on the following ART precedence selection rules (highest to lowest priority):

1. The ART provided by the DSR application if it exists (applies only when the Request message was received from a DSR application)
2. The ART assigned to the ingress Peer Node from which the Request message was received if it exists
3. The ART assigned to the Diameter Application ID in the Request message header if it exists
4. The default ART

The order of DSR applications which can process an ingress Request message is determined by operator configuration of one or more Application Route Tables.

- Each time the Diameter Routing Function receives a Request message from a Peer Node or DSR application, it searches the Application Route Tables to determine where to forward the message.

- The highest priority Application Routing Rule matched defines where to forward the message.
- If no Application Routing Rule match is found, the Diameter Routing Function begins Relay Agent routing to an upstream Peer Node.

When FABR or RBAR and the Diameter-MAP Interworking (DM-IWF) applications run in the same DA-MP, the same Diameter Request message can be processed by both applications.

For a Diameter-to-MAP Request message received from a Diameter Peer that needs to be processed by FABR followed by DM-IWF, two Application Routing Rules are needed; one for routing the message first to FABR and the second to reroute the message to DM-IWF after FABR processing is complete. In this order:

- After the Request is received from the Peer, the Diameter Routing Function searches the Application Routing Rules for the highest priority-matching rule. If this rule contains the FABR application name, the results route the Request to FABR.
- TheFABR processes the message and returns it to the Diameter Routing Function.
- The Diameter Routing Function searches the Application Routing Rules for the highest priority matching rule (excluding all rules that would result in routing of the Request to FABR again).This rule contains the DM-IWF application name and the results route the Request to DM-IWF.
- DM-IWF processes the message and sends it to an MD-IWF application (SS7-MP).

For a MAP-to-Diameter Request message received by DM-IWF from an MD-IWF application (SS7-MP), which needs processing by FABR after DM-IWF processing, a single Application Routing Rule is needed for routing the message to FABR after DM-IWF processing is completed. In this order:

- DM-IWF processes the message and sends it to the Diameter Routing Function.
- The Diameter Routing Function searches the Application Routing Rule for the highest priority matching rule (excluding all rules that would cause routing of the Request to DM-IWF again). This rule contains the FABR application name and results in the Request being routed to FABR for processing.
- FABR returns the message to the Diameter Routing Function to complete the routing process.

Request Message Validation

The derivation of a user identity address from the ingress diameter request message governed by the rules determined by user identity configuration. The configuration defines the supported application IDs, the supported command codes associated with each application ID, the preferred user identity types to search, and the associated AVPs that contain the user identity addresses.

The FABR application processes the diameter request message based on the configuration to extract the user identity addresses.

The diameter request message sent to FABR validates as followed:

- Determine whether the Application ID in the message header is defined in the configuration.

- If the diameter request message receives a valid (configured) Application ID, validate whether the pair (Application ID and command code) in the message is defined in the configuration.
- If the pair is configured, select the highest priority user identity type associated with the pair in the configuration for user identity address searching.
- Search for a valid user identity address from an AVP in the ingress message based on a prioritized set of AVPs assigned to the triplet (Application ID, command code, and then routing entity type).

If a user identity address cannot be found in searching the configured user identity types and AVPs, the `No Valid Routing Entity Address` routing exception handling procedure invokes.

Routing Exception Handling

When an ingress FABR request message cannot be resolved to a destination, (no address matched, no valid digits decoded, or any other error returns), FABR invokes a routing exception handling procedure based on user-defined configuration.

Routing exception handling procedures result in one of the following configured actions:

- Forward the message unchanged
- Forward the message using a user-defined default destination
- Send an Answer response with a user-defined result-code AVP value
- Send an Answer response with user-defined experimental-code AVP values
- Abandon Request

The routing exceptions types support the following:

- Unknown command code
- No valid routing entity addresses were found
- A valid routing entity address did not resolve to a configured address
- Blacklisted subscriber
- DP congestion
- DP errors

Supported AVPs

FABR supports the AVPs associated with the user identity types as defined in Table 3-1.

Note: There is no support for Service-Information: Subscription-ID-Data (4-Server Private) in FABR and not looked up when retrieving a user identity address.

Table 3-1 FABR Supported AVPs

AVPs	AVP Code	AVP Type	AVP Reference
User-Identity [Public-Identity] [MSISDN]	700	Grouped	Section 6.3.1 of 3GPP 29.329
MSISDN	701	OctetString	Section 6.3.2 of 3GPP 29.329
Public-Identity	601	UTF8String	Section 6.3.2 of 3GPP 29.229
Service-Information [Subscription-ID] […]	873	Grouped	Section 7.2.192 of 3GPP 32.299
Subscription-Id [Subscription-ID-Type [Subscription-ID-Data]	443	Grouped	Section 8.46 of RFC 4006
Subscription-ID-Type	450	Enumerated	Section 8.47 of RFC 4006
Subscription-ID-Data	444	UTF8String	Section 8.47 of RFC 4006
User-Name	1	UTF8String	Section 8.14 of RFC 3588bis
Wildcarded-Public-Identity	634	UTF8String	Section 6.3.35 of 3GPP 29.229
MSISDN	701	OctetString	Section 6.3.2 of 3GPP 29.329
Public Identity	601	UTF8String	Section 6.3.2 of 3GPP 29.229
User-Identifier: [User-Name] [MSISDN]	3102	Grouped	Section 6.4.2 of 3GPP 29.336
User-Name	1	UTF8String	Section 8.14 of RFC 6733
MSISDN	701	OctetString	Section 6.3.2 of 3GPP 29.329
External Identifier		UTF8String	Section 6.3.2 of 3GPP 29.336

Each of the configured user identity types supported in FABR is associated with certain AVPs that contains the user identity type as defined by various diameter application standards. Table 3-2 presents all possible combinations of the user identity types and the associated AVPs.

