# Oracle® Communications

# Diameter Signaling Router Rx ShUDR Application User's Guide

Release 9.0.0.0.0
F79495-01
April 2023

ORACLE

Oracle Communications Diameter Signaling Router Rx ShUDR Application User's Guide, Release 9.0.0.0.0

F79495-01

# Contents

# 6 RSA MEALs

# 1
# Introduction

The Rx ShUDR (Rx Gateway MCPTT) application allows the operator to enable the Push To Talk service.

A Diameter Custom Application (DCA) Framework is developed that enables Oracle engineers, consultants and customers to develop applications on top of DSR without the need to extend DSR itself. The Rx ShUDR application is developed as a DCA application. RSA menu options allow you to work with:

- Custom Measurements, Events, Alarms, and Logs (MEALs)
- General options
- Trial MPs assignment
- Application control
- System Options (SO Only)

## 1.1 References

- Diameter Custom Applications Feature Activation Guide
- Diameter User's Guide
- DCA Programmer's Guide

## 1.2 Intended Scope and Audience

This content is intended for personnel who perform RSA tasks, and it includes procedures for performing tasks using the product GUI.

This content does not describe how to install or replace software or hardware.

## 1.3 Content Organization

The content in this document is organized as follows:

- Introduction provides General information about RSA including overview, the organization of this content, and how to get technical assistance.
- Understanding RSA Functionality and Logic provides an understanding RSA Functionality and Logic.
- Upgrade DSR provides details of upgrading DSR.
- Configure RSA provides details about configuring RSA and customizing RSA resources.
- RSA Tables provides details about RSA Tables and provisioning RSA database.
- RSA MEALs provides details about RSA MEALs, RSA Measurements, SysMetrics, and Alarms.

# 1.4 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:

- 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**.
- For Hardware, Networking and Solaris Operating System Support, select **3**.

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.

# 2
# Understanding RSA Functionality and Logic

This section describes RSA functionality and logic.

RSA is a business logic application that functions within the DCA framework. The DCA framework is a prerequisite for RSA.

RSA must be activated to access RSA GUI menu and functionality.

> **Note:**
>
> DCA framework is a set of APIs and services that are made available to DCA developers who need to develop applications.
>
> The following documents contain information about the DCA framework applications and functionality:
>
> - DCA Feature Activation
> - Activating and enabling DCA applications and framework
> - Deactivating DCA applications and framework
> - DCA Programmer's Guide
> - Provisioning DCA
> - Developing stateless DCA applications
> - Monitoring DCA applications
> - Using DCA applications
> - Using Custom Meals
> - Using the DCA GUI
> - Understanding the development and environment
> - Using DCA APIs
> - Implementing DCA best practices

## 2.1 RSA Overview

Push To Talk (PTT) service provides an arbitrated method by which two or more users may engage in communication. Users may request permission to transmit (for example, traditionally by means of a press of a button). The Mission Critical Push To Talk (MCPTT) service supports an enhanced PTT service, suitable for mission critical scenarios.

The MCPTT Service is intended to support communication between several users (a group call), where each user has the ability to gain access to the permission to talk in an arbitrated manner. However, the MCPTT Service also supports Private Calls between pairs of users.

The primary target of MCPTT is to provide a professional Push to talk service (for example, public safety, transport companies, utilities or industrial and nuclear plants).

To avoid overloading RSA, the Application Routing Table (ART) is configured to route only the Rx diameter messages based on Application ID and Command code.

RSA can be enabled and disabled as a DCA framework application. Disabling RSA on a specific site is possible only if RSA has been disabled on all the DA-MPs for that specific site. RSA can be configured at the NO and SO level.

The DCA framework creates applications on top of the Diameter Signaling Router (DSR) allowing for a faster development cycle. There can be up to 10 versions of each DCA in the various states.

To use RSA for DCA, the DCA framework must be activated on the NO. Activation needs to be performed only once. See *Diameter Custom Applications Feature Activation Guide* for instructions on how to activate the DCA framework.

When RSA is initially installed, it is disabled, and you must manually enable it. See Enabling RSA to enable the application for every DMAP using RSA.

If RSA is in the DCA framework GUI menu, this means the application is already enabled, but that does not guarantee it is provisioned. See Disabling RSA to disable RSA.

DCA framework application functionality varies between the SO and NO. For example, System Options is available on the SO only.

