Oracle® Communications

IDIH User Guide

Release 9.2.0.0.0
G33007-01
September 2025

ORACLE

Oracle Communications IDIH User Guide, Release 9.2.0.0.0

G33007-01

Contents

Preface

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

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 9.2.0.0.0.

Release 9.2.0.0.0 - G33007-01, September 2025

- Replaced the term "Kafka Config" with "IDIH Server Config" in the IDIH Server Configuration on DSR section.
- Replaced the term "Kafka Broker Status" with "IDIH Server Status" in the IDIH Server Status section.
- Replaced the term "Kafka" with "IDIH" in the following sections:
  - IDIH Server Configuration Fields
  - IDIH Connection Maintenance
- Updated default and range value for the following fields in the IDIH Server Configuration Fields section:
  - Batch Size
  - Max Request Size
  - Socket Connection Timeout

1 Introduction

This document provides information about how to use Oracle Communications Integrated Diameter Intelligence Hub (IDIH).

Oracle Communications Integrated Diameter Intelligent Hub (IDIH) is a signaling troubleshooting and analysis tool. IDIH captures and stores network trace data from Diameter Signaling Router (DSR) which is network signalling or routing node for visualization and troubleshooting purposes.

IDIH provides a web-based UI, with graphical view of network messages along with ladder diagram and full decode of network trace data which is easy to understand. It captures and stores additional metadata related to network traffic which provides information about the internal processing applied within the routing nodes to the network traffic. The configuration data from network routing nodes is pulled and converted into human-readable format.

In addition to visualization of signaling data, IDIH allows you to manage and run queries on captured network traffic, each query can have advanced filtering on individual protocol attributes or combination of attributes aligned with various logical operators. You can also save or update these queries for later usage. It also allows you to export individual network transactions or a complete trace in HTML and PCAP format.

IDIH provides statistical data about each captured trace, which displays the success and failures of a trace. It also provides a response code wise distribution for each trace.

For more information about deployment, see *Oracle Communications Integrated Diameter Intelligence Hub Installation Guide*.

1.1 References

Refer to the following document for more information:

Oracle Communications Diameter Signaling Router Cloud Installation Guide

2
IDIH GUI

IDIH GUI analyze traces and allows you to manage traces from DSR to capture messages required for troubleshooting. It also displays traces with graphical visualization, allowing you to filter, view, and save the results.

IDIH GUI provides:

- A conceptual overview of the application's purpose, architecture, and functionality.
- Describes the pages and fields in the application Graphical User Interface (GUI).

Logging in

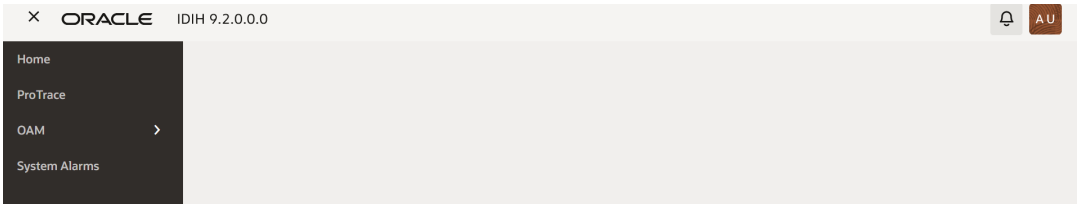
Perform the following procedure to log in:

1. Open a web browser.
2. Enter the URL.
3. Enter your login credentials.

> **Note**
>
> Presently there are three types of users: adminuser, traceuser, and guiadmin. For adminuser and traceuser the credentials remain same as per the respective user. the password must be redet upon logging in. See Change password

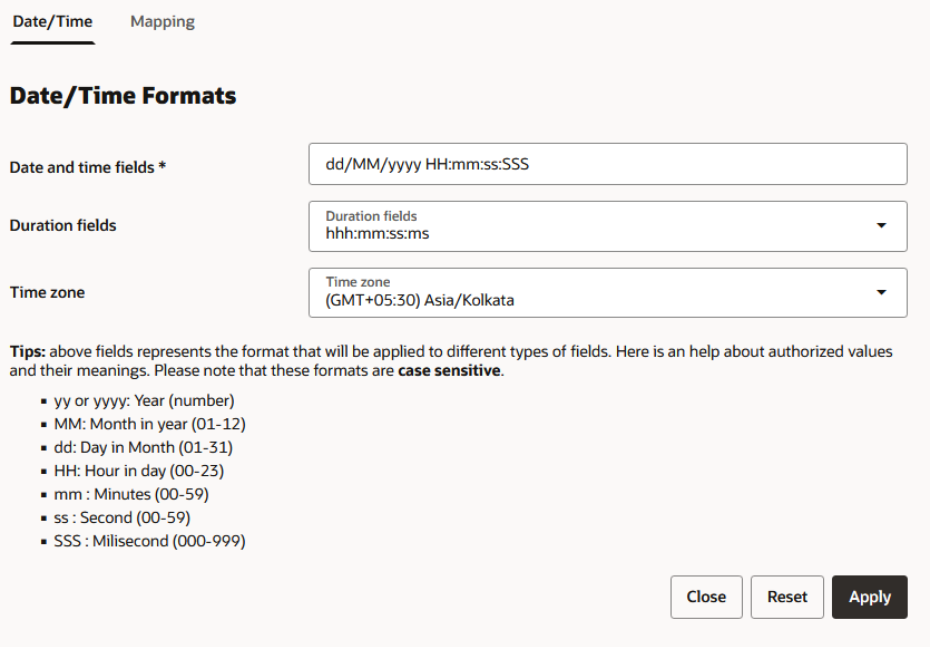
4. Click **Sign in**.
   The IDIH Home page opens.

Figure 2-1 Homescreen



5. In the right navigation pane of the IDIH home page, you can view your profile. When you click the profile you will view:
   a. Preferences
      Perform the following procedure to set the time format:
      i. On the IDIH Home page, in the right-side pane, click **profile**, and then, click **preferences**.
      ii. In the Preferences dialog box, perform the following:
         i. Click the **Date and time fields**.
            The Date and time fields is displayed. The asterisk denotes a required field.

Figure 2-2 Date/time settings



> **Note**
>
> Read the Tips on the screen to help configure the time format.

ii. Select the **Duration** field, using the drop-down arrow.
Duration: hours, minutes, seconds, and milliseconds of the Time format is displayed.

iii. Select the **Time zone**field, using the drop-down arrow. The local time zone must be chosen to get local time.

iv. Click **Close** to exit the window.

v. Click **Reset** to reset time.

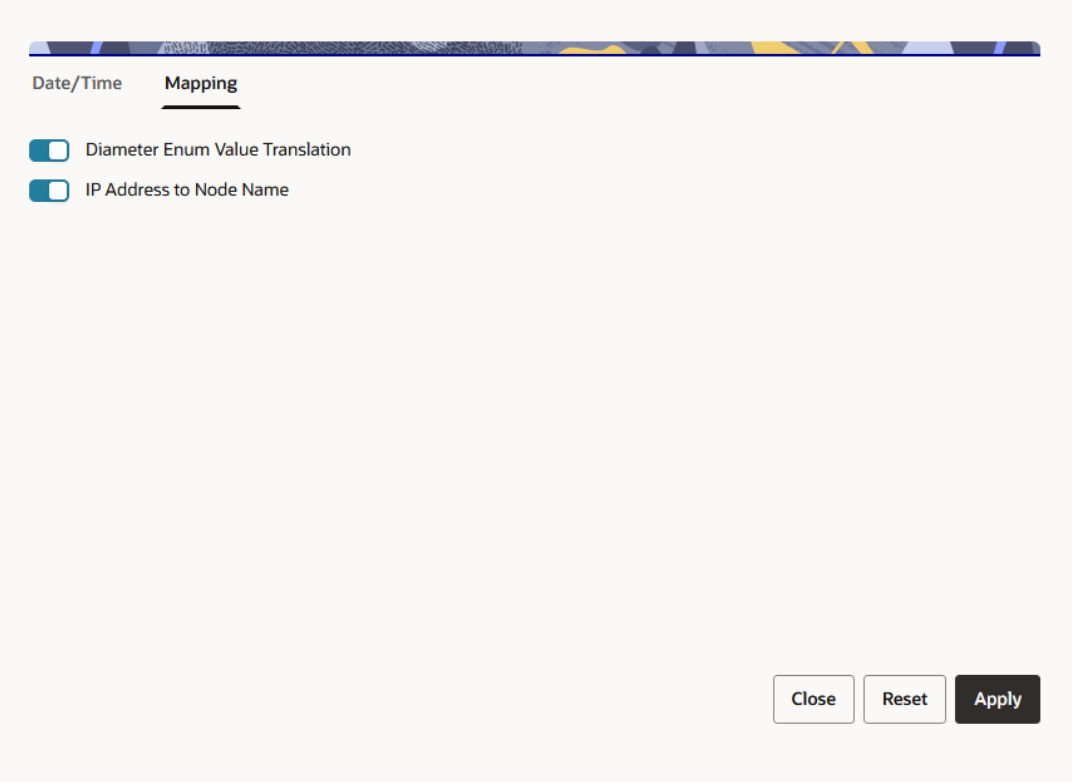
vi. Click **Apply** to save settings.