Table 3-2 Combinations of User Identity Types and Associated AVPs

User Identity Types/AVPs	IMSI	MSISDN	IMPI	IMPU
MSISDN		Applicable		Applicable
User-Identity: MSISDN		Applicable		Applicable
Public-Identity	Applicable	Applicable	Applicable	Applicable
User-Identity: Public-Identity	Applicable	Applicable	Applicable	Applicable
User-Name	Applicable	Applicable	Applicable	Applicable
Subscription-ID-Data (0-E.164)		Applicable		Applicable
Service-Information: Subscription-ID-Data (0-E.164)		Applicable		Applicable
Subscription-ID-Data (1-IMSI)	Applicable		Applicable	
Service-Information: Subscription-ID-Data (1-IMSI)	Applicable		Applicable	
Subscription-ID-Data (2-SIP URI)	Applicable	Applicable	Applicable	Applicable
Service-Information: Subscription-ID-Data (2-SIP URI)	Applicable	Applicable	Applicable	Applicable
Subscription-ID-Data (3-NAI)	Applicable	Applicable	Applicable	Applicable

Table 3-2 (Cont.) Combinations of User Identity Types and Associated AVPs

User Identity Types/AVPs	IMSI	MSISDN	IMPI	IMPU
Service-Information:	Applicable	Applicable	Applicable	Applicable
Subscription-ID-Data (3-NAI)				
Wildcarded-Public-Identity				Applicable
User-Identifier: User-Name	Applicable		Applicable	
User-Identifier: MSISDN		Applicable		Applicable
User-Identifier: External Identifier	Applicable	Applicable		

A user identity type can be associated with one or more data formats that is examined when deriving the user identity address from the associated AVPs. The relation between user identity types and the corresponding data formats to be encountered in the ingress diameter request message are listed in Table 3-3.

Table 3-3 Relation between Configured User Identity Types and Data Formats

Configurable User Identity Types/User Identity Formats in Messages	IMSI	MSISDN	IMPI	IMPU
IMSI Format: ASCII Example: 311480123456789	Applicable		Applicable	
MSISDN Format: ASCII and TBCD Example: 19194605500		Applicable		Applicable
SIP URI with IMSI Format: ASCII	Applicable		Applicable	

Table 3-3 (Cont.) Relation between Configured User Identity Types and Data Formats

Configurable User Identity Types/User Identity Formats in Messages	IMSI	MSISDN	IMPI	IMPU
Examples: sip:123456789012345@nai.epc.mnc456.mcc123.3gppnetwork.org sip:6311150999995555@ims.mnc015.mcc311.3gppnetwork.org sip:311480999995555@my.network.org sip:6311480999995555@my.network.org				
SIP URI with MSISDN Format: ASCII Examples: sip: +1-919-460-5500 @xyz.com;user= phone sip: 311480999995555 @my.network.or g		Applicable		Applicable
SIP URI with NAI Format: ASCII Example: sip: 311480999995555 @mynetwork.or g			Applicable	Applicable
SIP URI with Wildcarded PSI Format: ASCII Example: sip:WP- A_ServiceType-!. *!@att.com				Applicable
TEL URI with MSISDN FORMAT: ASCII Examples: tel:+1-919-460-5500; phone-context=example.com tel:+19258889999 tel:19195551212		Applicable		Applicable

Table 3-3 (Cont.) Relation between Configured User Identity Types and Data Formats

Configurable User Identity Types/User Identity Formats in Messages	IMSI	MSISDN	IMPI	IMPU
NAI with IMSI/ MSISDN Format: ASCII Examples: 123456789012345@xyz.com 123456789012345 311480999995555@ims.mnc480.mcc311.3gppnetwork.org 6311150999995555@xyz.com 6311150999995555@ims.mnc015.mcc311.3gppnetwork.org	Applicable	Applicable	Applicable	Applicable
NAI Format: ASCII Example: handy.manny@xyz.com			Applicable	Applicable

Identifying IMSIs and MSISDNs

In certain Diameter messages over the Cx interface (and possibly over the Sh interface), certain AVPs that typically carry an IMSI sometimes can carry an MSISDN.

Address resolution applications like Full Address Based Resolution (FABR) and Range Based Address Resolution (RBAR) need to categorize user Identities (digit strings) decoded from the diameter request AVPs as either MSISDN or IMSI, to allow looking up the user identity in the appropriate lookup table.

Most of the time, these applications can clearly categorize the decoded user identity based on:

- The configured routing entity type
- The contents of the AVP

  For instance, if the user identity has been decoded from a SIP URI that has a plus sign before the digits (such as sig:+1-919-460-5500@oracle.com), it can be directly categorized as an MSISDN.
- The number of digits in the user identity

In certain cases, none of these methods allow a clear categorization (for example, if the number of digits needs to be used and the received number of digits are applicable to both IMSIs and MSISDNs, and thus leads to an ambiguous determination; or if there is no plus sign before the digits).

If FABR has been configured to decode an IMPU from a user identity (digit string), but cannot determine whether the user identity is an IMSI or an MSISDN based on digit analysis, a tie-breaker is needed to properly categorize the user identity.

If the routing entity type is IMPU, the user identity extracted results in only digits, and the length of the digits in the user identity falls within an overlap digits range of MSISDN and IMSI, the following logic can be used to determine if the user identity is an IMSI or MSISDN.

- FABR extracts the first 5 or 6 digits of the user identity and compares them against a list of configured 5- or 6-digit MCC-MNC combinations.

  The **Diameter Common** > **Network Identifiers** > **MCCMNC** pages can be used to configure up to 2500 distinct combinations of Mobile Country Code (MCC) and Mobile Network Code (MNC). (Refer to *Diameter Common User's Guide* and Help for procedures to configure MCC-MNC combinations.)

- If a match occurs, the user identity is considered as an IMSI and used for IMSI lookup.

- If a match does not occur, the user identity is considered as an MSISDN and used for MSISDN lookup.

Multiple DSR Application Invocation Prevention

The DSR provides a mechanism for preventing the same DSR application from being invoked on two different DSR nodes:

- When a DSR application does not want to be invoked a second time on another DSR, it can insert a DSR AVP called DSR-Application-Invoked containing its DSR Application ID.

