Oracle® Communications Diameter Signaling Router

RADIUS User's Guide

Release 8.1

E87967 Revision 02

July 2017

ORACLE®

Oracle Communications Diameter Signaling Router RADIUS User's Guide, Release 8.1

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Topics:

This section contains an overview of the available information for configuring DSR for RADIUS support and the RADIUS-Diameter IWF application.

Revision History

Date	Description
June 2016	Accessibility changes throughout.

Overview

This document describes the features associated with RADIUS (Remote Authentication Dial In User Service).

This document will also:

- Provide a conceptual overview of the purpose, architecture, and functionality of RADIUS
- Describe the pages and elements on the RADIUS GUI
- Provide procedures for using the RADIUS interface
- Explain the organization of and how to use this document

Scope and Audience

This document is intended for anyone responsible for configuring and using the RADIUS application. Users of this manual must have a working knowledge of telecommunications and network installations.

Manual Organization

This manual is organized into the following chapters:

- *Introduction* contains general information about the RADIUS 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, including information about how the interface options are organized, how to use widgets and buttons, and how filtering and other page display options work.
- *RADIUS Overview* describes an overview of RADIUS and includes information about important fundamental concepts, as well as high-level functionality.
- *Configuration* describes configuration of RADIUS components.

Documentation Admonishments

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

Table 1: Admonishments

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

Related Publications

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

Locate Product Documentation on the Oracle Help Center Site

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

1. Access the Oracle Help Center site at *http://docs.oracle.com*.
2. Click **`Industries`**.

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

Customer Training

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

http://education.oracle.com/communication

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

www.oracle.com/education/contacts

My Oracle Support (MOS)

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

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

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

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

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

Emergency Response

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

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

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

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

Chapter 2

User Interface Introduction

Topics:

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

User Interface Organization

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

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

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

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

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

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

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

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

User Interface Elements

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

Table 2: User Interface Elements

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

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

Main Menu Options

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

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

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

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

Table 3: Main Menu Options

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

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

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

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

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

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

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

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

Missing Main Menu options

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

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

Common Graphical User Interface Widgets

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

Supported Browsers

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

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

System Login Page

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

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

Customizing the Login Message

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

Figure 1: Oracle System Login

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

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

Accessing the DSR Graphical User Interface

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

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

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

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

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

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

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

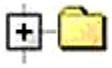
   The DSR GUI for the SOAM appears

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

Main Menu Icons

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

Table 4: Main Menu Icons

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

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

Work Area Displays

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

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

Tables

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

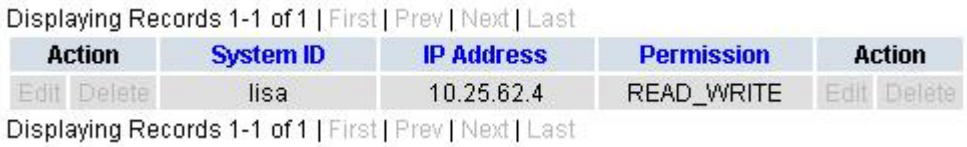
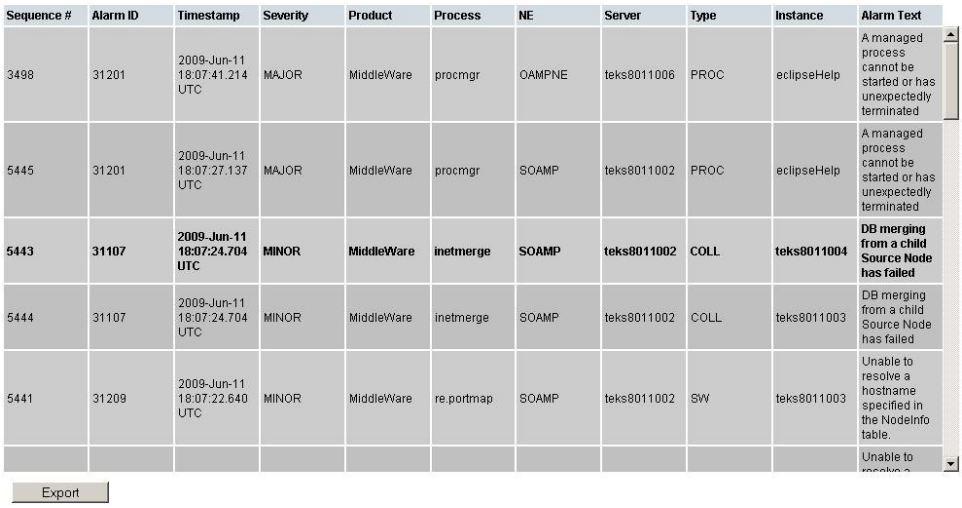


Figure 2: Paginated Table

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



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

Export

Figure 3: Scrollable Table

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

Forms

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

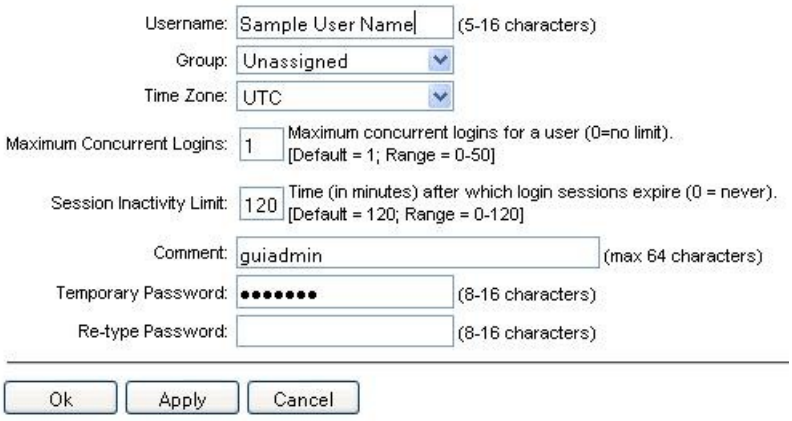
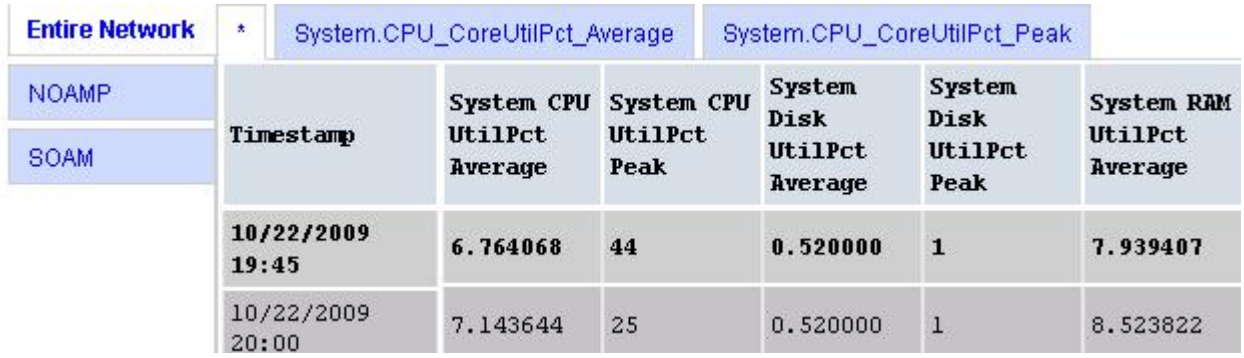