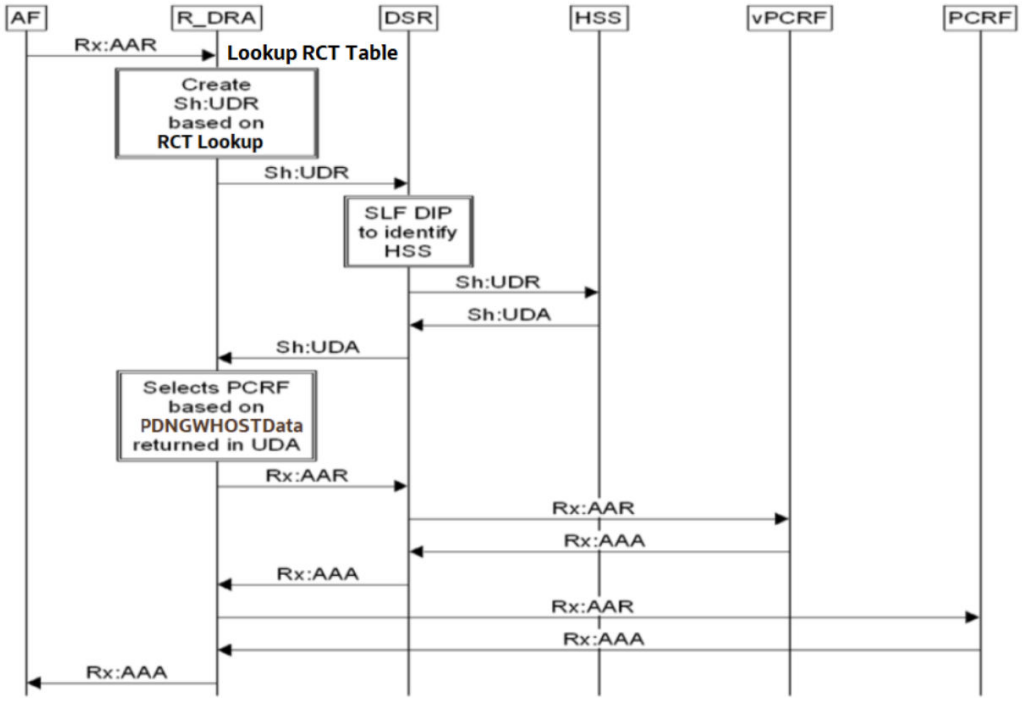
## 2.2 Understanding RSA Functionality

RSA allows the operator to screen Rx Sh message at Roaming DRA .Oracle Roaming DRA (R-DRA) Virtual DSR establishes Diameter Rx connection with Oracle PCRF (PNF) segments. All vPCRF segments will be behind Oracle DSR (Core DRA/SLF) taking Gx, Rx, Sh, Sy traffic. R-DRA is the Virtual DSR deployed for Roaming use case. Core-DRA is the reference to Baremetal DSR running FABR use case

RSA process the messages for following use cases:

1. Use Case A: Rx:AAR to Rx:Sh:UDR conversion (R:AAR messages converted to Sh:UDR message based on RCT Look up table (DSA Config Table).

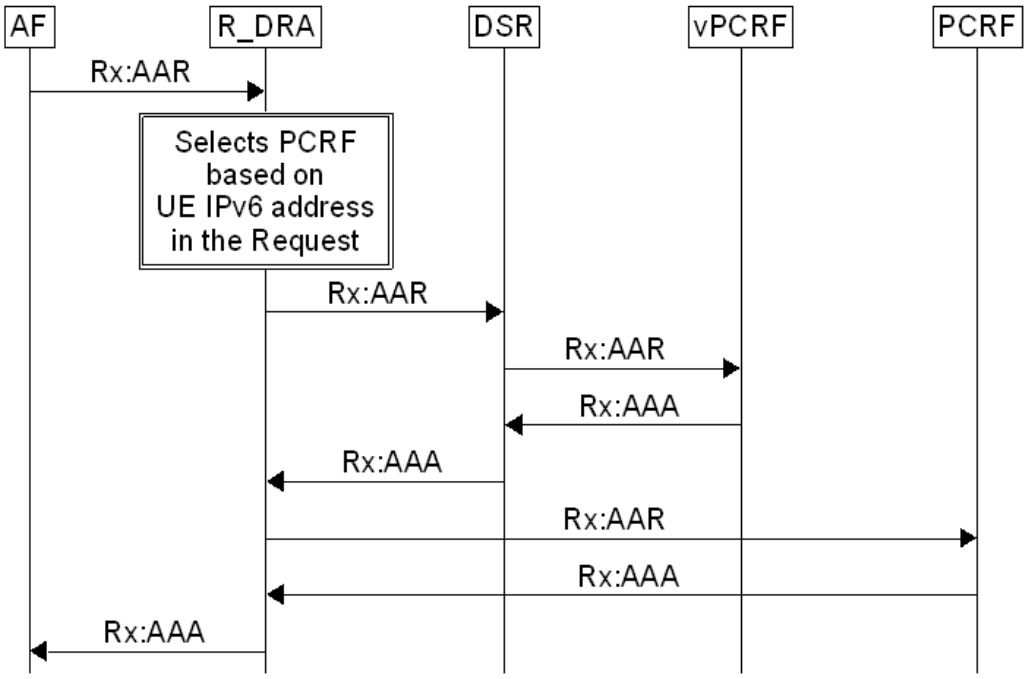
**Figure 2-1 Use Case A: Rx AAR to Rx ShUDR conversion**




- ART rule configured to route all Rx message to DCA Application (Rx ShUDR Application)
- New DCA Application **Rx ShUDR Application** receives all the Rx messages and checks for Rx AAR Initial (Rx-Request-Type AVP set to INITIAL_REQUEST) received at R-DRA in look up RCT table for **Sh lookup**.
- Every other Rx Request message received at R-DRA will lookup **RCT table** for **Topology hiding**. If Topology hiding is enabled for MCPTT Client, then look up **THT table** for pseudo FQDN to PCRF address is mapped. If any match is found, replace Dest Host as PCRF address and sends the message out for further routing. If match is not found, then the messages is forwarded for further default routing.
- Application will look up RCT Table based on incoming origin-host AVP FQDN value. If Sh lookup required is **Yes**, originated **Rx:AAR** converts to **Sh:UDR** message and is sent out for further routing. Sh :UDR message contains:
  - Session-Id> - To be assigned by DSR (copied from AAR)
  - {Auth-Session-State} - NO_STATE_MAINTAINED value 1
  - {Origin-Host} – DSR host-id, as it is the originator of the Sh:UDR (filled through Configuration Table)
  - {Origin-Realm} – DSR realm, as it is the originator of the Sh:UDR ( filled through Configuration Table)
  - {Route-record} – To be filled with peer FQDN value
  - {User-Identity} – : filled with Subscription-Id AVP value received in Rx:AAR message
    - Subscription-Id Type 0 -- MSISDN/END_USER_E164 -MSISDN goes in User-Identity[MSISDN]