- When the Diameter Routing Function searches an ART, it ignores any Application Routing Rules associated with a DSR application that has inserted the DSR-Application-Invoked AVP

DSR-Application-Invoked AVP

To prevent the same DSR application from being invoked on multiple DSRs in a network (and processing the same message twice by the same DSR application), a DSR application can (optionally) add to the Request message a DSR-Application-Invoked AVP containing the DSR Application ID as shown in DSR Application-Invoked AVP.

Table 3-4 DSR Application-Invoked AVP

Byte 1	Byte 2	Byte 3	Byte 4
AVP Code = 2468			
Flags=10000000		Length = 16	
Vendor ID = 323			
DSR Application ID = Unsigned32			

This AVP is decoded by the Diameter Routing Function before ART processing to prevent multiple invocations of the same DSR application. Any Application Routing Rule with this DSR Application ID is ignored by the Diameter Routing Function.

This AVP can be repeated in the Request to indicate different DSR applications, but is inserted only once per DSR application.

Insertion of a DSR Application-Invoked AVP is controlled by DSR application specific configuration on the **FABR** > **Configuration** > **System Options** GUI page, such as:

Allow Subsequent FABR Invocation - Checked = Yes, Unchecked = No
If checked, subsequent invocation of FABR on a different DSR node in the network is allowed.

Transaction Metadata Recording for Integrated DIH (IDIH)

Integrated Diameter Intelligence Hub (**IDIH**) can be used to capture detailed information about selected Diameter transactions, and transmit this information to **DIH** for further analysis.

The Diameter Routing Function and invoked DSR applications record detailed information about each Diameter transaction - called transaction metadata. Each metadata record describes an important event in the lifetime of a Diameter transaction. Metadata appears in the Trace Transaction Record (**TTR**) in the order that the metadata-generating events actually occurred. Together, all of the metadata records combine to document the processing performed on the entire transaction, and can later be used to provide diagnostic information when performing troubleshooting. Metadata is recorded to a TTR for each transaction so that, even if the transaction is selected to be sent to DIH at an Answer Troubleshooting Trigger Point (TTP-IA or TTP-EA), the metadata for all of the messages in the transaction is present.

The functions of IDIH are described in the *Integrated DIH User's Guide* and Help.

FABR records the application-specific metadata events described in Table 3-5.

Table 3-5 FABR Metadata-Generating Events

Event	Type	Scope	Instance Data	When Recorded
Address Resolution Match found	Address Resolution Match	App Data	• Routing Entity Type (such as IMSI) • Routing Entity AVP (such as Public-Identity) • Routing Entity Address (such as 311480123456789)	After FABR searches and finds a valid Routing Entity address in an ingress Request message using a prioritized set of AVPs associated with the highest priority Routing Entity Type assigned to the Address Resolution order pair (Diameter Application ID, Command Code).
DP Query Event Sent to DP for processing	DP Query Sent	App Data	• Routing Entity Data Format (such as IMSI) • Routing Entity Address (such as 123456789012345) • Destination Type (such as IMS-HSS)	When FABR sends a DP query event to the DP for Destination address resolution.

Table 3-5 (Cont.) FABR Metadata-Generating Events

Event	Type	Scope	Instance Data	When Recorded
DP Response Event Received from DP	DP Response Received	App Data	• DP IP Address Type (such as IPv4) • DP IP Address (such as 10.240.55.25) • Result Code String (such as Blacklisted) • Destination Realm (such as xyz.com) • Destination FQDN (such as hss1.hss.xyz.com)	When FABR receives a response to a previous DP query.
Routing Exception	Routing Exception	App Data	• Routing Exception Type (such as DP Congestion) • Routing Exception Action (such as Abandon Request)	After any Routing Exception is encountered.
DP Query Failure	DP Query Failure	App Data	• DP IP Address Type (such as IPv4) • DP IP Address (such as 10.240.55.25)	After any DP Query failure other than a response timeout is encountered.
DP Response Timed out	DP Response Timeout	App Data	• DP IP Address Type (such as IPv4) • DP IP Address (such as 10.240.55.25)	When FABR times out waiting to receive a response from the DP to a previous Destination address resolution query.

4

Configuration of FABR

This section describes the procedures used to configure the FABR application.

Pre-Configuration Activities

Before FABR configuration can be performed, the following activities need to be performed in the system:

- Verify server status
- Gather information required for Diameter, Diameter Common, and FABR configuration
- Configure Diameter Common components required for FABR configuration
- Configure Diameter components required for FABR configuration
- Configure SDS DP Remote servers in Communication Agent (**ComAgent**)

Verifying Server status

Use this task to verify server status before FABR configuration.

1. From the active **SOAM** in a DSR topology, click **Status & Manage** > **Server**.
2. Verify that for each server the **Appl State** field is **Disabled**, and the **DB**, **Reporting Status**, and **Proc** fields are **Norm**.

Diameter Common Configuration for FABR

The following Diameter Common configuration must be done before FABR configuration can be performed.

Use the *Diameter Common User's Guide* to complete the Diameter Common configuration, including the Diameter Common components needed for use with FABR.

SOAM Diameter Common Configuration

Diameter Common configuration for MCC Ranges Network Identifiers and MP Profile assignment for FABR is done from the **SOAM GUI** in a DSR topology.

1. **MPs**

   Click **Diameter Common** > **MPs** > **Profile Assignments**, and verify the correct Database MP Profiles have been assigned for FABR DA-MPs shown in the DA-MP list. If assignments need to be made or changed, use the **Diameter Common** > **MPs** > **Profile Assignments** page to assign the correct MP Profiles.

2. **MCC Ranges**

   Use the **Diameter Common** > **Network Identifiers** > **MCC Ranges [Insert]** page to specify up to 10 distinct, non-overlapping MCC Ranges.