Figure 4: Form Page

Tabbed pages

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



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

Figure 5: Tabbed Pages

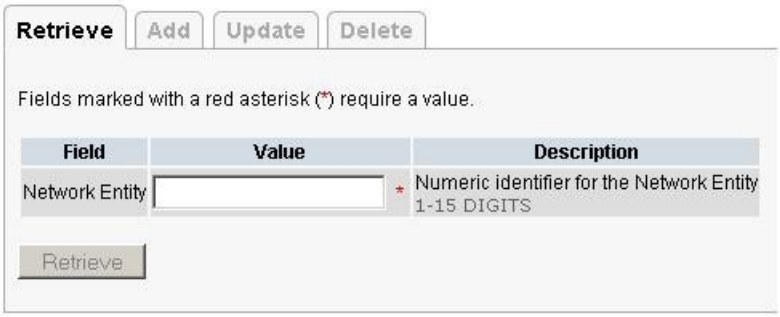


Figure 6: Tabbed Pages

Reports

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

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

User Account Usage Report

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

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

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

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

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

End of User Account Usage Report

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

Figure 7: Report Output

Customizing the Splash Page Welcome Message

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

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

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

Column Headers (Sorting)

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

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

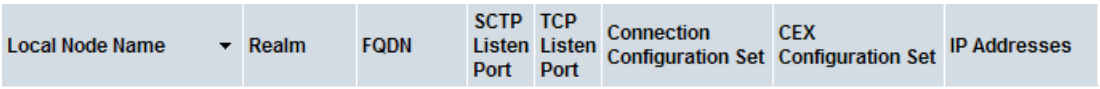


Figure 8: Sorting a Table by Column Header

Page Controls

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

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

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

Table 5: Example Action Buttons

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

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

Some Action buttons take you to another page.

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

Table 6: Submit Buttons

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

Clear Field Control

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

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

Figure 9: Clear Field Control X

Optional Layout Element Toolbar

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

Figure 10: Optional Layout Element Toolbar

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

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

Notifications

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

Figure 11: Automatic Error Notification

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

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

Opening an Element in the Toolbar

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

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

Filters

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

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

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

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

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

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

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

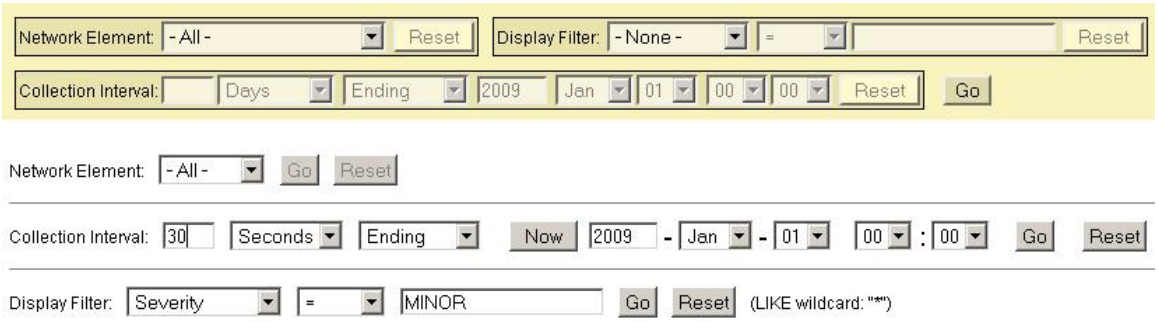


Figure 12: Examples of Filter Styles

Filter Control Elements

This table describes filter control elements of the user interface.

Table 7: Filter Control Elements

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

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

Filtering on the Network Element

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

1. Click **Filter** in the optional layout element toolbar.
2. Select a Network Element from the **Network Element** 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.

Chapter 3

RADIUS Overview

Topics:

This section introduces the RADIUS application, key concepts, and basic functionality.

Overview

RADIUS (Remote Authentication Dial In User Service) is an Authentication, Authorization and Accounting (AAA) protocol that is a predecessor to Diameter. RADIUS is still widely in use, especially in WLAN networks and even some 3G mobile data applications. DSR will be deployed in networks requiring support for both Diameter and RADIUS nodes as well in RADIUS-only networks.

RADIUS has some similarities to Diameter, but is significantly different in many ways. RADIUS is primarily supported on DSR by a new connection layer called the RADIUS Connection Layer (RCL), while using the existing routing services of the Diameter Routing Layer (DRL) and the existing Diameter-based message interface to/from the DRL.

- Ingress RADIUS Request/Response messages are encapsulated in Diameter Request/Answer messages respectively. Diameter Request message content is created by RCL based on a set of predefined rules using both configuration data and RADIUS message content. Diameter Answer message content is created by RCL based on a set of predefined rules using mostly the Diameter Request message content associated with the transaction.
- Because RADIUS Request message routing is based upon the associated Diameter Request message which encapsulates the RADIUS message, the user must be intimately familiar with the how the Diameter Request capsule is created so they can properly configure the DRL to route RADIUS Request messages.
- DRL provides required information to RCL to allow forwarding of RADIUS messages to the peer
- The RCL prevents accidental routing of non-RADIUS messages to a RADIUS connection due to misconfiguration.

RADIUS versus Diameter

Because the Diameter protocol was developed as a fundamental improvement to RADIUS, there are some similarities and significant differences between the two protocols. The protocols have similarities such as transaction requests/responses, Response messages must always be sent along the same path as the Request message, as well as messages comprised of header and set of tag-length-value attributes. Several of the RADIUS attributes have Diameter equivalents in order to support interworking between Diameter and RADIUS networks as shown in *Table 8: Major Differences between Diameter and RADIUS*.

Table 8: Major Differences between Diameter and RADIUS

Diameter	RADIUS
Application IDs	No Application IDs.
Capabilities exchange procedure	Does not exist. Messages supported on a connection are determined through static configuration.
End-to-End Transaction IDs	No End-to-End Transaction IDs.
32-bit Hop-by-Hop ID	8-bit Hop-by-Hop ID (called an Identifier in RADIUS)
Duplicate transactions received by a node from any path can be detected (using the T-bit, Session-ID, End-to-End ID)	A RADIUS Server is able detect that a received Request is a duplicate of a previously received Request message if the Request message have the

Diameter	RADIUS
	same Source IP address, Source Port Number and RADIUS header Identifier values.
Answer contains error code	Transaction responses do not universally contain an error code. When a transaction failure is detected, the most common practice is to discard the Request rather than sending a Response.
Ability to send Congestion response	No ability to indicate congestion. DSR features that are based on the congestion response such as Remote Busy are difficult to support.
Nodes are assigned a FQDN which can be used to address a transaction to a specific Node.	RADIUS transactions can only be addressed to a RADIUS node called a NAS. Transactions sent to a RADIUS authentication or accounting server contain no destination address.
Request messages always contain a universal address (FQDN) of the node that initiated the transaction.	Only transactions initiated by an access node referred to as a NAS must contain an originating node address. However, a NAS can have up to three different address types which are not guaranteed to be unique across networks.
Requests always contain an origin and destination Realm.	Realms are not a fundamental capability of RADIUS. The User-Name attribute may contain a Realm.
Universal Watchdog procedure used for detecting peer node failures must be supported by all Diameter nodes.	RADIUS procedures exist for monitoring a path between RADIUS Peer Nodes (such as Status-Server) but are not mandatory. This RADIUS procedure is not considered a true "watchdog" procedure.
All transactions contain a Session-ID which has the originating node's FQDN making Session-IDs unique across multiple networks.	Not all transactions contain a Session-ID equivalent and there is no guarantee that it is unique across networks.
Command Code identical in Request and Answer	Command Code (Code in RADIUS) is different in Request and Answer (Response in RADIUS).
Transaction path recording and message loop detection (via Route-Record)	Does not exist.
Mandatory/non-mandatory flag for message attributes.	Not supported.

RADIUS and Diameter Command Codes and AVP Codes are defined to prevent overlap/ambiguities. RADIUS Command and AVP codes values are in the range of 1-255, while Diameter values are 256 or more.