        - Subscription-Id Type 1 -- IMSI - Goes into [Public-Identity]
        - Subscription-Id Type 2 -- END_USER_SIP_URI - Goes into [Public-Identity]
      - *{Data-Reference} – RepositoryData value as 0
      - {Destination-Realm} – To be Assigned by DSR from Rx-AAR.
      - ServiceIndication = Called-Station-Id (copied from AAR message)
    - Sh:UDR sent out to DRL for further routing to core-DRA.
    - Core-DRA perform FABR lookup based on IMSI/MSIDN and route to corresponding HSS.
    - HSS process the Sh:UDR and sends back Sh:UDA to core DRA with **PDNGWHOSTData** data in UserData AVP.
    - Core DRA route Sh:UDA to R-DRA which further route to **Rx ShUDR Application** based on ART route.(ART rule: Sh:UDR/UDA application messages route to Rx ShUDR Application DCA application)
    - Rx ShUDR application process the Sh:UDA answer message and create/modify the Rx:AAR message (which is stored as cookies when first AAR message is received) with lookup the PDNGWHOST in PPMTTable and get the PCRF FQDN, sets Dest Host as PCRF FQDN and sends it out for further routing.
    - PCRF sends back the Rx:AAA with PCRF Address as Origin Host.
    - Rx-ShUDR application process the Rx:AAA message as answer message and create/modify the RX:AAA message with lookup in **RCT Table** and verifies if Topology Hiding is required or not.
    - If Topology hiding required is **Yes** for Rx Client then search **THT table** (using PCRF FQDN present in origin Host ), replaces the original origin Host with pseudo FQDN from **THT Table** and sends it to DRL for routing to Rx Client.
    - Rx client uses Pseudo FQDN as Dest-Host for future diameter transactions. New DCA Application **Rx ShUDR Application** receive messages other than Rx AAR Initial (Rx-Request-Type AVP set to INITIAL_REQUEST) will lookup RCT table for **Topology hiding**. If Topology hiding is enabled for origin host, then look up **THT table** for pseudo FQDN to PCRF address is mapped. If any match is found then replace Dest Host as PCRF address and sends out for further routing. If match is not found, then the message is forwarded as is for further routing.
2. Use Case B: Rx-AAR -> RBAR lookup -> PCRF
    - If Sh lookup required is **No** forward the message as is to DRL for further routing using RBAR lookup.
    - RBAR Application look up in RBAR table only for Rx AAR Initial (Rx-Request-Type AVP set to INITIAL_REQUEST),select the PCRF based on **Framed IPv6 prefix** and sends to DRL for further routing (either directly or through Core DRA).
    - PCRF installs desired policy and sends back Rx:AAA (with PCRF as Origin Host) to R-DRA (directly or through Core DRA).
    - PCRF sends back the Rx:AAA with PCRF Address as Origin Host.

**Figure 2-2 Use Case B**




- Rx ShUDR Application processes the Rx:AAA message as answer message and create/ modify the RX:AAA message with lookup in **RCT Table** and verifies if Topology hiding is required.
- If Topology hiding is required for Rx Client **FQDN()**, then search **THT table** (using PCRF FQDN present in origin Host), replace the original origin Host with pseudo FQDN from **THT Table** and sends it to DRL for further routing to Rx Client.
- Rx client uses Pseudo FQDN as Dest-Host for future diameter transactions, Rx-ShUDR Application receives message other than Rx AAR Initial (Rx-Request-Type AVP set to INITIAL_REQUEST) will lookup RCT table for **Topology hiding**. If Topology hiding is enabled for origin host, then look up **THT table** for pseudo FQDN to PCRF address mapping. If match is found, then replace Dest Host as PCRF address and sends out for further routing. If match is not found then forward message as is for further default routing.

## 2.3 RSA Logic Process

To trigger RSA logic, some prerequisite conditions are required. For example, the DCA framework must be activated and RSA must be activated, enabled, and provisioned.

RSA logic is triggered when RSA receives Rx Diameter message. Once Rx Diameter message is received, RSA starts executing based on Rx_Client Table. If Sh_Lookup_Required field is **Yes**, the Rx:AAR message converts to Sh:UDR User Case. If Sh_Lookup_Required field is **No**, it proceeds for RBAR look up execution (RSA Application forwards the message to DRL layer) and then routes through ART Lookup (application chaining).

## 2.3.1 DSA Mandatory Configuration

The Rx ShUDR application uses these tables for holding the configuration value.

**Table 2-1 Configuration tables for the Rx ShUDR application**

| Table Name | Table Description | Single row indicator | Table Level |
|---|---|---|---|
| Rx_Client | This table includes the configuration parameters for each Rx Client regarding the details of Sh Lookup and Topology hiding. This is a table generated by the DCA Framework. | No | NO |
| PDNGWHost_PCRF_Mapping | This table contains one to one mapping between PDN Gateway Host and PCRF. This is a table generated by the DCA Framework. | No | NO |
| Topology_Hiding | This table contains 1:1 mapping between PCRF FQDN and corresponding Pseudo FQDN for each PCRF MPEs. This is a table generated by the DCA Framework. | No | NO |
| Error_Action_Config | This table contains the error action configuration parameters to be applied for send answer during runtime errors while processing Sh UDR/UDA message. | No | NO |
| System_Config_Options | This table contains system wide common configurable options required to process Rx-ShUDR application. | Yes | SO |

### Rx_Client Table

This table contains the list of Rx Client FQDN's and the corresponding details of Sh Lookup and Topology Hiding for each Rx client.

