Oracle® Communications Diameter Signaling Router

RADIUS User Guide

Release 9.0.0.0.0
F79186-01
April 2023

Oracle Communications Diameter Signaling Router RADIUS User Guide, Release 9.0.0.0.0

F79186-01

Contents

My Oracle Support

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

Call the Customer Access Support 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 My Oracle Support, select **2**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

What's New in This Guide

This section introduces the documentation updates for release 9.0.0.0.0.

Release 9.0.0.0.0 - F79186-01, April 2023

Updated the range to 8-128 ASCII character string for Network-scoped Shared Secret field in Network Options elements and Shared Secret Configuration Sets elements sections.

1 Introduction

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

1.1 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

1.2 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.

1.3 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.
- #unique_19 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.

1.4 Documentation Admonishments

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

Table 1-1 Admonishments

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

1.5 Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center 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 **Oracle Communications documentation** link.

   The Communications Documentation page displays. Most products covered by these documentation sets display under the headings Network Session Delivery and Control Infrastructure and Platforms.
4. Click on your product and then the release number.

   A list of the documentation set for the selected product and release displays.
5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

1.6 Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training at http://education.oracle.com/communication.

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site at www.oracle.com/education/contacts.

1.7 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 system ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

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

2
RADIUS Overview

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

2.1 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.

2.1.1 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 2-1.

Table 2-1 Major Differences between Diameter and RADIUS

Diameter	RADIUS
Application IDs	No Application IDs.

Table 2-1 (Cont.) Major Differences between Diameter and RADIUS

Diameter	RADIUS
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 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.

2.2 RADIUS Messages

The types of RADIUS messages that are supported are:

Table 2-2 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.

2.3 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.

2.4 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.

2.5 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.

2.5.1 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.

2.5.2 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.

2.5.3 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.

2.5.4 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.

2.6 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.

2.7 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.

2.8 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.

2.9 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.

2.10 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**, and then **Configuration**, and then **Configuration Sets**, and then **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*.

2.11 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**, and then **View Active** and **Alarms & Events**, and then **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**, and then **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**, and then **Report** GUI page.

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

2.12 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

3
Configuration

This section describes the RADIUS application GUI pages.

3.1 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.

3.2 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.

3.2.1 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**, and then **Configuration**, and then **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**, and then **Configuration**, and then **Peer Nodes [Insert]** page to configure the Peer Nodes for RADIUS client port ranges and server listening ports.
3. **Connections**
   Use the **Diameter**, and then **Configuration**, and then **Connections [Insert]** page to configure new connections
4. **Route Groups**
   Use the **Diameter**, and then **Configuration**, and then **Route Groups [Insert]** page to configure new route groups

5. **Connection Configuration Sets**
   Use the Radius Options tab on the **Diameter**, and then **Configuration**, and then **Configuration Sets**, and then **Connection Configuration Sets [Insert]** page to configure new Connection Configuration Sets.
6. **System Options**
   Use the RADIUS UDP Options tab on the **Diameter**, and then **Configuration**, and then **System Options** to configure System Options for RADIUS
7. **Configuration Capacity**
   Use the **Diameter**, and then **Configuration**, and then **Capacity Summary** to configure Configuration Capacity for RADIUS.

3.3 RADIUS NOAM Configuration

This section describes the **RADIUS**, and then **Configuration** GUI pages on the NOAM.

3.3.1 Network Options

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

The fields are described in Network Options elements.

3.3.1.1 Network Options elements

Table 3-1 describes the elements on the **RADIUS**, and then **Configuration**, and then **Network Options** page on the NOAM.

Table 3-1 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: 8-128 ASCII character string

3.3.1.2 Inserting Network Options

Use this task to configure Network Options on the NOAM.

The fields are described in Table 3-1.

1. Select **RADIUS**, and then **Configuration**, and then **Network Options**.

   The **RADIUS**, and then **Configuration**, and then **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**.

3.4 RADIUS SOAM Configuration

This section describes the **RADIUS**, and then **Configuration** GUI pages on the SOAM.

3.4.1 Configuration Sets

On the **RADIUS**, and then **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)

3.4.1.1 Message Authenticator Configuration Sets

On the **RADIUS**, and then **Configuration**, and then **Configuration Sets**, and then **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**, and then **Configuration**, and then **Configuration Sets**, and then **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**, and then **Configuration**, and then **Configuration Sets**, and then **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.

3.4.1.1.1 Message Authenticator Configuration Sets elements

Table 3-2 describes the elements on the **RADIUS**, and then **Configuration**, and then **Configuration Sets**, and then **Message Authenticator Configuration Sets** page on the SOAM.

Table 3-2 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

Table 3-2 (Cont.) Message Authenticator Configuration Sets Elements

Fields (* indicates a required field)	Description	Data Input Notes
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
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

3.4.1.1.2 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 3-2.

1. Select **RADIUS**, and then **Configuration**, and then **Configuration Sets**, and then **Message Authenticator Configuration Sets**.