   The following two MCC Ranges are reserved by telephony standards and are recommended to be created in addition to other specified ranges:

   a. 000-199

   b. 800-899

NOAM Diameter Common Configuration

Diameter Common configuration for MCCMNC Network Identifiers for FABR is done from the **NOAM** GUI in a DSR topology.

1. Use the **Diameter Common** > **Network Identifiers** > **MCCMNC [Insert]** page to configure MCCMNC entries.

Diameter Configuration for FABR

The following Diameter configuration must be done before FABR configuration can be performed.

All Diameter Configuration is done using the **SOAM GUI** in a DSR topology.

Use the *Diameter User's Guide* to complete the Diameter configuration, including the Diameter components needed for use with FABR.

1. **Application IDs**

   Diameter Application IDs must be configured prior to making them available for use in a FABR Address Resolution. Use the **Diameter** > **Configuration** > **Application Ids [Insert]** page to configure Diameter Application IDs.

   The Application IDs that need to be configured depend on the types of Diameter servers being supported, including **HSS**, **PCRF**, **OFCS**, **OCS**, and **AAA**.

2. **Command Codes**

   Diameter Command Codes must be configured prior to using them in a FABR Address Resolution. Use the **Diameter** > **Configuration** > **Command Codes [Insert]** page to configure Diameter Command Codes.

   Configure any Command Codes that need to be handled by FABR. The Command Codes are associated with the Diameter applications supported by the Diameter servers (for example, HSS, PCRF, OCFS, OCS, or AAA), which are the destination of Diameter Requests being routed by FABR. For example, the combination of Application ID = S6a and Command Code = ULR/ULA might be relevant for HSS.

3. **Application Route Tables**

   Either use the default Application Route Table (always available), or use the **Diameter** > **Configuration** > **Command Codes** > **Application Route Tables [Insert]** page to configure one or more Application Route Tables in addition to the default. Application Route Tables contain Application Routing Rules that direct messages to FABR and other DSR applications.

4. **Application Routing Rules**

On the **Diameter** > **Configuration** > **Command Codes** > **Application Route Tables** page, select an Application Route Table Name and click **View/Edit Rules**.

Use the Viewing Rules for Application Route Table page to insert or edit an Application Routing Rule with the Application Name set to FABR so messages are directed to FABR.

If the FABR application and the DM-IWF application are chained so both of them can process the same Request message, insert or edit a second Application Routing Rule with the Application Name set to DM-IWF.

Set the Priority in each of the two Application Routing Rules to indicate which application processes the message first (the higher priority processes first).

- Set the **Application Name** to **FABR**.
- In the **Conditions** field, set the **Application-Id Operator** to**Equals** and the**Value** to **4**. For all other parameters, set the**Operator** to **Always True**.

SDS DP Remote Server Configuration

Use this procedure to configure **SDS DP** Remote Servers to allow FABR to use SDS for address lookup and resolution.

1. From the active **NOAM**, click **Communication Agent** > **Configuration** > **Remote Servers**.
2. Click **Insert**.
3. Enter a unique **Remote Server Name**.
4. Enter the **Remote Server IP Address**.

   Specify the IP address that can be reached via a server's Internal Management Interface (IMI). The IP address uniquely identifies the Remote Server and provides the means by which **Communication Agent** can establish transport connections to/from the Remote Server.
5. For **Remote Server Mode**, select **Server**.
6. Assign the Remote Server to one of the **Available Local Server Groups**.
7. Click **Ok**.
8. Select **Communication Agent** > **Configuration** > **Connection Groups**
9. Select the `DPSvcGroup` and click **Edit**.
10. Assign the Remote Server you just created to the DPSvcGroup Connection group.
11. Click **Ok**.
12. Expand the **Servers** assigned to the `DPSvcGroup` to see that the new Remote Server is now included.

The operational status of what was provisioned can be verified by using the **Communication Agent** > **Maintenance** pages.

- Click **Communication Agent** > **Maintenance** > **Connection Status** to verify all Remote Server connections added are shown as `InService` on all local servers.

- Click **Communication Agent** > **Maintenance** > **Routed Service Status** to verify the status is `Available` for all local servers that are provisioned to connect.

FABR Configuration

The **FABR** > **Configuration** pages allow you to manage FABR application configuration.

FABR configuration typically occurs in the following order:

1. Add Diameter **Applications** to a list of FABR supported Diameter applications.
2. If necessary, configure **Default Destinations**.
3. If necessary, edit routing **Exceptions**.

   Note: If a **Routing Exception Action** of **Forward Unchanged** is configured, configure a **Default Destination**.

4. Configure **Address Resolutions**.
5. If necessary, change the **System Options**.

Applications configuration

The FABR > Configuration > Applications page allows you to access a list of Diameter applications supported by FABR.

From the FABR > Configuration > Applications page, you can:

- Filter the list of supported Diameter applications to display only the desired application(s).
- View a list of supported Diameter applications.
- Insert a supported Diameter application.

  Note: When an Application entry is added, Routing Exceptions (Unknown Command Code, No valid Routing Entity Address, No Address Match) are automatically inserted with the Routing Exception Action value as Forward Unchanged.

- Delete a Diameter application from the list of supported Diameter applications.

  Note: When an Application entry is deleted, the associated Routing Exceptions are automatically deleted.

Applications configuration elements

Table 4-1 describe the fields on the Applications insert page.

Table 4-1 Applications Configuration Elements

Field	Description	Data Input Notes
*Application ID	Diameter Application ID, command code, and routing entity type are useful to determine address resolution for routing request messages.	Format: list Range: Configured Diameter Application IDs Default: none
*Routing Mode (Read only)	Method of routing for request messages received that contain the diameter Application ID.	Format: Disabled list with a value of **Proxy**.

Inserting a supported Diameter application

Use this task to add a new Diameter application.

Inserting a supported Application automatically adds Routing Exceptions (**Unknown Command Code**, **No valid Routing Entity Address**, **No Address Match Found**, **DP Errors**, and **DP Congestion**) with the **Routing Exception Action** set to `Forward Unchanged`.

