

# Oracle® Communications

## IDIH User's Guide



Release 8.2.3.1

F34199-02

April 2022



Copyright © 2011, 2022, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle, Java, and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

# Contents

## 1 Introduction

---

Revision History	1-1
Overview	1-1
Scope and Audience	1-2
Manual Organization	1-2
My Oracle Support	1-2

## 2 Support for Service Capability Exposure Function

---

## 3 IDIH Configuration and Maintenance on DSR GUI

---

Help Organization	3-1
Remote Servers	3-1
IDIH Options Configuration on DSR	3-1
Options Elements	3-1
IDIH Global Options Configuration on DSR	3-2
Global Options Elements	3-2
Trace Overview	3-3
Network IDIH	3-4
Site Traces	3-4
Network Traces	3-5
IDIH Traces Configuration on DSR	3-6
Traces Elements	3-6
Insert	3-8
Edit	3-11
Delete	3-13
IDIH Traces Maintenance on DSR	3-14
Accessing IDIH from DSR	3-16
IDIH Access Control	3-16

## 4 Trace Analysis

---

ProTrace	4-1
Trace List Panel	4-1
Alarm Status Indicator	4-1
Trace List Toolbar	4-3
Query List Panel	4-3
Query List Toolbar	4-4
Creating or Modifying a Query	4-5
Executing a Query	4-7
Trace Viewer	4-7
TDR Panel	4-7
TDR Panel Toolbar	4-9
TDR List Retrieval	4-10
Message Copy	4-10
TTR Events Panel	4-11
Ladder Diagram	4-13
ProTrace Full Decoding Panel	4-16
Custom AVPs, Commands, and Vendors	4-17
Changing the Page Layout	4-23
IDIH Trace Statistics	4-24
Setting User Preferences on IDIH Dashboard	4-24
Setting Time Format	4-24
Setting Mapping Preferences	4-25

## List of Figures

---

3-1	IDIH Trace Overview	3-3
4-1	Alarm Status Indicator	4-2
4-2	Alarm List	4-2
4-3	Trace List Toolbar	4-3
4-4	Query List Toolbar	4-4
4-5	Query Dialog	4-5
4-6	TDRs List Toolbar	4-9
4-7	TDR List Retrieval	4-10
4-8	Event List Panel	4-11
4-9	Ladder Diagram	4-13
4-10	ProTrace Full Decoding Panel	4-17

## List of Tables

---

3-1	IDIH Options Elements	3-2
3-2	IDIH Global Options Elements	3-2
3-3	IDIH Traces Elements	3-6
4-1	Event Diagram Properties	4-11
4-2	Ladder Diagram Visualization	4-14
4-3	ProTrace Full Decoding Panel	4-17
4-4	Vendors	4-21

# 1

## Introduction

This section contains an overview of the available information for the Integrated Diameter Intelligence Hub (IDIH) feature. The contents include sections on the organization, scope, and audience of the documentation, as well how to receive customer support assistance.

## Revision History

Date	Description
April 2022	No changes done in this release.
August 2016	Initial release
August 2016	Updated based on support for U-SBR
October 2020	Added a new section <a href="#">Support for Service Capability Exposure Function</a> .

## Overview

This documentation provides information about the functions of the Integrated Diameter Intelligence Hub (IDIH) feature.

This feature:

- Allows the user to create and manage trace filters on DSR and Service Capability Exposure Function (SCEF) to capture messages needed for troubleshooting service issues
- Presents traces to the user using the graphical visualization capabilities provided by IDIH
- Allows the user to filter, view, and store the results with IDIH

The IDIH feature allows the user to capture detailed information about selected Diameter/RADIUS transactions and transmit this information to IDIH for further analysis. The integration of troubleshooting capabilities into the DSR and SCEF provides a high value proposition for customers to be able to troubleshoot issues that might be identified with the Diameter/RADIUS traffic transmitted to the DSR and SCEF.

These troubleshooting capabilities can supplement other network monitoring functions provided by the customer's OSS and network support centers to help quickly pinpoint the root cause of signaling issues associated with connections, peer signaling nodes, or individual subscribers.



### Note:

IDIH is not a replacement of the features in previous DIH releases.

## Scope and Audience

This documentation is intended for personnel who maintain operation of the DSR.

## Manual Organization

Information in this document is organized into chapter:

- [Introduction](#) contains general information about this document.
- [IDIH Configuration and Maintenance on DSR GUI](#) provides configuration and maintenance information of the IDIH feature.
- [Trace Analysis](#) provides information about traces used by the IDIH.

## 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.



# 2

## Support for Service Capability Exposure Function

IDIH supports Service Capability Exposure Function (SCEF) Diameter interfaces to allow users manage trace filters on SCEF related Diameter interfaces to capture messages required for troubleshooting service issues.

IDIH supports the following SCEF Diameter interfaces:

- T6a/T6b
- S6t
- S6m/S6n
- T4

For information about SCEF and supported Diameter interfaces, refer to the *Service Capability Exposure Function User's Guide*

# 3

## IDIH Configuration and Maintenance on DSR GUI

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

### Help Organization

Information in this online help is organized into sections:

- [IDIH Configuration and Maintenance on DSR GUI](#) provides configuration and maintenance information of the IDIH feature.
- [Trace Analysis](#) provides information about traces used by the IDIH.

### Remote Servers

To use IDIH, a remote server connection must be configured. The **Communication Agent**, and then **Configuration**, and then **Remote Servers** page on the NOAM is used to configure connections to remote servers.

Once a remote server with IDIH is configured on the NOAM, the IP address for the server appears in the IDIH IP Address field on the **Diameter**, and then **Troubleshooting with IDIH**, and then **Configuration**, and then **Options** page on the SOAM.

For detailed information about configuring remote servers in DSR, refer to the *Communication Agent User's Guide*.

For detailed information about configuring remote servers in IDIH, refer to the *IDIH Installation* document.

### IDIH Options Configuration on DSR

The **Diameter**, and then **Troubleshooting with IDIH**, and then **Configuration**, and then **Options** GUI screen on an SOAM Server is used to configure Options for the IDIH on DSR. If these options are not configured, the user will not be able to access IDIH from DSR.

### Options Elements

[Table 3-1](#) describes the fields on the IDIH Options screen.

The correct IDIH Host Name corresponds with the name of the configured ComAgent remote server.

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

**Table 3-1 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 Host Name	The Host Name of the peer IDIH server used for sending the messages.	Format: pulldown list Default: N/A
IDIH Visualization Address	The IP address or FQDN of the remote IDIH server that visualizes the trace (when the <b>Analyze with IDIH</b> link is clicked on the <b>Maintenance</b> screen).  If an IP address is used in place of a FQDN, then IDIH SSO functionality does not work from the DSR SOAM.	Format: text box Default: N/A

## IDIH Global Options Configuration on DSR

The **Diameter**, and then **Troubleshooting with IDIH**, and then **Configuration**, and then **Global Options** GUI screen on an SOAM Server is used to configure Global Options for the IDIH on DSR.

### Global Options Elements

[Table 3-2](#) describes the fields on the IDIH Global Options screen.

**Table 3-2 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

**Table 3-2 (Cont.) IDIH Global Options Elements**

Field	Description	Data Input Notes
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

## Trace Overview

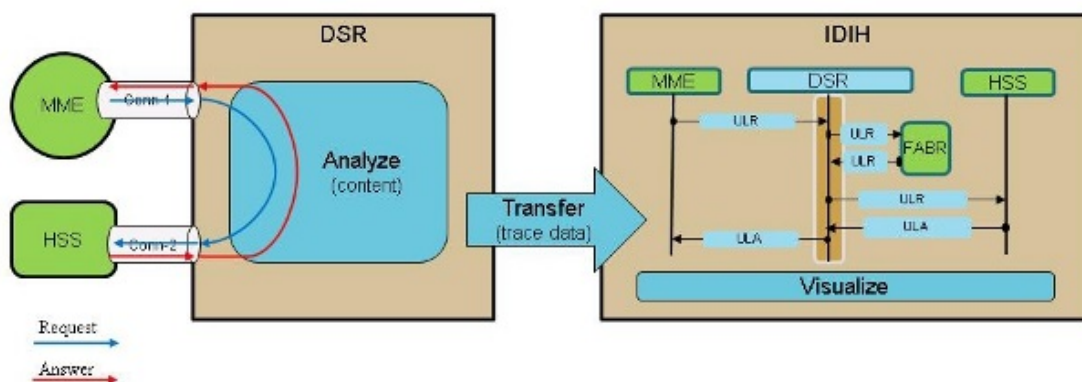
A trace is a set of conditions (subdivided into scope and content) which, when met, cause trace data to be forwarded to IDIH.