**Table 2-2 Details of the Rx_Client table for the Rx-ShUDR application**

| Parameter Name | Unique | Mandatory | Range and default value | Description |
|---|---|---|---|---|
| Rx_Client_FQDN | No | Yes | DiameterIdentity Default: n/a, | Indicates the Fully Qualified Domain Name of Rx Client (MCPTT Client). |

**Table 2-2 (Cont.) Details of the Rx_Client table for the Rx-ShUDR application**

| Parameter Name | Unique | Mandatory | Range and default value | Description |
|---|---|---|---|---|
| Sh_Lookup_Required | No | Yes | Enumerated, Yes/No Default=No | Decides whether Sh Lookup is required upon receiving Rx AAR from Rx(MCPTT) Client.<br>If configured as Yes, then Sh Lookup is performed by Rx-ShUDR application.<br>If configured as No, then AAR message is forwarded without processing at Rx-ShUDR application. |
| Topology_Hiding_Required | No | Yes | Enumerated, Yes/No Default=No | Decides whether Topology hiding should be applied for answer messages.<br>If it is configured as **Yes**, then Topology hiding is performed for AAR answer message before routing the answer message from PCRF to Policy client.<br>If it is configured as **No**, then no topology hiding is applied for the AAR answer message. |

### PDNGWHost_PCRF_Mapping Table

This table contains one to one mapping between PDN Gateway Host and PCRF.

**Table 2-3 Details of the PDNGWHost_PCRF_Mapping Table**

| Parameter Name | Unique | Mandatory | Range and default value | Description |
|---|---|---|---|---|
| PDNGW_Host | No | Yes | DiameterIdentity Default: n/a, | Indicates the PDN Gateway FQDN |
| PCRF_FQDN | No | Yes | DiameterIdentity Default: n/a, | Indicates the FQDN of the PCRF |

### Topology_Hiding Table

This table contains the list of Actual Hostnames and their Pseudo Hostnames in this PCRF Topology Hiding Configuration.

**Table 2-4 Details of Topology_Hiding table records**

| Parameter Name | Unique | Mandatory | Range and default value | Description |
|---|---|---|---|---|
| PCRF_FQDN | Yes | Yes | DiameterIdentity Default: n/a, | Indicates the actual hostname of the PCRF |
| Pseudo_FQDN | No | Yes | DiameterIdentity Default: n/a, | Indicates the Pseudo hostname value to be populated in the Diameter Origin-Host AVP for request/answer messages routed from a PCRF to a policy client, or the Diameter Destination-Host AVP for request/answer messages routed from a PCRF to a policy client. |

### Error_Action_Config Table

This table contains the error action configuration parameters applied to send answer during runtime errors while processing Sh UDR/UDA message.

**Table 2-5 Details of Error_Action_Config table records**

| Parameter Name | Unique | Mandatory | Range and default value | Description |
|---|---|---|---|---|
| Result_Code | Yes | Yes | Integer<br>Min:1000<br>Max:5999 | This configuration is applicable when the application is configured to send answer during runtime errors while processing AAR/AAA message. This value is used to set the Result-Code AVP of the Answer Message. [Range = 1000 - 5999] |
| Error_Message | No | Yes | UTF8String<br>Max Length: 64, | This configuration is applicable when the application is configured to send answer during runtime errors while processing AAR/AAA. If specified, the Answer is added with Error-Message AVP with the specified Text. [Range = 1 to 64 character] |

**Table 2-5 (Cont.) Details of Error_Action_Config table records**

| Parameter Name | Unique | Mandatory | Range and default value | Description |
|---|---|---|---|---|
| Vendor_Id | No | No | Integer<br>Min:1<br>Max: 4294967295 | This configuration is applicable when the application is configured to send answer during runtime errors. If the value is specified, the Answer Message consists of Experimental-Result grouped AVP with the specified Vendor-ID [Range=1-4294967295] |

### System_Config_Options Table

This table contains system wide common configurable options required to process Rx ShUDR Application. This is single record table and configurable from active SOAM server.

**Table 2-6 Details of System_Config_Options table records**

| Parameter Name | Unique | Mandatory | Range and default value | Description |
|---|---|---|---|---|
| Result_Code | Yes | Yes | Integer<br>Min:1000<br>Max:5999 | This configuration is applicable when the application is configured to send answer during runtime errors while processing AAR/AAA message. This value is used to set the Result-Code AVP of the Answer Message. [Range = 1000 - 5999] |
| Error_Message | No | Yes | UTF8String<br>Max Length: 64, | This configuration is applicable when the application is configured to send answer during runtime errors while processing AAR/AAA. If specified, the Answer is added with Error-Message AVP with the specified Text. [Range = 1 to 64 character] |
| Vendor_Id | No | No | Integer<br>Min:1<br>Max: 4294967295 | This configuration is applicable when the application is configured to send answer during runtime errors. If the value is specified, the Answer Message consists of Experimental-Result grouped AVP with the specified Vendor-ID [Range=1-4294967295] |

**Table 2-6 (Cont.) Details of System_Config_Options table records**

| Parameter Name | Unique | Mandatory | Range and default value | Description |
|---|---|---|---|---|
| Origin_Host | No | No | DiameterIdentity<br>Default: n/a, | Indicates the Origin-Host value to be used while Sending Sh UDR message from Rx-ShUDR application Business Logic. |
| Origin_Realm | No | No | DiameterIdentity<br>Default: n/a, | Indicates the Origin-Realm value to be used while Sending Sh UDR message from Rx-ShUDR application Business Logic. |

## 2.4 RSA Stateless Application Logic

Stateless application does not require maintenance of any State-Data (in UDR) for validation of the diameter message.