1. Click **FABR** > **Configuration** > **Applications**.
2. Click **Insert**.
3. Select **Application ID** from the list.

Note:

The Application IDs presented in this list are those created using **Diameter** > **Configuration** > **Application IDs**.

Note the **Routing Mode** field is disabled.

4. Click **OK**, **Apply**, or **Cancel**.

Deleting a Diameter application from the list of supported Diameter applications

Use this task to delete a Diameter application from the list of supported Diameter applications.

An application cannot be deleted if it is being used by an Address Resolution. Before you perform this task, delete any Address Resolution that uses the Application.

1. Select **FABR** > **Configuration** > **Applications**.
2. Select the application you want to delete and click **Delete**.

Note: An error message appears if the application has already been removed.

3. Click **OK** or **Cancel** on the confirmation screen.

Exceptions configuration

The **FABR** > **Configuration** > **Exceptions** page allows you to specify the routing procedure to invoke when FABR is unable to resolve an address to a Destination for each supported Diameter application and Routing Exception Type.

There are Routing Exception entries automatically inserted with the **Routing Exception Action** set to `Forward Unchanged` as the default action for a supported Diameter application entry when that application entry is added.

- **Unknown Command Code**
- **No valid Routing Entity Address**
- **No Address Match Found**
- **DP Errors**
- **DP Congestion**
- **Blacklist**

Similarly, these Routing Exceptions that are associated with an application entry are automatically deleted when that application entry is deleted.

From the **FABR** > **Configuration** > **Exceptions** page, you can:

- Filter the list of exceptions to display only the desired exceptions.
- View a list of supported Diameter applications and their associated Routing Exception Types and Routing Exception Actions.
- Edit the Routing Exception Action and its associated attributes for a supported Diameter application.

Exceptions configuration elements

Table 4-2 describes the fields on the Exceptions edit page.

Table 4-2 Exceptions Configuration Elements

Field	Description	Data Input Notes
*Application ID	Application ID in a diameter message - Read only	none
Application Name	Name of the application corresponding to the Application ID - Read only.	none
*Routing Exception Type	The routing exception that prevented address resolution - Read only. This field displays one of the following values: • Unknown Command Code • No Valid Routing Entity Address • No Address Match Found • DP Errors • DP Congestion • **Blacklist**ed Subscriber	none

Table 4-2 (Cont.) Exceptions Configuration Elements

Field	Description	Data Input Notes
Routing Exception Action	Action that FABR takes associated with the **Routing Exception Type**	Format: options Range: • Forward Unchanged • Forward to Destination • Send Answer with Result-Code AVP • Send Answer with Experimental-Result AVP • Abandon Request
Destination	Destination to where the message is forwarded associated with the **Routing Exception Type**. This field is enabled when the **Routing Exception Action** is set to `Forward to Destination`.	Format: list Range: Available user-configured destinations
Result-Code Value	Result code associated with this **Routing Exception Type**. This field is enabled when the **Routing Exception Action** is set to either `Send Answer with Result-Code AVP` or `Send Answer with Experimental-Result AVP`.	Format: • field • list Range: • field: 1000–5999 • list with available diameter result codes Default: none
Vendor-ID	Value returned in the Vendor-ID AVP of the answer message associated with this **Routing Exception Type**. This field is enabled when the **Routing Exception Action** is set to `Send Answer with Experimental-Result AVP`.	Format: field Range: 1–4294967295 Default: none
Error Message	Value returned in the Error-Message AVP of the answer message. This field is enabled when the **Routing Exception Action** is set to either `Send Answer with Result-Code AVP` or `Send Answer with Experimental-Result AVP`.	Range: 0–64 characters Default: null string, no Error-Message AVP in Answer message

Editing a Routing Exception

Use this task to edit a Routing Exception.

1. Click **FABR** > **Configuration** > **Exceptions**.
2. Select the Application ID/Name you want to edit and click **Edit**.

Note: An error message appears if the application has already been removed.

3. Update the relevant fields.

   For more information about each field, see Table 4-2.

   - An error is displayed if **Vendor-ID** is not configured when `Send Answer with Experimental-Result` AVP is selected as a value for **Routing Exception Action**.
   - An error is displayed if **Destination** is not configured when `Forward to Destination` is selected as a value for **Routing Exception Action**.
   - An error is displayed if **Result-Code Value** is not configured when `Send Answer with Result-Code` AVP or `Send Answer with Experimental-Result` AVP is selected as a value for **Routing Exception Action**.

4. Click **OK**, **Apply** or **Cancel**.

Default Destinations configuration

The FABR > Configuration > Default Destinations page contains the attributes associated with a Default Destination to which FABR routes a message. FABR uses these attributes to modify the contents of a received message before forwarding the message.

Each Default Destination can be configured with any combination of a Realm and FQDN such as Realm-only, FQDN-only, or Realm and FQDN.

From the FABR > Configuration > Default Destinations page, you can:

- Filter the list of Default Destinations to display only the desired destinations.
- View a list of Default Destinations.
- Insert a Default Destination.
- Edit a Default Destination.
- Delete a Default Destination.

Default Destinations configuration elements

Table 4-3 describes the fields on the Default Destinations insert and edit pages.

Table 4-3 Destinations Configuration Elements

Field	Description	Data Input Notes
***Name**	Unique name of the destination	Format: field Range: 1–32 characters
Realm	**Realm** of the default destination The realm and fully qualified domain name cannot both be empty; otherwise, an error message appears.	Format: field Range: A valid Realm or FDQN. Default: none

Table 4-3 (Cont.) Destinations Configuration Elements

Field	Description	Data Input Notes
Fully Qualified Domain Name	Unique fully qualified domain name of the default destination If a duplicate FQDN is entered, an error message appears. The **Fully Qualified Domain Name** and **Realm** cannot both be empty; otherwise, an error message appears.	

Inserting a Default Destination

Use this task to add a new Default Destination.

