

Oracle® Communications Session Monitor

Operations Monitor User Guide



Release 6.1
G41892-01
December 2025

ORACLE®

Copyright © 2014, 2025, 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, software documentation, data (as defined in the Federal Acquisition Regulation), 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," "commercial computer software documentation," or "limited rights data" 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, MySQL, and NetSuite 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

About this Guide

Revision History

1 Connecting Operations Monitor to Your Network

2 Initial Configuration

Logging In	1
Viewing Last Login Information	2
Changing the Default Administrator Password	2
Resetting the Password for a Non-Admin User	3
Adjusting System Settings	3
Adjusting Platform Settings and Defining the Network Topology	4
Defining Web Interface Users	5

3 User Interface

General	1
Requirements	1
Interface Arrangement	1
My Favorites	2
What's New	3
Left Navigation Pane	4
System Highlights	6
Icon Glossary	7
Tooltips and Help	8
Panels	8
Windows	9
Refresh Button	9
Tables	10
Filters	10

Quick User Inspection	13
Charts	13
Controls Used in Panning a Chart	14
Working with Message Flows	15
Displaying a Message Flow	15
Arranging Message Flows	16
Customizing the Display of Contents within Message Flows	17
Customizing the Visibility and Position of Network Devices within Message Flows	19
Viewing Individual Protocol Messages	20
Viewing Call Event ISUP Protocol Messages	21
Obfuscation of Call Data During Export	22
Obfuscation of Message Headers	23
Saving a Message Flow as an HTML File	24
Saving a Call Event Message Flow as a PDF File	24
BICC Support	26
Dashboard	27
Understanding the Dashboard Utilities	29
Configuring Your Default Dashboard Tab	29
Panels	30
Adding a Dashboard Panel to the Default Tab	31
Closing, Cutting and Pasting a Dashboard Panel from the Default Tab	32
Rearranging Dashboard Panels	32
Working with Dashboard Tabs	33
Adding a Dashboard Tab	33
Editing a Dashboard Tab	35
Auto Switch	35
Sharing Dashboard Tabs	36
Alerts	37
Alerts Table	38
Alert Definitions Tab	40
Creating Alert Definitions	41
Alert Actions	42
Alert Name and Priority	44
Voice Quality Alerts for Individual Platform Devices	44
Parameters	46
Statistics Metrics	46
Synthetic KPIs	48
Device Monitoring	49
Phone Number Alerting	49
Traces	50
Packet Buffer	51
Traces Info Panel	51

Signaling Traffic Capture Panel	51
Examples	52
Running and Finished Traces Panel	53
Packet Inspector	55
Packet Inspector Page	55
Query Panel	55
Search Results Preview Panel	56
Query Examples	57
Apps	58
App Descriptions	59
Available Apps	60
Uploading Apps	61
Running Apps	61
Scheduling Apps	62
View App Runs	62
View App Results	63
Scheduling App Execution	63
Removing an App Schedule	64
Cron Expressions	65

4 Operations

KPI/Metrics	1
KPI/Metrics Monitoring Chart	1
Creating a KPI/Metrics Chart with Dual Axis	4
KPI/Metrics Monitoring Grid	5
Library: Platform-Wide Metrics and KPIs	5
Pre-Defined Metrics	6
Advanced Metrics	6
IETF KPIs and Metrics	8
Library: Per-Device Metrics and KPIs	12
Pre-Defined Metrics	14
IETF Metrics	14
Advanced Metrics	15
Filtering in the Metrics/KPIs List	16
Restricting the Scope of Metrics/KPIs	17
Average Metrics/KPIs	18
Favorite Metrics/KPIs	20
Bulk KPI/Metrics Creation and Removal	21
Invocation	21
Information Shown	22
Usage	22

Limitations	23
About Synthetic KPIs	23
Creating Synthetic KPI	24
Editing Synthetic KPI	24
Deleting Synthetic KPI	24
Arithmetic Expression Syntax	25
Calls	25
Call Legs	26
DTMF Tones in Call Flow	26
Call States	27
Active Calls Chart	28
Recent Calls	29
The Recent calls Toolbar	29
Recent Calls Table	31
Filtering	39
Advanced Filtering	43
Filters - Column Header	45
Text-Based Filtering	46
Right-Click Menu	47
Exclusion of Numbers	49
Paging	51
Call Info or Call Details Window	52
Call Details Toolbar	53
Segments	53
Messages	53
Media Summary	55
Downloading Call Details to a PCAP File	56
Device Visibility in Realms	56
STIR/SHAKEN Monitoring	58
Enabling STIR/SHAKEN Support	58
STIR/SHAKEN Call Flow and Verification Process	59
Correlation of HTTP and SIP Traffic	60
Voice Quality	60
Voice Quality Source	60
Operations Monitor RTP Probes	60
User Agent Statistics	61
SIP Voice Quality Events (application/vq-rtcpxr)	62
Other Voice Quality Monitors	62
Voice Quality Chart	62
Device-Specific Voice Quality Dashboard Panel	63
Voice Quality Chart for MOS	63
Voice Quality chart for Packet Loss	65

Voice Quality Chart for Jitter	65
CSV Export	67
Active Calls During a Period of Bad Quality	67
Voice Quality Charts Per Device	68
Media Summary	68
Media Details	71
Audio Status	72
Media Recording	73
Recording RTP Streams	75
Downloading Recorded RTP Streams	75
Registrations	76
Registered Users Panel	77
Registrations Table	77
Registrations Table Actions	79
Paging	80
Registration Details	81
Registration Event Categories	83
Skype for Business Registration Events	83
User Devices	84
User Devices Chart	84
Operations on User Devices	85
Devices List Panel	86
Right-Click Menu	86
Users Using a Specific User Device	87
Subscriptions	87
System Settings for Subscription	88
Platform Setup Application Initial Log In	88
Data Retention	93
Subscribed Users Panel	95
Subscriptions Table	96
Right-Click Contextual Menu - Subscriptions	97
Subscription Table Actions	98
Subscription Details	98
Subscription Event Categories	100
Subscriptions Panel in User Tracking	101
Subscribed Users Panel in IP Tracking	102
Subscriptions Tab in Devices Page	102
Trunks/Prefixes	103
Devices	104
Device Map	105
Device Map Toolbar	106
Device Selection Panel	107

Device Monitoring Status	108
Device Metrics Chart	108
Calls Going Through This Device Tab	110
Terminated Calls Tab	110
Originated Calls Tab	111
Registrations Tab	111
Subscriptions Tab in Devices Page	111

5 Customers

User Tracking	1
User Search Panel	1
Registrations Panel in User Tracking	1
Subscriptions Panel in User Tracking	2
User Calls Panel	3
User Actions	4
IP Tracking	6
IP Search Panel	6
Registered Users Panel	6
Subscribed Users Panel in IP Tracking	7
Calls Panel in IP Tracking Page	7
Link Quality	8
Check Link Quality to a Subscriber	8
Check Link Quality to a Proxy	8

6 Control Plane Monitor

KPI/Metrics	1
Transactions	3
Filtering Columns	3
Transaction Details	4
Message Flow	5
Devices	5
Incoming Transactions	6
Outgoing Transactions	6
IMSI Search	6

7 Settings

General Settings	1
Status	1
Actions	2

External IP/hostname	3
REST API	3
UCaaS CCaaS Monitoring	4
UCaaS CCaaS Monitoring Activation	4
Enabling the UCaaS CCaaS Extension	4
Enabling UCaaS CCaaS System Settings	5
Configuring UCaaS CCaaS Settings	6
Configuring Microsoft Teams	7
Configuring MS Teams Settings in Operations Monitor User Interface	9
UCaaS CCaaS Monitoring - Additions in the Calls Page	10
UCaaS CCaaS - Filtering	10
UCaaS CCaaS – Changes in Calls Info	12
UCaaS CCaaS - KPI Page	17
UCaaS CCaaS - User Management	18
UCaaS CCaaS Header Notification	19
Disabling UCaaS CCaaS Monitoring	21
Network	21
Probes	21
Mediation Engine Connector	23
Disconnecting Mediation Engine from Mediation Engine Connector	24
Number Determination Sources	25
Platform	25
Platform Devices	25
Device Types	26
SBC/B2BUA Call Merging	28
3PCC Options	30
Device Identification	32
Providing a Name	34
Visibility Configuration	34
Configuring Devices for the Mediation Engine Connector	35
Enabling or Disabling Device Map for a Device	35
Configuring Devices for Voice Quality Measurement	36
Searching for Platform Devices	37
Device Monitoring	38
Enabling Device Monitoring	38
Adding and Editing Monitored Devices	38
Device Monitoring Parameters	39
IP Tags	39
Prefix Tags	40
Automatic Realm Pattern Import	41
About Formatting the CSV File	42
Sorting Realms	42

Importing Realms at a Daily Frequency	42
Editing the CSV File	43
Realms	43
Realms Table	44
Searching for Realm Patterns	45
Realm Patterns	45
Searching for Realm Patterns	48
Realms Header Specification	49
Custom Headers for the Calls Page	50
Creating Custom Headers for Calls	51
Viewing the Custom Header Columns in the Calls Panel	53
Viewing History of Calls Custom Headers	54
KPI Management	55
User Management Permissions for KPI	55
Creating a KPI Custom Template	56
KPI Templates	57
Before Applying Templates to a Device or Tag	58
Applying a Default Template for KPIs to a Device or Tag	58
Applying a Custom Template for KPIs to a Device or Tag	59
Applying the None Template for KPIs to a Device or Tag	60
Common User KPIs	61
KPIs for Imported Devices in Configuration Savepoint	62
System Management	62
List of System Settings	63
System Settings	81
B2B Backlog Search for Merging 3PCC Call	83
B2B Incoming Backlog Search for Merging	83
B2B Outgoing Backlog Search for Merging	84
Call Flow Messages	84
Call Flow Maximum Height/Width	84
Call Flow Parallel Loading	84
Calls Partition Size	84
Call Report Maximum Number of Messages	84
Enabled Device Map	84
Future Maximum Search	84
High Threshold for MOS	85
Group New Registrations from the Same User	85
Ignore Internal Registrations	85
Low Threshold for MOS	85
Match Registration Events by Comparing a Suffix of the Username	85
Matching a Message to a Device	85
Matching a Message to an Existing Call Leg	86