A DSR DA-MP plays the role of determining which messages should be captured based on trace criteria created and activated by the user. The trace criteria identifies the scope and content.

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

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

**Figure 3-1 IDIH Trace Overview**



IDIH does not guarantee a fixed number of days of data storage. Storage life is based on disk space. Some of the factors impacting storage life are trace parameters (very inclusive or very discriminatory) and record size.

During congestion, DSR suspends trace forwarding until the condition clears, at which time, trace forwarding resumes.

**Note:**

Trace data lost during the time of congestion is not recovered.

## Network IDIH

Network IDIH is an extension of the IDIH feature. The IDIH feature allowed users to capture targeted transactions at a single site, and to store and visualize them at a local IDIH. Network IDIH introduces the concept of a network trace, which allows users to capture targeted transactions simultaneously at all DSR sites. Captured records are still stored at the local IDIH, however Network IDIH allows the user to visualize the captured records on any IDIH, regardless of where within the network they were captured. The single-site traces available in IDIH are still supported, and are referred to as site traces in this document.

## Site Traces

### Creating A Site Trace

A site trace is created from the **Diameter**, and then **Troubleshooting with IDIH**, and then **Configuration**, and then **Traces** screen. Select **Trace Location as Site Trace** when creating the trace. All trace content types, content values, scope types, and scope values are supported.

A site trace can only be created (and edited and deleted) on the site that will run the trace. When a site trace is created, IDIH will record the site at which the trace was created, and will only allow a GUI launched from that site to edit, delete, start or stop the trace.

### Starting A Site Trace

A site trace is started from the **Diameter**, and then **Troubleshooting with IDIH**, and then **Maintenance**, and then **Traces** screen. A site trace can only be started from the GUI at the site that created the trace.

### Running A Site Trace

The site trace is only executed on the DA-MPs in the site where the site trace was created. DA-MPs will send all TTRs that match site traces to the local site IDIH.

### Stopping A Site Trace

A site trace can be manually stopped from the from the **Diameter**, and then **Troubleshooting with IDIH**, and then **Maintenance**, and then **Traces** screen. A site trace can only be stopped from the GUI at the site that is running the trace. A site trace will be automatically stopped when either the Time Duration or Number of Matches limits are reached.

### Viewing Site Trace Status

The status of site traces can be viewed from the **Diameter**, and then **Troubleshooting with IDIH**, and then **Maintenance**, and then **Traces**. The status of a site trace can only be viewed from the GUI at the site that is running the trace.

## Network Traces

### Creating A Network Trace

A network trace is created from the **Diameter**, and then **Troubleshooting with IDIH**, and then **Configuration**, and then **Traces** screen. Select **Trace Location as Network Trace** when creating the trace. All trace content types, content values, scope types, and scope values are supported.

Network traces can be created at any site, and can be edited, deleted, started or stopped at any site. A network trace created at Site A, for example, could be edited at Site B and deleted at Site C.

### Starting A Network Trace

A network trace is started from the **Diameter**, and then **Troubleshooting with IDIH**, and then **Maintenance**, and then **Traces** screen. Network traces can be started at any site.

### Running A Network Trace

All sites will attempt to run every active network trace. However, it is possible for the user to specify a scope type/value that will prevent some sites from matching the trace. For example, a network trace created at Site A specifies Peer scope, and selects the peer Peer1. Only sites that have a peer named Peer1 will be able to match the scope. DA-MPs at all sites should verify that they can match the scope type/value of each network trace. If not, then the network trace should not be run. (This trace would still count against the site's active network trace limit)

DA-MPs will send all TTRs that match network traces to the local site IDIH.

### Stopping A Network Trace

A network trace can be manually stopped from the **Diameter**, and then **Troubleshooting with IDIH**, and then **Maintenance**, and then **Traces** screen. Network traces can be manually stopped at any site. Network traces are automatically stopped if they have reached their configured time duration.

Network traces are not automatically stopped if they hit their match count limit. The site that reached its match count limit will no longer attempt to match the trace once the match count limit is reached, but other sites will continue to attempt to match the trace. Even if all sites hit their match count limit, the network trace will not be automatically stopped; it continues to count as an active network trace until its time duration is exhausted, or until it is manually stopped.

### Viewing Network Trace Status

The status of network traces can be viewed from the **Diameter**, and then **Troubleshooting with IDIH**, and then **Maintenance**, and then **Traces**. The status of a network trace can be viewed from the GUI at any site, however the information that is displayed is the status of the trace at the local site. Summary status of the network trace over all sites is not available.

## 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.

## Traces Elements

[Table 3-3](#) describes the fields on the Traces screen.

**Table 3-3 IDIH Traces Elements**

Field (* indicates a required field)	Description	Data Input Notes
Trace Name*	A name that uniquely identifies the Trace.	Format: text box 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	Format: option button
Trace Content		

**Table 3-3 (Cont.) IDIH Traces Elements**

Field (* indicates a required field)	Description	Data Input Notes
Content Type*	<p>The Diameter message contents to be matched for this trace. The combination of content type/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 DIH.</p> <p>Content Type:</p> <ul style="list-style-type: none"> <li>• Non-success answers - answers with (Experimental) Result-Code <math>\geq</math> 3000, or any message with the E-bit set</li> <li>• (Ad Hoc)Requests - any request that matches the specified content values</li> <li>• (Ad Hoc Answers) - any answer that matches the specified content values</li> <li>• 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.</li> <li>• 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.</li> </ul>	<p>Format: pulldown list</p> <p>Range: Non-success answers, Requests, Answers, Ad Hoc Requests, Ad Hoc Answers, User Identity, Equipment Identity</p> <p>Default: -Select-</p>
Content Values	<p>After selecting the content type, the screen displays the Content Values for selecting content elements and entering content values.</p>	Default: N/A
Trace Scope		



Table 3-3 (Cont.) IDIH Traces Elements

Field (* indicates a required field)	Description	Data Input Notes
Scope Type*	The scope used for this trace. Scope Type: <ul style="list-style-type: none"> <li>• Connection - messages arriving or leaving on specified connection are candidates for tracing</li> <li>• Peer - messages arriving or leaving on specified peer are candidates for tracing</li> <li>• DSR Application - messages going to or returning from specified DSR application are candidates for tracing</li> <li>• All - all messages are candidates for tracing</li> </ul>	Format: pulldown list 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.	Format: pulldown list Default: -Select-
Trace Duration Number of Matches*	Number of Matches - stop the trace after matching this many messages	Format: text box; numeric 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)	Format: text box; numeric Range: 00:00:01 - 96:00:00 Default: N/A
Notes	Descriptive information about the trace	Format: Text box Range: A 255-character string Default: N/A

## Insert

The **Diameter**, and then **Troubleshooting with IDIH**, and then **Configuration**, and then **Traces [Insert]** screen is used to create a new trace.



### Note:

A maximum of 100 traces may be inserted.

The fields are described in [Traces Elements](#).

1. Select **Diameter**, and then **Troubleshooting with IDIH**, and then **Configuration**, and then **Traces**.

2. Click **Insert**.

The **Diameter**, and then **Troubleshooting with IDIH**, and then **Configuration**, and then **Traces [Insert]** screen appears.

3. Enter a trace name in the **Trace Name** field.

The name must meet these 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: Non-success answers, Requests, Answers, Ad Hoc Requests, Ad Hoc Answers, User Identity, and Equipment Identity.

6. 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 user 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/RADIUS interfaces. Additionally, all other parameters may be left blank as wild cards.