RADIUS Messages

The types of RADIUS messages that are supported are:

Table 9: RADIUS Messages

Request	Response(s)
Authentication-Request	Authentication-Accept Authentication-Reject Authentication-Challenge
Accounting-Request	Accounting-Response
CoA-Request	CoA-ACK CoA-NACK
Disconnect-Request	Disconnect-ACK Disconnect-NACK
Status-Server (Receipt from clients only. DSR does not send Status-Server messages).	Authentication-Accept Accounting-Response

With the exception of Status-Server messages, all other messages are routed through the DSR using standard DSR routing rules.

Status-Server messages are queries to the server and are the only RADIUS message for which the DSR generates a RADIUS response message (either none, Access-Accept, or Accounting-Response), depending on how the Ingress Status-Server Configuration Set is configured.

RADIUS Connection Layer

The RCL is a connection layer function that looks identical to the Diameter Connection Layer (DCL) from a signaling perspective. Both RCL and the DCL reside on the same DA-MP. RCL receives RADIUS messages and converts them to Diameter messages suitable for routing by DRL. DRL routing rules can be configured by the operator to forward the message to a RADIUS peer (through a RADIUS connection) or to another DSR (through a Diameter connection). RCL converts Diameter messages received from DRL to RADIUS before forwarding the RADIUS message to the peer.

RCL is designed to make RADIUS transparent to the DRL as much as possible. In order to make the RADIUS protocol completely transparent to the DRL, RCL must be RADIUS-transaction stateful for both ingress and egress transactions.

RADIUS Connections

RADIUS clients initiate transactions. RADIUS servers route/process transactions received from clients and send responses. The RADIUS protocol primarily uses a connectionless datagram service as a transport layer between peer nodes. Although a connectionless transport service is used, RADIUS connections allow a simple adaptation of the Diameter connection oriented feature set for use with

RADIUS. A RADIUS connection is defined as the tuple consisting of a client IP address, a server IP address and a server destination port. Because of the connectionless client-server model, a DSR RADIUS connection is transactionally uni-directional, meaning that DSR can either send or receive RADIUS transactions on a RADIUS connection, but not do both. In this regard, from DSR's perspective, RADIUS connections are configured as either client or server.

- RADIUS Client Connection - A RADIUS connection used by DSR for sending RADIUS Requests and receiving RADIUS Response to/from a RADIUS server node. RCL never forwards RADIUS Requests received from a RADIUS Client Connection.
- RADIUS Server Connection - A RADIUS connection used by DSR for receiving RADIUS Requests and forwarding RADIUS Responses from/to a RADIUS client node. RCL never forwards RADIUS Requests to a RADIUS Server Connection.

RADIUS supports up to 256 outstanding transactions per source IP address and port, owing to the 8-bit Identifier field in the RADIUS header. RADIUS clients that need to send more than 256 outstanding requests typically use more than one source port. DSR does not validate or enforce the source port number for RADIUS requests received from clients. DSR supports the notion of a configurable source port range which is used when forwarding RADIUS requests to a peer.

A DSR RADIUS Server Connection is the association of:

- Source/RADIUS Client's IP Address
- Destination/DSR's IP Address
- Destination/DSR's Port Number

In contrast, a DSR RADIUS Client connection is an association of:

- Source/DSR's IP Address
- Destination/RADIUS Server's IP Address
- Destination/RADIUS Server's Port Number

A port number is configured on DSR to serve as the destination of Requests that are sent by RADIUS clients to DSR. Note that the same DSR (IP address and) port number can be used to configure multiple RADIUS server connections, as long as the clients IP address is unique for each RADIUS server connection.

Message Conversion

RCL receives RADIUS messages from peers (over server connections) and converts them to Diameter to allow them to be routed by DRL. The routable Diameter message is populated with relevant Diameter AVPs using configuration information and information from the RADIUS message. The received RADIUS message is then embedded into the converted Diameter message, providing access to the receiving RADIUS message contents for forwarding.

DRL routes the Diameter message, which eventually ends up in RCL. RCL extracts the embedded RADIUS message from the Diameter message, updates the message, and forwards it to the peer.

RADIUS to Diameter Request Message Conversion

RADIUS Request messages received from a peer node are encapsulated into a Diameter Request message and forwarded to the DRL for routing purposes. DRL Diameter Request message routing is

based on message content, which has basic information such as Application ID, Command Code, source/destination Realms and source/destination node addresses (FQDNs). RCL generates this information using information from the RADIUS message and configuration data. Most of this information does not exist in RADIUS and needs to be inferred by RCL. Network Access Server (NAS) originated messages (e.g. Access-Request, Accounting-Request) typically contain information that can identify the source of the message (NAS-Identifier, IPv4 address, IPv6 address). Similarly, NAS terminated messages (e.g. CoA-Request and Disconnect-Request) typically contain information that can identify the destination of these messages.

Because RADIUS messages lack basic information such as Realms, Application IDs, or the source address of the node which initiated a message to a NAS node, the creation of Diameter Request message content is based both upon the message content, if available, or configuration data associated with the ingress Peer Node or RADIUS connection, if not. The generated Diameter information can then be used to setup appropriate routing rules in DRL.

RCL supports an optional NAS Node that can be used to infer either the origin or the destination host information depending on the type of the RADIUS request. The NAS Node can be populated with information that may be obtained from NAS identifying attributes in the RADIUS message (NAS Identifier, IPv4 address, IPv6 address) which is mapped to an FQDN which may serve as the origin or destination host information. RCL extracts this information from RADIUS requests and attempt to find a matching entry in the NAS Node.

1. NAS Identifier address (NAS-Identifier attribute)
2. IPv4 address (NAS-IP-Address attribute)
3. IPv6 address (NAS-IPv6-Address attribute)

Each instance of address type is used until a match is found or list of addresses found in the message has been exhausted. If no match is found, then the Realm/FQDN associated with the ingress RADIUS Peer Node is used. Multiple instances of each address type may exist. Only the first instance of the NAS Identifier address is added to the search list while all instances of the IPv4 and IPv6 addresses are added to the search list.

The Diameter Application ID and Command Code assigned to the Diameter Request is determined statically using pre-configured mappings read from the Message Conversion Configuration Set. For information on how to view the Message Conversion Configuration Set, refer to *Message Conversion Configuration Set*.

RADIUS to Diameter Answer Message Conversion

RADIUS Response messages received from a peer node are encapsulated into a Diameter Answer message and forwarded to the DRL. The content of the Diameter Answer message header is based upon the content of the corresponding Diameter Request received from the DRL. This information is stored by RCL in the egress transaction record.

Diameter to RADIUS Request Message Conversion

If RCL receives a Diameter Request from DRL containing an embedded RADIUS Request, RCL forwards the RADIUS request on the RADIUS client connection specified by DRL.

If RCL receives a Diameter Request message that doesn't contain an embedded RADIUS Request message, RCL discards the message.

Diameter to RADIUS Answer Message Conversion

RADIUS Response messages received from a peer node are encapsulated into a Diameter Answer message.

If RCL receives a Diameter Answer message containing an embedded RADIUS Response message, RCL forwards the RADIUS Response on the RADIUS connection specified by DRL. The content of the Diameter Answer message header is based upon the content of the corresponding Diameter Request received from the DRL. This information is stored by RCL in the egress transaction record.

If RCL receives a Diameter Request message that doesn't contain an embedded RADIUS Request message, RCL discards the message.

Ingress Transaction Management

Ingress transaction management involves creation and management (including management of lifetime) of ingress transaction records maintained for each new ingress Request received from a client.

Ingress transaction management supports three main functions:

- Avoid creation of duplicate egress transactions resulting from retransmitted ingress requests from clients
- Address potential loss of response sent to the client by caching previously forwarded responses. When the client retransmits a request, the cached response (if available) is forwarded to the client
- Storing the information associated with an ingress transaction which is needed for updating the RADIUS response associated with the transaction

RADIUS clients send Requests to RADIUS servers. Typically, if a RADIUS client does not receive a response in a timely manner, RADIUS clients retransmit the request to the RADIUS server a few times, using the same source IP address, source port, RADIUS Header Identifier and Authenticator, before failing over to an alternate server. If the server receives a request multiple times, and if it cannot detect the request as a duplicate, it could result in the transaction being processed more than once, which is not desirable.