Maximum Concurrent Sessions	86
Maximum Stored Script Runs	86
Maximum Script Output Size	86
Maximum Simultaneous Script Runs	87
Newest Search Cache	87
Oldest Search Cache	87
Recurrent Alerts Threshold	87
Registrations Gone Events	87
Search for Matching Registration Segments	87
Session-Timeout For Calls	88
Timeout for Mediation Engine Querying	88
Timeout for Restore Savepoint	88
User Devices Ignore Internal Registrations	88
Users Loose Searching	88
Use User Domains	88
Web Session Timeout	89
Oracle SBC Config Upload	90
Import Window	91
Language Settings	91
Privacy Settings	91
SIP Header Anonymization	92
Anonymizing SIP Headers	93
SFB	94
Skype For Business Filter	94
External Devices	94
RADIUS Authentication	95
SNMP Options	96
SNMP Traps	96
SNMP Daemon	97
Exported Counters	97
System Monitoring	99
SFTP Server	99
Enabling Access using SFTP	99
Voice Quality Collector	100
Configuration Savepoints	101
User Management	103
Setting Field Visibility (Calls Panel) for a User	104
The User Administrator Role	105
Enable User Roles	105
Add the User Administrator User	106
Tasks List of the User Administrator User	107
Add a New User	108

User Information	108
Selecting a Role	108
User Permissions	109
User Realm	113
Overview Information	114
Requirements for RADIUS Authentication	114
Role Management	115
Adding a Role	116
Editing a Role	117
Deleting a Role	117
Adding Rights to a Role	117
Removing Rights from a Role	118
Searching for a User Role	118
External Authentication Authorization	118
Password Settings	118
Enabling or Disabling User Accounts	119
View Logged in Users in the Mediation Console	120
Log Out Users in the Mediation Engine Console	120

8 Call Merging Algorithms

Merging and Correlating Calls	1
Syntax	2
Tests Reference	3
call_id ([suffix])	3
hf_equals (header)	4
hf_any_equals (headers)	4
hf_any_equals_all (headers)	4
hf_equals_prefix (length, header)	4
hf_param_equals (header, param)	4
hf_uri_param_equals (header, param)	4
sdp_media_ip_port ()	4
sdp_session_id ()	5
time_diff (interval1, interval2)	5
uri_user (suffix, list_of_headers)	5
uri_user_max (suffix, list_of_headers)	6
uri_user_all (suffix, list_of_headers)	6
uri_user_all_max (suffix, list_of_headers)	7
cxpn_uri (suffix, list_of_headers)	7
cxpn_uri_max (suffix, list_of_headers)	7
cxpn_uri_all (suffix, list_of_headers)	7
cxpn_uri_all_max (suffix, list_of_headers)	7

cdpn (suffix)	7
cgpn (suffix)	7
Test Usage Limitations	7
Examples	8
Match by the Caller and the Callee	8
Match by Generic Algorithm	8

9 Implementing Apps

Structure of an App	1
Apps API	2
Using the Apps API Examples	20
Remote App Procedure Calls	21
Invoking an App	22
Retrieving the Results of an App Run	22

10 REST API

Interface Description	2
The Format of List Resources	11

11 New REST API

API Key	1
Getting Started	2
Usecase Backup	3
Usecase High Availability	4
Examples	4
Reference	5
Fundamental Concepts	5
Configuration Savepoints	6
Calls	8
Filter Design Template	8
Creating a Filter for a Specific Column	9
Registrations	15
Fields and Types for getRegsPaged	17
KPI	17
Reverse Engineering of API Calls	22

12 Client-Side Add-Ons

Structure of an Add-On	1

	Packaging	3
	Management	3
	Code Examples	4
13	Diameter Transaction Records (TDRs)	
14	Public CDR Generation	
	Customizing CDR Generation	7
15	Voice Quality Records (MDRs)	
16	Troubleshooting	
	First Aid	1
	Suggestions for Specific Error Cases	1
17	Health Check Daemon	
	Introduction	1
	Editing cghealth Daemon Configuration File	1
	Setting Hard Limit for Services	2
	Restarting Services	2
	Nightly Check for Individual Service Memory Usage	3
18	Multiple-VSP - Overview	
	Enabling or Disabling Multiple-VSP	1
19	MGCP Correlation	
	Introduction	1
	Configuring the MGCP Correlation	1
	Understanding MGCP NCS Signalling	1
	Mapping Endpoint IDs to Phone Numbers	1
	Working with MGCP Endpoints With a disp Prefix	3
	Endpoint Utilities Reference	3

20	Storage Expansion Support for Mediation Engine	
	Expanding Storage	1
	Options for Storage Expansion Command	4
	Storage Soft Limits	5
21	Key Performance Indicator Reference	
	KPIs	1
	Platform-Wide and Prefix Tag KPIs	1
	Device, Trunk and IP Tag KPIs	29
A	Supported Codecs	

About this Guide

This guide describes how to use Oracle Communications Operations Monitor to monitor, detect, and troubleshoot IP Multimedia Subsystem (IMS), Voice over Long-Term Evolution (VoLTE), and next-generation network (NGN) networks.

This guide applies to both the Oracle Communications Operations Monitor and the Oracle Communications Enterprise Operations Monitor. The Oracle Communications Session Monitor product family includes the following products:

- Operations Monitor
- Enterprise Operations Monitor
- Control Plane Monitor

Documentation Set

Table 1 Documentation Suite for Session Monitor Release 6.1

Document Name	Document Description
Backup and Restore Guide	Provides instructions for backing up and restoring Session Monitor.
Developer Guide	Contains information for using the Session Monitor SAU Extension.
Installation Guide	Contains information for installing Session Monitor
Mediation Engine Connector User Guide	Contains information for configuring and using the Mediation Engine Connector.
Operations Monitor User Guide	Contains information for monitoring and troubleshooting IMS, VoLTE, and NGN networks using the Operations Monitor.
Release Notes	Contains information about the Session Monitor Release 6.1, including new features.
Security Guide	Contains information for securely configuring Session Monitor.
Upgrade Guide	Contains information for upgrading Session Monitor.

Revision History

This section provides a revision history for this document.

Date	Description
December 2025	Initial Release. Includes documentation for new and enhanced features in the Oracle Communications Session Monitor Release 6.1.

1

Connecting Operations Monitor to Your Network

Oracle Communications Operations Monitor software module includes the operating system, and can be installed on standard x86-64 architecture machines. The number of network ports may vary, although a minimum of two is required.

Operations Monitor distinguishes between two kinds of network interfaces:

Management interfaces

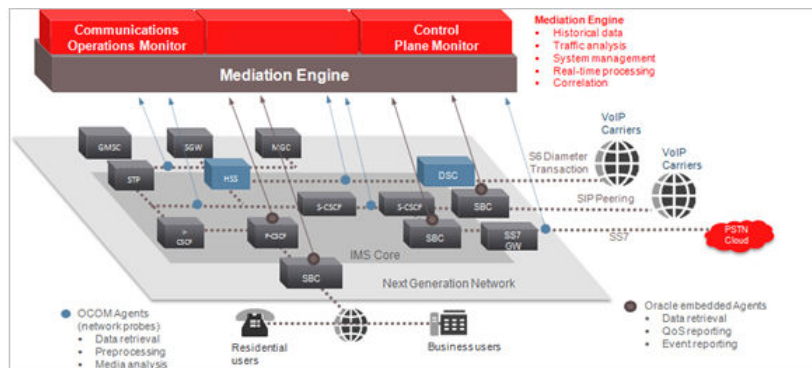
Management interfaces are used for accessing the Operations Monitor web user interface and other management network traffic (including REST, CDR access, SNMP, ICMP, connection to probe).

Monitoring interfaces

Monitoring interfaces are used for passively receiving the signaling and/or media traffic to be analyzed by the Oracle Communications Session Monitor (Session Monitor) family of products. Monitoring interfaces do not require an IP address and are not assigned one by default.

The following figure represents where network traffic can be sent to Operations Monitor.

Figure 1-1 Network traffic sent to Operations Monitor



The Oracle Communications Session Monitor Mediation Engine Connector can receive traffic from multiple locations on the network and provide a single end-to-end view of the network. The more data that is made available to Operations Monitor, the more comprehensive the results are. The signaling or media-related traffic captured depends on the licensed extensions. Licenses include, but are not limited to:

- SIP
- RTP
- RTCP
- SIGTRAN/ISUP/SS7

- H.248/Megaco
- MGCP
- Diameter
- ENUM

The traffic is copied from the active paths to the monitoring interfaces using mirroring port features of network switches (for example SPAN), remote port mirroring protocols (for example RSPAN), or tapping devices. In addition network data can be retrieved directly by configuring the Operations Monitor probe within Oracle Communications Session Border Controller (Session Border Controller). Using Session Border Controller is the only way to analyze otherwise encrypted signaling traffic.

Note

For information on configuring the network switches, refer to the manual provided by your switch manufacturer.

The number of monitored network segments is not limited by the number of network interfaces of the machine that hosts Operations Monitor. Aggregating traffic from multiple tapping points into one single monitoring port works as well as configuring any number of external network probes.

Note

The Session Monitor product family is not compatible with third party probes.

2

Initial Configuration

This chapter guides you through the configuration steps required to get Oracle Communications Operations Monitor started. You must first install an instance of Operations Monitor, connect it to your network, and access the web interface via a web browser. See the referenced sections when changing settings for additional required information.

Note

The web interface requires a browser with Javascript enabled. Refer to the Requirements section for the list of supported browsers. Allowing HTTP cookies is strongly recommended to enable several convenience features.

Logging In

To log in to the Operations Monitor:

1. Open the Operations Monitor URL in a browser. Contact your System Administrator for the website URL.

Point the browser to the configured IP address of the management interface to load the log in screen.

2. Do one of the following:
 - If you are an admin, log in to the pre-configured account with the username admin and password oracle. If you select **Remember me** checkbox, Operations Monitor remembers your login details for a week on your computer.
 - If you are a user, login with your user credentials. Contact your System Administrator for user credentials. If you select the **Remember me** checkbox, Operations Monitor remembers your login details for a week on your computer.
 - Select the **Disable add-ons(0)** check box to any disable add-ons. Add-ons are used to customize and enhance the user interface.

Note

Your account gets locked after three unsuccessful attempts and by default unlocks after 15 minutes. For more information, see the Password Settings section.

3. At your first login, you will be prompted to choose a unique password for your account. Choose the password.

The menu on the left provides general Operations Monitor functions and individual product features. The main features are described in the User Interface section. In the top-right corner, the current logged-in user is displayed.