# 3
# Upgrade DSR

RSA supports upgrade as it does not maintain any state in UDR.

Following are the steps to upgrade from old DSR (DCA with U-SBR) to new DSR (DCA with UDR Release).

1. Import new application JSON file on NOAM server for Business logic as well as configuration/schema.
2. Compile the Business logic from NOAM server GUI.
3. Enable RSA Application through SOAM GUI. See Enabling RSA.
4. Configure ART Rule to route the Rx Message to Rx ShUDR Application. See Configuring ART for RSA.

Now setup is ready to handle Rx Message for new DCA Application (Rx ShUDR Application).

# 4
# Configure RSA

This section contains information about RSA and describes the procedures used to activate, configure, and deactivate RSA.
RSA uses the following tables for holding configuration values:

- Rx_Client Table
- PDNGWHost_PCRF_Mapping Table
- Topology_Hiding Table
- Error_Action_Config Table
- System_Config_Options Table

### Rx_Client Table

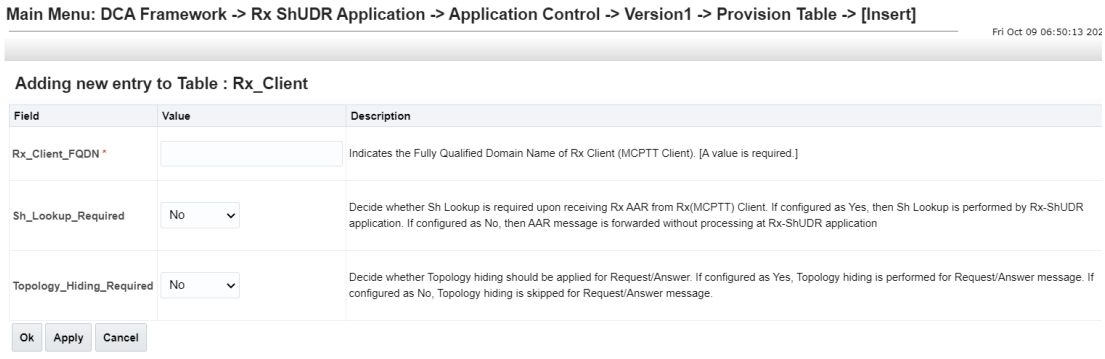
This is the first table Application lookup when Rx Initial message is received from client.

**Figure 4-1 Rx_Client Provision Table**

Table: Rx_Client

| Rx_Client_FQDN | Sh_Lookup_Required | Topology_Hiding_Required |
|---|---|---|
| abc | Yes | No |
| mno | No | No |
| xyz | No | Yes |
| plm | Yes | Yes |

**Figure 4-2 Rx_Client Provision Table Insert Screen**




### PDNGWHost_PCRF_Mapping Table

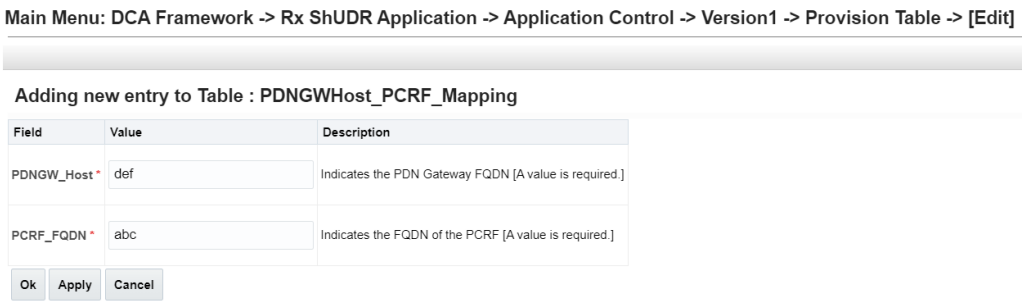
This table gets the PCRF address from PDNGW_Host received from HSS (Sh:UDA Response).

**Figure 4-3 PDNGWHost_PCRF_Mapping table**

Table: PDNGWHost_PCRF_Mapping

| PDNGW_Host | PCRF_FQDN |
|---|---|
| def | abc |
| ghi | mno |
| pqr | xyz |

**Figure 4-4 PDNGWHost_PCRF Provision Table Insert Screen**




## Topology_Hiding Table

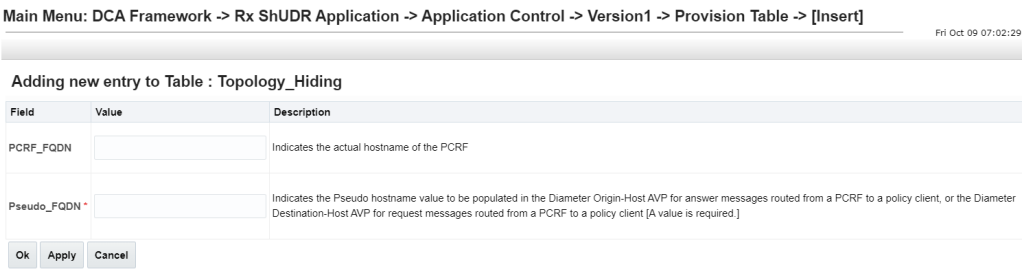
This table is used when a AAA Response is reeived from PCRF, message generated from PCRF, message generated from Rx Client other than AAR Initial message for apply the topology hiding (replace the PCRF address with Pseudo FQDN).