RCL ingress transaction processing supports detecting duplicate requests and preventing duplicate transactions from being processed. When DSR successfully processes a RADIUS request, a response is forwarded to the RADIUS client. Owing to the unreliable nature of the transport protocol, this request might be lost in transit. If the RADIUS client then retransmits the request as a result, RCL has the capability to cache previously sent responses for some time, detect duplicate requests received during that time and forward the previously sent response, thus preventing a duplicate transaction from being processed. This behavior is configured through the **RADIUS Options** tab of the **Connection Configuration Sets** page (refer to the *Diameter User's Guide* for further information on Connection Configuration Sets).

If duplicate ingress transaction detection and prevention for a RADIUS server connection is enabled, RCL supports certain functionalities:

- For each RADIUS Request received on the connection which is not a duplicate transaction, RCL creates an Ingress Transaction Record (ITR) for the transaction. The ITR serves as the mechanism for detecting duplicate ingress transactions.

  Note: The ITRs are searched to determine whether the ingress transaction is a duplicate.

- For each duplicate RADIUS Request received on the connection, RCL discards the message to prevent duplicate processing of the same transaction. If a Response message is cached in the ITR, then RCL resends the Response message back to the RADIUS client. The Response remains cached for a user-configurable lifetime. When the lifetime duration is reached, both the cached Response and ITR are deallocated.
- When a RADIUS response is sent to the RADIUS client for the first time for the transaction, RCL caches a copy of the response in the ITR.

A RADIUS transaction is considered a duplicate if the previously processed Request message and the newly received Request message both contain the same Source IP Address, Source Port Number, Destination IP Address, Destination Port Number, Identifier and Authenticator header fields. RCL can detect a duplicate transaction until the corresponding ITR is present.

Egress Transaction Management

The main functions of egress transaction management are:

- Support DRL controlled RADIUS compliant retransmissions of requests
- Creating, monitoring, and closing of source ports
- RADIUS ID acquisition and release
- Store information for conversion of a RADIUS Response message to a Diameter Answer message

Egress transaction management uses an egress pentransaction manager to support creation, lookup, extraction, and expiration of egress transaction record to support RADIUS compliant retransmission.

Egress transaction management uses a port number and a RADIUS ID to allocate and release RADIUS IDs for use in egress request messages.

The Local Node associated with RADIUS client connections are configured with client port ranges. RADIUS source ports are opened when any client connection associated with a Local Node needs a RADIUS ID and one is not already available. RCL shall create as many source ports as needed to cater to the number of RADIUS IDs required - that are in use (outstanding) waiting for a response.

Authentication of Transactions Between Peers

Transactions between clients and servers are authenticated using a Shared Secret. The NOAM level Shared Secret is used encrypt/decrypt RADIUS messages that have the RADIUS client connection on one site and the corresponding RADIUS server connection on another site (refer to *Network Options* for further information). By contrast, the SOAM Shared Secret must match the Shared Secret configured on the RADIUS peer node connection (refer to *Shared Secret Configuration Sets* for further information).

A RADIUS client and Server that exchange RADIUS messages must use the same Shared Secret when generating and validating authentication information. The recipient of a message uses the provisioned Shared Secret that is associated with the Source IP Address of the packet. For DSR, Shared Secrets are defined via a Shared Secret Configuration Set, an instance of which is assigned to RADIUS connections. Multiple RADIUS connections can be configured with the same Shared Secret if required by the operator.

DSR supports generating and validating the Message-Authenticator attribute before forwarding messages to and after receiving messages from the peer.

Duplicate Transaction Detection

Ingress Duplicate Transaction Detection

A RADIUS Server is able detect that a received Request is a duplicate of a previously received Request message if the Request messages have the same source IP address, Source port number and RADIUS header Identifier field values. Retransmitted Requests sent to the same (Destination IP Address, Destination Port Number) must use the same source IP address, source port number, RADIUS header Identifier and Authenticator field values.

Egress Duplicate Transaction Detection

When DRL forwards a Request message to RCL, an egress transaction record is maintained by RCL, storing the source IP address, source port number, RADIUS Header Identifier and Authenticator in the transaction record indexed by the DRL selected RADIUS client connection. If a Response is not received in a timely manner and DRL reroutes the same Request to the same RADIUS client connection, RCL utilizes previously stored information from this egress transaction record so that the retransmitted Request message has the same information such as source IP address and source port. If DRL fails to receive a response, and reroutes the Request message to a different peer (different RADIUS client connection), a new egress transaction record is created.

Note: For information on DRL configuration information for rerouting, refer to the *Diameter User's Guide*. RCL maintains egress transaction records for the same duration as DRL's Pending Answer Timeout (PAT), until a valid Response is received or this duration expires.

RADIUS-Diameter Interworking Function

RADIUS-Diameter Interworking (RD-IWF) allows the user to decide for which messages and based on which conditions RD-IWF is activated

If RCL is configured not to detect the retransmissions of the same Request and it forwards all Requests (original and retries) to the DRL where the RD-IWF is invoked, the DER message will be updated with the new End-To-End Identifier. The End-To-End Identifiers are unique within a given period only under a single site. If two DA-MPs from two different sites send DER messages to the same Diameter server then they should be configured to include different Origin-Host AVP values in the Diameter messages because the combination of the Origin-Host AVP value and the End-To-End Identifier is used to detect duplicates. The option **Prevent duplicate transactions due to ingress retransmissions** on the **RADIUS Options tab** of the **Diameter** > **Configuration** > **Configuration Sets** > **Connection Configuration Sets** screen determines how DSR processes duplicate requests received from a client.

RCL should be configured to detect the retransmissions of the same Request and to avoid forwarding the retries to the DRL.

In order to configure RD-IWF, enable the Mediation feature, configure appropriate Mediation components, and copy the RD-IWF perl script to the target directory. For information on Mediation and how to configure it, refer to the *Mediation User Guide*.

RADIUS Alarms, KPIs, Measurements, and Metrics

This section describes how to access alarm, KPI, measurement, and metric information that is available for RADIUS in the DSR GUI. Refer to the *Alarms and KPIs Reference* for detailed alarm and KPI information, *Measurements Reference* for detailed measurement information, and *Diameter Common User's Guide* for detailed metric information.

Active alarms and events, as well as alarm and event history can be displayed on the **Alarms & Events** > **View Active** and **Alarms & Events** > **View History** GUI pages.

Key Performance Indicators, or KPIs, provide a means to convey performance information to the user in near real-time. KPIs can be displayed on the **Status & Manage** > **KPIs** GUI page.

Measurements for RADIUS are collected and reported in various measurement groups. A measurement report and measurement group can be associated with a one-to-one relationship. Measurement reports may be generated from the **Measurements** > **Report** GUI page.

Metrics are collected and displayed on the DSR Dashboard. Dashboard metrics can be displayed from the **Diameter Common** > **Configuration** > **Metric Groups** NOAM GUI page.

Assumptions and Limitations

- DNS is not supported.
- Message Priority Configuration is not supported for RADIUS messages. Message priority settings are limited to fixed assignments of Priority=0 for Requests and Priority=3 for Answers
- Floating/IPFE RADIUS connections are not supported
- Remote Busy is not supported for RADIUS connections
- Receipt and response to Status-Server message is supported. Sending of Status-Server message to query status of RADIUS servers is not currently supported
- RADIUS over TCP is not supported

Chapter 4

Configuration

Topics:

This section describes the RADIUS application GUI pages.