Viewing Last Login Information

To view the last login information for a user:

1. In the top-right corner of the Operations Monitor web interface, select **admin** and then select **My Profile**.

The **Edit own user information** dialog box opens, as shown:

Figure 2-1 Edit Own User Information

2. The User Information page has two sections, **General** and **Login Information**.
3. The **Login Information** area displays the user's last successful login date and time before the current session, date and time since the current session has been active, and the date and time when the current password is expired.

The value of the current password expires is displayed as "never, if the "Force users to change their password regularly" is not selected in the Password settings. For more information, see the Password Settings section.

Note

The time zone displayed is the configured time zone for the server.

Changing the Default Administrator Password

To change the default administrator password:

1. In the top-right corner of the Operations Monitor web interface, select **admin** and then select **My Profile**.

The Edit own user information dialog box opens, as shown in Figure 2-1.

2. In the **Set password** field, enter a new password.
3. In the Repeat password field, re-enter the password used in the **Set password** field, which verifies that the password value was entered correctly.

4. Click **Finish**.

Figure 2-2 Edit own user information screen

Note

Important:

The default administrator password, which is provided in the documentation is not secure. Oracle strongly recommends that you change it to a secure password, especially before creating sub-users.

Resetting the Password for a Non-Admin User

A non-admin user can reset password using the **Forgot password** link on the Mediation Engine login page.

You must have a valid email ID that has been configured in the Mediation Engine.

1. Login to the Mediation Engine using the External IP/hostname URL. For example: <https://ocom.example.com/me/>.
2. Click the Forgot Password link on the right corner of the screen.
3. Enter your username and email ID, and click **Send**.
4. Check your email inbox. The email includes a link to reset password
5. Open the link using browser.
6. Set a new password and then click **Reset my password**

After resetting the password, you can now login using the new password.

Adjusting System Settings

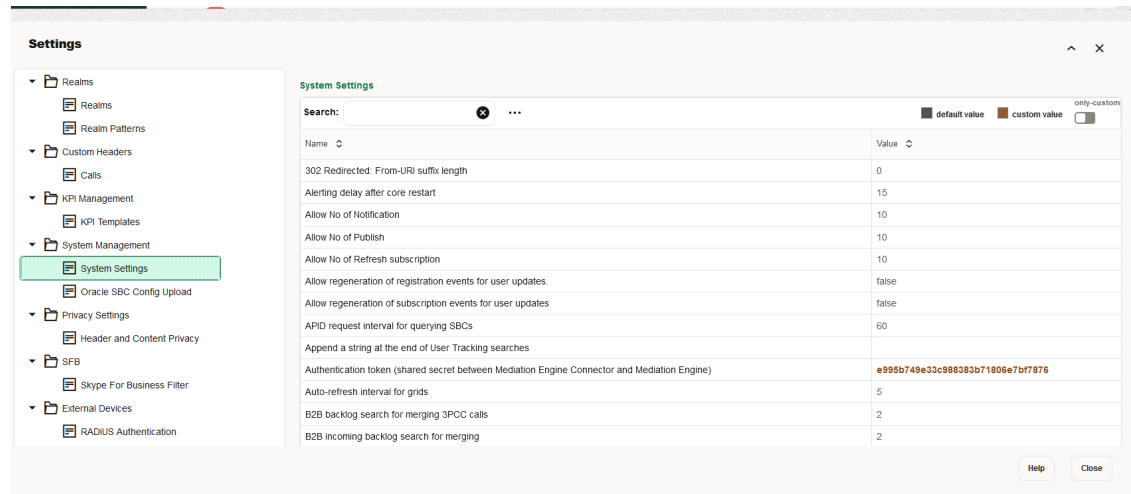
Operations Monitor provides the ability to filter network traffic for relevant IP addresses and ports. By default, Operations Monitor filters SIP messages that use ports 5060 to 6000. If you

have SIP messages that use other ports, or other protocols you want to analyze, you can change that in the Signaling Protocols section in the Platform Setup Application.

The **Use User Domains** setting allows you to customize how a subscriber is identified. By default, Operations Monitor identifies a subscriber by the user portion of SIP URI. If domain names are significant in your network for identifying the users, you should set this option to Enabled. For more information, see the **Use User Domains** section.

These options can be found in the **System Settings** menu entry from the **Settings** window. For more information, see the System Settings section.

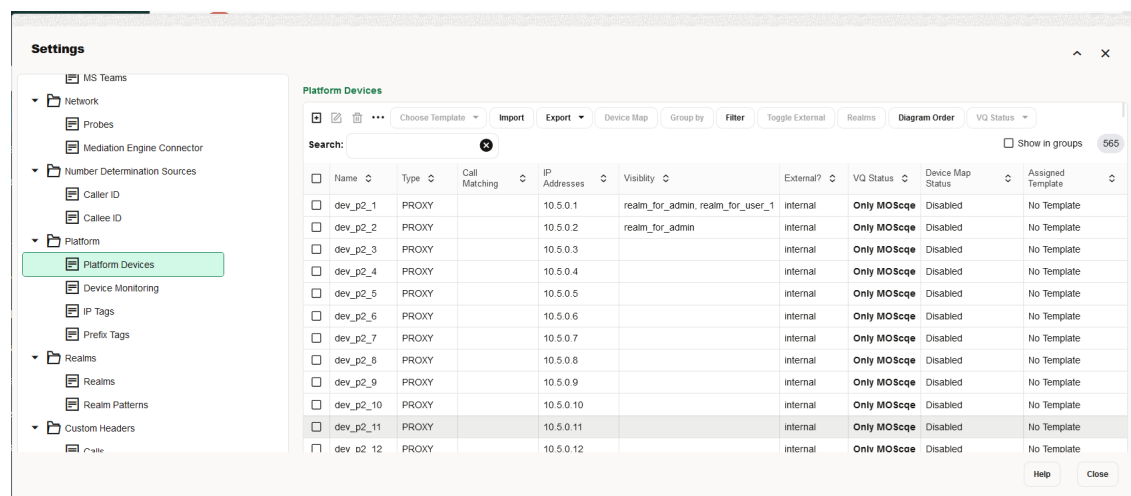
Figure 2-3 System Settings section from the Settings window



Adjusting Platform Settings and Defining the Network Topology

Operations Monitor can trace calls end-to-end while they traverse your network. This is also true for when SBC and B2BUA devices are in use. Operations Monitor shows comprehensive per-device statistics, including response and transit times. Operations Monitor can also monitor your SIP devices and raise alerts when a device is detected as non-responsive.

Figure 2-4 Platform Devices

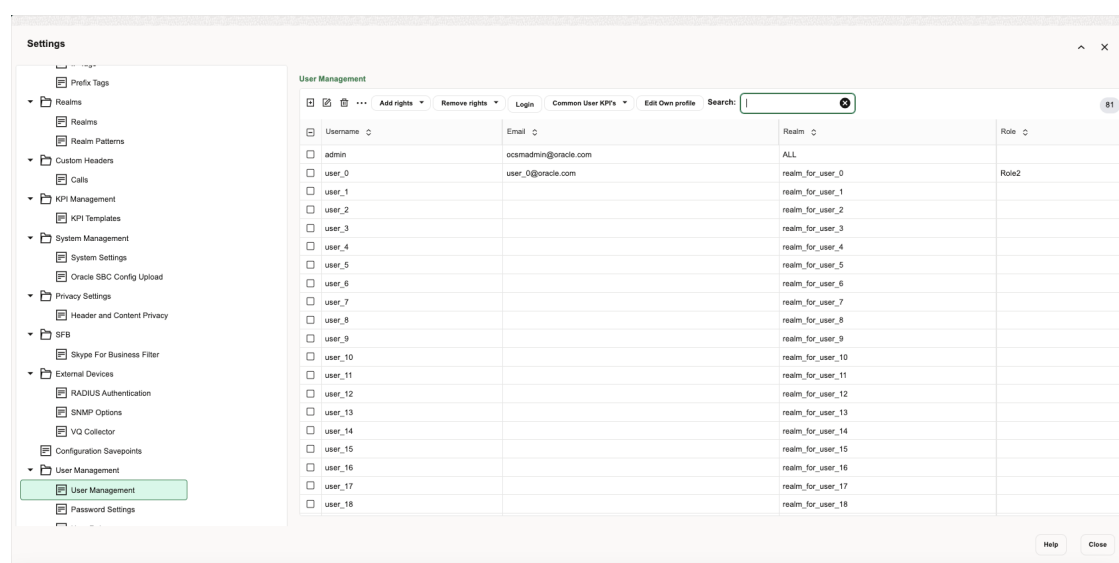


In order to correlate sessions end-to-end correctly, you need to define your network topology by configuring the devices (network equipment) that process and relay the sessions and registrations in your network. For instructions on how to do this, see the Platform Devices section.

Defining Web Interface Users

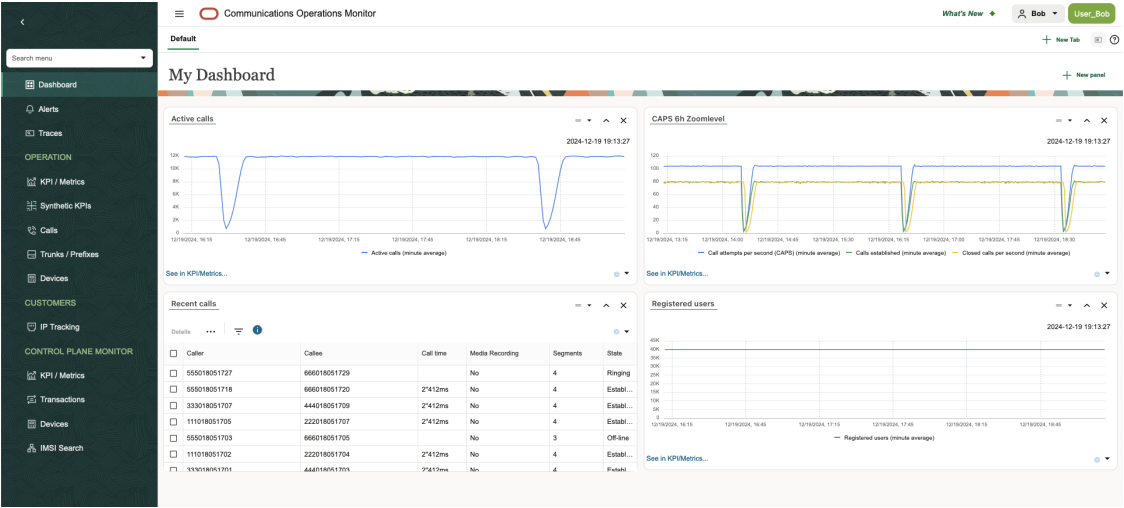
Operations Monitor offers a comprehensive system to manage user permissions that allows you to restrict certain views and functions for users.