Setting Map preferences

Perform the following procedure to set the Map preferences:

1. On the IDIH Home page, in the right-side pane, click **Profile**, and then, click **Preferences**.
2. Toggle to **Mapping**.
3. In the **Mapping** dialog box, do the following:

Figure 2-3 Mapping



a. Toggle **Translate ENUM values** button to display text instead of numerals. Enumeration is used by TDRs to display text values instead of numeric. Rather than showing the numeral for Alarm Severity, the user interface will show the actual word, such as Major or Critical.

b. Check **IP Address to Node** Name to translate an IP Address to a textual Node Name.

c. Click **Reset** to reset the Mapping values to default.

d. Click **Apply** to save the changes.

Change password

Perform the following steps to change password:

1. On the IDIH home page, in the right-side pane, click profile, and then, click **Change password**.
   a. Enter the **Old Password** in the textbox.
   b. Enter the **New Password**.
   c. Confirm **New Password**.
   d. Click **Apply**, to apply the changes.

Logout

On the IDIH home page, in the right-side pane, click profile, and then, click **Logout** to exit user from the GUI. The user will be redirected to login page.

3
Diameter Application Supported

The following table describes the supported diameter application.

Table 3-1 Dictionaries

Application Name	Application ID
Base	0
Cx/Dx	16777216
Default	0
Gq Prime	16777222
Gx	16777238
Gxx	16777266
Rf	3
Ro/Gy	4
Rx	16777236
S13	16777252
S6a/S6d	16777251
S6b	16777272
S6m/S6n	16777310
S6t	16777345
S9	16777267
Sd	16777303
Sh/Dh	16777217
SLg	16777255
SLh	16777291
STa	16777250
Stats	NA
SWm	16777264
SWx	16777265
Sy	16777302
T4	16777311
T6a/T6b	16777346
Zh	16777221
TraceList	NA
UserQuery	NA

4

IDIH Configuration and Maintenance on DSR GUI

This chapter contains information on how to configure IDIH on the DSR GUI.

4.1 IDIH Options Configuration on DSR

Navigate to **Main Menu**, **Diameter**, **Troubleshooting with IDIH**, and **Configuration**, click **Options** to enable the **Launch IDIH** option from **Trace Maintenance** screen. The user has to configure IP or FQDN on the options screen (For FQDN, SSO (Single Sign-On) configuration is required).

4.1.1 Options Elements

The IDIH visualization address is entered by the user and is necessary for single sign-on to access IDIH directly from DSR without credentials.

The following table describes the fields on the IDIH Options screen:

Table 4-1 IDIH Options Elements

Field (* indicates a required field)	Description	Data Input Notes
Max Bandwidth*	The maximum amount of bandwidth specified in Mbps that is used for sending TTRs to IDIH. When the TTR bandwidth exceeds the configured maximum, DSR discards TTRs so the bandwidth required to send the remaining TTRs between DA-MP and IDIH does not exceed the configured maximum	Format: text box; numeric Range: 0-25 Default: 25 Mbps (26214400 bps)
IDIH Visualization Address	The IP address or FQDN of the remote IDIH server that visualizes the trace (when the **Analyze with IDIH** link is clicked on the **Maintenance** screen). If FQDN is configured then IDIH SSO will work. Hence SSO configuration is required. For more information, refer to Single Sign-On.	Format: text box Default: N/A

4.2 IDIH Global Options Configuration on DSR

Navigate to **Main Menu**, **Diameter**, **Troubleshooting with IDIH**, **Configuration**, and click **Global Options** to configure Global Options for the IDIH on DSR.

4.2.1 Global Options Fields

Table 4-2 describes the fields on the IDIH Global Options screen.

Table 4-2 IDIH Global Options Elements

Field	Description	Data Input Notes
Max active network traces	The number of max active network traces indicates how many active network traces are allowed at each DSR site within the network.	Format: Text box Default: 2 Range: 2-8
Max active site traces (per site)	The number of max active site traces (per site) indicates how many active site traces are allowed at each DSR site within the network. The number is automatically updated when the number of Max active network traces is changed.	Format: Text box Default: 6 Range: 0-6

4.3 Trace Overview

A trace is a set of conditions which, when met, causes trace data to be forwarded to IDIH for further analysis.

DSR determines which message should be captured based on trace criteria created and activated. The trace criteria identifies the following scope and content:

- Scope refers to the non protocol related elements such as connections or peers, used to select messages to evaluate trace content.
- Content refers to the protocol related elements such as command codes and AVPs, used to refine the trace criteria.

As DSR processes request and response messages, they are analyzed for matching any of the active trace definitions. If a match is found, message components along with supplemental information, known as trace data is transferred to the IDIH. The IDIH assembles the trace data and provides it to the user leveraging graphical visualization interfaces for additional filtering and analysis.

The above call flow shows IDIH trace cycle (ProTrace visualization). The LIR (Request) is routed to the local node, which then forwards the LIR to the HSS after mapping with various parameters, and finally the LIR reaches the HSS, which answers to the LIR. Here is an illustration (LIA is the response) that will be forwarded to MME.

4.4 Site Traces

A site trace is created for troubleshooting purposes, such as when traffic stops or does not process. These traces are related to specific traffic, different traces are created using DSR GUI with set of conditions which, when met, cause trace data to be forwarded to IDIH for further analysis.

Creating a Site Trace

A site trace is created from the **Traces** screen. The trace content types, content values, scope types, and scope values are supported. A site trace can only be created, edited, and deleted on the site that will run the trace.

Starting a Site Trace

A site trace is started from the **Traces** screen. A site trace can only be started from the GUI at the site.

Running a Site Trace

The site trace runs where the site trace was created.

Stopping a Site Trace

The **Traces** panel allows you to manually stop a site trace. A site trace can only be terminated from the GUI of the site where it is running. A site trace will be automatically stopped when either the time duration or number of matches limit is reached.

Viewing Site Trace Status

The **Maintenance** screen displays the current status of site traces. It can only be viewed from the GUI at the site that is running the trace.

For more information about creating Traces, see *Oracle Communications Diameter Signaling Router User Guide*.

4.5 IDIH Traces Configuration on DSR

The Diameter, and then Troubleshooting with IDIH, and then Configuration, and then Traces GUI screen on an SOAM server is used to configure traces used by the IDIH.

On the Diameter, and then Troubleshooting with IDIH, and then Configuration, and then Traces screen, the user can:

- Filter the list of entries, to display only the desired entries.
- Sort the list entries in ascending or descending order by clicking the column heading. By default, the list is sorted in ascending alphabetical order.
- Click Insert.
  The Diameter, and then Troubleshooting with IDIH, and then Configuration, and then Traces [Insert] screen opens. The user can add new Traces.
- Select a Trace entry in the list, and click Edit.
  The Diameter, and then Troubleshooting with IDIH, and then Configuration, and then Traces [Edit] screen opens. The selected Trace entry can be edited.
- Select a Trace entry in the list, and click Delete to remove the selected entry.