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

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

 **Note:**

The optional AVP is based on what AVPs are configured in the AVP Dictionary. For further information about the AVP Dictionary, refer to the *Diameter User's Guide*.

 **Note:**

For a non-grouped AVP all operators for the specified data type are allowed. For a grouped AVP only the Exists and Does not exist operators are allowed.

If the **Content Type** is set to Ad Hoc Answers, then the user may select an Application-ID, Command-Code, Origin-Host, and/or Origin-Realm. Additionally, an optional content value is 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/RADIUS interfaces to which the user may also add. Additionally, all other parameters may be left blank as wild cards.

 **Note:**

The optional AVP is based on what AVPs are configured in the AVP Dictionary. For further information about the AVP Dictionary, refer to the *Diameter User's Guide*.

 **Note:**

For a non-grouped AVP all operators for the specified data type are allowed. For a grouped AVP only the Exists and Does not exist operators are allowed.

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

 **Note:**

After an Application-ID is selected, the user 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 the user may select an Application-ID. The Application-ID option lists a pre-defined list of supported Diameter/RADIUS interfaces, although the user cannot add anything new to the list.

 **Note:**

After an Application-ID is selected, the user 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 for a trace can be for a specific **Connection**, specified **Peers**, specified **DSR Applications**, or **All** messages.

8. Select a Scope Value from the **Scope Value** options

The scope value is determined by which Scope Type is selected.

9. Enter a number of matches for the trace to find in the **Number of Matches** field.

 **Note:**

A maximum of 1000 matches is permitted.

10. Enter a duration time for the trace in the **Time of Duration** field.  
The duration can be up to 96 hours.
11. Enter a comment describing the trace in the **Notes** field.

 **Note:**

Entering a value in the **Notes** field is optional.

## Edit

The **Diameter**, and then **Troubleshooting with IDIH**, and then **Configuration**, and then **Traces [Edit]** screen is used to edit a trace.

 **Note:**

If a trace is Active, it cannot be edited.

The fields are described in [Traces Elements](#).

1. Navigate **Diameter**, and then **Troubleshooting with IDIH**, and then **Configuration**, and then **Traces**.
2. Click **Edit**.
3. 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 user 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/RADIUS interfaces. Additionally, all other parameters may be left blank as wild cards.

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

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

 **Note:**

The optional AVP is based on what AVPs are configured in the AVP Dictionary. For further information about the AVP Dictionary, refer to the *Diameter User's Guide*.

 **Note:**

For a non-grouped AVP all operators for the specified data type are allowed. For a grouped AVP only the Exists and Does not exist operators are allowed.

If the **Content Type** is set to Ad Hoc Answers, then the user may select an Application-ID, Command-Code, Origin-Host, and/or Origin-Realm. Additionally, an optional content value is 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/RADIUS interfaces to which the user may also add. Additionally, all other parameters may be left blank as wild cards.

 **Note:**

The optional AVP is based on what AVPs are configured in the AVP Dictionary. For further information about the AVP Dictionary, refer to the *Diameter User's Guide*.

 **Note:**

For a non-grouped AVP all operators for the specified data type are allowed. For a grouped AVP only the Exists and Does not exist operators are allowed.

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

 **Note:**

After an Application-ID is selected, the user 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 the user may select an Application-ID. The Application-ID option lists shows a pre-defined list of supported Diameter/RADIUS interfaces, although the user cannot add anything new to the list.

 **Note:**

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

4. Select a Scope Type from the **Scope Type** options.  
The scope for a trace can be for a specific **Connection**, specified **Peers**, specified **DSR Applications**, or **All** messages.
5. Select a Scope Value from the **Scope Value** options.  
The scope value is determined by which Scope Type is selected.
6. Enter a number of matches for the trace to find in the **Number of Matches** field.

 **Note:**

A maximum of 1000 matches is permitted.

7. Enter a duration time for the trace in the **Time of Duration** field.  
The duration can be up to 96 hours.
8. Edit the comment in the **Notes** field.

 **Note:**

Editing the **Notes** field is optional.

## Delete

The **Diameter**, and then **Troubleshooting with IDIH**, and then **Configuration**, and then **Traces** screen allows a trace to be deleted.

 **Note:**

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

The fields are described in [Traces Elements](#).

1. Select **Diameter**, and then **Troubleshooting with IDIH**, and then **Configuration**, and then **Traces**.
2. Select the trace to be deleted.
3. Click **Delete**.  
A confirmation pop up window appears.
4. Perform one of these actions:
  - Click **OK** - the trace will be deleted.

- Click **Cancel** - to return to the previous screen without deleting the trace.

## IDIH Traces Maintenance on DSR

Once 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**. Once 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 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
- Disabled on All MPs (network traces only)
- Throttled

### Note:

This state can occur for 2 reasons:

- The IDIH has exceeded 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 Elements](#) has been reached
- Time Limit Reached - the duration time configured in [Traces Elements](#) 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/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. Refer to the *ProTrace User's Guide* for further information.

 **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 **idihtrace** user ID to access IDIH. See [Accessing IDIH from DSR](#) for further information about the **idihtrace** user.

 **Note:**

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.

## 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 then **Troubleshooting with IDIH**, and then **Maintenance**, and then **Traces**.
4. Click **Launch IDIH**.
5. Alternatively, select a trace and click **Analyze With IDIH**.

In the absence of a DNS server, the user may authenticate directly on the IDIH server using the **idihtrace** 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 **idihtrace** user ID is almost the same as for signing in using single sign-on with the exception of replacing **FQDN** with **IP Address**.

## 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, refer to the *Operations, Administration, and Maintenance (OAM) User's Guide*.

# 4

## Trace Analysis

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

### ProTrace

ProTrace is the tool that is used to view traces that have been configured on DSR.

The main screen contains two areas - Trace List Panel and Query List Panel.

### Trace List Panel

With the ProTrace application, the trace list shows all traces configured by DSR. The list can also be filtered.

The traces list contains six columns. Most of the column headings can be used to sort the displayed sessions list by clicking on the heading. Click once to sort in ascending order and again to sort in descending order for that column.

The column headings are:

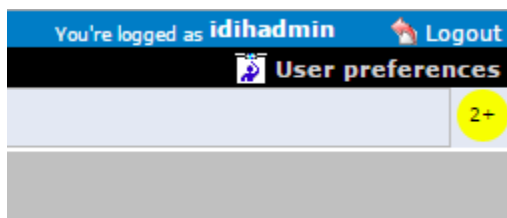
- Trace Name - trace name
- Status - the completion status of the trace, which can be either In-Progress or Completed.
- Type - the type of trace, which is either Site or Network based on trace records details and can be filtered
- Start Time - the start date and time for the trace
- Stop Time - the end date and time of the trace
- TTR Count - the number of messages matched in a particular trace

### Alarm Status Indicator

When logged in to IDIH, either directly or from **DSR** launch, the portal header displays a count of current alarms, as shown in [Figure 4-1](#). The alarm status indicator is a count of the highest severity of all open alarms and the alarm status indicator (circle) is the color (user defined, idihadmin) of the highest severity. For example, if there are zero critical, two major, one minor, and three warnings, then the alarm status indicator contains 2+ and the color is the user-defined color for major severity. The + is used to indicate that there are additional alarms at a lesser severity. The + does not appear if, for example, there are zero critical, two major, zero minor, and zero warnings.

Initially, the alarm status is empty (non-visible). Then, after a short interval, the system queries for open alarms and updates the alarm status indicator. After the first update, the system updates the alarm status indicator every 30 seconds.