Figure 2-5 User Management



You can customize restrictions per user for certain pages, tabs, and product features. For example, you can restrict the ability to view raw SIP messages, change settings, and the option to create PDF reports. For details about how to define users and assign rights, please refer to the **User Management** section. For more information on restrictions extended to single phone numbers/subscribers, see the Realms Definitions section.

Figure 2-6 Non-Admin User Dashboard



3

User Interface

This chapter describes how to work with the Oracle Communications Operations Monitor web user interface.

General

This section provides an introduction to the web interface, requirements, and frequently used interface elements of Operations Monitor.

Requirements

Operations Monitor runs in any major web browser without extra plug-ins or add-ons.

Note

Operations Monitor does not require Flash, Java or Microsoft Silverlight.

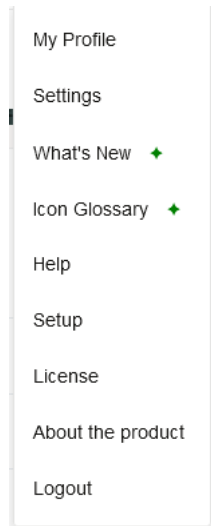
For information on the web browsers on which we test the web interface, see the [Session Monitor 6.0 Release Notes](#).

In order to use the web interface of Operations Monitor, you must enable Javascript. It is recommended that you enable HTTP cookies for features such as remembering login credentials and the state of tables.

Interface Arrangement

On the left side of the Operations Monitor web user interface is the navigation pane. This navigation bar allows access to many of the features of Operations Monitor.

The right side of the Operations Monitor menu bar displays your username, which contains a list with following options:

Figure 3-1 Interface Arrangement

1. **My Profile** for user settings.
2. **Settings** for administrative features.
3. **What new** Lists the new features and the enhancements made in the GUI for this release.
4. **Icon Glossary** Lists the icons used in the user interface along with the task they perform.
5. **License** for the Oracle Communications Session Monitor license terms.
6. **About the product** for the Operations Monitor copyright information.
7. **Help** for access to the Operations Monitor online manual.
8. **Setup** to access the Session Monitor Platform Setup Application.
9. **Logout** to sign out.

My Favorites

The **My Favorites** page allows you to view and manage pages marked as Favorite within the application. It provides quick access to frequently used or preferred items without having to search for them each time.

The My Favorites option is available for the following pages:

- Add New Platform Devices
- Add New Device Monitoring Entry
- Add New IP Tags
- Add New Prefix Tags
- Add New Realms
- Add New Realms Patterns
- Oracle SBC Config Upload
- System Settings
- Add New User

- Upload Apps
- Add New KPI Template
- Configuration Savepoints

Note

The visibility of pages depends on the access permission of the current user.

You can mark a page as a Favorite using any of the following options:

- My Favorite option

or

- admin > Manage My Favorites

Once you mark a page as a Favorite, you can quickly access such a page, using the My Favorites option in the left navigation menu.

What's New

The **What's New** feature is designed to enhance user engagement by providing easy access to the latest updates and functionalities within the application.

To launch What's New:

1. What's New can be launched in two ways:
 - a. Header or Title bar: What's New is prominently displayed on the header for quick access.
OR
 - b. Username drop down: You can see What's New option in the drop down menu associated with the current logged-in username. What's New is displayed in a new browser tab.

Figure 3-2 Launching What's New

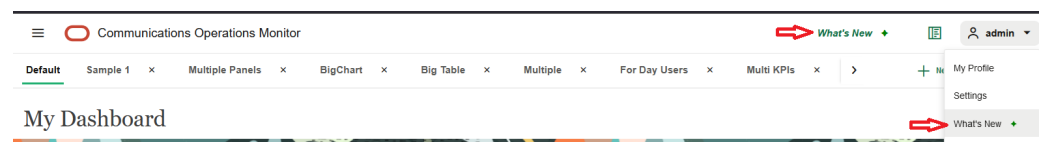
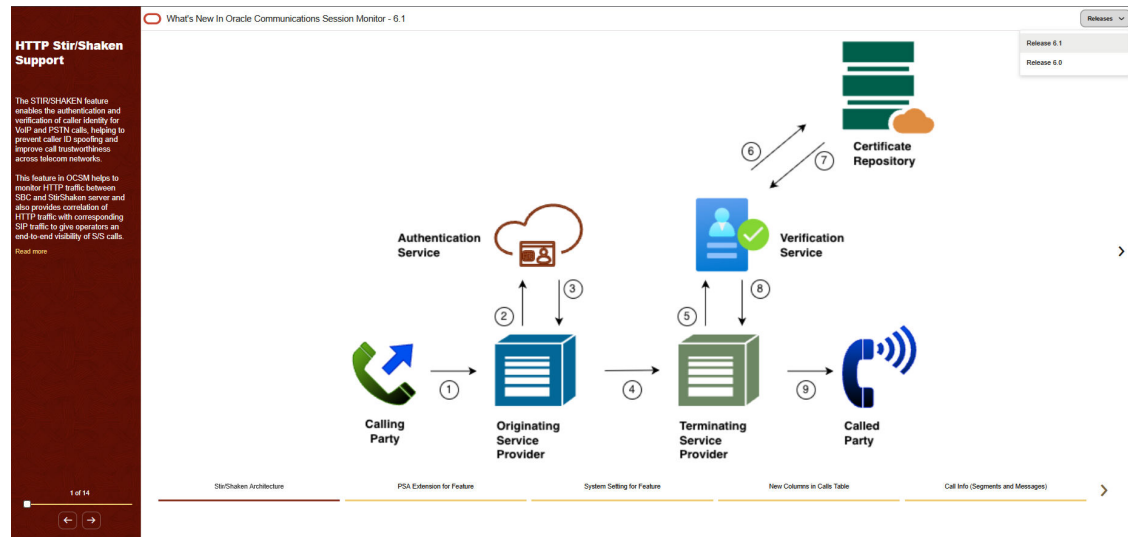


Figure 3-3 What's New



- **Comprehensive List of New Features** This section details all the new functionalities added in the latest release, ensuring users are informed about enhancements and changes.
- **Demo Animations:** Each new feature is accompanied by a demonstration in the form of animated GIFs. This visual aid helps you to quickly familiarize with the features and understand how to use them effectively.

The **What's New** feature serves as an essential tool to be informed and engaged with the latest developments in the application. It offers easy access and visual demonstrations, and enhances user experience and supports effective utilization of new features.

Viewing “What’s New” by Release

A new Releases dropdown is displayed on the right side of the Dashboard, allowing you to select and view the What's New information you want to view based on the selected Release/version.

By default, the page displays the What's New content for the current Release. You can confirm this from the page header and the URL.

To view details for a different version, select the Release number from the dropdown menu. The What's New page for the selected version opens in a new browser tab.

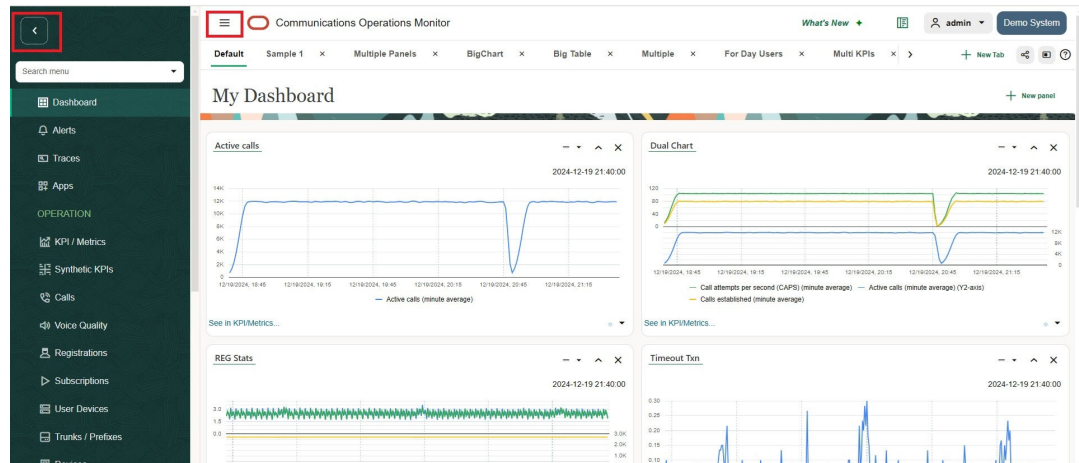
Left Navigation Pane

The Enterprise Operations Monitor web user interface provides three distinct viewing states to enhance usability and accessibility.

On the left side of the interface, you will find two key buttons that help with navigation:

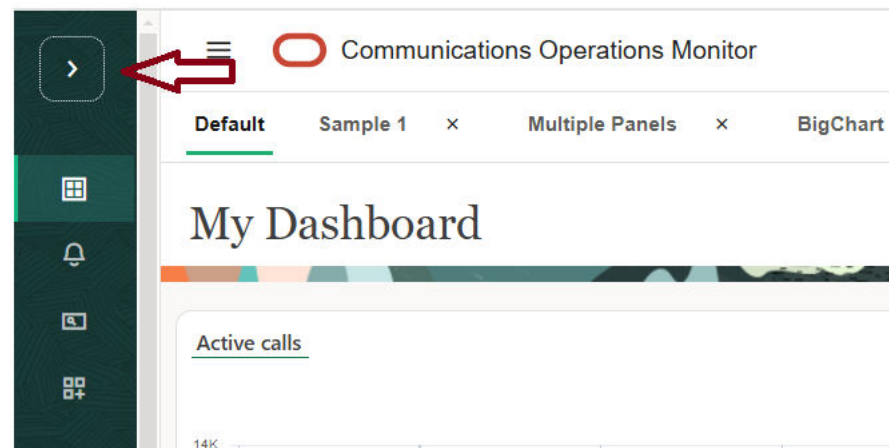
- **Collapse Navigation Button**

Figure 3-4 Collapse Left Navigation Pane



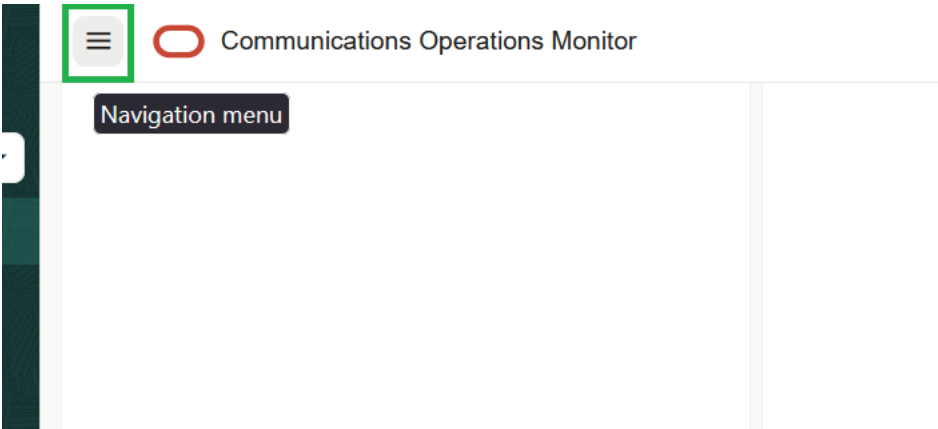
- Location: At the top of the left navigation panel.
- Functionality: When you click this button, it collapses the navigation items, turning the panel into a streamlined view with icons. This gives you access to essential navigation options while maximizing screen space for your content.
- **Toggle Button**