   The **RADIUS**, and then **Configuration**, and then **Configuration Sets**, and then **Message Authenticator Configuration Sets** page appears.

2. Click **Insert**.

   The **RADIUS**, and then **Configuration**, and then **Configuration Sets**, and then **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.

3.4.1.1.3 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**, and then **Configuration**, and then **Configuration Sets**, and then **Message Authenticator Configuration Sets**.

   The **RADIUS**, and then **Configuration**, and then **Configuration Sets**, and then **Message Authenticator Configuration Sets** page appears.

2. Click **Edit**.

   The **RADIUS**, and then **Configuration**, and then **Configuration Sets**, and then **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.

3.4.1.1.4 Deleting Message Authenticator Configuration Sets

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

The fields are described in Table 3-2.

1. Select **RADIUS**, and then **Configuration**, and then **Configuration Sets**, and then **Message Authenticator Configuration Sets**.

   The **RADIUS**, and then **Configuration**, and then **Configuration Sets**, and then **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**, and then **Configuration**, and then **Configuration Sets**, and then **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.

3.4.1.2 Shared Secret Configuration Sets

On the **RADIUS**, and then **Configuration**, and then **Configuration Sets**, and then **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**, and then **Configuration**, and then **Configuration Sets**, and then **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**, and then **Configuration**, and then **Configuration Sets**, and then **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.

3.4.1.2.1 Shared Secret Configuration Sets elements

Table 3-3 describes the elements on the **RADIUS**, and then **Configuration**, and then **Configuration Sets**, and then **Shared Secret Configuration Sets** page on the SOAM.

Table 3-3 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: 8-128 ASCII character string

3.4.1.2.2 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 3-3.

1. Select **RADIUS**, and then **Configuration**, and then **Configuration Sets**, and then **Shared Secret Configuration Sets**.

   The **RADIUS**, and then **Configuration**, and then **Configuration Sets**, and then **Shared Secret Configuration Sets** page appears.
2. Click **Insert**.

   The **RADIUS**, and then **Configuration**, and then **Configuration Sets**, and then **Shared Secret Configuration Sets [Insert]** page appears.
3. Enter a unique **Shared Secret Name**.
4. Enter a unique **Shared Secret**.

3.4.1.2.3 Editing Shared Secret Configuration Sets

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

The fields are described in Table 3-3.

1. Select **RADIUS**, and then **Configuration**, and then **Configuration Sets**, and then **Shared Secret Configuration Sets**.

   The **RADIUS**, and then **Configuration**, and then **Configuration Sets**, and then **Shared Secret Configuration Sets** page appears.
2. Click **Edit**.

   The **RADIUS**, and then **Configuration**, and then **Configuration Sets**, and then **Shared Secret Configuration Sets [Edit]** page appears.
3. Edit the unique **Shared Secret Name**.
4. Edit the unique **Shared Secret**.

3.4.1.2.4 Deleting Shared Secret Configuration Sets

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

The fields are described in Table 3-3.

1. Select **RADIUS**, and then **Configuration**, and then **Configuration Sets**, and then **Shared Secret Configuration Sets**.

   The **RADIUS**, and then **Configuration**, and then **Configuration Sets**, and then **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**, and then **Configuration**, and then **Configuration Sets**, and then **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.

3.4.1.3 Ingress Status Server Configuration Sets

On the **RADIUS**, and then **Configuration**, and then **Configuration Sets**, and then **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**, and then **Configuration**, and then **Configuration Sets**, and then **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**, and then **Configuration**, and then **Configuration Sets**, and then **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.

3.4.1.3.1 Ingress Status Server Configuration Sets elements

Table 3-4 describes the elements on the **RADIUS**, and then **Configuration**, and then **Configuration Sets**, and then **Ingress Status Server Configuration Sets** page on the SOAM.

Table 3-4 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

3.4.1.3.2 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**, and then **Configuration**, and then **Configuration Sets**, and then **Ingress Status Server Configuration Sets**.

   The **RADIUS**, and then **Configuration**, and then **Configuration Sets**, and then **Ingress Status Server Configuration Sets** page appears.
2. Click **Insert**.

   The **RADIUS**, and then **Configuration**, and then **Configuration Sets**, and then **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**.

3.4.1.3.3 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**, and then **Configuration**, and then **Configuration Sets**, and then **Ingress Status Server Configuration Sets**.

   The **RADIUS**, and then **Configuration**, and then **Configuration Sets**, and then **Ingress Status Server Configuration Sets** page appears.
2. Click **Edit**.

   The **RADIUS**, and then **Configuration**, and then **Configuration Sets**, and then **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**.

3.4.1.3.4 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**, and then **Configuration**, and then **Configuration Sets**, and then **Ingress Status Server Configuration Sets**.

   The **RADIUS**, and then **Configuration**, and then **Configuration Sets**, and then **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**, and then **Configuration**, and then **Configuration Sets**, and then **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.

3.4.1.4 Message Conversion Configuration Set

The **RADIUS**, and then **Configuration**, and then **Configuration Sets**, and then **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.