1. Click **FABR** > **Configuration** > **Default Destinations**.
2. Click **Insert**.
3. Enter a unique name for the destination in the **Name** field.
4. Enter the realm in the **Realm** field.
5. Enter a unique FQDN in the **Fully Qualified Domain Name** field.
6. Click **OK**, **Apply** or **Cancel**.

Editing a Default Destination

Use this task to edit a Default Destination.

1. Click **FABR** > **Configuration** > **Default Destinations**.
2. Select the Destination you want to edit and click **Edit**.

   Note: An error message appears if the Destination has already been removed.

3. Update the relevant fields.

   For more information about each field, see Table 4-3.

   The **Name** field is read-only and cannot be edited.

4. Click **OK**, **Apply** or **Cancel**.

Deleting a Default Destination

Use this task to delete a Default Destination. A Default Destination cannot be deleted if it is being used by a Routing Exception. Before this task is performed, delete the association with any Routing Exception either by changing the Routing Exception Action to something other than `Forward To Destination`, or by deleting the supported application, thereby deleting the associated Routing Exceptions.

1. Click **FABR** > **Configuration** > **Default Destinations**.

2. Select the Default Destination you want to delete and click **Delete**.
3. Click **OK** or **Cancel** on the confirmation screen.

Address Resolutions configuration

FABR performs off-board database lookups for user identities decoded from Diameter messages. The **FABR** > **Configuration** > **Address Resolutions** page allows you to configure which (and how) user identities are to be decoded from the messages. You can provision combinations of Diameter Application ID, and Command Code (the key matched to the messages) and configure the Routing Entity Type(s) to be decoded and a prioritized list of AVPs from which to decode these entity types. An Address Resolution supports up to three prioritized Routing Entity Types for each Application ID and Command Code (from highest priority to lowest priority - Primary Routing Entity Type, Secondary Routing Entity Type, and Tertiary Routing Entity Type) .

From the **FABR** > **Configuration** > **Address Resolutions** page, you can:

- Filter the list of address resolutions to display only the desired records.
- View a list of address resolutions.
- Insert an address resolution.
- Edit an address resolution.
- Delete an address resolution.

Address Resolutions configuration elements

Table 4-4 describes the fields on the Address Resolutions insert and edit pages. Data input notes only apply to the insert and edit pages.

Table 4-4 Address Resolutions Configuration Elements

Field	Description	Data Input Notes
*Application ID	Application ID in a diameter message. The application ID is an **IANA**-assigned diameter application ID, which is a 32-bit field that is mandatory in all diameter messages. It is commonly used for screening and routing messages between diameter nodes. If a combination of the Application ID and command code already exists, an error message appears.	Format: list Range: application IDs configured for FABR
*Command Code	Command Code in a diameter message If a combination of the Application ID and command code already exists, an error message appears.	Format: list Range: command codes configured for diameter

Primary Routing Entity/Secondary/Tertiary Routing Entity sections

Table 4-4 (Cont.) Address Resolutions Configuration Elements

Field	Description	Data Input Notes
*Routing Entity	Routing entity type. The same routing entity type cannot be selected for both the primary and the secondary routing entity; if the same type is selected, an error message appears. If the routing entity type is not specified for the primary routing entity, an error message appears.	Format: list Range: • IMSI • MSISDN • IMPI • IMPU • External Identifier
*Primary AVP	Primary AVP used for extracting the routing entity address. The same primary AVP and secondary AVP cannot be selected for either the primary routing entity or for the secondary routing entity; if the same AVP is selected, an error message appears. If primary AVP is not selected for the primary routing entity, an error message appears.	Format: list Range: • Public Identity • ServiceInfo.Subscription-ID(0) • ServiceInfo.Subscription-ID(1) • ServiceInfo.Subscription-ID(2) • ServiceInfo.Subscription-ID(3) • Subscription-ID(0) • Subscription-ID(1) • Subscription-ID(2) • Subscription-ID(3) • UserIdentifier.External-Identifier • UserIdentifier.MSISDN • UserIdentity.MSISDN • UserIdentity.Public-Identity • MSISDN • UserName • UserIdentifier.External-Identifier • Wildcarded-Public-Identity
Secondary AVP	Secondary AVP used for extracting the routing entity address. The same primary AVP and secondary AVP cannot be selected for either the primary routing entity or for the secondary routing entity; if the same AVP is selected, an error message appears.	

Table 4-4 (Cont.) Address Resolutions Configuration Elements

Field	Description	Data Input Notes
*Destination Type	Type of Destination for this routing entity type.	Format: list Range: • AAA • IMS-HSS • LTE-HSS • MTC-HSS • OCS • OFCS • PCRF • USERDEF1 • USERDEF2
Prefix Search Enabled	Enables the IMSI/MSISDN prefix based lookup to be performed if the full address lookup did not find a match.	Format: check box Default: none
Blacklist Search Enabled	Enables the IMSI/MSISDN blacklist lookup to be performed before the full address lookup.	Format: check box Default: none
FallBack Search Enable	Enables the Domain-Identifier lookup to be performed when the external identifier lookup did not find an exact match.	Format: check box Default: none

Inserting an Address Resolution

Use this task to add a new Address Resolution.

Before this task is performed, make sure there is at least one supported Diameter application configured in the system.

1. Click **FABR** > **Configuration** > **Address Resolutions**.
2. Click **Insert**.
3. Select the **Application ID** from the list.

   Note: The Application IDs presented in this list are those created using **FABR** > **Configuration** > **Applications**.

4. Select the **Command Code** from the list.

   Note: The Command Codes presented in this list are those created using **Diameter** > **Command Codes**.

5. For the Primary Routing Entity section, perform the following:
   a. Select the **Routing Entity** from the list.
   b. Select the **Primary AVP** from the list.

c. If needed, select the **Secondary AVP** from the list.

d. Select the type of destination from the **Destination Type** list.

e. Check the **Prefix Search Enabled** checkbox to perform the IMSI/MSISDN prefix based lookup.

f. Check the **Blacklist Search Enabled** checkbox to perform the IMSI/MSISDN blacklist lookup.

g. Check the **FallBack Search Enabled** checkbox to perform the Domain-Identifier lookup.