4.5.1 Traces Fields

Table 4-3 Traces Fields

Field (*indicates a required field)	Description
Trace Name	A name that uniquely identifies the Trace. Range: A 32-character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Default: N/A
Trace Location	Indicates whether a trace runs at the current site or at all sites in the network.
Trace Content	The Diameter message content to be matched for this trace. The combination of content type or content values specify the content elements and content values that a candidate message must match before the transaction that the message belongs to is sent to IDIH. Content Type: • Non-success answers: Answers with (Experimental) Result-Code>= 3000, or any message with the E-bit set. • Ad Hoc Requests: Any request that matches the specified content values. • Ad Hoc Answers: Any answer that matches the specified content values. • User Identity: Any message that contains the specified IMSI or MSISDN. AVPs searched for the specified IMSI or MSISDN value are automatically determined by the application ID(s) selected. • Equipment Identity : Any message that contains the specified IMEI. AVPs searched for the specified IMEI value are automatically determined by the application ID(s) selected. Range: Non-success answers, Requests, Answers, Ad Hoc Requests, Ad Hoc Answers, User Identity, Equipment Identity. Default: Select
Content Values	Provides the real value. The screen displays the Content Values to select the required parameter, operator, and value. Default: N/A
Scope Type	The scope used for the trace. Scope Type: • Connection: Messages arriving or leaving on specified connection are candidates for tracing. • Peer: Messages arriving or leaving on specified peer are candidates for tracing. • DSR Application: Messages going to or returning from specified DSR application are candidates for tracing. • All: all messages are candidates for tracing. Range: Connection, Peer, DSR, Application, All. Default: Select
Scope Value	The scope value used for the trace. Values will be populated based on the Scope Type selected. Default: Select
Number of Matches	The scope value used for the trace. Values will be populated based on the Scope Type selected. Default: Select
Time Duration	Stops the trace after it has been active for this amount of time (HH:MM:SS). Range: 00:00:01 - 96:00:00 Default: N/A

Table 4-3 (Cont.) Traces Fields

Field (*indicates a required field)	Description
Notes	Descriptive information about the trace Range: A 255-character string Default: N/A

4.5.2 Creating a Trace

Perform the following procedure to create a Trace:

1. Select **Diameter**, **Troubleshooting with IDIH**, and **Configuration**, and then **Traces**.
2. Click **Insert**. Navigate to **Diameter**, **Troubleshooting with IDIH**, and **Configuration**, and then Traces [Insert] screen appears.
3. Enter the **Trace Name** in the trace name field.
   The name must meet the following requirements:
   - Maximum length of 32 characters.
   - Valid characters are alphanumeric and underscore, must contain at least one alpha and must not start with a digit.
4. Select a **Trace Location** by selecting either **Site Trace** or the **Network Trace**.
5. Select a Content Type from the **Content Type** options.
   There are seven Content Types supported:
   a. Non-success answers
   b. Requests
   c. Answers
   d. AdHoc Requests
   e. Ad Hoc Answers
   f. User Identity
   g. Equipment Identity

Table 4-4 Content type

Field (* indicates a required field)	Description
Content Type*	The Diameter message content to be matched for this trace. The combination of content type or content values specify the content elements and content values that a candidate message must match before the transaction that the message belongs to is sent to IDIH. Content Type: • Non-success answers: answers with (Experimental) Result-Code>= 3000, or any message with the E-bit set. • Ad Hoc Requests: any request that matches the specified content values. • Ad Hoc Answers: any answer that matches the specified content values. • User Identity - any message that contains the specified IMSI or MSISDN. AVPs searched for the specified IMSI/MSISDN value are automatically determined by the application ID(s) selected. • Equipment Identity: any message that contains the specified IMEI. AVPs searched for the specified IMEI value are automatically determined by the application ID(s) selected. Range: Non-success answers, Requests, Answers, Ad Hoc, Requests, Ad Hoc Answers, User Identity, Equipment Identity. Default: -Select
Content Values	After selecting the content type, the screen displays the content values for selecting content elements and entering content values.

Table 4-5 Trace Scope

Field (* indicates a required field)	Description
Scope Type*	The scope used for this trace. Scope Type: • Connection: Messages arriving or leaving on specified connection are candidates for tracing. • Peer: Messages arriving or leaving on specified peer are candidates for tracing. • DSR Application: Messages going to or returning from specified DSR application are candidates for tracing. • All: - All messages are candidates for tracing. • Range: Connection, Peer, DSR, Application, All. Default: Select
Scope Value	The scope value used for this trace. Selection values will be populated based on the Scope Type selected.

Table 4-6 Trace Duration

Field (* indicates a required field)	Description
Number of Matches*	Number of Matches: stops the trace, after matching this many messages. Range: 1-1000 Default: N/A
Time of Duration*	Time: stop the trace after it has been active for this amount of time (HH:MM:SS). Range: 00:00:01 - 96:00:00 Default: N/A

Table 4-6 (Cont.) Trace Duration

Field (* indicates a required field)	Description
Notes	Descriptive information about the trace. Range: A 255-character string. Default: N/A

The Content Type field determines what Content Values are available. If the **Content Type** is set to Non-success answers, then no other content values are available. If the Content Type is set to Requests, then you may select an Application-ID, Command-Code, Origin-Host, Origin-Realm, Destination-Host, and or Destination-Realm. Application-ID, and Command-Code option, which contain a pre-defined list of supported Diameter interfaces. Additionally, all other parameters may be left blank as wildcards.

If the Content Type is set to Answers, then you may select an Application-ID, Command-Code, Origin-Host or Origin-Realm, Application-ID, and Command-Code option, which contain a pre-defined list of supported Diameter interfaces. Additionally, all other parameters may be left blank as wild cards.

If the Content Type is set to Ad Hoc Requests, then you may select an Application-ID, Command-Code, Origin-Host, Origin-Realm, Destination-Host, and or Destination-Realm. An optional content value is available to select an AVP (Attribute Value Pair) to be checked. Application-ID and Command-Code options contain a pre-defined list of supported Diameter interfaces to which you may also add. Additionally, all other parameters may be left blank as wild cards.

Note

- When the Content Type is set to Ad Hoc Requests or Ad Hoc Answers, an optional content value is available to select an AVP to be checked. This optional AVP is based on what AVPs are configured in the AVP Dictionary. For further information about the AVP Dictionary, see Oracle Communications Diameter Signaling Router Diameter User Guide
- For a non-grouped AVP all operators for the specified data type are allowed. For a grouped AVP, exists and does not exist operators are allowed only for the parent AVP. Checking is not allowed for either grouped or non-grouped Child AVPs.

If the Content Type is set to Ad Hoc Answers, then you may select an Application-ID, Command-Code, Origin-Host or Origin-Realm. Additionally, an optional content valueis available to select an AVP to be checked. Application-ID and Command-Code are selected from dropdown list and contain a pre-defined list of supported diameter interfaces to which you may also add. Additionally, all other parameters may be left blank as wild cards.

If the Content Type is set to User Identity, you may select an Application-ID. The Application-ID option lists a pre-defined list of supported Diameter interfaces, although you cannot add anything new to the list.

Note

After an Application-ID is selected, you can specify a user in the associate AVP as the criteria for selecting messages, which is identified by either IMSI or MSISDN.

If the Content Type is set to Equipment Identity, then you may select an Application-ID. The Application-ID option lists a pre-defined list of supported Diameter interfaces, although you cannot add anything new to the MSISDN list.

> **Note**
>
> After an Application-ID is selected, you can specify equipment in the associated AVP as the criteria for selecting messages, which is identified by IMEI.

a. Select the **Content Value** with appropriate **parameter**, **operator**, and **value**.
b. Select the **Scope Type**.
   The scope for a trace can be for a specific Connection, specified Peers, specified DSR Applications, or All messages.
c. Select the **Scope Value**.
   The scope value is determined by which Scope Type is selected.
d. Enter the **Number of Matches**.

> **Note**
>
> A maximum of 1000 matches is permitted.

e. Enter the Time Duration in HH:MM:SS format.

> **Note**
>
> The duration can be up to 96 hours.

f. Click **Submit**.

4.5.3 Editing a Trace

> **Note**
>
> If a trace is Active, it cannot be edited.

Perform the following procedure to edit a Trace:

1. Log in to the DSR GUI with your user credentials.
2. From the Main Menu of DSR, click **Diameter**, **Troubleshooting with IDIH**, and then **Traces**.
3. Select the trace you want to Edit and click **Edit** on the upper menu of the Traces Table.
4. **Editing Trace Data** dialog box opens. The selected Trace entry can be edited.
5. The **Content Type** field determines what content values are available.
   If the Content Type is set to Non-success answers, then no other content values are available.

If the Content Type is set to Requests, then the you may select an Application-ID, Command-Code, Origin-Host, Origin-Realm, Destination-Host, and/or Destination-Realm.Application-ID and Command-Code options, which contain a pre-defined list of supported Diameter interfaces. Additionally, all other parameters may be left blank as wildcards.

If the Content Type is set to Answers, then you may select an Application-ID, Command-Code, Origin-Host, or Origin-Realm. Application-ID and Command-Codeoptions, which contain a pre-defined list of supported Diameter interfaces. Additionally, all other parameters may be left blank as wild cards.

If the Content Type is set to AdHoc Requests, then you may select an Application-ID, Command-Code, Origin-Host, Origin-Realm, Destination-Host, or Destination-Realm. Additionally, an optional content value is available to select an AVP (Attribute Value Pair) to be checked. Application-ID and Command-Code options, which contain a pre-defined list of supported Diameter interfaces to which you may also add. Additionally, all other parameters may be left blank as wild cards.

Note

- When the Content Type is set to Ad Hoc Requests or Ad Hoc Answers, an optional content value is available to select an AVP to be checked. This optional AVP is based on what AVPs are configured in the AVP Dictionary. For further information about the AVP Dictionary, see Oracle Communications Diameter Signaling Router Diameter User Guide.
- For a non-grouped AVP all operators for the specified data type are allowed. For a grouped AVP, exists and does not exist operators are allowed only for the parent AVP. Checking is not allowed for either grouped or non-grouped Child AVPs.