Figure 3-5 Toggle Button



- Location: Next to the Collapse Navigation Button.
- Functionality: When you activate this button, it hides the entire left navigation panel, showing only icons with tooltips. This allows you to use the full screen for your tasks, giving you an unobstructed view of the content.
- **Hide/Show Left Navigation Pane:**

Figure 3-6 Hide or Show Left Navigation Pane



This option lets you completely hide the left-side navigation menu, giving you more space to view the panels and tabs.

These navigation options gives you flexibility in viewing and accessing menu options in the Operations Monitor GUI. You can easily switch between different views to suit your preferences and tasks, ensuring a more efficient workflow.

System Highlights

Added in the Session Monitor Release 6.1, system highlights provides a high level view of the health of the system.

Note

System Highlights feature can be viewed only by the Admin user.

On the Header panel of the Operations Monitor web user interface, click the System Highlights tool to access the System Highlights dialog box. The System Highlights dialog box can be viewed in a split view while navigating to other sections/pages of the user interface.

Figure 3-7 System Highlights



Table 3-1 Components of the System Highlights Window

Component	Description
Date and Time and Welcome message	As stated in the Component column.
Unread alerts	Shows the number of unread alerts requiring the users attention.

Table 3-1 (Cont.) Components of the System Highlights Window

Component	Description
Apps currently running	Apps currently running in the background
Traffic overview	Shows 10 Platform-wide KPIs. This list of KPIs can be configured using the Edit KPIs button provided. Probe Bandwidth and Active Probes are mandatory KPIs that cannot be deleted from this view.
Charts: • User Device Distribution • Call State Distribution for last 50 Calls • Voice quality	Shows user device distribution and calls state distribution chart for 50 calls and voice quality charts
System overview	Provides high level of the system: • Logged in users • Number of prefix tags • Number of IP tags • Number of Realm Patterns • Number of Platform Devices • Number of Realm Patterns Click on any entry to navigate to the specific page.
Quick links	• My Dashboard - Click to go to the current Dashboard. • Search for IP address: click to go to the IP tracking page. • Search for User: click to go to the User Tracking page.

- Key insights into critical alerts, traffic overview, system overview, and quick links.
- A snapshot of essential machine metrics, including KPIs, calls, voice quality, prefix tag counts, platform devices, and more.

 Note

Traffic overview KPIs can be customized by the admin. The user device distribution graph has been redesigned. The recent calls state distribution has been updated and can now support up to 50 calls.

Icon Glossary

Operations Monitor Release 6.1 introduces **Icon Glossary** as a newly added feature in the user interface that enhances the user experience and accessibility. You can access the Icon Glossary using the menu bar on the right side of the interface, where you can view your <username>.

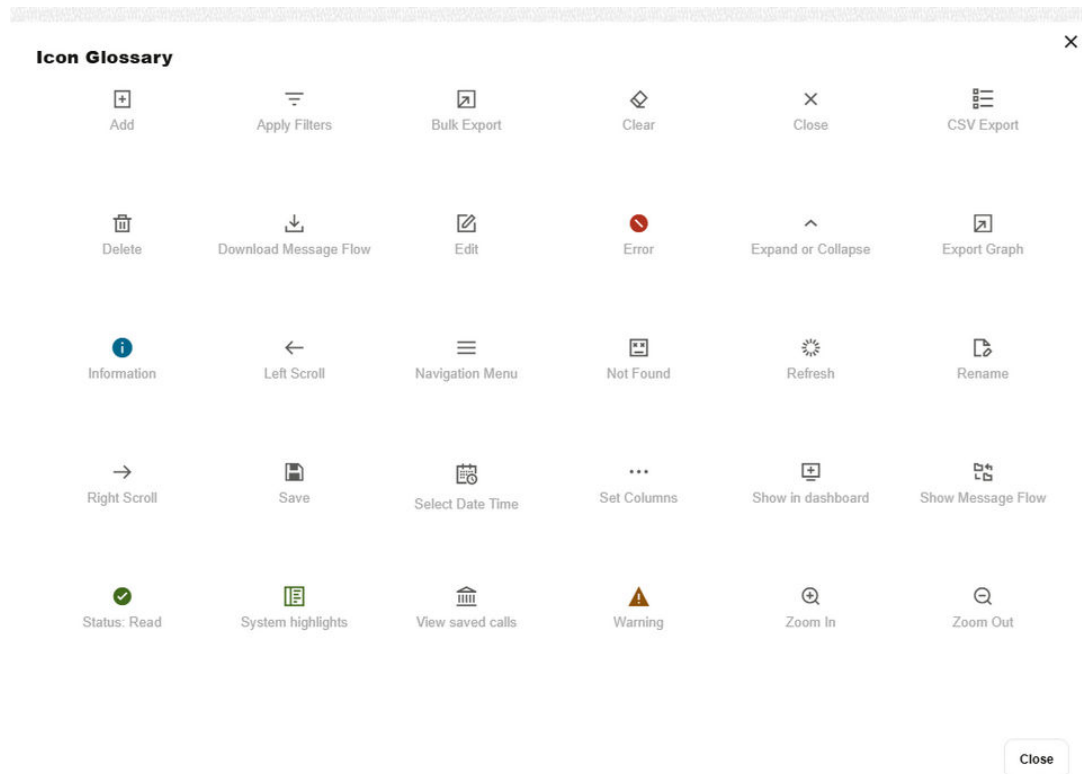
Accessing the Icon Glossary

1. Click the drop-down associated with your username.
2. Click **Icon Glossary**.

When you click the **Icon Glossary** option, a new window is displayed which shows a list of icons used throughout Operations Monitor. Each icon is accompanied by its respective

name. This information provides clarity on the graphical representations used in the user interface.

Figure 3-8 Icon Glossary



The **Icon Glossary** serves as a visual reference, allowing users to quickly identify and understand the various icons in the Operations Monitor user interface.

Tooltips and Help

In the title bar of each panel is a ?-symbol. This is the information box. When you hover over the information box, a tooltip provides a brief description of the panel. When you click the ?-symbol, the corresponding section of the user manual appears in a new browser window or tab describing the panel and its functions.

Other user interface elements support tooltips. Hovering over an element with the mouse pointer often brings up a small box explaining the element underneath.

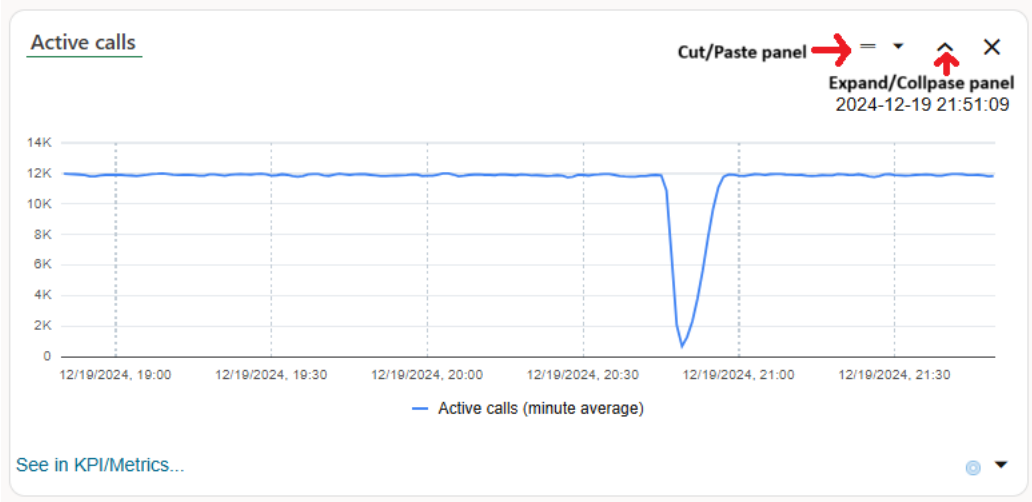
Panels

When you click an element in the navigation pane, a panel appears in the center of the browser window. This panel is a user interface element that displays data.

Many panels can be added to your dashboard for at-a-glance viewing. For more information, see the Dashboard section.

To collapse panels and display titles only, you can click the angle-bracket in the upper-right hand corner.

Figure 3-9 Panels



Another common user interface element is the tab panel.

Figure 3-10 Tabs Panel

Alerts

My Alerts						Alert Definitions	
☒	☐	☒	Mark as new	Details	☐	☐	☐
☐	Status	Date	Type	Message	Priority		
☐	🔴	2024/12/19 16:10:16	Generic Metrics	The minute sum of "Active calls" rose above 10	high		
☐	🟢	2024/12/18 17:35:16	Generic Metrics	The minute sum of "Active calls" rose above 10	high		
☐	🟢	2024/12/17 17:00:16	Generic Metrics	The minute sum of "Active calls" rose above 10	high		

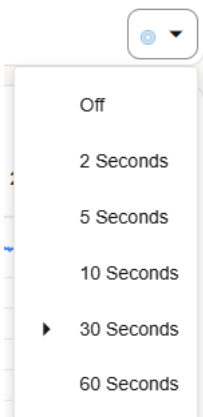
Windows

You may encounter modal windows overlaid on the user interface, similar to the windows of your desktop environment. These windows can be dragged by their title bar, and closed by clicking on the x-symbol or pressing the **ESC** key. These windows also contain **Help** and **Close** buttons at the bottom. The **Help** button opens the online Help in a new window, describing the current page and its functionality.