Figure 4-1 Alarm Status Indicator

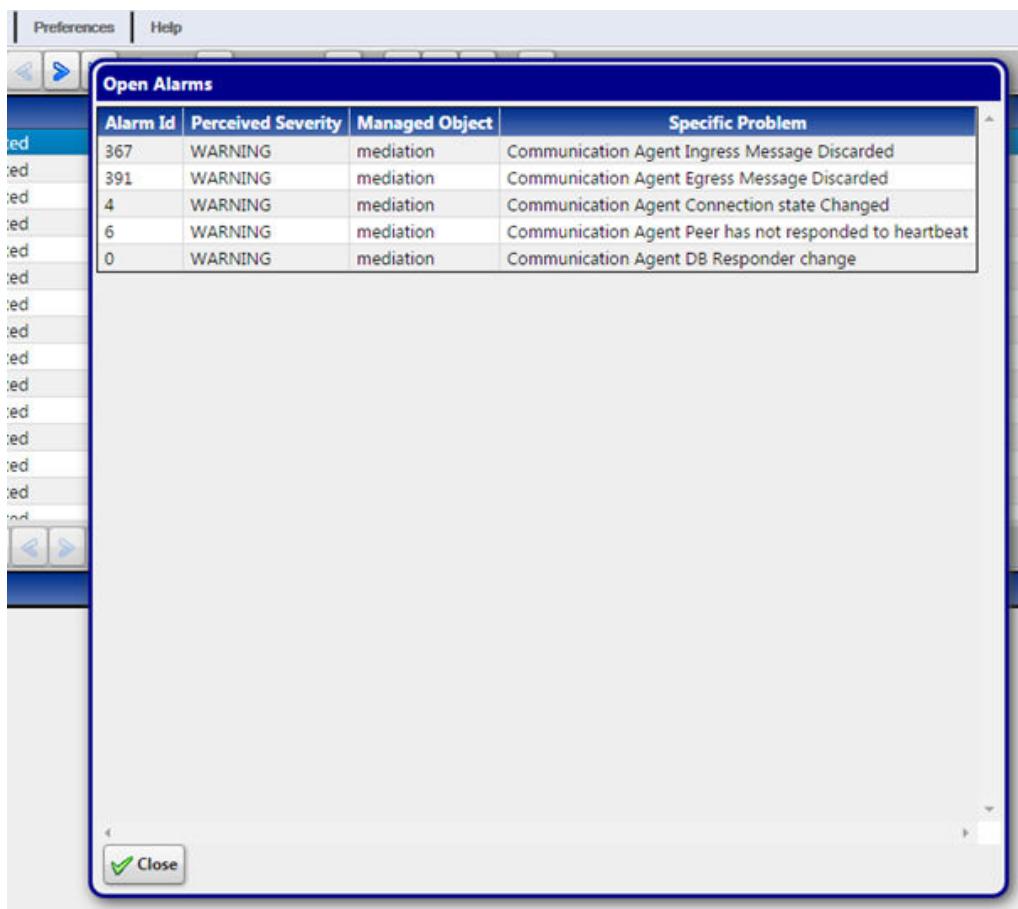


Selecting the alarm status indicator shows a brief description of the open alarms. The system displays the list of open alarms in tabular form, as shown in Figure 4-2. This list can be dismissed by pressing the **Close** on the Open Alarm dialog window.

**Note:**

Only open alarms may be viewed. No other actions are provided such as clear or acknowledge.

Figure 4-2 Alarm List



## Trace List Toolbar

The toolbar provides a means of selecting and organizing traces.

**Figure 4-3 Trace List Toolbar**



**Filter** - opens the System Query Dialog popup where you can filter the list of sessions displayed by the various columns and their values.

**First page** - opens the first page of sessions.

**Previous page** - opens the previous page of sessions.

**Next page** - opens the next page of sessions.

**Last page** - opens the last page of sessions.

**Set Size** - use this button to set the number of selected trace records and/or total trace records displayed from 10-500 per page.

**Refresh** - re-loads the current screen and shows any changes that have been made.

**Delete** - deletes a selected trace.

**Obtain Trace Conditions** - opens a popup window that provides additional details about a selected trace.

**Obtain Trace Info** - displays a popup dialog displaying trace information for the selected row from the Trace List page. The information displayed includes the summary information for the selected trace, and all the Network IDIH sites and their counts for the selected trace.

**Run Default Query** - runs a query on the selected trace in the list and provides a detailed analysis for those traces.

In addition to these buttons, there is also a saved filters pull-down to select a saved filter, and a page count showing what page out of the total sessions pages being viewed.

## Query List Panel

The Query List panel contains list of queries the user can execute on the selected trace. These queries are user's saved queries or queries shared by other users. The list has a toolbar where the user can quickly invoke operation on a selected query. It includes:

- Creating a new query
- Modifying selected query
- Deleting selected query
- Executing selected query

When the user selects a trace in Trace List panel, the queries in Query List is reloaded. Only queries which are compatible with selected trace are show.

The Query List panel table contains four columns. The table queries change depending on what view is selected based on which trace is selected, but the columns are constant. The column headings can be used to sort the list by clicking on the heading. Click once to sort in ascending order and again to sort in descending order for that column.

The column headings are:

- Query Name - that shows the name of the query
- Query Description - shows a description of a given query
- Owner - shows the user name that created the query
- Created - shows the date the query was created

## Query List Toolbar

The toolbar provides a means of selecting and organizing queries.

**Figure 4-4 Query List Toolbar**



**Filter** - opens the System Query Dialog page where you can filter out all non-essential queries.

**First page** - opens the first page of queries.

**Previous page** - opens the previous page of queries.

**Next page** - opens the next page of queries.

**Last page** - opens the last page of queries.

**Set Size** - use this button to set the queries list size from 10-500 per page.

**Refresh** - re-loads the current screen and shows any changes that have been made.

**Create New Query** - opens the Query Dialogue screen to add a specific query.

**Modify 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.

### Note:

The user can only view/operate on a single trace at a time.

**Change Begin/End Time for the Query** - opens the Query Settings page where the user can modify the begin and end dates and times for a given query.

In addition to these buttons there is also a queries count showing how many queries are in the list and what range you are viewing.

## Creating or Modifying a Query

To create a new query or modify existing query, click **Create New Query** or **Modify Selected Query**.

Figure 4-5 Query Dialog

Field	Operator	Value
-------	----------	-------

The query must have at least one dictionary. To add a dictionary, select a dictionary from the **Available Dictionaries** list and click **(+)**. To remove a dictionary, click **(-)**.

Once the dictionary has been added to the query, the conditions can be added by clicking **Add**. The query can have no conditions, otherwise the query matches all Transaction Detail Records (TDRs) for a given dictionary. Each dictionary has its own conditions, making it possible to search for TDRs from different dictionaries with different conditions.


When adding a condition, the corresponding label is added into the **Expression** field. It is added to the end of the expression with the selected **Operator** (AND or OR). Similarly, when the condition is removed from the query, the corresponding label is automatically removed from the expression and the expression is adjusted. When **Use Bracket** is selected, then the whole expression is closed in brackets before adding the new condition.

 **Note:**

The user can edit the expression to be more complex such as (A AND B) or C

The query is validated before it is saved or executed. Several things are verified:

- Name is filled (verified for Save operation only, for Query Execution operation the name can be empty)
- All conditions have correct operator and correct value (an empty value is not allowed and it must correspond to field type)

 **Note:**

The user can also use wild cards in the value field. To see descriptions of these wild cards, hover on the most right-hand ? in the query dialog after selecting a field.

- Expression is well formed Boolean expression

Whenever any error occurs, the user is notified either in the Message Panel at the top of the Dialog box or beside the GUI element which caused the error (a condition or expression box).

 **Note:**

For filtering on source and destination node fields, provide either the IP address or select the node name from the list. Selecting the node name means filtering on the list of IP addresses assigned to the selected node. If the same IP Address is being reused across the nodes, filtered data would display other nodes as well.

By default, when a dictionary is added into the query, all displayable fields from that dictionary are selected as Displayed Fields. If desired, change the Display Fields in the Displayed Fields tab. There are 3 modes to choose from:

1. All fields (all fields are added into Displayed Fields)
2. Common (all common fields from all dictionaries are selected; if there is just one dictionary then all fields are selected)
3. Custom fields (the user can select fields of his/her choice)

The Displayed Fields are selected separately per dictionary. If there is more than one dictionary, then fields in the query result are merged together based on the field name. All fields with the same name are displayed in the same column.

Click **Save** to save a query for later use. The query appears in the Query List panel.