6. If needed, for the Secondary Routing Entity section, perform the following:

a. Select the appropriate Routing Entity type from the **Routing Entity Type** list.

b. Select the Primary AVP from the **Primary AVP** list.

c. If needed, select the Secondary AVP from the **Secondary AVP** list.

d. Select the type of destination from the **Destination Type** list.

e. Check the **Prefix Search Enabled** checkbox to perform the IMSI/MSISDN prefix based lookup.

f. Check the **Blacklist Search Enabled** checkbox to perform the IMSI/MSISDN blacklist lookup.

g. Check the **FallBack Search Enabled** checkbox to perform the Domain-Identifier lookup.

7. If needed, for the Tertiary Routing Entity section, perform the following:

a. Select the appropriate Routing Entity type from the **Routing Entity Type** list.

b. Select the Primary AVP from the **Primary AVP** list.

c. If needed, select the Secondary AVP from the **Secondary AVP** list.

d. Select the type of destination from the **Destination Type** list.

e. Check the **Prefix Search Enabled** checkbox to perform the IMSI/MSISDN prefix based lookup.

f. Check the **Blacklist Search Enabled** checkbox to perform the IMSI/MSISDN blacklist lookup.

g. Check the **FallBack Search Enabled** checkbox to perform the Domain-Identifier lookup.

8. Click **OK**, **Apply**, or **Cancel**.

Editing an Address Resolution

Use this task to edit an Address Resolution.

1. Click **FABR** > **Configuration** > **Address Resolution**.

2. Select the Address Resolution you want to edit and click **Edit**.

Note: An error message appears if the Address Resolution has already been removed.

3. Update the relevant fields.

   For more information about each field, see Table 4-4.

   The following fields are read-only and cannot be edited:

   - **Application ID**
   - **Command Code**

4. Click **OK**, **Apply**, or **Cancel**.

Deleting an Address Resolution

Use this task to delete an Address Resolution.

1. Click **FABR** > **Configuration** > **Address Resolutions**.
2. Select the Address Resolution you want to delete and click **Delete**.
3. Click **OK** or **Cancel** on the confirmation screen.

System Options configuration

The System Options page allows you to modify the default system values for FABR global parameters, for example, FQDN/Realm, Allow Subsequent FABR Invocation, or Application Unavailable action.

System Options elements

Table 4-5 describes the fields on the System Options page.

Table 4-5 System Options Elements

Field	Description	Data Input Notes
ASCII Excluded Digits	List of **ASCII** characters to ignore while parsing MSISDN digits from a raw AVP data field of AVP Type UTF8String. If an invalid character is entered, an error message appears.	Format: field Default: none Range: ASCII printable characters except percentage sign (%), commercial sign (@), colon sign (:), and semi-colon (;).
Exclude Space	Defines whether ASCII character space is ignored while parsing MSISDN digits from a raw AVP data field of AVP Type UTF8String If checked, ASCII character space is ignored. If not checked, ASCII character space is not ignored.	Format: check box Default: unchecked

Table 4-5 (Cont.) System Options Elements

Field	Description	Data Input Notes
TBCD Excluded Digits	Defines whether the associated digits is ignored while parsing digits from a raw AVP data field of AVP Type OctetString encoded as a **TBCD**-string If checked, digits are ignored. If not checked, digits are not ignored.	Format: check boxes Range: checked, unchecked for each option: *(1010), #(1011), a(1100), b(1101), c(1110) Default: all unchecked
Allow Subsequent FABR Invocation	Enables the subsequent invocation of FABR on a different **DSR** node in the network.	Format: check box Default: unchecked
Remove Destination-Host	If checked, FABR deletes any instance of `Destination-Host` AVPs in the message when performing Realm only resolution.	Format: check box Default: unchecked
Realm	Value to be placed in the Origin-Realm AVP of the Answer message generated by FABR. A Realm must be paired with a Fully Qualified Domain Name. If entering a value for Realm, then a value for Fully Qualified Domain Name must also be entered; otherwise, an error message appears. If a value is not entered, the local node Realm for the egress connection is used.	Format: field Range: A valid Realm Default: none
Fully Qualified Domain Name	Value to be placed in the Origin-Host AVP of the Answer message generated by FABR. A Fully Qualified Domain Name must be paired with a Realm. If entering a value for Fully Qualified Domain Name, then a value for Realm must also be entered; otherwise, an error message appears. If not configured, local node FQDN for the egress connection is used.	Format: field Range: A valid FQDN - up to 255 characters; label-up to 63 characters. Default: none
Resource Exhaustion Result-Code	Result-Code or Experimental-Result-Code value to be returned in an Answer message when a message is not successfully routed because of internal resource being exhausted. If Vendor-ID is configured, this result-code value is encoded as Experimental-Result-Code AVP; otherwise the result-code is encoded as Result-Code AVP.	Format: • field • list Range: • field: 1000–5999 • list with available Code values Default: 3004
Resource Exhaustion Error Message	Error-Message AVP value to be returned in an Answer message when a message is not successfully routed because of internal resource being exhausted.	Range: 0–64 characters Default: FABR Resource Exhausted

Table 4-5 (Cont.) System Options Elements

Field	Description	Data Input Notes
Resource Exhaustion Vendor-ID	Vendor-ID AVP value to be returned in an Answer message when a message is not successfully routed because of internal resource being exhausted.	Format: field Range: 1–4294967295
Application Unavailable Action	Defines action to be taken when FABR is not available to process messages. If the `Default Route` option is selected, an entry must be provided for the Application Unavailable Route List.	Format: options Range: • Continue Routing • Default Route • Send Answer with Result-Code AVP • Send Answer with Experimental-Result AVP Default: Continue Routing
Application Unavailable Route List	Defines where the requests are routed when FABR is not available. Peer Routing Rules are bypassed. A route list must be entered if `Default Route` is selected as the **Application Unavailable Action**.	Format: list Range: Available Route List entries
Application Unavailable Result-Code	Result-Code or Experimental-Result-Code value to be returned in an Answer message when a message is not successfully routed because FABR is not available. If Vendor-ID is configured, this result-code value is encoded as Experimental-Result-Code AVP; otherwise the result-code is encoded as Result-Code AVP. A code must be entered if either the `Send Answer with Result-Code AVP` or the `Send Answer with Experimental Result-Code AVP` option is selected as the **Application Unavailable Action**.	Format: • field • list Range: • field: 1000–5999 • list with available Code values Default: 3002