3.4.1.4.1 Message Conversion Configuration Set elements

Table 3-5 describes the elements on the **RADIUS**, and then **Configuration**, and then **Configuration Sets**, and then **Message Conversion Configuration Set** page on the NOAM.

Table 3-5 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	
	Diameter Application ID	The 32-bit Diameter message Application ID	
	Diameter Command Code	The 24-bit Diameter message Command Code	

3.4.2 NAS Node

On the **RADIUS**, and then **Configuration**, and then **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**, and then **Configuration**, and then **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**, and then **Configuration**, and then **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.

3.4.2.1 NAS Node elements

Table 3-6 describes the elements on the **RADIUS**, and then **Configuration**, and then **Ingress NAS Node** page on the SOAM.

Table 3-6 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

Table 3-6 (Cont.) NAS Node Elements

Fields (* indicates a required field)	Description	Data Input Notes
Realm*	Realm of an NAS Node 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.	Format: Text box 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.

3.4.2.2 Inserting an NAS Node

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

The fields are described in Table 3-6.

1. Select **RADIUS**, and then **Configuration**, and then **NAS Node**.

   The **RADIUS**, and then **Configuration**, and then **NAS Node** page appears.

2. Click **Insert**.

   The **RADIUS**, and then **Configuration**, and then **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**.

3.4.2.3 Editing an NAS Node

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

The fields are described in Table 3-6.

1. Select **RADIUS**, and then **Configuration**, and then **NAS Node**.

   The **RADIUS**, and then **Configuration**, and then **NAS Node** page appears.
2. Click **Edit**.

   The **RADIUS**, and then **Configuration**, and then **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**.

3.4.2.4 Deleting an NAS Node

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

The fields are described in Table 3-6.

1. Select **RADIUS**, and then **Configuration**, and then **NAS Node**.

   The **RADIUS**, and then **Configuration**, and then **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**, and then **Configuration**, and then **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.

3.4.3 Radius Routing Tables

The Radius Routing Tables option displays the configured Radius Routing Table managed object instances. The Radius Routing Tables configuration is done automatically by DSR with default values.

You can add, edit, and remove a configured instance.

3.4.3.1 Radius Routing Table Elements

The following table describes the elements of Radius Routing Table.
Use the **Filter** button to display only the required data in the Radius Routing Table. To sort and arrange the listed instances in each column, click the respective column heading.

Table 3-7 Radius Routing Table Elements

Field	Description	Data Input Notes
Key AVP*	Indicates the Attribute Value Pairs (AVPs) for Radius messages. This is a mandatory field. **Note:** If this field is set to **APN**, it disables **VRFID** and **Auth MPN** fields.	Format: Text box Default: N/A Range: APN or VRFID
APN	Indicates the Access Point Name.	Format: Text box Default: N/A Range: 1-100 character string. This string is case-sensitive. Valid characters are alphabet (A-Z and a-z), digits (0-9), hyphen (-), and period (.). This string must start and end with an alphabetic character or a digit.
VRFID	Indicates the Virtual Route Forwarding Identifier.	Format: Text box Default: N/A Range: 1-10 character string. This string is case-sensitive. Valid characters are alphabet (A-Z and a-z), digits (0-9), hyphen (-), and period (.). This string must start and end with an alphabetic character or a digit.
Auth MPN	Forwards Radius request to MPN.	Default: Unchecked Range: Checked/Unchecked

3.4.3.2 Adding a New Radius Routing Table

Perform the following procedure to add a new Radius Routing Table.

1. On the Oracle Communications Diameter Signaling Router GUI, in the left-navigation pane, click **RADIUS**, and then **Configuration**, and then **Radius Routing Tables**.

   The system displays the list of configured Radius Routing Table managed object instances.
2. To add a new instance, click **Insert**.
3. In the Adding a new Radius Routing Table area, configure the fields as described in Table 3-7.
4. Click **Apply**.

5. Click one of the following buttons:
   - **Ok**: To update the configured data in the database and re-render Radius Routing Tables with a new instance.
   - **Cancel**: To terminate the creation of a new instance.

3.4.3.3 Editing or Removing a Radius Routing Table

Perform the following procedure to edit or remove an existing Radius Routing Table.

1. On the Oracle Communications Diameter Signaling Router GUI, in the left-navigation pane, click **RADIUS**, and then **Configuration**, and then **Radius Routing Tables**.

   The system displays the list of configured Radius Routing Table managed object instances.
2. Select the instance that you want to edit or remove.

   > **Note:**
   >
   > You can select only a single instance at a time.
3. Click one of the following buttons:
   - **Edit**: To modify the fields of the selected instance as described in Table 3-7.
   - **Delete**: To remove the instance from Radius Routing Tables.
4. Click **Ok** for the changes to take effect.

3.5 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

3.5.1 Bulk Import and Export

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

- **Help**, and then **Diameter Common**, and then **Bulk Import**
- **Help**, and then **Diameter Common**, and then **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**, and then **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**, and then **Files** screen), 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 screens. 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**, and then **Files** screen), 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.