Refresh Button

Some areas of the interface contain a **Refresh** button that controls the update interval for the content of the page, panel, or section. It is identified by a circle of dots (flashing during refresh). Click the button once to refresh the corresponding content. It also contains a drop-down list to set the interval for the **Auto Refresh**.

Figure 3-11 Refresh Panel Data



Tables

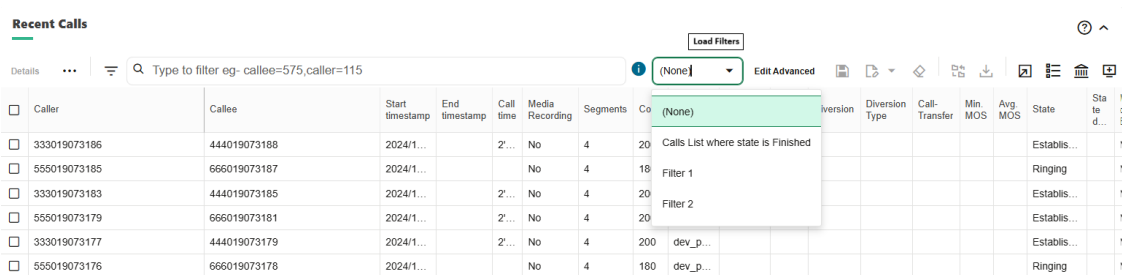
The tables used in the Operations Monitor user interface offer some features to make the data most useful to you.

To adjust tables, hover above a *column* header. A down-arrow appears on the right side of the column header. To access the *table menu*, click the *down arrow*. The table menu options may differ depending on the data presented in the table.

Filters

Tables such as Calls, Registrations support the Filters feature. If a table column can be filtered, the **Filters** button is visible on the table menu bar.

Figure 3-12 Filters



- **String Filter** Filters the table to display rows that contain the entered value as a sub-string. The input value is not exclusive. This filter menu provides a text field for entering the string.
- **Numeric Comparison Filter** Restricts the table to rows where the comparison of the column value with the entered numeric results is 'true'. This filter menu provides three fields, one for each of the supported operators (>, <, =). The = field cannot be used simultaneously with any of the other fields.
- **Date Comparison Filter** Restricts the table to rows where the column value in the selected date range. This filter menu provides three items for choosing a date (Before, After, On). With Before and After you can select the rows where the time stamp of the column values

lies before and/or after the chosen day. With On you can select the rows of only the chosen day.

- **List Filter** Restricts the table to rows where the column values contains the selected value. This filter menu provides a list of possible values, which you can choose by selecting or deselecting the corresponding check box.

Hiding and Unhiding Columns in Tables

You can choose to hide or unhide certain columns in each table.

- In the Table view, drag the column separator to adjust the width of the column. The column width is maintained even after you log out of Session Monitor.
- Select or deselect the check box to the left of each entry to select the entire row.
- Click **Set Columns** to see a list of the available controls for hiding or unhiding columns for this table.

Figure 3-13 Set Columns window

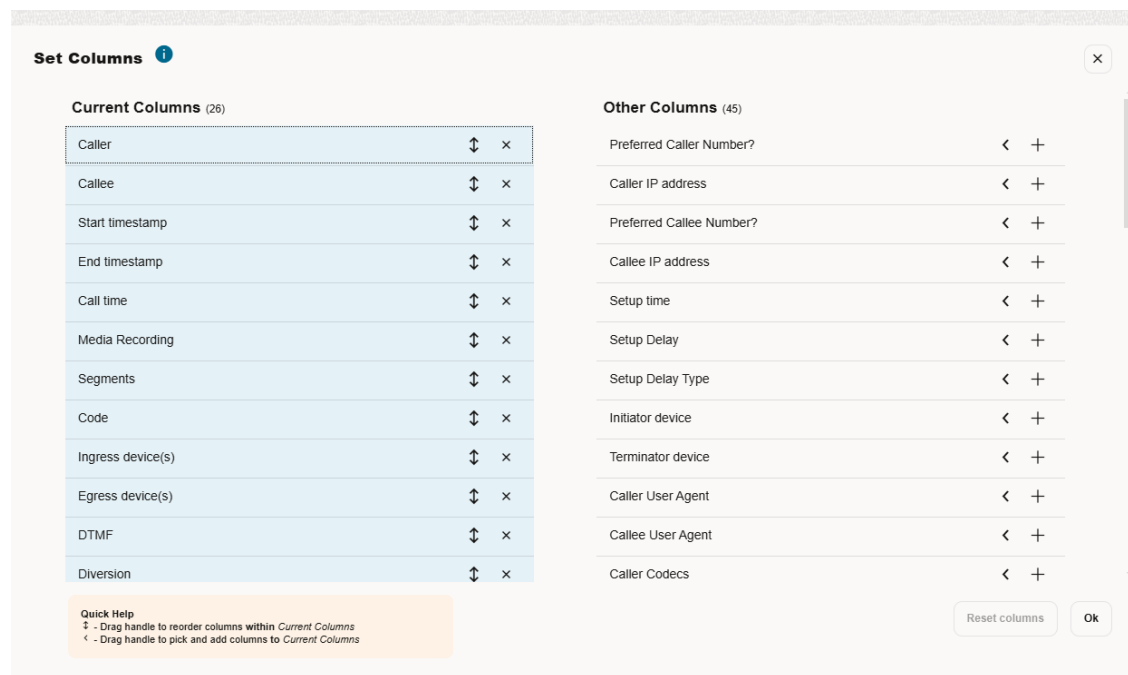


Table 3-2 Set Columns Icons

Icons	Description
Figure 3-14 Drag to Reorder 	Drag the tool next to the column name to reorder the column's appearance in the Table view.

Table 3-2 (Cont.) Set Columns Icons

Icons	Description
Figure 3-15 Remove a Column 	Click the tool next to the column to remove the column from the Table view. You can remove all columns, but for one, to save the changes made.
Figure 3-16 Drag to Add Column 	In the Other Columns section, use the Drag tool to add the column to be displayed in the Table view, and also use this tool to reorder the position of the column in the display.
Figure 3-17 Append Column 	In the Other Columns section, use the Add tool to append the column to be displayed in the Table view. You can add all columns to the current view.
Reset Columns	Deletes any customization made to the columns displayed, and reverts to the Default display of columns.

You can see the Set Columns controls in the following pages:

- Registrations
- Subscriptions
- Dashboard panels for Calls, Registrations, and Subscriptions
- Devices
- User Tracking
- IP Tracking

Pagination

Note the paging toolbar at the bottom of tables. The presence of this toolbar means that the table offers page-wise access to its data:

Figure 3-18 Paging Toolbar

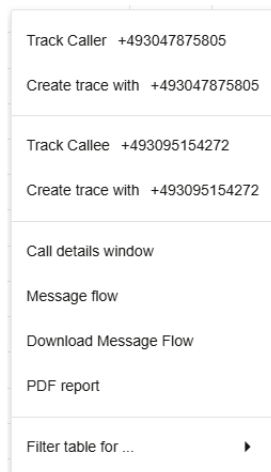


- Click **Now** to show current data.
- Click **Auto Refresh** to toggle auto refresh to On or Off. The Auto Refresh button displays animation to indicate that the data is being refreshed.
- Click the **Calendar** control to show data for a specific date.
- Click the **Next** or **Previous** button to go to the next or previous page.
- Click **Stop** to stop the loading data into the table.

Quick User Inspection

Tables such as Recent calls, Registrations, and the user table in User Devices have context menu entries to quickly trace or track a user. You can right-click on a table row to track or trace the user (in the Recent calls table, you can quickly inspect both the caller and the callee). For more information, see the Recent Calls, Registrations, and User Devices sections.

Figure 3-19 Context Menu for Calls

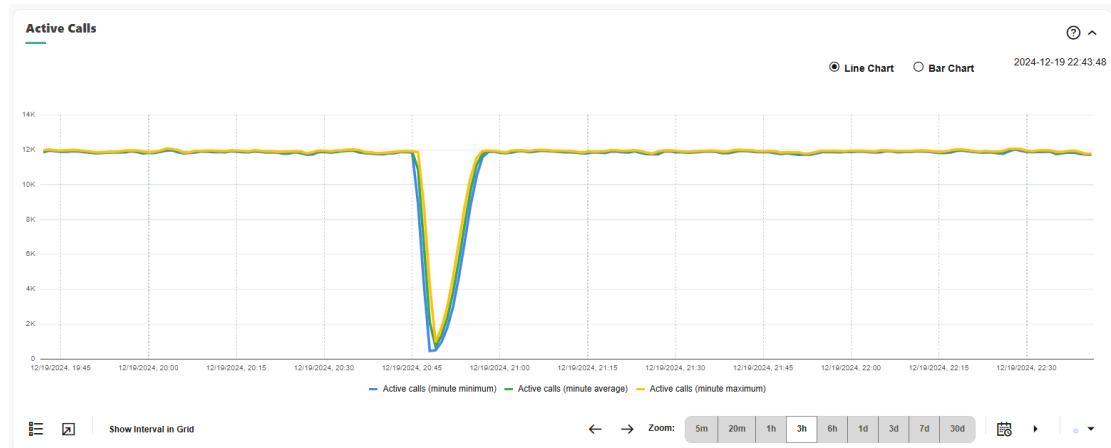


Charts

You may encounter metric charts that display values of a numeric property over a certain time span. Metric charts provide two important features:

- Adjusting the temporal resolution.
- Panning of the visible portion along the time line.

Figure 3-20 Charts



Details of the chart are displayed in a pop-up box on hovering the mouse over the chart. If more than 1 metric is selected to be displayed in the chart, they are color coded to indicate the different metrics

Adjusting the temporal resolution can be achieved using the Zoom buttons in the bottom-right corner of the chart. The buttons correspond to resolutions of five minutes to thirty days.

Operations Monitor's time-lined charts can be updated by clicking the Refresh button. This button also offers Automatic Refresh functionality from the button's drop-down list. For more information, see the Refresh Button section.