RADIUS Configuration Overview

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

Pre-Configuration Activities

Before RADIUS configuration can be performed, certain activities need to be performed in the system:

- Gather component information that is required for Diameter and RADIUS configuration, including component item naming conventions and names, IP addresses, hostnames, and numbers of items to be configured.
- Configure Diameter Configuration components that are required for RADIUS configuration. See *Diameter Configuration for RADIUS* for more information.
- If running Radius to Diameter traffic is planned, the Mediation application must be activated. Refer to the *Mediation User's Guide* for activation information.

Diameter Configuration for RADIUS

Diameter configurations must be done before RADIUS configuration can be performed.

All Diameter Configuration for RADIUS is done using the SOAM GUI.

Use the explanations and procedures in the Diameter Configuration help and the *Diameter User's Guide* to complete the Diameter configuration, including the Diameter components needed for use with RADIUS.

1. **Local Nodes**

   Use the **Diameter** > **Configuration** > **Local Nodes [Insert]** page to configure the Local Nodes for RADIUS client port ranges and server listening ports.

   It is also possible to create a separate Local Node for RADIUS connections if desired or use a single Local Node for both RADIUS and Diameter capability.

2. **Peer Nodes**

   Use the **Diameter** > **Configuration** > **Peer Nodes [Insert]** page to configure the Peer Nodes for RADIUS client port ranges and server listening ports.

3. **Connections**

   Use the **Diameter** > **Configuration** > **Connections [Insert]** page to configure new connections

4. **Route Groups**

   Use the **Diameter** > **Configuration** > **Route Groups [Insert]** page to configure new route groups

5. **Connection Configuration Sets**

   Use the Radius Options tab on the **Diameter** > **Configuration** > **Configuration Sets** > **Connection Configuration Sets [Insert]** page to configure new Connection Configuration Sets.

6. **System Options**

   Use the RADIUS UDP Options tab on the **Diameter** > **Configuration** > **System Options** to configure System Options for RADIUS

7. **Configuration Capacity**

   Use the **Diameter** > **Configuration** > **Capacity Summary** to configure Configuration Capacity for RADIUS.

RADIUS NOAM Configuration

This section describes the **RADIUS** > **Configuration** GUI pages on the NOAM.

Network Options

On the **RADIUS** > **Configuration** > **Network Options** page on an NOAM displays the existing Network-scoped Shared Secret.

The fields are described in *Network Options elements*.

Network Options elements

Table 10: Network Options Elements describes the elements on the **RADIUS** > **Configuration** > **Network Options** page on the NOAM.

Table 10: Network Options Elements

Fields (* indicates a required field)	Description	Data Input Notes
Network-scoped Shared Secret*	A unique RADIUS Shared Secret to be used across the network. It can contain characters: a-z, A-Z, 0-9, and the special characters ~!@#$%^&*()_+ | \=-'{}[]:"';<>?/.,	Format: Text box Default: N/A Range: 10-128 ASCII character string

Inserting Network Options

Use this task to configure Network Options on the NOAM.

The fields are described in *Table 10: Network Options Elements*.

1. Select **RADIUS** > **Configuration** > **Network Options**.
   The **RADIUS** > **Configuration** > **Network Options** page appears.
2. Enter a unique **Network-scoped Shared Secret**.

   Note: The NOAM Shared Secret is used encrypt/decrypt RADIUS messages that have the RADIUS client connection on one site and the corresponding RADIUS server connection on another site.

3. Click **Apply**.

RADIUS SOAM Configuration

This section describes the **RADIUS** > **Configuration** GUI pages on the SOAM.

Configuration Sets

On the **RADIUS** > **Configuration** page on an SOAM, the following **Configuration Sets** can be configured:

- Message Authenticator Configuration Sets
- Shared Secret Configuration Sets
- Ingress Status Server Configuration Sets
- Message Conversion Configuration Sets (read only)

Message Authenticator Configuration Sets

On the **RADIUS** > **Configuration** > **Configuration Sets** > **Message Authenticator Configuration Sets** page on an SOAM, various actions can be performed:

- Filter the list of Message Authenticator Configuration Sets
- Sort the list of entries in ascending or descending order. There are 2 separate tabs with entries that can be sorted.

  On the **Server Connections Options** tab, the entries can be sorted by Message Authenticator Set Name, Encode Message-Authenticator in response to Status-Server, Encode Message-Authenticator in egress to Access-Accept, Encode Message-Authenticator in egress to Access-Reject, Encode Message-Authenticator in egress to Access-Challenge, Encode Message-Authenticator in egress CoA-ACK, Encode Message-Authenticator in egress CoA-NACK, Encode Message-Authenticator in egress Disconnect-ACK, or Encode Message-Authenticator in egress Disconnect-NACK.

  On the **Client Connections Options** tab, the entries can be sorted by Message Authenticator Set Name, Encode Message-Authenticator in egress Access-Request, Encode Message-Authenticator in egress CoA-Request, or Encode Message-Authenticator in egress Disconnect-Request

- Click **Insert**.

  The **RADIUS** > **Configuration** > **Configuration Sets** > **Message Authenticator Configuration Sets [Insert]** page opens. New Message Authenticator Configuration sets can be added. See *Inserting Message Authenticator Configuration Sets*.

- Select a Message Authenticator Configuration Set Name and click **Edit**.

  The **RADIUS** > **Configuration** > **Configuration Sets** > **Message Authenticator Configuration Sets [Edit]** page opens. The selected Message Authenticator Configuration Set Name can be edited. See *Editing Message Authenticator Configuration Sets*.

- Select a Message Authenticator Configuration Set Name and click **Delete**.

  The selected Message Authenticator Configuration Set Name is deleted. See *Deleting Message Authenticator Configuration Sets*.

The fields are described in *Message Authenticator Configuration Sets elements*.

Message Authenticator Configuration Sets elements

Table 11: Message Authenticator Configuration Sets Elements describes the elements on the **RADIUS** > **Configuration** > **Configuration Sets** > **Message Authenticator Configuration Sets** page on the SOAM.

Table 11: Message Authenticator Configuration Sets Elements

Fields (* indicates a required field)	Description	Data Input Notes
Message Authenticator Set Name*	A name that uniquely identifies the Message Authenticator Set	Format: Text box Default: N/A Range: A 32-character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit
Server Connections Options tab		
Encode Message-Authenticator in response to Status-Server	Specifies whether DSR should add a Message-Authenticator attribute to the Accounting-Response or Access-Accept message that is sent in response to a Status-Server request.	Format: Check box Default: No Range: Yes, No
Encode Message-Authenticator in egress Access-Accept	Specifies whether DSR should add a Message-Authenticator attribute to a RADIUS Access-Accept message prior to forwarding the message to the RADIUS connection. If the message contains an EAP-Message attribute, a Message-Authenticator will be added and this attribute will be ignored by DSR.	Format: Check box Default: No Range: Yes, No
Encode Message-Authenticator in egress Access-Reject	Specifies whether DSR should add a Message-Authenticator attribute to a RADIUS Access-Reject message prior to forwarding the message to the RADIUS connection. If the message contains an EAP-Message attribute, a Message-Authenticator will be added and this attribute will be ignored by DSR.	Format: Check box Default: No Range: Yes, No
Encode Message-Authenticator in egress Access-Challenge	Specifies whether DSR should add a Message-Authenticator attribute to a RADIUS Access-Challenge message prior to forwarding the message to the RADIUS connection. If the message contains an EAP-Message attribute, a Message-Authenticator will be added and this attribute will be ignored by DSR.	Format: Check box Default: No Range: Yes, No