**Figure 4-5 Topology_Hiding table Provision Table**

Table: Topology_Hiding

| PCRF_FQDN | Pseudo_FQDN |
|---|---|
| abc | jkl |
| xyz | vwv |
| mno | stu |

**Figure 4-6 Topology_Hiding Provision Table Insert Screen**



### Error_Action_Config Table

This table used when non success response is received from HSS (Sh:UDA Response from HSS) to map to AAA Response (Result code, Error Message, Vendor Id).

**Figure 4-7 Error_Action_Config table Provision Table**

Table: Error_Action_Config

| Result_Code | Error_Message | Vendor_Id |
|---|---|---|
| 3002 | DIAMETER_UNABLE_TO_DELIVER | 10415 |
| 3001 | DIAMETER_COMMAND_UNSUPPORTED | 10415 |
| 3003 | DIAMETER_REALM_NOT_SERVED | 10415 |
| 3004 | DIAMETER_TOO_BUSY | 10415 |
| 3005 | DIAMETER_LOOP_DETECTED | 10415 |
| 3006 | DIAMETER_REDIRECT_INDICATION | 10415 |
| 3007 | DIAMETER_APPLICATION_UNSUPPORTED | 10415 |
| 3008 | DIAMETER_INVALID_HDR_BITS | 10415 |
| 3009 | DIAMETER_INVALID_AVP_BITS | 10415 |
| 3010 | DIAMETER_UNKNOWN_PEER | 10415 |
| 4001 | DIAMETER_AUTHENTICATION_REJECTED | 10415 |

**Figure 4-8 Error_Action_Config Provision Table Insert Screen**

Main Menu: DCA Framework -> Rx ShUDR Application -> Application Control -> Version1 -> Provision Table -> [Insert]

Tue Dec 15 23:57:08 202

Adding new entry to Table : Error_Action_Config

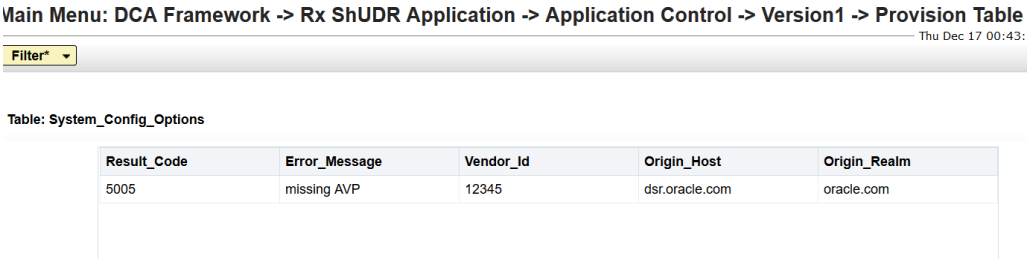
| Field | Value | Description |
|---|---|---|
| Result_Code * | | This configuration will be applicable when the application is configured to send answer for runtime errors while processing Sh UDR/UDA message. This value will be used to set the Result-Code AVP of the Answer Message. [Range = 1000 - 5999] [A value is required.] |
| Error_Message * | | This configuration will be applicable when the application is configured to send answer for runtime errors while processing Sh UDR/UDA. If specified, the Answer will be added with Error-Message AVP with the specified Text. [Range = 1 to 64 character] [A value is required.] |
| Vendor_Id | | This configuration will be applicable when the application is configured to send answer for runtime errors while processing Sh UDR/UDA. If specified, Answer will consist of Experimental-Result grouped AVP with the specified Vendor-ID[Range=1-4294967295 |

Ok Apply Cancel

### System_Config_Options Table

This table is used to configure system wide configuration that is used for Sh UDR message creation and sends the error response to Rx Client.

**Figure 4-9 System Config Option table**




# 4.1 RSA Prerequisites

Before activating RSA as a DCA application, DCA framework must be activated on the NO. See *Diameter Custom Applications Feature Activation Guide* for detailed information.

After DCA framework activation, RSA can be activated.

> **Note:**
>
> After RSA is activated, by default, the application is in the disabled state. When disabled, no diameter traffic is delivered to RSA. See *Diameter User's Guide* for the procedure to enable the application.
> RSA's operational status is unavailable until a successful compiled version (production or trial version) of RSA is configured.

# 4.2 Activating RSA

This procedure activates RSA. See *Diameter Custom Applications Feature Activation Guide* for detailed information.

1. Ensure that the DCA framework is activated.
2. Activate RSA using the DCA Application Activate procedure.
   a. Recommended DCA Short Name: **RSA**
   b. Recommended DCA Long Name: **Rx ShUDR Application**
3. Post RSA activation, check the visibility of RSA subtree in the main menu **DCA Framework**, and then **Diameter Security Application**.

This procedure verifies that RSA is activated before enabling RSA and perform the provisioning activities.

1. Confirm the RSA folder is visible on the GUI under the main menu **DCA Framework**.
2. Check if all measurements and KPIs associated with the DCA framework are visible on the **Measurements**, and then **Report** and **Status & Manage**, and then **KPIs** screens.

After activation, RSA becomes visible across DSR (for example, ART and maintenance).

> **Note:**
>
> After activating DCA, the DCA framework allocates a default set of resources to it.