Click **Save As** to open a prompt asking for a new name. Confirms the name. A new query is created and saved for later use. The query appears in the Query List panel.

Now the query is ready for execution. Execute the query by clicking **Apply**.

## Executing a Query

When a query is executed, it is always executed on the currently selected trace from the Trace List panel and Trace Viewer is displayed. A query can be executed in multiple ways:

1. By clicking **Apply** from the Query Dialog window (when creating or modifying a query)
2. By clicking **Run Default Query** on the Trace List toolbar
3. By selecting the query in Query List panel and clicking **Run Selected Query** in the Query List toolbar

Enter the time in which the search is about to be performed. The Begin and End time are pre-populated with the real begin and end date of the selected trace. Click on the icons beside the date and time text boxes and select the date in calendar and time in time selection widgets for better convenience.

By selecting **Execute in New**, the Trace Viewer is shown in a new browser window and the query is executed.

## Trace Viewer

The Trace Viewer is displayed when the user executes a trace and contains the TDRs for the trace for the user to analyze.

The Trace Viewer is divided into three panels:

- TDRs List Panel
- Event List Panel (Event List or Event Diagram)
- ProTrace Full Decoding Panel

ProTrace allows the user to organize the panels in 6 different layouts (positions of each panel). Some layouts contain only some panels. Each layout is depicted by an icon which shows how the panels are organized. For information about how to change the layout, refer to [Changing the Page Layout](#).

## TDR Panel

The TDR panel contains lists of transactions (TDRs) that matched a given query. If the query does not have any conditions, then the panel includes all TDRs captured for the selected trace and for interfaces selected by the query. The TDRs belonging to the same TTR are displayed beside each other with the same background color. The fields displayed in the result are defined in Query display fields. The result is divided into pages (the user can define the page size) and the user can navigate through the pages (first page, previous and next page).

The user is also able to perform a variety of actions:

- Use navigation buttons to go to first, previous or next page
- Reverse sorting (Ascending, descending)
- Set the page size (number of records per page) for TDR table
- Get the number of records which match the current query
- Display statistics of the current trace



- Modify the query and re-execute it to refine the transactions
- Export a file that contains a summary of TDR records, an event diagram, a list of TTR events, and a full decoding panel for every Diameter, RADIUS, or RADIUS embedded within a Diameter payload message. There are multiple formats in which the file may be exported:
  - Export TTR as HTML - exports the file from the currently selected TTR in an HTML format
  - Export TTR as PCAP - exports the file from the currently selected TTR in a PCAP format that is directly downloaded to the user's server without a progress bar or a way to cancel the export
  - Export trace as PCAP - exports the contents of a trace into a PCAP format that is directly downloaded to the user's server, indicated by a progress bar that also allows the user to cancel the export. If the export is cancelled, ProTrace exports all information that was downloaded prior to the cancellation.

 **Note:**

ProTrace exports payload data in IPv4 or IPv6 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.

 **Note:**

Payloads sent from DSR to IDIH contain Diameter/RADIUS 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 export exports up to 1 MB of payload data. The rest of the payloads are ignored. The user can refine the query to accommodate all the payloads the user wants to export and re-export it again. When TLS or DTLS is used as the transport, the export displays TCP for TLS and SCTP for DTLS as the Transport value.

 **Note:**

When encoding and displaying RADIUS 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/TTR PCAP export.

- Change the layout of the panels

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.

## TDR Panel Toolbar

The function buttons on the TDRs list toolbar are as follows:

**Figure 4-6 TDRs List Toolbar**



**First page** - opens the first page of queries.

**Previous page** - opens the previous page of queries.

**Next page** - opens the next page of queries.

**Reverse Sorting** - reverses the sort order of the xDR list.

**Set Size** - this shows how many TDRs are displayed per page, the user can modify the number of TDRs on the page by typing in another number and clicking the **check**. The user can set the page size from 10 to 5000 TDRs per page. A larger page size will take longer to display.

**Pause refresh** - stops automatic refresh so that you can work on filters or records without data changing.

**Go Back to Trace List** - returns to the Trace List.

**Show Statistics** - opens the Trace Statistics window and shows statistics associated with the selected trace. See [IDIH Trace Statistics](#) for further information.

**Modify Query** - opens the Query dialog screen of an existing query.

### **Note:**

A user can also add conditions to a query by right clicking an individual cell in the TDRs List and clicking **Add to Conditions**. These new conditions are added to the current query and are not applied until the icon is used to apply the changed query.

**Change Begin/End time for the Query** - allows the user to change the time a query begins or ends.

**TTR Export** - exports the TTR results. These results are exported in HTML format.

**Search** - searches for specific TDR records.

**Search next** - continues search of TDR records.

**Change layout** - enables the user to change the page layout using a variety of combinations. See [Changing the Page Layout](#) for further information.

**Selected Trace** - Shows the name of the Trace currently being analyzed.

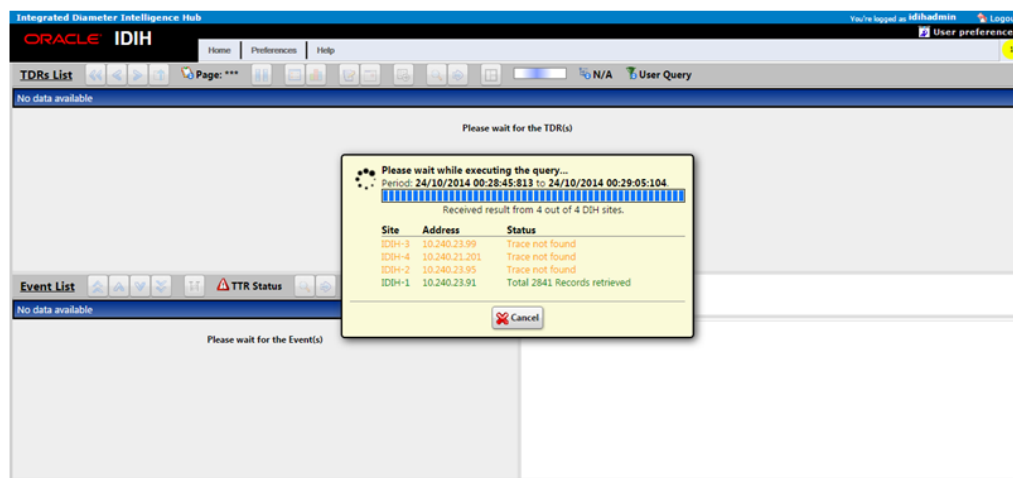
**Query selected** - placing the cursor over on this icon opens a small information pop-up showing the name, description, and network information of the query being run. This information is useful because it confirms the user is looking at the correct trace.

## TDR List Retrieval

Network traces require TDR data to be retrieved from multiple sites and may take longer to process based on factors such as the number of sites and network latency. When retrieving network trace results from the **Analyze with IDIH** function on the DSR GUI or from the main ProTrace page and the trace is a network trace, then ProTrace displays a progress dialog, which displays a variety of information as shown in Figure 4-7:

- Time Period
- Progress bar
- Network result status - x out of y processed, where x is the current number of processes and y is the total
- Network Table with individual IDIH site information (Name, address, and status)
- **Cancel**

Figure 4-7 TDR List Retrieval



## Message Copy

When the TTR was copied during the Message Copy feature to **DAS**, it is indicated in the TDR. The TDR contains two fields which have references to either the copied TTR or to the original TTR. The fields are called **LinkedTTR** and **CorrelationID**. If these references exist in the TDR (these fields are not empty), then the TDR is highlighted with a different text color.

When the user right clicks on a TDR, a popup menu is displayed and the user can select **Search Message Copy**.

When the user selects **Search Message Copy**, a new query is created and executed. The query populates the Trace Viewer with TDRs that have the same **LinkedTTR** or **CorrelationID** values as the original TDR that was used to start the search.

When the original Answer message appears in the copied message, it is included in the group AVP with code 2156 and vendor ID 323. This AVP appears in the Full Decoding Panel as **MSG-Copy-Answer**.