If the Content Type is set to Ad Hoc Answers, then you may select an Application-ID, Command-Code, Origin-Host, and/or Origin-Realm. Additionally, an optional content valueis available to select an AVP to be checked. Application-ID and Command-Code are selected from pulldown lists and contain a pre-defined list of supported Diameter interfaces to which you may also add. Additionally, all other parameters may be left blank as wild cards.

If the Content Type is set to User Identity, then you may select an Application-ID. The Application-ID option lists shows a pre-defined list of supported Diameter interfaces, although the you cannot add anything new to the list.

Note

After an Application-ID is selected, you can specify a user in the associate AVP as the criteria for selecting messages, which is identified by either IMSI or MSISDN.

6. If the Content Type is set to Equipment Identity, then you may select an Application-ID. The Application-ID option list displays a pre-defined list of supported Diameter interfaces, although the user cannot add anything new to the list.

> **Note**
>
> After an Application-ID is selected, you can specify equipment in the associated AVP as the criteria for selecting messages, which is identified by IMEI.

7. Select a **Scope Type** from the Scope Type options.
   The scope value is determined by which Scope Type is selected.
8. Provide **Number of Matches** for the trace to find in the number of matches field.

> **Note**
>
> A maximum of 1000 matches is permitted.

9. Enter the **Time Duration**.
   The duration can be up to 96 hours.
10. Click **Submit**.

4.5.4 Deleting a Trace

Perform the following procedure to delete a Trace:

> **Note**
>
> If a trace is "Active", it cannot be deleted.

1. Log in to the DSR GUI with your user credentials.
2. From the Main Menu of DSR, click **Diameter troubleshoot** and then **Troubleshooting with IDIH**, and then **Configuration**, and then **Traces**.
3. Select the trace to be deleted.
4. Click **Delete**, A confirmation dialog box appears.
5. click **OK** the trace will be deleted.
6. Click **Cancel** to return to the previous screen without deleting the trace.

4.6 IDIH Traces Maintainance on DSR

After a trace is created, it appears on the Diameter, and then Troubleshooting with IDIH, and then Maintenance, and then Traces GUI screen on the SOAM server.

The user can filter the list of entries to display only the desired entries, as well as sort the list entries in ascending or descending order by clicking on a column heading.

A trace begins with a Network Operational Status and a Site Operational Status of Inactive. Over the course of a trace's existence, the Network Operational Status may display a value of Inactive, Active, Completed, or None, depending on what action is occurring. The Site Operational Status displays a value of Inactive, Active, Impaired, or Completed.

To start a trace, select a trace in the list and click Start.

After a trace is started, its Status changes to Active. While a trace is Active, the Number of Matches, Matches Remaining, and Time Remaining will be displayed.

> **Note**
>
> To start multiple traces at once, hold CTRL, select the desired entries, and click Start. Only up to 8 traces may be Active at once (a combination of Network and Site traces depending on the settings configured on the Diameter, and then Troubleshooting with IDIH, and then Configuration, and then Global Options GUI screen).

If desired, the user can select a trace in the list and click Stop to stop it from running. To stop multiple traces at once, hold CTRL, select the desired traces, and click Stop.

If a problem occurs while the trace is running (due to trace limiting or trace throttling, for example), the trace will stop and its status changes to Impaired and the Impaired column will show as Yes.

Depending on if a trace's status is Active, Inactive, or Impaired, the site operational reason is:

- Inactive - a trace is not active because it is impaired
- Normal - a trace is running normally
- Disabled on Some MPs - a trace has been disabled on some MPs
- Throttled

  > **Note**
  >
  > This state can occur for 2 reasons:
  >
  > – The IDIH has exceed the max bandwidth configured in Options Elements.
  >
  > – An abatement threshold is reached

- DSR-IDIH Connection Down on Some MPs - the connection between DSR and IDIH is down on some MPs
- Manually Stopped - a running trace was stopped by the user
- Match Limit Reached - the limit on the number of matches configured in Traces Fields has been reached
- Time Limit Reached - the duration time configured in Traces Fields has been reached.
- DA MP Restarted - used only for the case where a trace is stopped due to an MP restarting or a DSR/IDIH connection status change
- Activation Failed on Some MPs
  When a trace is finished running, the Status changes to Completed.

  > **Note**
  >
  > The maximum allowed number of Completed traces is 1000. Once over that number, no more traces can be activated and the trace list must be cleaned up.

The Start or Stop Time column for Active traces shows the time that the trace was started. For Completed traces, it shows the time that the trace was stopped.

The Notes column displays additional user-contributed information about a trace being run.

The Action column allows the user to select the Analyze with IDIH link.

If the user clicks the Analyze with IDIH link associated with a particular trace, a more detailed analysis of that trace opens in the ProTrace Application.

> **Note**
>
> – When using Analyze with IDIH, the user is able to access IDIH using single sign-on. If single sign-on is unavailable, the user may use the `guiadmin` user ID to access IDIH. For more information about IDIH trace user see, Accessing IDIH from DSR.
>
> – Only up to 6 active traces may be analyzed at once.

If the user clicks **Launch IDIH**, a historical list of all available traces on IDIH will open.

The user can delete a trace in the list by clicking **Delete**.

> **Note**
>
> Traces can only be deleted if the Site Operational Status is Completed.

The user can also check the **Pause Updates** box to prevent the **Diameter**, and then **Troubleshooting with IDIH**, and then **Maintenance**, and then **Traces** screen from automatically refreshing.

4.7 Accessing IDIH from DSR

Users will be able to access IDIH using single sign-on which does not require the user to login again for IDIH, provided a primary DNS server is being used in conjunction with IDIH. However, using this mechanism, users will be able to access only the ProTrace application.

> **Note**
>
> Single sign-on must be configured prior to accessing IDIH from DSR. For information about how to configure single sign-on, refer to the *Operations, Administration, and Maintenance (OAM) User's Guide*.

To log into IDIH from DSR SOAM GUI:

1. Using a Web browser, type the **FQDN** for a DSR SOAM.
2. Log into the SOAM by entering the correct **User Name** and the corresponding **Password**.

> **Note**
>
> Check with the system administrator for the user name and password.

3. Navigate to **Diameter** and **Troubleshooting with IDIH**, and then **Maintenance**, and then **Traces**. Click Launch IDIH.
4. Alternatively, select a trace and click **Analyze With IDIH**.
   Example:
   - In the absence of a DNS server, the user may authenticate directly on the IDIH server using the **guiadmin** user ID. This user ID provides the same level of functionality as using single sign-on from the SOAM.
   - The procedure for accessing IDIH with the **guiadmin** user ID is almost the same as for signing in using single sign-on with the exception of replacing **FQDN** with **IP Address**.

4.7.1 IDIH Access Control

Access to IDIH can be permitted or restricted based on settings found on the **NOAM Main Menu**, and then **Administration**, and then **Access Control**, and then **Groups** page.

For further information about how to modify these settings, see *Oracle Communications Operations, Administration, and Maintenance User's Guide*.

4.8 IDIH Server Configuration on DSR

Perform the following procedure to configure IDIH broker details on DSR:

1. From the **Main Menu** of the GUI, click **Diameter**, and click **Troubleshooting with IDIH**, and then click **Configuration**.
2. From the **Configuration** menu, click **IDIH Server Config**.
3. On the **IDIH Server Configuration** page, provide the **Broker IPs** in the text box and configure other required parameters.

> **Note**
> - To enable SSL, select **SSL** from the drop-down menu of **Security Protocol** and configure the required fields (**SSL Certificate**, **SSL Key Password**, **SSL Key**, and **SSL CA**).
> - To enable SASL_SSL, select **SASL_SSL** from the drop-down menu of **Security Protocol** and configure the required fields (**SSL Certificate**, **SSL Key Password**, **SSL Key**, **SSL CA**, **SASL Username**, and **SASL Password**.
> - IDIH Server configuration screen can be edited only when DSR-IDIH connection is disabled.

4. Click **Apply** to apply the properties.

> **Note**
> - The above configuration steps are to configure DSR with IDIH (IDIH Server Configuration).
> - The IDIH broker configuration such as "creating topics" and "creating partitions" are configured during the IDIH installation.