# 4.3 Configuring RSA Business Logic and Database Schema

This procedure imports RSA business logic and the configuration database schema using the RSA JSON file.
See *DCA Programmer's Guide* for detailed information.

RSA NO JSON filename: **Rx_ShUDR_Application-Version1.json**

1. From the NO GUI main menu, **DCA Framework**, and then **Rx ShUDR Application**, and then **Application Control**.
2. Select the newly added **RSA Version Name**.
3. Click **Business Logic** in the Import section of the Application Control page.
4. Click **Browse** and select the **Rx_ShUDR_Application-Version1.json** file from the File upload screen.
5. Mark the **Abort on first error** checkbox to abort the import process in case of error.
6. Click **Import** to start the import process.

## Verification

Perform the following steps to verify if the RSA JSON has successfully imported before enabling RSA and performing provisioning activities.

1. From the NO GUI main menu, **DCA Framework**, and then **Rx ShUDR Application**, and then **Application Control** and ensure that an entry is added in DCA application version details table.
2. Select the newly added version and click **Config Tables and Data**.
3. Ensure that all DSA configuration tables are listed.
4. Select the newly added version and click **Development Environment**.
5. Ensure that DSA Perl business logic is present.

This ensures that the RSA JSON has successfully imported.

# 4.4 Configuring RSA Mandatory Options

This procedure configures various RSA Mandatory Options.

1. From the NO GUI main menu, **DCA Framework**, and then **Rx ShUDR Application**, and then **General Options**.
2. Update **Perl Subroutine for Diameter Request** to **process_request**.
3. Update **Perl Subroutine for Diameter Answer** to **process_answer**.

4. Uncheck the **Enable Opcodes Accounting** option to disable opcode accounting.
5. Click **Apply**.

You have successfully configured RSA mandatory options.

# 4.5 Configuring ART for RSA

ART rule is configured to route all Rx message to DCA Application (Rx ShUDR Application)

RSA processes ingress Rx Diameter messages received from foreign networks. For this:

1. Create an ART to route all the Rx traffic to RSA.
2. Assign the ART to all the foreign peers.

If you do not want to screen ingress diameter messages from a specific foreign peer, then skip the ART configuration for that peer.

RSA also processes egress diameter messages to send to a foreign network from a home network. For this:

1. Create an ART to route only egress traffic from a home network toward a foreign network to RSA.
2. Create an ART to route all the Rx Traffic based on Application ID.
3. Assign the ART only to those home network peers that can send egress messages to a foreign network.

If you want to screen the diameter message using Rx ShUDR Application, then assign the ART to the home peers that can send egress messages to a foreign network.

# 4.6 Enabling RSA

This procedure enables RSA on the SO.

1. Click **Diameter**, and then **Maintenance**, and then **Applications**.
2. Select DCA_RSA entries you want to enable.
3. Click **Enable**.

The selected DCA_RSA entries are enabled.

# 4.7 Disabling RSA

This procedure disables RSA on the SO.

1. Click **Diameter**, and then **Maintenance**, and then **Applications**.
2. Select DCA_RSA entries you want to disable.
3. Click **Disable**.

The selected DCA_RSA entries are disabled.

# 4.8 Deactivating RSA

This procedure deactivates RSA.

> **Note:**
>
> You cannot deactivate RSA while a version of the respective application is still in the Production and/or Trial state.

RSA must be disabled on all MPs in the network and no ART rules should refer to RSA.

1. Disable RSA for all the MPs from the SO GUI main menu, **Diameter**, and then **Maintenance**, and then **Applications**.
2. Delete ART rules referring to RSA.
3. Deactivate RSA using DCA Application Activate procedure in *Diameter Custom Applications Feature Activation Guide*.

RSA is deactivated.

# 5
# RSA Tables

RSA database schema defines various tables used to define and customize the application behavior.

Most of the RSA configuration tables are SO level tables, that is, provisioning in these tables is allowed only from the SO GUI. Only one RSA configuration Tables are NO level tables.

**Table 5-1 List of configuration tables for the Rx ShUDR application**

| Table Name | Table Description | Single row indicator | Table Level |
|---|---|---|---|
| Rx_Client | This table includes the configuration parameters for each Rx Client regarding the details of Sh Lookup and Topology hiding. This is a table generated by the DCA Framework. | No | NO |
| PDNGWHost_PCRF_Mapping | This table contains 1:1 mapping between PDN Gateway Host and PCRF. This is a table generated by the DCA Framework. | No | NO |
| Topology_Hiding | This table contains 1:1 mapping between PCRF FQDN and corresponding Pseudo FQDN for each PCRF MPEs. This is a table generated by the DCA Framework. | No | NO |
| Error_Action_Config | This table contains the error action configuration parameters to be applied for send answer during runtime errors while processing Sh UDR/UDA message. | No | NO |
| System_Config_Options | This table will contain system wide common configurable options required to process Rx-ShUDR application. | Yes | SO |

### Configures RSA Configuration tables

RSA configuration table (Error_Action_Config) are pre-populated if RSA is configured using RSA JSON file. See Configuring RSA Mandatory Options for more details.

Alternatively, RSA configuration tables can be configured manually using the following steps. See *DCA Programmer's Guide* for detailed information

1. From the NO GUI main menu, **DCA Framework**, and then **Rx ShUDR Application**, and then **Application Control**.
2. Select the newly added **RSA Version Name**.
3. Click **Config Table and Data**.

> **Note:**
>
> If RSA JSON is not used to import RSA business logic and the configuration database schema, then the configured table list is empty.