In the original TTR, apart from standard events, two new events appear if a message is copied - Message Copy Triggered and Message Copied. Depending on where the trigger point is set, there may be up to 4 Message Copy Triggered events. These events have the scope set as **IR** Data. Message Copied events have the scope set as **IA** Data. Each Message Copy Triggered event has Message Copy Configuration Set name (MCCS) as its instance data, as well as where the Message Copy was triggered.

A copied TTR start with a new Event - Copied Message. The Copied Message event's scope is **IG** (Internally Generated). MCCS is used as the instance data. **MCCS** results in selecting the route list and subsequently the route group. These standard events are seen, but their scope is IG Data.

## TTR Events Panel

The TTR Event Panel displays a list of all TTR events associated with the selected transaction (TDR). Whenever the user selects a TDR in the TDR Panel, the TTR Event Panel is refreshed with the corresponding TTR events. The Event table has a number of columns:

**Figure 4-8 Event List Panel**

Rec #	Time	Event Type	Event Scope	Transport Type	Connection	Source Node	Source Port	Destination Node	Destination Port	Event Data	Application
1	28/07/2014 06:20:01:000	Message Received	IR	TCP	hsc1_conn	hsc1 - 10.250.51.144	36137	fwb_dsr - 10.240.19.164	36164	-	3GPP S
2	-	Trace Match	IR Data	-	-	-	-	-	-	test_sd, TTP-IR	-
3	-	ART Rule Not Found	IR Data	-	-	-	-	-	-	Default	-
4	-	PRT Rule Not Found	IR Data	-	-	-	-	-	-	Default	-
5	-	Dest-Host Routing	IR Data	-	-	-	-	-	-	-	-
6	-	Trace Match	ER Data	-	-	-	-	-	-	test_sd, TTP-ER	-
7	28/07/2014 06:20:01:000	Message Sent	ER	TCP	hsc1_conn	fwb_dsr - 10.240.19.164	10001	hsc1 - 10.250.51.145	10001	-	3GPP S
8	28/07/2014 06:20:01:000	Message Received	IA	TCP	hsc1_conn	hsc1 - 10.250.51.145	10001	fwb_dsr - 10.240.19.164	10001	2001 - DIAMETER_SUCCESS	3GPP S
9	-	Trace Match	IA Data	-	-	-	-	-	-	Adhoc_ans_sd, TTP-IA	-
10	-	Trace Match	EA Data	-	-	-	-	-	-	Adhoc_ans_sd, TTP-EA	-

The user can also click **Toggle Ladder Diagram** to view events in an Event Diagram.

- **Time** (the column is populated for payload events only. It contains the time when the message was received or sent)
- **Event Type** and **Event Scope**

**Table 4-1 Event Diagram Properties**

Event Type	Event Scope
Message Received	IR (Ingress Request), IA (Ingress Answer)
Message Sent	ER (Egress Request), EA (Egress Answer)
Message Created	App Data (Application Data)
App Invoked	App (Application)
App Result	App Data
App Invocation Failed	IR Data, IA Data
Trace Match	IR Data, ER Data, IA Data, EA Data
Linked TTR	
ART Rule Match	IR Data

**Table 4-1 (Cont.) Event Diagram Properties**

Event Type	Event Scope
ART Rule Not Found	IR Data
PRT Rule Match	IR Data
PRT Rule Not Found	IR Data
Unavailability Action	IR Data, IA Data
Route List Selected	IR Data
Dest-Host Routing	IR Data
Alternate Implicit Routing	IR Data
Route Group Selected	IR Data
Mediation Rule Match	IR Data, IA Data, ER Data, EA Data
Request Rerouted	IR Data
Answer Timeout	IA
Answer Matching Failed	IA Data
Address Resolution Match	App Data
Routing Exception	App Data
DP Query Sent	App Data
DP Response Received	App Data
DP Query Failure	App Data
DP Response Timeout	App Data
SBR Query Sent	App Data
SBR Response Received	App Data
SBR Query Failure	App Data
SBR Response Timeout	App Data
Diameter Request processing routine invoked	IR Data
Diameter Answer processing routine invoked	IR Data
U-SBR Query send	IR Data
Callback invoked	IR Data
Subroutine name not found	IR Data
Runtime error	IR Data
Debug message	IR Data
U-SBR Query Result Received	IR Data
U-SBR Query Send Failed	IR Data

- **Transport Type** (TCP or SCTP for payload events only)
- **Connection Id** (The name of the connection defined in DSR)
- **Source Node** (<Node name> - <IP address> for payload events; IP is translated and node name is displayed if there is a record in Local Node or Peer Node reference data at DSR for the given IP address)
- **Source Port** (TCP/STCP IP port number for payload events)
- **Destination Node** (<Node name> - <IP address> for payload events; IP is translated and node name is displayed if there is a record in Local Node or Peer Node reference data at DSR for the given IP address)
- **Destination Port** (TCP/STCP IP port number for payload events)
- **Event Data** (Event data from TTR event; Event Data for Answer payload events contains the result code from ResultCode AVP (code 268) or

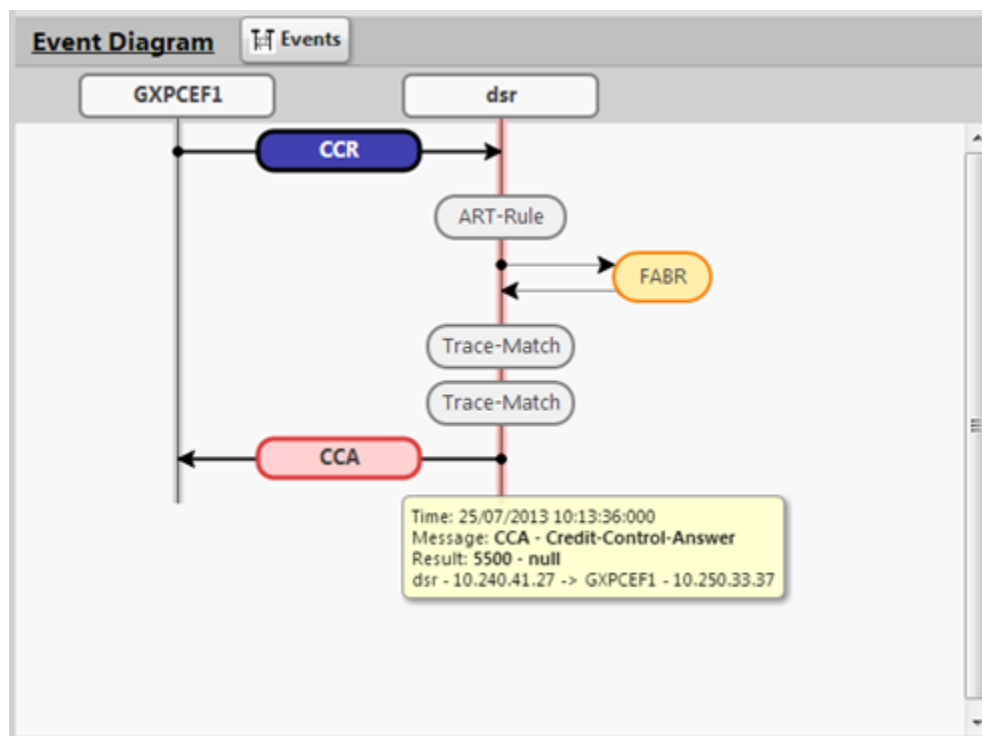
ExperimentalResultCode AVP (code 298) in the form of <Error Code> - <Error description>)

- **Application** (Diameter Application for payload events, empty for the rest)
- **Command Code** (Message command code in form of <Short name> - <Long name> for payload events)
- **Message Priority** (The numeric priority value from the priority services field in the diameter message)
- **DSR-DSR** (If the message transpired between two DSR nodes, then the column shows a YES value. If the message transpired between one DSR node and either a client (such as MME) or server (such as HSS), then the column shows a NO value. This value is required for N-IDIH to create a correct ladder diagram from the event list)

## Ladder Diagram

The Ladder Diagram shows the TTR events in graphical form, providing an additional form of information shown in the TTR Event panel. Additionally, ProTrace will process and display Client Redirect events when received.