4.8.1 IDIH Server Configuration Fields

Table 4-7 IDIH Configuration Fields

Field	Description	Data Input Notes
Remote Server Name*	Unique identifier used to label a Remote Server.	**Format**: Text box **Default**: NA **Range**: A 32 character string. Valid characters are alphanumeric, minus sign, period, and underscore. Must start with an alphanumeric or an underscore and end with an alphanumeric. A value is required.
Broker IPs*	IP and port of IDIH remote cluster.	**Format**: Text box **Default**: NA **Range**: Any valid IPv4 address with port. A value is required.
Topic Name *	Defines IDIH topic name which is a fundamental unit for event or message organization. Messages with the same topic name will be appended one after another creating a log file. Producers can push messages into the tail of these logs while consumers pull messages off from the head. It is possible to get logical segregation between messages and events, similar to how various tables in a database can contain different sorts of data. **Note** Topic name is default and cannot be modified.	**Format**: Text box **Default**: com.oracle.dsr.idih.ttr **Range**: Topic name can include the following characters: a-z, A-Z, 0-9, . (dot), _ (underscore), and - (dash). A value is required.
Compression Codec	Used for compressing message sets.	**Format**: Dropdown **Default**: Gzip **Range**: None, Gzip, Snappy, Lz4.
Compression Level	Compression level parameter for algorithm selected by configuration property `compression.codec`. Higher values will result in better compression at the cost of more CPU usage.	**Format**: Text box **Default**: 0 **Range**: [0-9] for gzip, [0-12] for lz4, only 0 for snappy.
Batch Size	The producer will attempt to batch records together into fewer requests whenever multiple records are being sent to the same partition.	**Format**: Text box **Default**: 2147483647 **Range**: 1-2147483647
Max Request Size	The maximum size of a request in bytes. This setting will limit the number of record batches the producer will send in a single request to avoid sending huge requests.	**Format**: Text box **Default**: 2147483647 **Range**: 1-2147483647

Table 4-7 (Cont.) IDIH Configuration Fields

Field	Description	Data Input Notes
Linger Time	Delay in milliseconds to wait for messages in the producer queue to accumulate before constructing message batches (MessageSets) to transmit to brokers.	**Format**: Text box **Default**: 0 **Range**: 0
Acknowledgements	Number of replicas to be written successfully before acknowledging the publish request.	**Format**: Text box **Default**: 1 **Range**: -1 or all, 0, 1
Max Idle Time	Closes idle connections after the number of milliseconds specified by this configuration.	**Format**: Text box **Default**: 540000 **Range**: 0-3600000
Socket Connection Timeout	The amount of time the client will wait for the socket connection to be established. If the connection is not built before the timeout elapses, client will close the socket channel.	**Format**: Text box **Default**: 10000 **Range**: 1000-2147483647
Send Buffer Size	The size of the TCP send buffer (SO_SNDBUF) to use when sending data. If the value is -1, the OS default will be used.	**Format**: Text box **Default**: 131072 **Range**: 0-131072
Max In Flight Request	The maximum number of unacknowledged requests the client will send on a single connection before blocking.	**Format**: Text box **Default**: 5 **Range**: 0 - 5
Max Request Timeout	This controls the maximum amount of time (in milliseconds) the client will wait for the response of a request. If the response is not received before the timeout elapses, the client will resend the request if necessary or fail the request if retries are exhausted.	**Format**: Text box **Default**: 30000 **Range**: 0-30000
Max Retries	Setting a value greater than zero will cause the client to resend any record whose send fails with a potentially transient error.	**Format**: Text box **Default**: 2147483647 **Range**: 0-2147483647
Max Delivery Timeout	An upper bound on how long it takes to communicate success or failure after calling send() returns. This limits the total time that a record will be delayed prior to sending the report, the time to await acknowledgment from the broker (if expected), and the time allowed for retriable send failure.	**Format**: Text box **Default**: 120000 **Range**: 0-120000
Metadata Max Age	The period of time in milliseconds after which we force a refresh of metadata even if we haven't seen any partition leadership changes to proactively discover any new brokers or partitions.	**Format**: Text box **Default**: 300000 **Range**: 0-300000
Reconnect Backoff Max Time	The maximum amount of time in milliseconds to wait when reconnecting to a broker that has repeatedly failed to connect. If provided, the backoff per host will increase exponentially for each consecutive connection failure, up to this maximum time. After calculating the backoff increases to 20% random jitter is added to avoid connection storms.	**Format**: Text box **Default**: 1000 **Range**: 0-1000

Table 4-7 (Cont.) IDIH Configuration Fields

Field	Description	Data Input Notes
Reconnect Backoff Time	The base amount of time to wait before attempting to reconnect to a given host. This avoids repeatedly connecting to a host in a tight loop. This backoff applies to all connection attempts by the client to a broker.	**Format**: Text box **Default**: 50 **Range**: 0-50
Retry Backoff Time	The amount of time to wait before attempting to retry a failed request to a given topic partition. This avoids repeatedly sending requests in a tight loop under some failure scenarios.	**Format**: Text box **Default**: 100 **Range**: 0-100
Max Connection Retry	Time in minutes within which the producer instance makes maximum number of retries to fetch the metadata from the IDIH server.	**Format**: Text box **Default**: 10 **Range**: 2-10 minutes
Security Protocol	Protocol used to communicate with brokers.	**Format**: Text box **Default**: SSL **Range**: PLAINTEXT, SSL

Table 4-8 SSL Properties

Field	Description	Data Input Notes
SSL Certificate	File name of the file in PEM format consisting the client certificate.	**Format**: Browse to select the file.
SSL Key	File name of the file in PEM format consisting the client private key in encrypted format.	**Format**: Browse to select the file.
SSL CA	File name of CA in PEM format used for certificate verification.	**Format**: Browse to select the file.
SASL Username	User name used for authenticating the IDIH client.	**Format**: Text box **Default**: NA **Range**: The length of the user name should be between 8 and 64 characters. The user name accepts only alphanumeric characters.
SASL Password	Password used for authenticating the IDIH client.	**Format**: Text box **Default**: NA **Range**: The length of the user name should be between 8 and 64 characters. The user name accepts only alphanumeric characters.

4.9 IDIH Connection Maintenance

4.9.1 Connection Status

On the Connection Status page, users can monitor, enable, and disable the IDIH connection.

Perform the following procedure to enable the IDIH connection:

1. From the main menu of the GUI, click **Diameter** and **Troubleshooting with IDIH** and then **Maintenance**, click **Connection Status**.

2. From the **Connection Status** page, select any of the available MPs.
3. Click **Enable** to enable the IDIH server connection or click **Disable** to disable the IDIH server connection.

> **Note**
>
> The **Admin Status** is automatically enabled after the restart of DAMP (Diameter Agent Message Processor).

4.9.2 IDIH Server Status

IDIH Server Status allows the users to view the connection status for the available MPs (Message Processors).

To view IDIH Server Status:

1. From the main menu of the GUI, click **Diameter** and **Troubleshooting with IDIH** and then click **Maintenance**.
2. Click **IDIH Server Status**.
3. On the **IDIH Server Status** page, select one of the MPs to view the connection status of the available MPs.

5
Trace Analysis

This chapter provides information about functionality that will be used within IDIH to analyze traces.

5.1 ProTrace

Using the ProTrace tab, you can view traces that are configured on DSR. ProTrace traces calls, transactions, and sessions using Trace Transaction Records (TTR), metadata, and DSR configuration data. The results are provided in the form of summary records, with each record having information specific to the DSR interface used to send or receive messages.

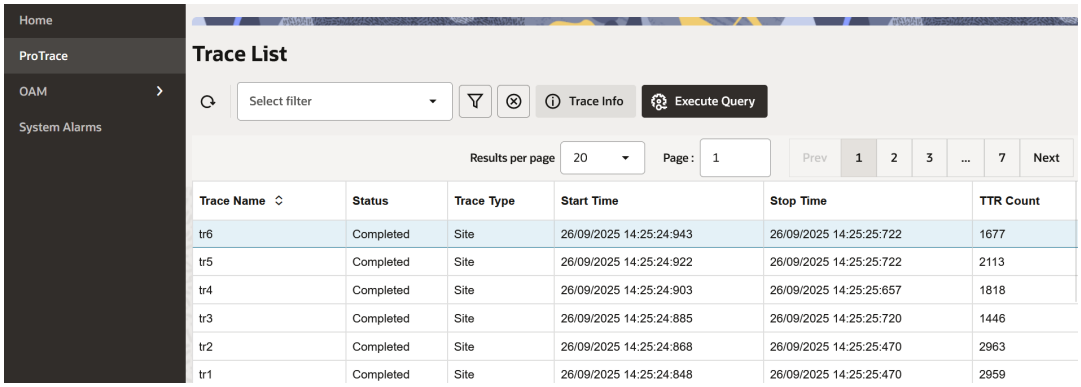
ProTrace operates within a trace context and enables you to manage, create, modify, delete and store queries for a specific interface. ProTrace serves as the end-user interface.

5.1.1 Viewing Traces

Perform the following procedure to view traces on the IDIH GUI:

1. On the IDIH GUI, in the left navigation pane, click the **ProTrace** tab. The following page appears with the list of traces.