Controls Used in Panning a Chart

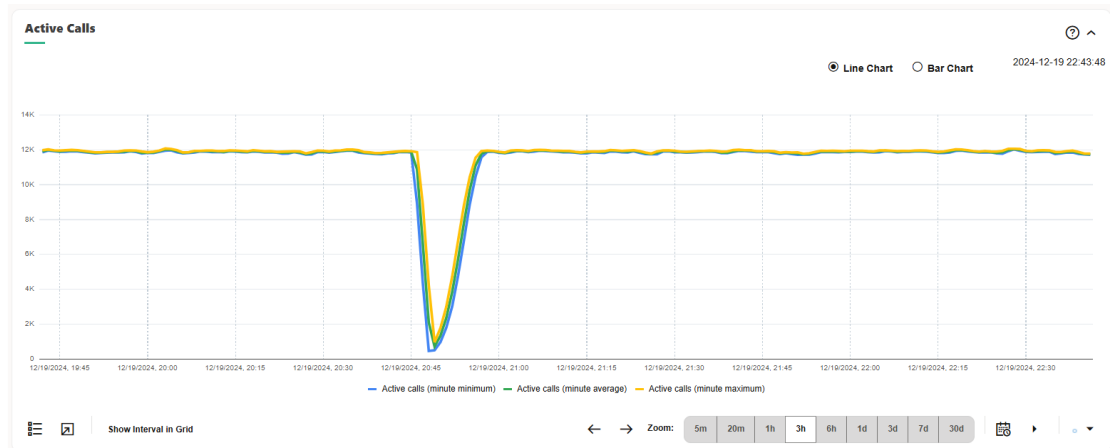
To pan the chart: click **Right scroll** or **Left scroll** buttons and drag. When you click Right scroll, the visible area is shifted further left (further in the past) on the time line. When you drag it to the left, the visible area is shifted further right (nearer to the present) on the time line.

Click **Show Interval in Grid** to filter the table to the time interval of the chart

Note

Panning stops the automatic refresh of a chart. Automatic refresh is re-enabled after clicking on the **Now** button at the bottom of the chart.

Figure 3-21 Charts



Working with Message Flows

A message flow is a diagram of a call event or a registration event. The message flow displays the network devices involved in the call event or registration event and the protocol messages that have been exchanged between the network devices. For more information on how to configure the hosts on which the network devices run, see the Platform Devices section.

Displaying a Message Flow

To display a message flow of a call event or a registration event:

1. In the navigation pane under **Operations**, do one of the following:

- To display a message flow for a call event:

- a. Click **Calls**.

The **Calls** page opens in the main display.

- b. In the **Recent calls** table, right-click the row for which to display the call event's message flow and select **Message flow** or click the **Show Message Flow for selected calls** button.

The **Message Flow for Call: caller and callee** window appears.

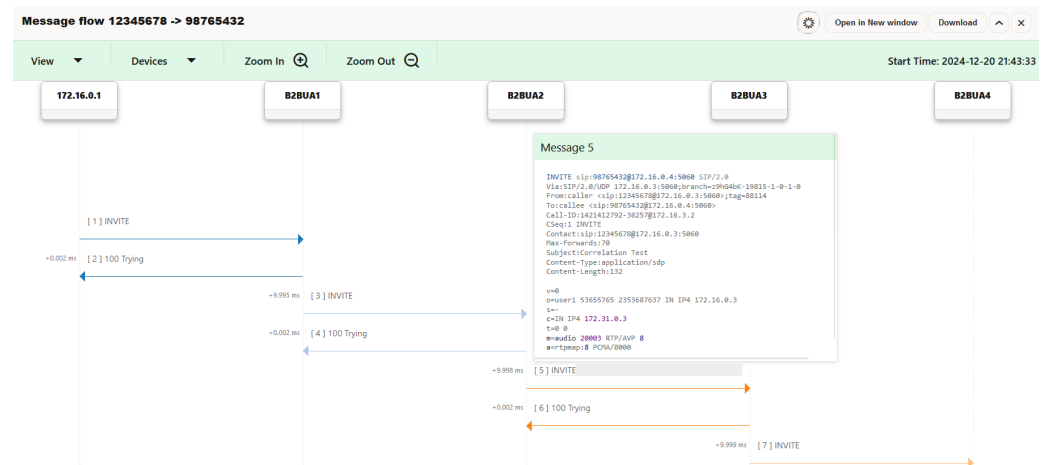
where *caller* is the number that initiated the call and *callee* is the call number that received the call.

On the right-side corner of the window, the call **Start date** along with the call **Start Time** is displayed in the message flow header.

Note

Message flows for a call event can also be displayed by right-clicking on the call row and selecting Message flow in the Calls going through this device tab on the **Devices** page.

Figure 3-22 Message Flow window



- To display a message flow for a registration event:
 - a. Click **Registrations**.
The **Registrations** page opens in the main display.
 - b. In the **Registrations** table, select a registration event for which to display a registration message flow.
 - c. From the **Registrations** table tool bar, click the **Message flow** button.
The **Registration registration_number** window appears.
where *registration_number* is the number of the registration event.
- 2. Press the **ESC** key, which closes the message flow window.

Arranging Message Flows

In order to compare the network devices and protocol messages contained in multiple call events or registration events, you can open multiple message flows to view side-by-side in the same browser window, or you can open multiple message flows to view side-by-side in multiple browser windows.

To adjust the message flow window to fit in your browser screen, view a message flow in a new browser window, resize the message flow window, or view more of the message flow, do one or more of the following:

- To adjust the width of the sequence diagram within the message flow window. In the message flow window's toolbar, click the **Zoom in** or **Zoom out** icons accordingly.
- To view more of the message flow without resizing the message flow's window. Inside the message flow window, drag the message flow, or use the message flow window's scroll bar.
- To view the message flow in another browser window. In the message flow window's toolbar, click the **Open in a new window** button.
- To refresh the message flow window. In the message flow window's toolbar, click the **Refresh** button. For more information, see the Refresh Button section.
- To select the parameters that must appear in the Device map, click the **View** drop-down list and select the parameters.

- To select the devices that must appear in the Device map, click the **Devices** drop-down list and select the devices.

Customizing the Display of Contents within Message Flows

The contents displayed in the sequence diagram, protocol messages, and network devices within the message flow are customizable.

To customize the display of contents within message flows:

1. Verify that the message flow is displayed.
2. In the message flow window's toolbar, select the View menu.
3. From the View menu, select or de-select one or more of the following check boxes:
4. Enter the text of the second step here.
 - **Pin Devices**
When enabled, the devices are always visible at the top of the scrolling area.
 - **Use Device Order**
 - **Unwind messaging**
By default, each network device appears only once and a transaction arrow is drawn for each message that passes between the hosts. When several messages are exchanged between two particular network devices, it becomes difficult to distinguish the call legs. When enabled, each call leg is drawn separately, which results in a wider diagram. Hosts that appear multiple times contain a number suffix, which is the number of times the host appears.
 - **Resolve IP addresses**
When enabled, Operations Monitor creates a reverse DNS lookup on the IP addresses of the network devices.
 - **Duplicates**
For retransmissions, only one SIP message appears. Enable this option to display all duplicate messages.
 - **URIs**
Request-URI — the specific endpoint the SIP INVITE request is being sent to.
 - **Protocol**
When enabled, the message flow displays the transport protocol (TCP or UDP).
 - **IPs**
When enabled, the message flow displays the IP addresses for the source and destination of the message.
 - **MAC addresses**
When enabled, this option displays the MAC addresses for the source and destination of the message. In a scenario where one server is realized by several machines, this can be used to determine which machine was used to process the request.
 - **VLAN**
Displays the Virtual Local Area Network (VLAN) ID associated. A value of 0 indicates that no specific VLAN tagging is applied.
 - **MACs**
Displays the source and destination Media Access Control (MAC) addresses
 - **OPC/DPC**

When enabled, this option displays the originating point code (OPC) and the destination point code (DPC) for the source and destination of the message.

- **Codecs**

When enabled, the message flow displays the media codecs of the caller and the callee. If the codecs are the same for both the caller and the callee after the INVITE transaction is completed, the codecs are grouped.

- **Absolute Time**

By default, the information below a transaction arrow displays the time that has passed after the first message was seen. When enabled, the date and time are displayed for each transaction arrow.

- **Media**

When enabled, protocol messages for media transport, such as RTP, are displayed in addition to the signal.

Note

For some protocols, the raw message is not available.

- **DTMF Events**

When enabled, protocol messages for RTP events of the type DTMF are visible. The DTMF event will show the name and code of the tone. For tones 0-9 the name and the code are the same.

DTMF Event '2' (2)

DTMF Event '#' (11)

Requires the View DTMF tones permission to be visible. See User Permissions.

- **Context IDs**

Unique identifier used to associate related messages within the same call or signaling session.

- **Termination IDs**

Unique identifier representing the media or signaling endpoint (for example, a port or channel) involved in the call or session.

- **Package Names**

Name of the protocol or feature package that defines the commands or functions used in the message.

- **SIP URIs**

When enabled, the transaction arrows display the recipient's URI.

- **Hide SIP Methods**

This submenu allows you to hide certain types of SIP messages based on their method. For example, enabling OPTIONS will remove all SIP messages from the diagram that have the method OPTIONS.

- **MEGACO**

This submenu allows you to hide selected MEGACO message properties.

5. Press the **ESC** key, which closes the message flow window.

Customizing the Visibility and Position of Network Devices within Message Flows

By default, all networking devices are displayed in the message flow in the order of the call event transaction or the registration event transaction. The visibility and position of a network device is customizable in a message flow.