Fields (* indicates a required field)	Description	Data Input Notes
Encode Message-Authenticator in egress CoA-ACK	Specifies whether DSR should add a Message-Authenticator attribute to a RADIUS CoA-ACK message prior to forwarding the message to the RADIUS connection.	Format: Check box Default: No Range: Yes, No
Encode Message-Authenticator in egress CoA-NACK	Specifies whether DSR should add a Message-Authenticator attribute to a RADIUS CoA-NACK message prior to forwarding the message to the RADIUS connection.	Format: Check box Default: No Range: Yes, No
Encode Message-Authenticator in egress Disconnect-ACK	Specifies whether DSR should add a Message-Authenticator attribute to a RADIUS Disconnect-ACK message prior to forwarding the message to the RADIUS connection.	Format: Check box Default: No Range: Yes, No
Encode Message-Authenticator in egress Disconnect-NACK	Specifies whether DSR should add a Message-Authenticator attribute to a RADIUS Disconnect-NACK message prior to forwarding the message to the RADIUS connection.	Format: Check box Default: No Range: Yes, No
Client Connections Options tab		
Encode Message-Authenticator in egress Access-Request	Specifies whether DSR should add a Message-Authenticator attribute to a RADIUS Access-Request message prior to forwarding the message to the RADIUS connection. If the message contains an EAP-Message attribute, a Message-Authenticator will be added and this attribute will be ignored by DSR.	Format: Check box Default: No Range: Yes, No
Encode Message-Authenticator in egress CoA-Request	Specifies whether DSR should add a Message-Authenticator attribute to a RADIUS CoA-Request message prior to forwarding the message to the RADIUS connection.	Format: Check box Default: No Range: Yes, No
Encode Message-Authenticator in egress Disconnect-Request	Specifies whether DSR should add a Message-Authenticator attribute to a RADIUS Disconnect-Request message prior to forwarding the message to the RADIUS connection.	Format: Check box Default: No Range: Yes, No

Inserting Message Authenticator Configuration Sets

Use this task to add a new Message Authenticator Configuration Set on the SOAM.

The fields are described in *Table 11: Message Authenticator Configuration Sets Elements*.

1. Select **RADIUS** > **Configuration** > **Configuration Sets** > **Message Authenticator Configuration Sets**.

The **RADIUS** > **Configuration** > **Configuration Sets** > **Message Authenticator Configuration Sets** page appears.

2. Click **Insert**.
   The **RADIUS** > **Configuration** > **Configuration Sets** > **Message Authenticator Configuration Sets [Insert]** page appears.
3. Enter a unique **Message Authenticator Set Name**.
4. On the **Server Connections Options** tab:
   a) Check or uncheck the **Encode Message-Authenticator in response to Status-Server** box.
   b) Check or uncheck the **Encode Message-Authenticator in egress Access-Accept** box.
   c) Check or uncheck the **Encode Message-Authenticator in egress Access-Reject** box.
   d) Check or uncheck the **Encode Message-Authenticator in egress Access-Challenge** box.
   e) Check or uncheck the **Encode Message-Authenticator in egress CoA-ACK** box.
   f) Check or uncheck the **Encode Message-Authenticator in egress CoA-NACK** box.
   g) Check or uncheck the **Encode Message-Authenticator in egress Disnconnect-ACK** box.
   h) Check or uncheck the **Encode Message-Authenticator in egress Disnconnect-NACK** box.
5. On the **Client Connections Options** tab:
   a) Check or uncheck the **Encode Message-Authenticator in egress Access-Request** box.
   b) Check or uncheck the **Encode Message-Authenticator in egress CoA-Request** box.
   c) Check or uncheck the **Encode Message-Authenticator in egress Disconnect-Request** box.

Editing Message Authenticator Configuration Sets

Use this task to edit configured Message Authenticator Configuration Sets on the SOAM.

The fields are described in *Ingress Status Server Configuration Sets elements*.

1. Select **RADIUS** > **Configuration** > **Configuration Sets** > **Message Authenticator Configuration Sets**.
   The **RADIUS** > **Configuration** > **Configuration Sets** > **Message Authenticator Configuration Sets** page appears.
2. Click **Edit**.
   The **RADIUS** > **Configuration** > **Configuration Sets** > **Message Authenticator Configuration Sets [Edit]** page appears.
3. Edit the unique **Message Authenticator Set Name**.
4. On the **Server Connections Options** tab:
   a) Check or uncheck the **Encode Message-Authenticator in response to Status-Server** box.
   b) Check or uncheck the **Encode Message-Authenticator in egress Access-Accept** box.
   c) Check or uncheck the **Encode Message-Authenticator in egress Access-Reject** box.
   d) Check or uncheck the **Encode Message-Authenticator in egress Access-Challenge** box.
   e) Check or uncheck the **Encode Message-Authenticator in egress CoA-ACK** box.
   f) Check or uncheck the **Encode Message-Authenticator in egress CoA-NACK** box.
   g) Check or uncheck the **Encode Message-Authenticator in egress Disnconnect-ACK** box.
   h) Check or uncheck the **Encode Message-Authenticator in egress Disnconnect-NACK** box.
5. On the **Client Connections Options** tab:
   a) Check or uncheck the **Encode Message-Authenticator in egress Access-Request** box.
   b) Check or uncheck the **Encode Message-Authenticator in egress CoA-Request** box.

c) Check or uncheck the **Encode Message-Authenticator in egress Disconnect-Request** box.

Deleting Message Authenticator Configuration Sets

Use this task to delete configured Message Authenticator Configuration Sets on the SOAM.

The fields are described in *Table 11: Message Authenticator Configuration Sets Elements*.

1. Select **RADIUS** > **Configuration** > **Configuration Sets** > **Message Authenticator Configuration Sets**.

   The **RADIUS** > **Configuration** > **Configuration Sets** > **Message Authenticator Configuration Sets** page appears.
2. Select the **Message Authenticator Set Name** to be deleted.
3. Click **Delete**.
   A popup window appears to confirm the delete.
4. Click

   - **OK** to delete the **Message Authenticator Set Name**.
   - **Cancel** to cancel the delete function and return to the **RADIUS** > **Configuration** > **Configuration Sets** > **Message Authenticator Configuration Sets** page.

   If **OK** is clicked and the selected **Message Authenticator Set Name** no longer exists, an error message is displayed. The page is refreshed and the deleted **Message Authenticator Set Name** no longer appears on the page.

Shared Secret Configuration Sets

On the **RADIUS** > **Configuration** > **Configuration Sets** > **Shared Secret Configuration Sets** page on an SOAM, various actions can be performed:

- Filter the list of Shared Secret Configuration Sets
- Sort the list of entries in ascending or descending order by Shared Secret Name.
- Click **Insert**.

  The **RADIUS** > **Configuration** > **Configuration Sets** > **Shared Secret Configuration Sets [Insert]** page opens. New Shared Secret Configuration sets can be added. See *Inserting Shared Secret Configuration Sets*.
- Select an Shared Secret Configuration Set Name and click **Edit**.

  The **RADIUS** > **Configuration** > **Configuration Sets** > **Shared Secret Configuration Sets [Edit]** page opens. The selected Shared Secret Configuration Set Name can be edited. See *Editing Shared Secret Configuration Sets*.
- Select a Shared Secret Configuration Set Name and click **Delete**.

  The selected Shared Secret Configuration Set Name is deleted. See *Deleting Shared Secret Configuration Sets*.

The fields are described in *Shared Secret Configuration Sets elements*.

Shared Secret Configuration Sets elements

Table 12: Shared Secret Configuration Sets Elements describes the elements on the **RADIUS** > **Configuration** > **Configuration Sets** > **Shared Secret Configuration Sets** page on the SOAM.