Figure 5-1 TraceList



2. To view the summary of a trace, click the required trace from the **Trace Name** column.
3. In the upper center of the page, click **Trace info**.

Figure 5-2 Trace Info

The summary of the trace appears on the screen.

Figure 5-3 Trace summary

5.1.2 Trace List

The Trace List displays all traces configured in DSR.

Trace List tool toolbar

The toolbar provides a means of selecting and organizing traces.

The following table describes the fields in the Trace List:

Table 5-1 Trace list tool bar

Field	Description
Results per page	Displays the total number of traces per page.
Prev page	Opens the previous page.
Next	Opens the next page of traces.
Refresh	Reloads the trace list.
Select filter	Allows the user to select the queries that are saved.
Saved trace query	Allows the user to select the queries that are saved.
Filter	Opens the saved queries page, where you can filter the list of queries.
Delete selected trace	Allows the user to delete a trace.
Trace info	Allows a user to view the summary of the selected trace from the trace list.
Execute Query	Allows the user to view the ladder diagram of the transactions and view the payload of message routing, and also allows to export the Trace in HTML and PCAP format.

Table 5-2 Trace List Table Fields

Field	Description
Trace name	A name that uniquely identifies the trace.
Status	The completion status of the trace, which can be either In-progress or Completed.

Table 5-2 (Cont.) Trace List Table Fields

Field	Description
Trace Type	The type of trace can either be site or network based.
Start time	The start date and time of the trace.
Stop time	The end date and time of the trace.
TTR count	The number of messages matched in a particular trace.

5.1.3 Query List

The Query List panel contains list of queries you can run on the selected trace. These queries are user's saved queries or queries shared by other users.

Table 5-3 Query List toolbar

Field	Description
Refresh	Reloads the current screen and displays if any new changes.
Select filter	Allows the user to select the saved queries.
Filter	Allows the user to filter the queries.
Create new query	Opens the dialogue screen to add a query.
Modified selected query	Opens the current query for modification.
Delete selected query	Deletes the current query
Run selected query	Runs a query of the selected trace in the list and provides a detailed analysis for the selected trace.

Below table describes the different fields available for each query:

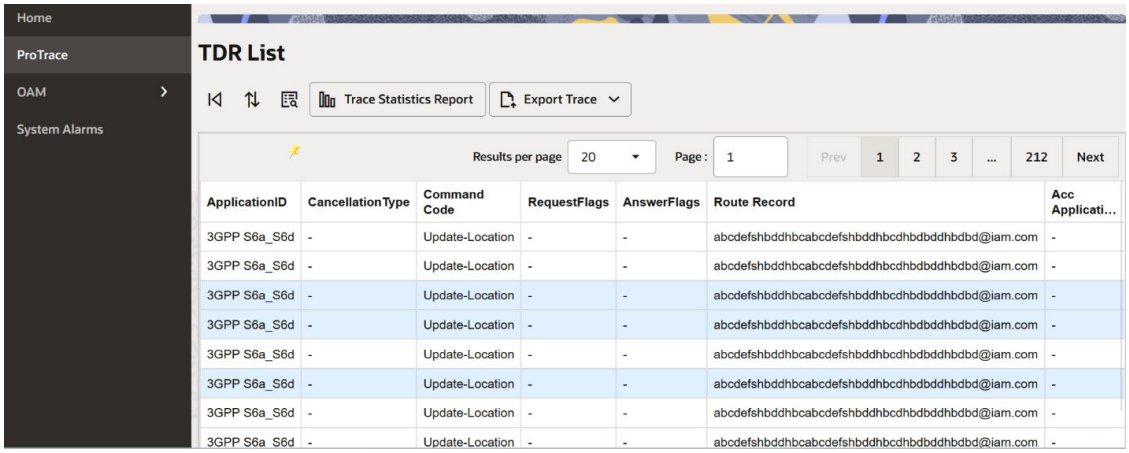
Table 5-4 Query List Table Fields

Field	Description
Name	Name of the query.
Description	Details of the query.
Owner	This field specifies the number of owners of the selected query.
Created	Specifies the time of creation

5.1.4 TDR Panel

The TDR panel displays a list of transactions (TDRs) that match a specific query. If no conditions are specified in the query, the panel displays all TDRs for the selected trace and interfaces. The TDRs for the same TTR are displayed next to each other with the same backdrop color.The result is divided into pages, you can define the page size and you can navigate through the pages such as, first page, previous, and next page.

Figure 5-4 TDR



TDR Panel Toolbar

A TDR is a database record that summarizes a DSR transaction, one request or answer message pair and associated TTR events and DSR metadata associated with it. Every TDR is associated with a dictionary, which describes its structure.

The following table describes the fields in the TDR:

Table 5-5 TDR Panel tool bar

Field	Description
Back	Returns to the trace list.
Sort	Sorts the TDRs in ascending and descendig order.
TDR table search	Searches for specific TDR records.
Trace Statistics Report	Opens the Trace Statistics window and displays statistics associated with the selected trace.
Export trace	Exports the TTR results. These results are exported in HTML and PCAP format.

Note

- ProTrace exports payload data in IPv4 based on the original transport type. TCP or SCTP transport is used in the export based on the original transport type. Source IP, source port, destination IP and destination port from the payload are used. When the payload size exceeds the maximum of TCP/SCTP packet size, the payload is segmented into multiple IP packets so that 3rd party tools can assemble and present it as a single diameter payload.
- Payloads sent from DSR to IDIH contain diameter layer only (no IP or TCP/SCTP layers). Therefore, IDIH makes a best effort to simulate those layers when constructing the PCAP file for export. Trace exports up to 1 MB of payload data. The rest of the payloads are ignored. You can refine the query to accommodate all the payload you want to export and re-export it.
- When TLS or DTLS is used as the transport, the export displays TCP for TLS and SCTP for DTLS as the transport value.
- When encoding and displaying AVP User-Password, IDIH does not decode the password and display it in a readable format, including in the ProTrace Decode Panel, HTML export, and TDR or TTR PCAP export.

The TDR list for a network trace highlights all TDRs related in the same fashion as highlighting is for site TDRs. All related TDRs are grouped and highlighted (white or blue), regardless if the TDRs are from a network trace or site trace. When TLS or DTLS is used as the transport, ProTrace displays these two protocols in the transport column.

5.1.5 TTR Events Panel

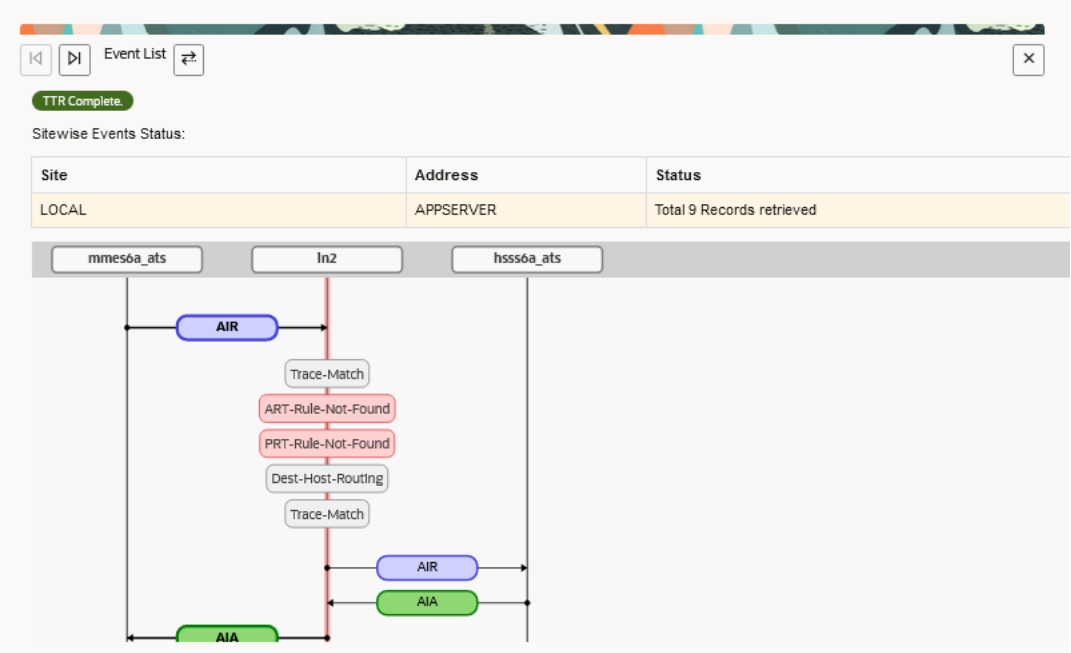
The TTR Event Panel displays a list of all TTR events related to the selected transaction (TDR). When you select a TDR in the TDR Panel, the TTR Event Panel is updated with the associated TTR events.