Table 4-5 (Cont.) System Options Elements

Field	Description	Data Input Notes
Application Unavailable Error Message	Error-Message AVP value to be returned in an Answer message when a message is not successfully routed because FABR is not available. A message can be entered, if needed, when either the `Send Answer with Result-Code AVP` or the `Send Answer with Experimental Result-Code AVP` option is selected as the **Application Unavailable Action**.	Range: 0–64 characters Default: FABR Unavailable
Application Unavailable Vendor-ID	Vendor-ID AVP value to be returned in an Answer message when a message is not successfully routed because FABR is not available. A vendor-ID must be entered if the `Send Answer with Experimental Result-Code AVP` option is selected as the **Application Unavailable Action**.	Format: field Range: 1–4294967295
Bundling Enabled	If enabled, allows FABR to bundle DP query Events to form a DP Bundled query Event to send to DP server.	Format: check box
Maximum Bundle Size	Maximum number of individual DP query Events that can be bundled.	Format: field Range: 2-20 Default: 5
Prefix Search Enabled	If enabled, IMSI/MSISDN prefix based lookup is performed if the full address lookup did not find a match.	Format: check box Default: unchecked
Blacklist Search Enabled	If enabled, IMSI/MSISDN blacklist lookup is performed prior to the full address lookup.	Format: check box Default: unchecked
FallBack Search Enable	If enabled, Domain-Identifier lookup is performed when the external identifier lookup did not have an exact match.	Format: check box Default: unchecked

Editing System Options

Use this task to edit System Options.

1. Click **FABR** > **Configuration** > **System Options**.
2. Update the relevant fields.

   For more information about each field, see Table 4-5.
3. Click **OK** or **Cancel**.

Post-Configuration Activities

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

- Enabling the FABR application, if it has not already been enabled.
- Status Verification

Enabling the FABR Application

Use this task to enable the FABR application.

1. From each active **SOAM** in a DSR topology, click **Diameter** > **Maintenance** > **Applications**.
2. Under **DSR Application Name**, select each **FABR** 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 have changed respectively to **Enabled**, **Available**, **Normal**, and **Normal**.

Status Verification

Use this task to verify FABR status after configuration is complete.

1. Verify Communication Agent (ComAgent) Connection status.
   a. From the active **SOAM** in a DSR topology, click **Communication Agent** > **Maintenance** > **Connection Status**.
   b. Verify that the **Automatic Connections Count** field displays **X of X in service** where X is the number of peer server connections.
2. Verify server status.
   a. From the active SOAM in a DSR topology, click **Status & Manage** > **Server**.
   b. Verify that for each server, the **Appl State** field is **Enabled**, and the **DB**, **Reporting Status**, and **Proc** fields are **Norm**.

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.

5

Maintenance of FABR

The **Diameter** > **Maintenance** GUI provides the FABR specific maintenance functions. In this section describes Admin State, Operational Status, Operational Reason, and Congestion Levels on the **Diameter** > **Maintenance** > **Applications** page.

Overview

The FABR application has no maintenance GUI pages of its own. The following Diameter > Maintenance pages provide functions and information that can be used with the FABR application:

- The Diameter > Maintenance > Applications page displays FABR status information including Admin State, Operational Status, and Operational Reason. The page also provides functions to enable and disable the application. See FABR Administrative State and Operational Status and refer to the *Diameter User Guide* and Help for explanations of the page and the status information.
- The Diameter > Maintenance > DA-MPs page displays status and connectivity information for the DA-MP that is running the FABR application. Refer to the *Diameter User Guide* and Help for explanations of the page and the status information.

FABR Administrative State and Operational Status

The FABR Administrative State (or Admin State) indicates the state that the operator desires the FABR application to be in, and can be manually enabled or disabled. The Operational Status indicates the actual status of the FABR application. The FABR Admin State and Operational Status is updated when the application is started or restarted and when FABR congestion is detected.

Next Generation Network Priority Service (**NGN-PS**) allows National Security/ Emergency Preparedness (NS/EP) users to make priority calls/sessions using public networks. The NGN-PS requests are never discarded due to congestion. NGN-PS requests are always processed by FABR application unless FABR application or DP is unavailable, in that case configured Exception Action is used for further routing. For a detailed description of NGN-PS, refer to the *Diameter User's Guide* and Help.

FABR Admin State and Operational Status lists the FABR Admin State and Operational Status related to the DP pool operational status and to FABR congestion levels. It specifies the actions that FABR takes in various situations.

Table 5-1 FABR Admin State and Operational Status

FABR Admin State	DP Operational Status/Congestion Level	FABR Congestion Level	FABR Operational Status	FABR Actions or Impacts on FABR
Disabled	Any	Any	Unavailable	The default shutdown state
Enabled	DP Operational Status = Normal or Degraded DP Congestion Level = Normal OR Minor	Normal/ CL1/CL2	Available	FABR receives requests from the DRL. FABR sends queries to the DP.
	DP Operational Status = Normal OR Degraded DP Congestion Level = Major OR Critical OR DP Congestion Abatement in progress	Normal/ CL1/CL2	Available	FABR receives requests from the DRL. FABR applies DP Congestion routing exception action.
	DP Operational Status = Normal OR Degraded DP Congestion Level = Any	CL3	Degraded	The DRL stops sending non-NGN-PS requests to FABR. DRL only sends NGN-PS requests to FABR.
	DP Operational Status = Down DP Congestion Level = Any	Any	Unavailable	FABR is shutting down. DRL stops sending requests to FABR.