Figure 4-9 Ladder Diagram



The user can hover or click on a bubble of the ladder diagram which may show information about that particular bubble in the Diameter Full Decoding Panel.

The user can also click **Toggle Event Table** to view events in tabular form, which also allows for a selected row to appear in the Diameter Full Decoding Panel.

[Table 4-2](#) defines how the TTR events are visualized in the ladder diagram:

**Table 4-2 Ladder Diagram Visualization**

Event Type	Event Scope	Event Diagram Visualization
Request Message Sent/ Received	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 tooltip
App Invocation Failed	IR Data, IA Data	App Invocation Failed makes the corresponding Application bubble red and appends text to its tooltip.
Trace Match	IR Data, ER Data, IA Data, EA Data	Gray bubble on DSR node
Linked TTR		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	Red bubble on DSR node
Unavailability Action	IR Data, IA 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		Alternate Implicit Routing makes previous metadata bubble red and appends a text in its tooltip.
Route Group Selected	IR Data	Gray bubble on DSR node
Mediation Rule Match	IR Data, ER Data, IA Data, EA Data	Gray bubble on DSR node
Request Rerouted	IR Data	Gray bubble on DSR node
Answer Timeout	IA	Arrow from source node to destination node
Answer Matching Failed	IA Data	Red bubble on DSR node
Address Resolution Match	App Data	Address Resolution Match appends a text to the corresponding Application bubble.
Routing Exception	App Data	Routing Exception appends a text to the corresponding Application bubble.

**Table 4-2 (Cont.) Ladder Diagram Visualization**

Event Type	Event Scope	Event Diagram Visualization
DP Query Sent	App Data	DP Query Sent appends a text to the corresponding Application bubble.
DP Response Received	App Data	DP Response Received appends a text to the corresponding Application bubble.
DP Query Failure	App Data	DP Query Failure appends a text to the corresponding Application bubble.
DP Response Timeout	App Data	DP Response Timeout appends a text to the corresponding Application bubble.
SBR Query Sent	App Data	SBR Query Sent appends a text to the corresponding Application bubble.
SBR Response Received	App Data	SBR Response Received appends a text to the corresponding Application bubble.
SBR Query Failure	App Data	SBR Query Failure appends a text to the corresponding Application bubble.
SBR Response Timeout	App Data	SBR Response Timeout appends a text to the corresponding Application bubble.
Message Copied	IA	MSG-Copied bubble appears on DSR node
Copied Message	IG (Internally Generated)	Copied-MSG bubble appears on DSR node
Message Copy Triggered	IR, ER	MC-Triggered bubble appears on DSR node
Request Redirected	IR Data	Gray bubble on DSR node
Diameter Request processing routine invoked	IR Data	Diameter Request processing routine invoked appends a text to the corresponding Application bubble.
Diameter Answer processing routine invoked	IR Data	Diameter Answer processing routine invoked appends a text to the corresponding Application bubble.
U-SBR Query send	IR Data	U-SBR Query appends a text to the corresponding Application bubble.
Callback invoked	IR Data	Callback invoked appends a text to the corresponding Application bubble.



**Table 4-2 (Cont.) Ladder Diagram Visualization**

<b>Event Type</b>	<b>Event Scope</b>	<b>Event Diagram Visualization</b>
Subroutine name not found	IR Data	Subroutine name not found appends a text to the corresponding Application bubble
Runtime error	IR Data	Runtime error appends a text to the corresponding Application bubble
Debug message	IR Data	Debug message appends a text to the corresponding Application bubble
U-SBR Query Result received	IR Data	U-SBR Query Result received appends a text to the corresponding Application bubble
U-SBR Query send failed	IR Data	U-SBR Query send Failed appends a text to the corresponding Application bubble

## ProTrace Full Decoding Panel

When the user selects a payload event in the Events Panel or a balloon from the Event Diagram, the corresponding message is displayed fully decoded in the Full Decoding Panel. This view explains every byte of the selected message.

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

Figure 4-10 ProTrace Full Decoding Panel



The detailed decoding list has certain columns:

- **Offset** (An offset address of the field from the beginning of the payload. The Version field of the Message Header has an offset 0)
- **AVP/Field Name**
- **Value and description** (Value and possible description)

Table 4-3 ProTrace Full Decoding Panel

AVP Type	Display
Integer32/Unsigned32	Numeric value
Integer64/Unsigned64	
Enumerated	Numeric value + description of the value if known
Grouped	Names of all child AVPs
UTF8String	UTF string from the bytes
OctetString	If all bytes are displayable (codes are from 32 to 128 <b>ASCII</b> ) then it is displayed as <b>UTF</b> string, otherwise the hex decode is displayed
IPAddress	D.D.D.D or XXXX:XXXX:....:XXXX:XXXX depending on IP version (IPv4 or IPv6) (where D is decimal digit and X hexadecimal digit)
Appld	Application Id and Name if known
VendorId	Vendor Id and Name if known

## Custom AVPs, Commands, and Vendors

The user can add custom AVPs, commands and vendors through an **XML** configuration file called diameter dictionary file. The Diameter decoder component, which is responsible for

diameter message/**AVP** decoding, will look at its start-up at the specific location (at the Application server itself) and if it finds the dictionary file there, it will use it to decode diameter messages.

If a change is made to this dictionary file, the application server must be restarted to pick-up the changes.

The custom diameter dictionary file must be valid **XML** file, which contains one single root element called dictionary. All other tags defining custom commands, vendors and AVP must be included inside of this tag.

### AVP Example

```
<?xml version="1.0" encoding="UTF-8"?>
<dictionary>
  <vendor vendor-id="VF" code="12645" name="Vodafone" />
  <command code="316" short-name="UL" name="Update-Location" />
  <avp name="3GPP:3GPP-IMSI" display="3GPP-IMSI" code="1" vendor-
id="3GPP" type="UTF8String"/>
  <avp name="Framed-Routing" display="Framed-Routing" code="10"
type="Enumerated" >
    <enum code="0" name="None"/>
    <enum code="1" name="Broadcast"/>
    <enum code="2" name="Listen"/>
    <enum code="3" name="Broadcast-Listen"/>
  </avp>
  <avp name="3GPP:User-Identity" display="User-Identity"
code="700" vendor-id="3GPP" type="Grouped">
    <avp ref="Public-Identity"/>
    <avp ref="3GPP:MSISDN"/>
    <avp ref="3GPP:Public-Identity"/>
  </avp>
</dictionary>
```

## Adding Custom AVPs

### Simple AVP Tag Format

The format must be used to define new custom AVP:

```
<avp name="<avpName>"
display="<displayText>"
[vendor-id="<vendorId>"]
code="<code>"
type="<type>"/>
```

where

- **name** must be a unique AVP identifier in the dictionary file, if the vendorId is present then the name should be preceded by vendor-id
- **display** is the text displayed for this AVP (usually the same as **name**)
- **vendor-id** is optional and, if present, then must be either defined in the custom dictionary file, or must be one of the predefined ones

- **type** must be a predefined type:
  - OctetString
  - Integer32, Unsigned32, Integer64, Unsigned64
  - UTFString
  - IPAddress
  - TBCD
  - Enumerated
  - Grouped

Example:

```
<avp name = "3GPP:3GPP-IMSI"
display="3GPP-IMSI"
code="1"
vendor-id="3GPP"
type="UTF8String"/>
```

### Enumerated AVP Tag Format

The XML tag format must be used to define new enumerated AVP

```
:
<avp name="<avpName>"
display="<displayText>"
[vendor-id="<vendorId>"]
code="<code>"
type=" Enumerated">
<enum code="<value>" name="<enumDisplayText>"/>
. . .
</avp>
```

where

- **name**, **display**, **vendor-id**, **code**, and **type** are the same as in the case of simple AVP format
- **code** is the numeric value
- **name** is a text which is displayed in the full decoding window. If the **name** value is not defined, the decoder displays just the simple numeric **code** value.