5.1.6 Ladder Diagram

The Ladder Diagram graphically represents the TTR events, offering more details beyond what is provided in the TTR event panel. Additionally, ProTrace will analyze and display client redirect events as they are received.

you can view the ladder diagram by clicking on any trace from the TDR list.

Figure 5-5 ladder diagram



You can hover over the ladder diagram to view details about that specific bubble in the Diameter Full Decoding Panel. You can also click Toggle button to view events in a table format, which allows a specific row to appear in the Diameter Full Decoding Panel.

5.1.7 Ladder Diagram Visualization

The following table describes the Ladder Diagram Visualization:

Table 5-6 Ladder diagram

Event type	Event Scope	Event diagram Visualization
Request Message Received/Sent	IR, ER	Blue bubble with arrow from source node to destination node
Answer Message Sent or Received with Success Result Code (RC< 3000)	IA, EA	Green bubble with arrow from source node to destination node
Answer Message Sent or Received with Success Result Code (RC< 3000)	IA, EA	Red bubble with arrow from source node to destination node
Message Created	App Data	Gray bubble on DSR node
App Invoked	App	Orange bubble beside DSR node with arrows from DSR to and from Application bubble
App Result	App Data	App Result appends a text to the corresponding Application's tool tip
App Invocation Failed	IR Data, IA Data	App Invocation Failed makes the corresponding Application bubble red and appends text to its tooltip.

Table 5-6 (Cont.) Ladder diagram

Event type	Event Scope	Event diagram Visualization
Trace Match	IR Data, ER Data, IA Data, EA Data	Gray bubble on DSR node
Linked TTR	IR Data	No visualization
ART Rule Match	IR Data	Gray bubble on DSR node
ART Rule Not Match	IR Data	Red bubble on DSR node
PRT Rule Match	IR Data	Gray bubble on DSR node
PRT Rule Not Match	IR Data, IA Data	Red bubble on DSR node
Unavailability Action	IR Data	Unavailability Action makes the previous event bubble red.
Route List Selected	IR Data	Gray bubble on DSR node
Dest-Host Routing	IR Data	Gray bubble on DSR node
Alternate Implicit Routing	IR Data, ER Data, IA Data, EA Data	Alternate Implicit Routing makes previous metadata bubble red and appends a text in its tool tip.
Route Group Selected	IR Data	Gray bubble on DSR node
Mediation Rule Match	IA	Gray bubble on DSR node
Request Rerouted	IA Data	Gray bubble on DSR node
Answer Timeout	App Data	Arrow from source node to destination node
Answer Matching Failed	App Data	Red bubble on DSR node
Address Resolution Match	App Data	Address Resolution Match appends a text to the corresponding Application bubble.

5.1.8 ProTrace Full decoding Panel

When you select a payload event from the Event Diagram, the complete decoding Panel displays the associated message. This view describes each byte of the selected message.

The ProTrace Full Decoding Panel is then divided into two panels. The first panel displays the payload bytes for the messages. The second panel displays the Message Header and all decoded AVPs in readable format. It displays every field from the header and AVP. Each field in the message header and AVP is displayed on a separate line.

5.1.9 IDIH Trace Statistics

The IDIH gathers statistics based on the trace selected from the trace list panel.

Table 5-7 Trace statistics field

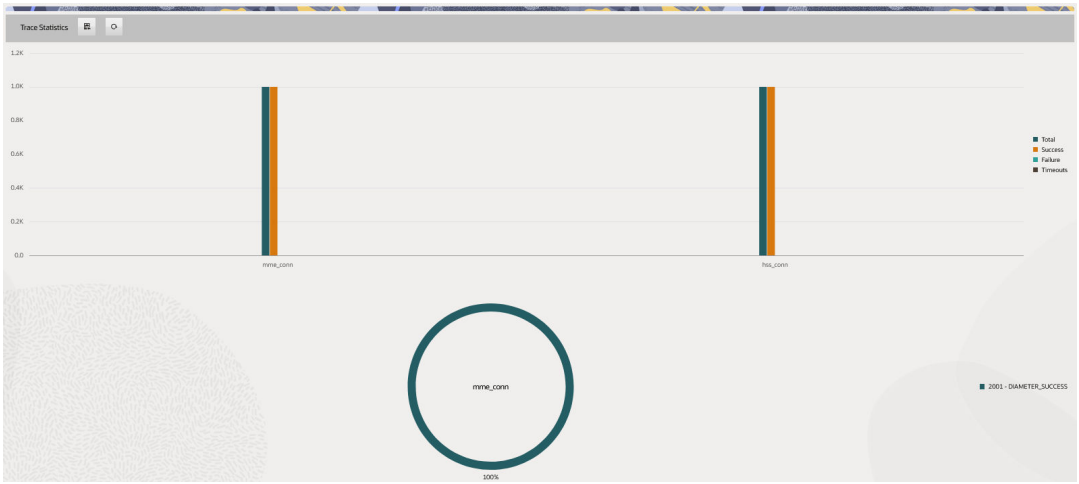
Field	Description
Back	Navigates to trace list panel.
Refresh	Reloads the current screen.

The statistics have various dimensions:

1. Total: displays the total value.

2. Success: displays the successful value of traces.
3. Failure: displays the failed value of traces.
4. Timeouts: number of time-out transactions.

Figure 5-6 Statistics



The statistics count the number of transactions for every combination of dimension values seen in received transactions. It counts transactions with result code only. If the TTR is missing an Answer message or the Answer message is missing a result code AVP, then the transaction is not counted. The statistics are continuously generated and stored in an mysql database. The complete statistics will be available up to five minutes after the trace has finished or has been stopped.

ProTrace reads the statistics and displays it in the form of bar and pie charts:

a. When you hover over the bar chart, it displays Node, Value, and Status.
   i. Node: Name of the trace.
   ii. Value: value of the trace.
   iii. Status: Provides the status of the trace.
b. Pie chart
   When you hover over the pie chart, it displays the Series and Value.

Figure 5-7 Pie chart

> **Note**
>
> If any stop event missed due to network issue or any other issues, IDIH GUI will mark those traces completed after 24 hours.

6
OAM

IDIH OAM application offers functionality to configure dictionaries and manage the visibility of AVPs (Attribute-Value Pairs). It also provides options for masking, filtering, and retrieving managed object data.

6.1 Dictionary

A dictionary is a metadata describing a set of key fields (along with information such as their name, type, description, and possible values) that are captured for a single transaction and summarize it. One dictionary describes transactions on one interface (such as DiameterS6a/S6d or Diameter Gx). Each interface supported by the ProTrace application has its own dictionary.

Table 6-1 Dictionary fields

Fields	Description
Refresh	Reloads the dictionaries.
Edit Dictionary	Allows to edit the selected dictionary.
Search	Allows to search the dictionary.
Delete	Allows to delete a dictionary.

ProTrace supports multiple dictionaries:

Table 6-2 Dictionaries

Dictionaries	Interface
Diameter Base	Base
Diameter Cx/Dx	Cx/Dx
Diameter Default	All unsupported applications
Diameter Gq Prime	Gq
Diameter Gx	Gx
Diameter Gxx	Gxx
Diameter Rf	Rf
Diameter Ro/Gy	Ro/Gy
Diameter Rx	Rx
Diameter S13	S13
Diameter S6a/S6d	S6a/S6d
Diameter S6b	S6b
Diameter S6m/S6n	S6m/S6n
Diameter S6t	S6t
Diameter S9	S9
Diameter Sd	Sd
Diameter Sh/Dh	Sh/Dh

Table 6-2 (Cont.) Dictionaries

Dictionaries	Interface
Diameter SLg	SLg
Diameter SLh	SLh
Diameter STa	STa
Diameter Stats	Stats
Diameter SWm	SWm
Diameter SWx	SWx
Diameter Sy	Sy
Diameter T4	T4
Diameter T6a/T6b	T6a/T6b
Diameter Zh	Zh
TraceList	NA
UserQuery	NA

6.1.1 Modifying Dictionary

Some attributes of dictionary fields can be modified, masked, or hidden from the display.