Table 12: Shared Secret Configuration Sets Elements

Fields (* indicates a required field)	Description	Data Input Notes
Shared Secret Name*	A name that uniquely identifies the Shared Secret	Format: Text box Default: N/A Range: A 32-character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit
Shared Secret*	A unique RADIUS Shared Secret to be used with the peer. It can contain characters: a-z, A-Z, 0-9, and the special characters ~!@#$%^&*()_+ | \=-'{}[]:"';<>?/.,	Format: Text box Default: N/A Range: 10-128 ASCII character string

Inserting Shared Secret Configuration Sets

Use this task to add a new Shared Secret Configuration Set on the SOAM.

Note: The SOAM Shared Secret must match the Shared Secret configured on the RADIUS peer node connection.

The fields are described in *Table 12: Shared Secret Configuration Sets Elements*.

1. Select **RADIUS** > **Configuration** > **Configuration Sets** > **Shared Secret Configuration Sets**.
   The **RADIUS** > **Configuration** > **Configuration Sets** > **Shared Secret Configuration Sets** page appears.
2. Click **Insert**.
   The **RADIUS** > **Configuration** > **Configuration Sets** > **Shared Secret Configuration Sets [Insert]** page appears.
3. Enter a unique **Shared Secret Name**.
4. Enter a unique **Shared Secret**.

Editing Shared Secret Configuration Sets

Use this task to edit a Shared Secret Configuration Set on the SOAM.

The fields are described in *Table 12: Shared Secret Configuration Sets Elements*.

1. Select **RADIUS** > **Configuration** > **Configuration Sets** > **Shared Secret Configuration Sets**.
   The **RADIUS** > **Configuration** > **Configuration Sets** > **Shared Secret Configuration Sets** page appears.
2. Click **Edit**.
   The **RADIUS** > **Configuration** > **Configuration Sets** > **Shared Secret Configuration Sets [Edit]** page appears.
3. Edit the unique **Shared Secret Name**.
4. Edit the unique **Shared Secret**.

Deleting Shared Secret Configuration Sets

Use this task to delete configured Shared Secret Configuration Sets on the SOAM.

The fields are described in *Table 12: Shared Secret Configuration Sets Elements*.

1. Select **RADIUS** > **Configuration** > **Configuration Sets** > **Shared Secret Configuration Sets**.
   The **RADIUS** > **Configuration** > **Configuration Sets** > **Shared Secret Configuration Sets** page appears.
2. Select the **Shared Secret Name** to be deleted.
3. Click **Delete**.
   A popup window appears to confirm the delete.
4. Click
   - **OK** to delete the **Shared Secret Name**.
   - **Cancel** to cancel the delete function and return to the **RADIUS** > **Configuration** > **Configuration Sets** > **Shared Secret Configuration Sets** page.

   If **OK** is clicked and the selected **Shared Secret Set Name** no longer exists, an error message is displayed. The page is refreshed and the deleted **Shared Secret Name** no longer appears on the page.

Ingress Status Server Configuration Sets

On the **RADIUS** > **Configuration** > **Configuration Sets** > **Ingress Status Server Configuration Sets** page on an SOAM, various actions can be performed:

- Filter the list of Ingress Status Server Configuration Sets
- Sort the list of entries in ascending or descending order by Ingress Status-Server Configuration Set Name, Send Response to Status-Server, or Status-Server Response Message Type.
- Click **Insert**.

  The **RADIUS** > **Configuration** > **Configuration Sets** > **Ingress Status Server Configuration Sets [Insert]** page opens. New Ingress Status Server Configuration sets can be added. See *Inserting Ingress Status Server Configuration Sets*.

- Select an Ingress Status-Server Configuration Set Name and click **Edit**.

  The **RADIUS** > **Configuration** > **Configuration Sets** > **Ingress Status Server Configuration Sets [Edit]** page opens. The selected Ingress Status-Server Configuration Set Name can be edited. See *Editing Ingress Status Server Configuration Sets*.

- Select an Ingress Status-Server Configuration Set Name and click **Delete**.

  The selected Ingress Status-Server Configuration Set Name is deleted. See *Deleting Ingress Status Server Configuration Sets*.

The fields are described in *Ingress Status Server Configuration Sets elements*.

Ingress Status Server Configuration Sets elements

Table 13: Ingress Status Server Configuration Sets Elements describes the elements on the **RADIUS** > **Configuration** > **Configuration Sets** > **Ingress Status Server Configuration Sets** page on the SOAM.

Table 13: Ingress Status Server Configuration Sets Elements

Fields (* indicates a required field)	Description	Data Input Notes
Ingress Status-Server Set Name*	A name that uniquely identifies the Ingress Status-Server Configuration Set	Format: Text box Default: N/A Range: A 32-character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit
Send Response to Status-Server	Specify whether DSR should silently discard incoming Status-Server messages	Format: Check box Default: Yes Range: Yes, No
Status-Server Response Message Type	Identify Status-Server Response message Type	Format: Radio button Default: Account-Response Range: Accounting-Response, Access-Accept

Inserting Ingress Status Server Configuration Sets

Use this task to add a new Ingress Status Server Configuration Set on the SOAM.

The fields are described in *Ingress Status Server Configuration Sets elements*.

1. Select **RADIUS** > **Configuration** > **Configuration Sets** > **Ingress Status Server Configuration Sets**.

   The **RADIUS** > **Configuration** > **Configuration Sets** > **Ingress Status Server Configuration Sets** page appears.
2. Click **Insert**.
   The **RADIUS** > **Configuration** > **Configuration Sets** > **Ingress Status Server Configuration Sets [Insert]** page appears.
3. Enter a unique **Ingress Status-Server Set Name**.
4. Check or uncheck the **Send Response to Status-Server** box.
5. Select a **Status-Server Response Message Type**.

Editing Ingress Status Server Configuration Sets

Use this task to edit configured Ingress Status Server Configuration Sets on the SOAM.

The fields are described in *Ingress Status Server Configuration Sets elements*.

1. Select **RADIUS** > **Configuration** > **Configuration Sets** > **Ingress Status Server Configuration Sets**.

   The **RADIUS** > **Configuration** > **Configuration Sets** > **Ingress Status Server Configuration Sets** page appears.
2. Click **Edit**.

The **RADIUS** > **Configuration** > **Configuration Sets** > **Ingress Status Server Configuration Sets [Edit]** page appears.

3. Check or uncheck the **Send Response to Status-Server** box.
4. Select a **Status-Server Response Message Type**.

Deleting Ingress Status Server Configuration Sets

Use this task to delete configured Ingress Status Server Configuration Sets on the SOAM.

The fields are described in *Ingress Status Server Configuration Sets elements*.

1. Select **RADIUS** > **Configuration** > **Configuration Sets** > **Ingress Status Server Configuration Sets**.

   The **RADIUS** > **Configuration** > **Configuration Sets** > **Ingress Status Server Configuration Sets** page appears.
2. Select the **Ingress Status-Server Set Name** to be deleted.
3. Click **Delete**.
   A popup window appears to confirm the delete.
4. Click

   - **OK** to delete the **Ingress Status-Server Set Name**.
   - **Cancel** to cancel the delete function and return to the **RADIUS** > **Configuration** > **Configuration Sets** > **Ingress Status Server Configuration Sets** page.

   If **OK** is clicked and the selected **Ingress Status-Server Set Name** no longer exists, an error message is displayed. The page is refreshed and the deleted **Ingress Status-Server Set Name** no longer appears on the page.

Message Conversion Configuration Set

The **RADIUS** > **Configuration** > **Configuration Sets** > **Message Conversion Configuration Set** page on an SOAM displays the existing Message Conversion Set Names.

Note: This set is read-only.

The fields are described in *Message Conversion Configuration Set elements*.

Message Conversion Configuration Set elements

Table 14: Message Conversion Configuration Set Elements describes the elements on the **RADIUS** > **Configuration** > **Configuration Sets** > **Message Conversion Configuration Set** page on the NOAM.