Example:

```
<avp name="Framed-Routing" display="Framed-Routing" code="10"
type="Enumerated" >
  <enum code="0" name="None"/>
  <enum code="1" name="Broadcast"/>
  <enum code="2" name="Listen"/>
  <enum code="3" name="Broadcast-Listen"/>
</avp>
```

## Grouped AVP Tag Format

The XML tag format must be used to define new custom grouped AVP:

```
<avp name="<avpName>"
display="<displayText>"
[vendor-id="<vendorId>"]
code="<code>"
type="Grouped">
<avp ref="<refAvpName>"/>
. . .
</avp>
```

where

- **name**, **display**, **vendor-id**, **code**, and **type** are the same as in the case of simple AVP format
- **avp** contains the **ref** name, which must be the name of an existing AVP defined in the custom dictionary

Example:

```
<avp name="3GPP:User-Identity" display="User-Identity" code="700"
vendor-id="3GPP" type="Grouped">
  <avp ref="Public-Identity"/>
  <avp ref="3GPP:MSISDN"/>
  <avp ref="3GPP:Public-Identity"/>
</avp>
```

## Adding Custom Commands

### Command Tag Format

Custom commands are only required if there isn't a code previously defined in the default dictionary. The XML tag format must be used to define new custom command code:

```
<command code="<code>"
short-name="<shortName>"
name="<commandName>"/>
```

where

- **code** is the command code
- **short-name** is the text that appears in the ladder diagram events
- **name** is the text that appears in the full decoding of a message

Example:

```
<command code="316"
short-name="UL"
name="Update-Location"/>
```

## Adding Vendors

Custom vendors are only required if there isn't a vendor previously defined in the default dictionary. Some vendors are already defined and can be used without defining them again:

**Table 4-4 Vendors**

Vendor ID	Vendor Code	Vendor
3GPP	10415	3GPP
3GPP2	5535	3GPP2
ATT	74	AT and T
ATTCCCE	2897	AT and T Capital Corp Ernest
ATTENS	9496	AT and T Enhanced Network services
ATTGNMC	2560	AT and T GNMC Amsterdam
ATTLINA	11976	AT and T Labs Intelligent Network analysis
ATTWireless	971	AT and T Wireless
BS	6431	Broadsoft
ER	193	Ericsson AB
ETSI	13019	ETSI
HP	11	Hewlett Packard
HW	2011	Huawei
IETF	0	IETF
JuniperNetworks	1411	Juniper Networks
JuniperNetworksInc	2636	Juniper Networks Inc
Merit	61	Merit Networks
MTS	29732	MTS
MTSALLSTREAM	23398	MTS Allstream Inc
MTSSPA	18390	MTS SPA
Nokia	94	Nokia
ORACLE	111	ORACLE
ORANGEDK	3531	Orange DK
ORANGEJ	31908	Orange Jordan
ORANGENBV	27585	Orange Nederland BV
ORANGER	23320	Orange Romania SA
ORANGES	11365	Orange Slovakia
ORANGESUS	2083	Orange Services US
RivadaNetworks	44107	Rivada Networks
Sprint	1421	Sprint
SprintPCS	2792	Sprint PCS
Sun	42	Sun Microsystems
TKLC	323	Tekelec
USR	9086	US Robotics
Verizon	32902	Verizon
VerizonBusiness	25516	Verizon Business
VerizonCardOperator	23170	Verizon Card Operator

**Table 4-4 (Cont.) Vendors**

Vendor ID	Vendor Code	Vendor
VerizonESG	14542	Verizon ESG
VerizonWireless	12951	Verizon Wireless
VF	12645	Vodafone

If the new vendor needs to be added, then the tag must appear in the custom AVP file:

```
<vendor vendor-id="<id>"
code="<code>"
name="<description>"/>
```

Example:

```
<vendor vendor-id="VF"
code="12645"
name="Vodafone"/>
```

where

- **vendor-id** is the vendor identified
- **code** is the vendor code
- **name** is the vendor name that appears in the full decoding of a message

Example:

```
<vendor vendor-id="VF"
code="12645"
name="Vodafone"/>
```

## Managing Custom AVPs

This section contains details necessary to add/modify custom AVPs and load them into the system.



### Note:

General Unix/Linux knowledge is required for this section.

## Login

This section describes the necessary steps to login to the application server and change to the correct dictionary for custom AVP.

1. Login or remote shell into the application as user **admusr**.

```
% ssh admusr@192.168.11.1
```

2. Change the user to **tekelec**

```
%sudo su - tekelec
```

3. Change the dictionary to custom AVP.

```
% cd diameter
```

## Edit/Modify AVP File

This section describes the necessary steps to edit/modify the custom AVP file.

1. Login or remote shell into the application.
2. Copy example file to custom-avps.xml file

```
% cp custom-avps.xml.example custom-avps.xml
```

3. Edit custom AVP file.

```
% vi custom-avps.xml
```

## Load AVP File

This section describes the necessary steps to load (install) the custom AVP file into the application server.

1. Login or remote shell into the application.
2. Load custom AVP file.

```
% ./xmlload -l custom-avps.xml
```

### Note:

Users must logout from the IDIH portal/system before changes can be recognized.

## Unload AVP File

This section describes the necessary steps to unload (remove) the custom AVP file into the application server.

1. Login or remote shell into the application.
2. Unload custom AVP file.

```
% ./xmlload -d custom-avps.xml
```

## Changing the Page Layout

The user can change the page layout of the TDR viewer (or Trace viewer) to re-arrange or hide the TDR, PDU, and Full Decode views.

1. Click **Change Layout**.

The layout pop-up opens.

2. Select a **Layout**.

The page layout changes to match the user's choice.



 **Note:**

This new layout will now be the default layout for this session type.

## IDIH Trace Statistics

IDIH gathers statistics about transactions for active traces. The statistics have various dimensions:

- TimeTag - end of the interval for which the record contains statistics
- TraceInstance - identifies trace to which this record belongs
- Node - IP address of the node
- DbLevel - **MCL** (Managed Object ChangeLevel)
- ResultCode - value of ResultCode AVP (code 268)
- ExperimentalResultCode - value of ExperimentalResultCode AVP (code 298)

and the following measures for the given matching dimension values:

- Count - total number of transactions
- Timeouts - number of time-out transactions

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 Oracle 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 them to the user in the form of bar and pie charts.

- If the user double clicks on a bar, it executes a new query and displays TDRs for the clicked node and category (all, errors, success, timeouts)
- If the user double clicks a section in the pie chart, then it displays TDRs with the clicked result code for the selected node

The user can refresh the statistics presented by clicking **Refresh Statistics**.

The user also can return to the [TDR Panel Toolbar](#) by clicking **Return to Traces**.

## Setting User Preferences on IDIH Dashboard

Once inside IDIH, a user can set user preferences. These include:

- Time specifications (such as date format, time zone)
- Enumeration values (numerals vs. text)

## Setting Time Format

Follow these steps to set the time format:

1. Click **User Preferences** on the Application board.  
The User Preferences screen is displayed.
2. Click the **Date/Time** tab.  
The Date/Time screen is displayed. The red asterisk denotes a required field.

 **Note:**

Use the tips on the screen to help configure the time format.

3. Enter the format for these time-related displays.
  - **Date format**
  - **Time format**
  - **Date and time fields**
4. Select the formats for these time-related displays by using the drop-down arrow.
  - **Duration fields** - how the hours, minutes, seconds, and milliseconds of the Time format is displayed
  - **Time zone**

 **Note:**

The local time zone must be chosen to get local time.

5. To reset the time-related displays to default settings, click **Reset**.
6. Click **Apply** to save settings.

## Setting Mapping Preferences

The user can set the Mapping settings using the User Preferences feature.

Follow these steps to set Mapping preferences.

1. Click **User Preferences** in the Application board.  
The User Preferences screen is displayed.
2. Click the **Mapping** tab.  
The Mapping screen is displayed.
3. Check **Translate ENUM values** 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.
4. Check **IP Address to Node Name** to translate an IP Address to a textual Node Name.
5. To reset the Mapping values to the default, click **Reset**.
6. Click **Apply** to save the changes.