When you select any dictionary and click **Edit Dictionary**, the display changes to show the fields for the selected dictionary. Following are the various attributes of fields that can be modified:

- Short Name
- Description
- Name
- Enumeration
- Filterable
- Displayable - If checked, field is displayed in ProTrace output
- Mask Action
  - None - No characters are hidden, Masked Characters value remains 0 (zero - not editable).
  - All - All characters are hidden, Masked Characters value remains 0 (zero - not editable).
  - From Start - Valid Masked Characters value is 0 to 2147483647
  - From End - Valid Masked Characters value is 0 to 2147483647
- Editing attributes of fields:
  1. To change a non-checkbox field, double click the field and enter or change the value. Clicking return or navigating to a new field or row will automatically save your changes.
  2. To change a checkbox field, click the box to toggle the value. Again, click return or navigate away from the field will, which will automatically change the value.
  3. The Esc key will help discard a change while editing.
- Modifying Enum Display Fields

If the dictionary field has Enum field (Enumeration check box has a check), then the Short Name value for each enumeration is editable. The enumeration values will appear automatically in the 2nd grid of the page, with a header of Enum Value Mappings.

6.1.2 Deleting a Dictionary

Following are the steps to delete a dictionary:

1. Select a Dictionary row and click **Delete** icon.

> **Note**
>
> The only method to recover a lost dictionary from any interface is to restart the microservice from the backend service virtual machine.

2. The selected Dictionary is deleted.

6.2 AVP Hiding

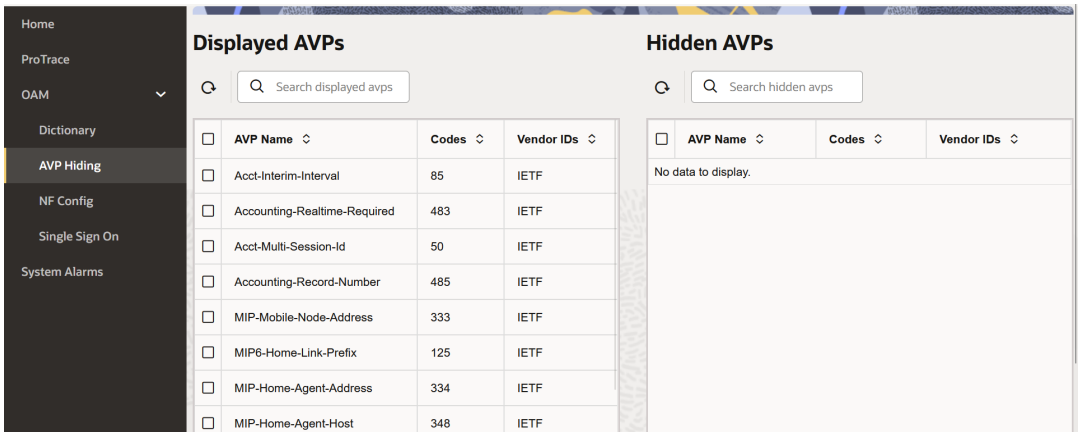
The user can hide the visible AVPs, which will be hidden across the entire UI for all the dictionaries.

To hide an AVP:

1. From the left navigation pane of the main menu, click **OAM** and select **AVP Hiding**.
2. In the **Displayed AVPs** screen, select the AVP name that you want to hide by checking in the check box.
3. Click and drag the AVP from the **Displayed AVPs** to **Hidden AVPs**.

> **Note**
>
> In case of Group AVPs, hiding the parent AVP also hides the child AVPs.

Figure 6-1 Displayed AVPs



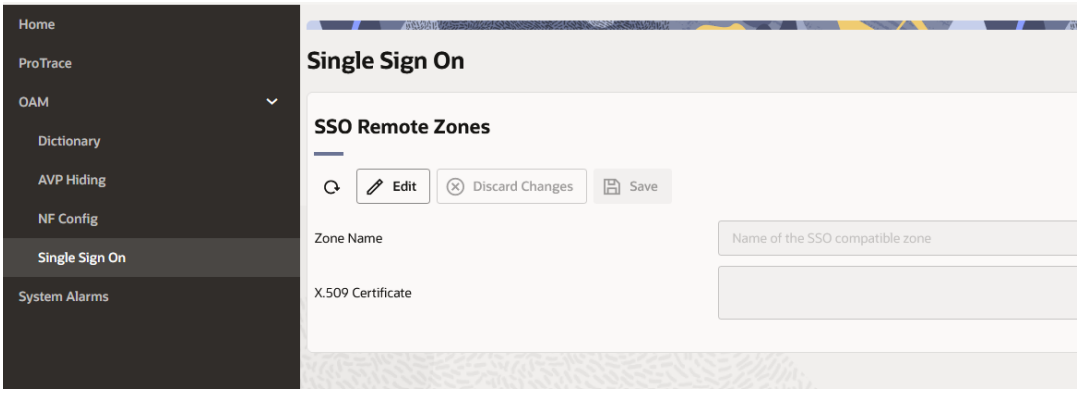
6.3 Single Sign-On

Single sign on (SSO) is a session and user authentication service that permits you to use one set of login credentials for example, a username and password to access multiple applications.

Perform the following steps to configure single sign-on

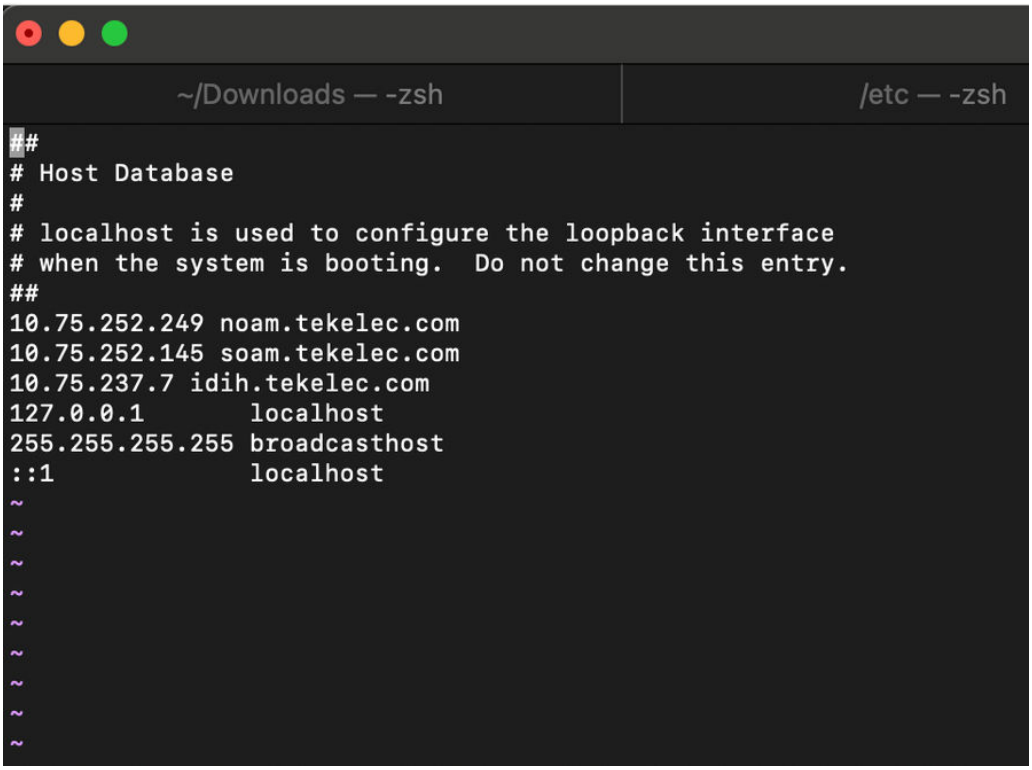
1. From the DSR NOAM, navigate to main menu **Administration** and then **General Options**, and in the **General Options** page, set **Certificate Domain Name** to `tekelec.com`.
2. From the Main Menu, navigate to **Administration**, **Access Control**, and **Certificate Management**, select **Establish SSO Zone**.
3. Provide **Certificate Name** as tekelec, select **Report** and copy only certificate(not private key).
4. From the main menu, navigate to **Diameter**, **Troubleshooting with IDIH Configuration**, click **Options**, and then set **IDIH Visualization address** to **IDIH FQDN** only.
5. Ensure **API Gateway Service SSL** is enabled.
   a. Login to service VM.
   b. Edit `cnidih_VM.yaml` file in the cnidih portal section.
   c. Modify the following property `GBU_RAPID_PUBLIC_SERVER_URL=https:\/\/idih.tekelec.com`.
6. From the OAM, click **Single Sign On** and provide `tekelec` as certificate name and the copied certificate from NOAM in the certificate section.

Figure 6-2 Single Sign On



7. The local system environment file where the user accesses SOAM and IDIH must be modified.
   For example:
   - 10.75.252.249 noam.tekelec.com
   - 10.75.252.145 soam.tekelec.com
   - 10.75.249.238 idih.tekelec.com

Figure 6-3 System Host File



- SSL certificate must have idih.tekelec.com and tekelec.com as DNS.

8. In your browser, open SOAM using FQDN soam.tekelec.com instead of IP. Then, click **Analyze with IDIH** for any trace. IDIH will open a new tab with FQDN without requiring you to log in.