4. Click **Insert**.
5. Fill the fields to define the table.
6. Click **Add** to add multiple Table Fields.
7. Click **OK/Apply**.
8. Similarly repeat steps 4 to 7 for all other configuration tables.

### Provision RSA Tables

This procedure imports RSA default provisioning data using RSA JSON file.

RSA SO JSON filename: **Rx_ShUDR_Application-Version1_Default_Config.json**

See the *DCA Programmer's Guide* for detailed information.

1. From the NOAM GUI main menu, **DCA Framework**, and then **Rx ShUDR Application**, and then **Application Control**
2. Select the newly added **RSA Version Name**.
3. Click **A Level Config Data** in the Import section of the Application Control page.
4. Click **Browse** and select the **Rx_ShUDR_Application-Version1_Default_Config.json** file.
5. Mark the **Abort on first error** checkbox to abort the import process in case of error.
6. Click **Import** to start the import process.

Apart from the default entries, additional provisioning needs to be done manually using the following procedure.

1. From the SO GUI main menu, **DCA Framework**, and then **Rx ShUDR Application**, and then **Application Control**.
2. Select the newly added **RSA Version Name**.
3. Click **Config Data**.

> **Note:**
>
> If DSA JSON is not used to import RSA business logic and the configuration database schema, then the configured table list is empty.

4. Select the table that needs to be provisioned.
5. Click **Provision Table**.
6. Click **Insert**.
7. Fill the values for required fields of the table.
8. Click **OK/Apply**.

# 6
# RSA MEALs

RSA MEALs defines various Measurements, SysMetric, and Alarms used for reporting the application behavior. All these RSA MEALs are defined using DCA Custom MEAL Framework.

## 6.1 Configure RSA MEALs

RSA MEALs are pre-populated if RSA is configured using RSA JSON file. See Configuring RSA Business Logic and Database Schema for more details.

Alternatively, RSA MEALs can be configured manually using the following steps. See *DCA Programmer's Guide* for detailed information.

1. From the NO GUI main menu, **DCA Framework**, and then **Diameter Security Application**, and then **Custom MEALs**.
2. Click **Insert**.
3. Fill in the fields to define the MEAL.
4. Repeat steps 2 to 4 for each MEAL.

## 6.2 Measurements

The following tables lists the total Rx interface messages, total Rx Interface messages (AAR/RAR/STR/ASR) processed and sent by the Rx- ShUDR application.

**Table 6-1 Rx-ShUDR Measurements**

| Measurement Tag | Measurement Purpose | Measurement Details |
|---|---|---|
| TotalRxIntMsgProcessed | Total number of Rx Interface messages (AAR-I/U, RAR, STR and ASR) processed successfully and forwarded to PCRF. | Table 6-2 |
| TotalRxIntMsgRejected | Total number of Rx Interface messages (AAR-I/U, RAR, STR and ASR) rejected with error answer due to failure occur in the business logic execution. | Table 6-3 |
| TotalShUDRMsgCreated | Total number of Sh:UDR diameter messages created and sent by RSA application to HSS successfully. | Table 6-4 |
| ShUDRCreateAndSendFailCnt | Total number of Sh:UDR diameter messages creation/ Send failed due to runtime failures occured in business logic execution. | Table 6-7 |

**Table 6-1 (Cont.) Rx-ShUDR Measurements**

| Measurement Tag | Measurement Purpose | Measurement Details |
|---|---|---|
| TotalShUDRAnsSuccess | Total number of Sh:UDR answer messages received successfully. | Table 6-5 |
| TotalShUDRAnsFailed | Total number of Sh:UDR error answer messages received at Rx ShUDR application. | Table 6-6 |

**Table 6-2 totalRxInterfaceMsgProcessed Custom Meal**

| | |
|---|---|
| **Measurement Tag** | TotalRxInterfaceMsgProcessed |
| **Template Type** | Counter |
| **Measurement type** | Scalar |

**Table 6-3 totalRxInterfaceMsgRejected Custom Meal**

| | |
|---|---|
| **Measurement Tag** | TotalRxInterfaceMsgRejected |
| **Template Type** | Counter |
| **Measurement type** | Scalar |

**Table 6-4 TotalShUDRMsgCreated Custom Meal**

| | |
|---|---|
| **Measurement Tag** | TotalShUDRMsgCreated |
| **Template Type** | Counter |
| **Measurement type** | Scalar |

**Table 6-5 TotalShUDRAnsSuccess Custom Meal**

| | |
|---|---|
| **Measurement Tag** | TotalShUDRAnsSuccess |
| **Template Type** | Counter |
| **Measurement type** | Scalar |

**Table 6-6 TotalShUDRAnsFailed Custom Meal**

| | |
|---|---|
| **Measurement Tag** | TotalShUDRAnsFailed |
| **Template Type** | Counter |
| **Measurement type** | Scalar |

**Table 6-7 ShUDRCreateAndSendFailCnt Custom Meal**

| | |
|---|---|
| **Measurement Tag** | ShUDRCreateAndSendFailCnt |
| **Template Type** | Counter |
| **Measurement type** | Scalar |

# 6.3 Alarms

This Alarm will be raised if any failure occurs in Application business logic execution which may result in traffic loss.

**Table 6-8 Alarms**

| | |
|---|---|
| **Alarm Name** | RxShUDRAppExecFailed |
| **Template Type** | Event |
| **Alarm Description** | Failed executing Rx-ShUDR application business logic. Disable the Application until the problem is resolved. |
| **Alarm Autoclear Interval** | 90 |
| **Alarm Throttling Interval** | 60 |