Table 14: Message Conversion Configuration Set Elements

Fields (* indicates a required field)		Description	Data Input Notes
Message Conversion Set Name			Format: Read only
Message Conversion Set Rules	Conversion Type	Specifies the type of conversion that this rule applies	Format: Read only
	Radius Code	The 8-bit RADIUS message code header	

Fields (* indicates a required field)		Description	Data Input Notes
	Diameter Application ID	The 32-bit Diameter message Application ID	
	Diameter Command Code	The 24-bit Diameter message Command Code	

NAS Node

On the **RADIUS** > **Configuration** > **NAS Node** page on an SOAM, various actions can be performed:

- Filter the list of NAS Nodes
- Sort the list of entries in ascending or descending order by NAS Node Name, FQDN, Realm, or NAS Node Identifier.
- Click **Insert**.

  The **RADIUS** > **Configuration** > **NAS Node [Insert]** page opens. New NAS Nodes can be added. See *Inserting an NAS Node*.

- Select an NAS Node and click **Edit**.

  The **RADIUS** > **Configuration** > **NAS Node [Edit]** page opens. The selected NAS Node can be edited. See *Editing an NAS Node*.

- Select an NAS Node and click **Delete**.

  The selected NAS NODE is deleted. See *Deleting an NAS Node*.

NAS Node elements

Table 15: NAS Node Elements describes the elements on the **RADIUS** > **Configuration** > **Ingress NAS Node** page on the SOAM.

Table 15: NAS Node Elements

Fields (* indicates a required field)	Description	Data Input Notes
NAS Node Name*	A name that uniquely identifies the NAS Node	Format: Text box Default: N/A Range: A 32-character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit
Realm*	Realm of an NAS Node	Format: Text box

Fields (* indicates a required field)	Description	Data Input Notes
	A Realm defines the scope over which all NAS addresses (NAS-Identifier, NAS-IP-Addresses, and NAS-IPV6-Addresses) are unique. Realm is a case-sensitive string consisting of a list of labels separated by dots, where a label may contain letters, digits, dashes (-), and underscores (_). A label must start with a letter, digit, or underscore and must end with a letter or digit. Underscores may be used only as the first character. A label must be at most 63 characters long and a Realm must be at most 255 characters long.	Default: N/A Range: A valid Realm
FQDN*	Fully Qualified Domain Name of an NAS Node FQDN is a case-insensitive string consisting of a list of labels separated by dots, where a label may contain letters, digits, dashes (-), and underscores (_). A label must start with a letter, digit, or underscore and must end with a letter or digit. Underscores may be used only as the first character. A label must be at most 63 characters long and a FQDN must be at most 255 characters long.	Format: Text box Default: N/A Range: A valid FQDN
NAS Node Identifier	A unique String to identify the NAS originating Requests. The NAS-Identifier attribute is a string that contains alphanumeric characters and the special characters ~!@ #$%^&*()_+ | \=-'{}[]:"';<>?/.,	Format: Text box Default: N/A Range: 1-253 characters
NAS IP Addresses	The IP address list of an NAS Node. A maximum of 2 IPv4 and a maximum of 2 IPV6 addresses are supported	Format: Text box Default: N/A Range: 1-4 entries **Note:** There is support of 0 to 2 IPv4 addresses and 0 to 2 IPv6 addresses.

Inserting an NAS Node

Use this task to add a new NAS Node on the SOAM.

The fields are described in *Table 15: NAS Node Elements*.

1. Select **RADIUS** > **Configuration** > **NAS Node**.
   The **RADIUS** > **Configuration** > **NAS Node** page appears.
2. Click **Insert**.

The **RADIUS** > **Configuration** > **NAS Node [Insert]** page appears.

3. Enter a unique **NAS Node Name**.
4. Enter a unique **Realm**.
5. Enter a unique **FQDN**.
6. Enter a unique **NAS Node Identifier**.
7. Enter an **NAS IP Address**.

Editing an NAS Node

Use this task to edit an NAS Node on the SOAM.

The fields are described in *Table 15: NAS Node Elements*.

1. Select **RADIUS** > **Configuration** > **NAS Node**.
   The **RADIUS** > **Configuration** > **NAS Node** page appears.
2. Click **Edit**.
   The **RADIUS** > **Configuration** > **NAS Node [Edit]** page appears.
3. Edit the unique **NAS Node Name**.
4. Edit the unique **Realm**.
5. Edit the unique **FQDN**.
6. Edit the unique **NAS Node Identifier**.
7. Edit an **NAS IP Address**.

Deleting an NAS Node

Use this task to delete an NAS Node on the SOAM.

The fields are described in *Table 15: NAS Node Elements*.

1. Select **RADIUS** > **Configuration** > **NAS Node**.
   The **RADIUS** > **Configuration** > **NAS Node** page appears.
2. Select the **NAS Node Name** to be deleted.
3. Click **Delete**.
   A popup window appears to confirm the delete.
4. Click
   - **OK** to delete the **NAS Node Name**.
   - **Cancel** to cancel the delete function and return to the **RADIUS** > **Configuration** > **NAS Node** page.

   If **OK** is clicked and the selected **NAS Node Name** no longer exists, an error message is displayed. The page is refreshed and the deleted **NAS Node Name** no longer appears on the page.

Post-Configuration Activities

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

- Enable Diameter Connections with Peer Nodes
- Enabled RADIUS Connections with Peer Nodes
- Status Verification

Bulk Import and Export

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

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

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

Bulk Import

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

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

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

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

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

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

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

Multiple Import operations can be performed:

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

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

Bulk Export

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

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

Configuration data can be exported in one Export operation:

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

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

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

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

Glossary

A

AVP — Attribute-Value Pair

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

C

CTF — Charging Trigger Function

D

DCA — DOIC Capabilities Announcement

DCL — Diameter Connection Layer

The software layer of the stack which implements Diameter transport connections.

DNS — Domain Name System

A system for converting Internet host and domain names into IP addresses.

DRA — Diameter Routing Agent

A functional element in a 3G or 4G (such as LTE) wireless network that provides real-time routing capabilities to ensure that messages are routed among the correct elements in a network.

D

DRL	Diameter Routing Layer - The software layer of the stack that implements Diameter routing.
DSCP	Differentiated Services Code Point Provides a framework and building blocks to enable deployment of scalable service discrimination in the internet. The differentiated services are realized by mapping the code point contained in a field in the IP packet header to a particular forwarding treatment or per-hop behavior (PHB). Differentiated services or DiffServ is a computer networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying and managing network traffic and providing quality of service (QoS) on modern IP networks.

G

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

H

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

I

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

K

KPI	Key Performance Indicator

L

LDAP	Lightweight Directory Access Protocol A protocol for providing and receiving directory information in a TCP/IP network.

M

MAP	Mobile Application Part An application part in SS7 signaling for mobile communications systems.

M

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

N

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

O

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

P

P

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

R

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

S

S

SBR	Session Binding Repository A highly available, distributed database for storing Diameter session binding data.
SFTP	SSH File Transfer Protocol (sometimes also called Secure File Transfer Protocol) A client-server protocol that allows a user on one computer to transfer files to and from another computer over a TCP/IP network over any reliable data stream. It is typically used with version two of the SSH protocol.
SNMP	Simple Network Management Protocol. An industry-wide standard protocol used for network management. The SNMP agent maintains data variables that represent aspects of the network. These variables are called managed objects and are stored in a management information base (MIB). The SNMP protocol arranges managed objects into groups.
SOAM	System Operations, Administration, and Maintenance
SS7	Signaling System #7 A communications protocol that allows signaling points in a network to send messages to each other so that voice and data connections can be set up between these signaling points. These messages are sent over its own

S

network and not over the revenue producing voice and data paths. The EAGLE is an STP, which is a device that routes these messages through the network.

T

TSA

Target Set Address

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

U

UDR

User Data Repository

A logical entity containing user data.