To customize the visibility and position of network devices within message flows:

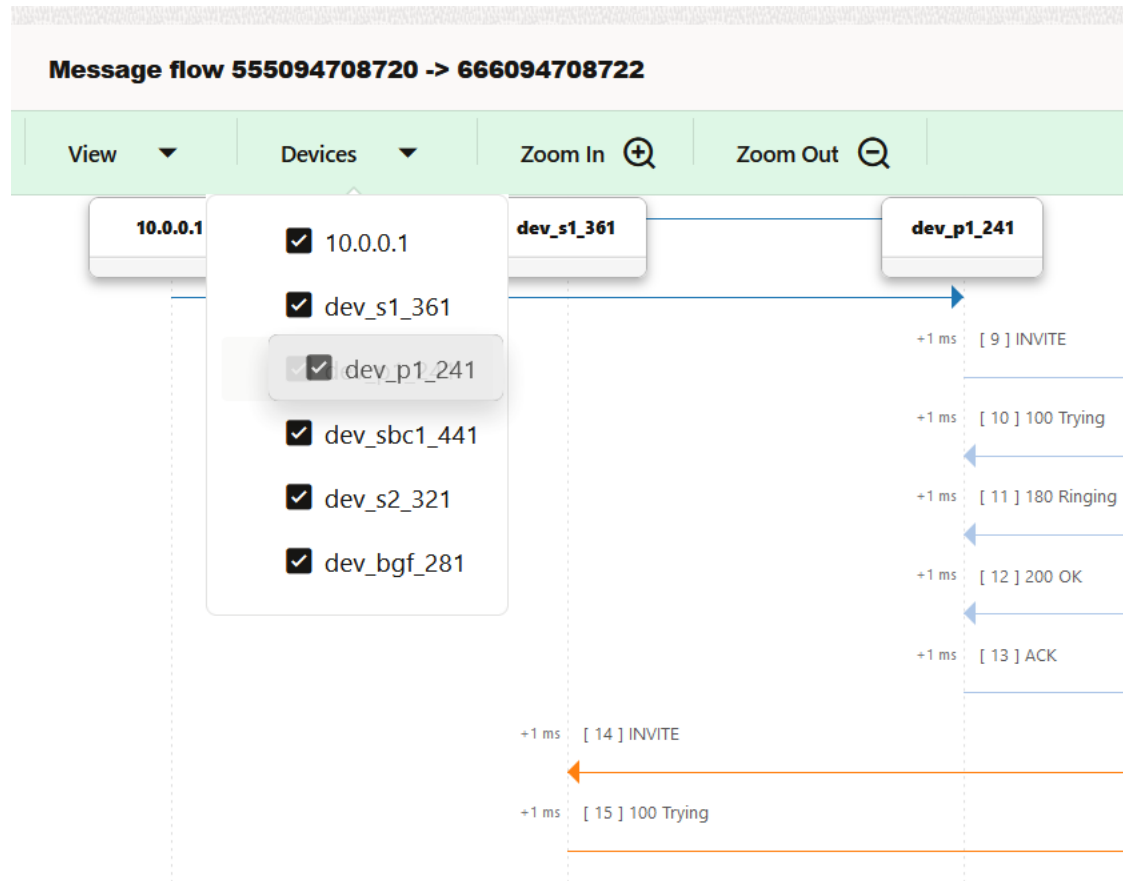
1. Verify that the message flow is displayed.
2. In the message flow window's toolbar, select the **Devices** menu.
3. Do one or both of the following:
 - To hide a network device, deselect the check box of the network device you want to hide. Alternatively, select the check box of the network device you want to display.
 - To reposition a device in the sequence diagram, select the check box row of the network device you want repositioned and drag and drop the device to the position you require. Corresponding to the new position of the device, the message flow diagram is displayed. See the following figure.

Note

Drag-and-drop functionality allows you to easily reorder devices in a message flow, providing a dynamic and user-friendly interface. This feature helps you to visualize device connections and interactions. The new order persists after saving, enabling users to adjust operations, prioritize actions, and align configurations effortlessly.

4. Press the ESC key, which closes the message flow window.

Figure 3-23 Devices in the Message Flow Window



Viewing Individual Protocol Messages

Protocol messages of the sniffed packet can be viewed and saved. For more information on saving a protocol message, see "Saving a Message Flow as an HTML File".

Each protocol message is numbered in brackets in the order of the call event transaction or the registration event transaction between the network devices.

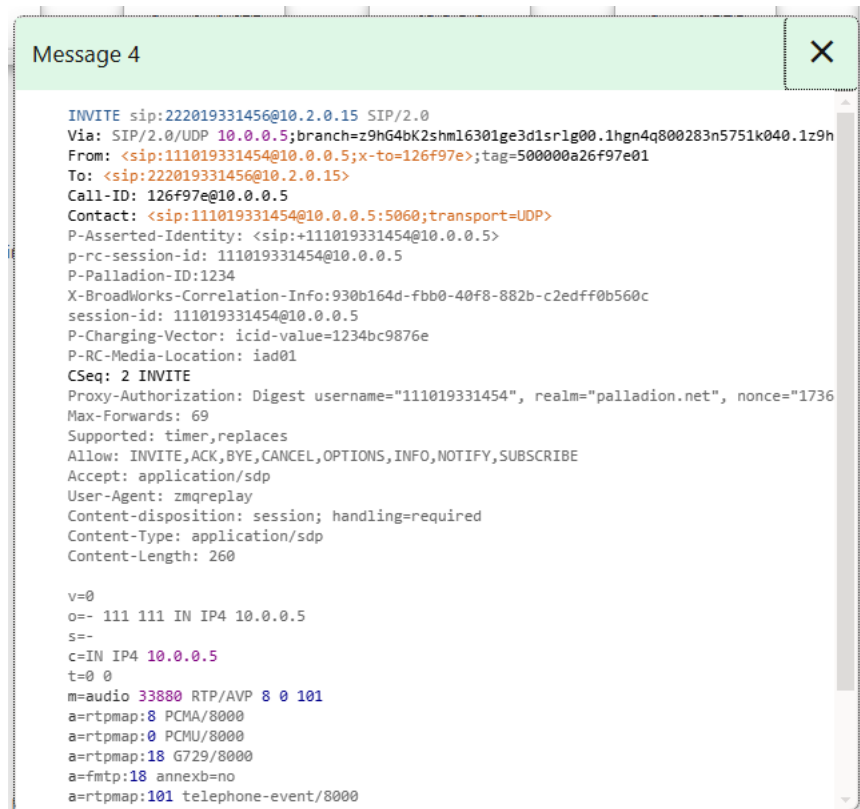
To view individual protocol messages:

1. Verify that the message flow is displayed.
2. In the message flow, click the message type you wish to view, which appears above the message transaction arrow.

The **Message transaction_number** window appears, where *transaction_number* is the number associated with the order of the transaction between the network devices.

3. (Optional) Resize, or move the protocol message by dragging the title bar of the protocol message's window to the required position within the message flow.
4. When you have finished viewing the protocol message, click the **Close** icon in the protocol message window's title bar.
5. Press the **ESC** key, which closes the message flow window.

Figure 3-24 Individual Protocol Message Window



Note

The maximum number of messages for a flow is limited. You can change the limit value in System Settings. For more information, see "System Settings".

Viewing Call Event ISUP Protocol Messages

When a call event contains ISDN User Part (ISUP) binary content, you can view the ISUP binary content as human readable text.

To view call event ISUP protocol messages:

1. Verify that the message flow is displayed.
2. In the message flow, click the message type identified by [1], which appears above the message transaction arrow.

The **Message transaction_number** window appears.

3. Scroll down the protocol message until you see the **Content-Type** header. Do one of the following:

- If the **Content-Type** header's value contains either, **multipart/mixed** and one of the multiple parts is **application/ISUP**, or **application/ISUP**, go to step 4.
For example:

Content-Type:application/ISUP;boundary=A6B35A2329D0F2312C9F4692

- If the **Content-Type** header's value does not contain either, **multipart/mixed** and one of the multiple parts is **application/ISUP**, or **application/ISUP**, close the protocol message and click the next message.
4. Scroll down the protocol message until you see the **decode ISUP body** link.
 5. Click the **decode ISUP body** link.

The ISUP binary content is decoded into human readable text and an **ISUP message contained in Message *transaction_number*** window appears.
 6. When you have finished viewing the ISUP message, click the **Close** icon in the ISUP protocol message window's title bar.
 7. When you have finished viewing the protocol messages, click the **Close** icon in the protocol message window's title bar.
 8. Press the **ESC** key, which closes the message flow window.

Obfuscation of Call Data During Export

In compliance with the need for privacy of confidential information, the **Obfuscate Details in Message-flow Exports** feature allows you to enable obfuscation of sensitive call data such as IP addresses, Phone numbers, MAC addresses and device names when the Call Data ladder diagrams are exported as PDF, HTML, or SVG formats.

The setting **Obfuscate Details in Message-flow Exports** under **Settings** → **System Management** → **System Settings** is disabled by default can be optionally enabled.

When enabled, obfuscation applies to exported ladder diagrams (PDF, HTML, SVG formats) and the message structure sections of exported data. There is no change in the GUI for the message flow diagram. The message flow diagram in the GUI will show full, unmasked information - with the exception of SVG format. SVG data will be masked in the GUI also if the setting is enabled.

As an additional layer of data masking, you can configure the system setting **Obfuscate Message Headers** to customize the masking of SIP headers. This ensures improved data protection and user control over shared information. For more information, see [Obfuscation of Message Headers](#).

Table 3-3 Masked Information

Field	Message Flow Format	Description	Examples
IP Address (IPv4, IPv6)	- HTML - PDF - SVG	- IP addresses are obfuscated using randomized letters and digits. - Only the final octet will be visible. The preceding octets are replaced with random alphanumeric characters. - Each masked IP is unique across the ladder diagram. This preserves traceability without exposing full IP details.	- IPv4: 100.1.53.234 → AGB.Z.1B.234 - IPv6: :3fff::172:16:46:29 -> Azzz:aaaa:aaaa:aaa a:9Sf:9s:is:29
Phone Number	- HTML - PDF - SVG	Numbers are masked using a placeholder character, the asterisk (*)	- Phone Number: +493074214428 -> +493****4428 1399557349-933 -> 139***7391-933
Device Names	- HTML - PDF - SVG	Device names are completely masked using the asterisk (*), except for the first and last character.	Device: BUBUA1 → B****1
MAC Address	- HTML - PDF - SVG	- MAC addresses are masked using random letters and digits for all segments except the last segment. - Each masked MAC Address is unique across the ladder diagram. This preserves traceability without exposing the full MAC Address details.	Mac Address aa:bb:cc:dd:00:06 → ZB:N4:R5:JW:Wl:06

Obfuscation of Message Headers

The **Obfuscate Message Headers** feature allows users to specify custom headers that must be masked. The selected header is completely masked in all future exports of the call ladder diagram message headers.

1. Click **Settings > Privacy Settings > Obfuscate Details in Message-flow Exports**.

2. The next page displays all previously added Headers. If you have not added any header earlier, then this page is blank.

Note

You cannot add the same Header multiple times, as duplicate Header entries are not allowed.

3. To add a new Header, key in the Header name. You can add and manage up to 20 custom headers. Constraints ensure that the Header entered is valid and consistent:
 - Duplicate entries are not allowed
 - If an entry is already in the list, notification error message is displayed.
 - Headers containing spaces, commas, colons or equal signs are invalid
4. Click **Save** to save the entry.

Saving a Message Flow as an HTML File

You can save a message flow as an HTML file on your computer to view at another time or share with others. This is important when diagnosing issues.

To save a message flow as an HTML file:

1. Verify that the message flow is displayed.
2. In the message flow window's toolbar, click the **Download** button.
The Save As dialog box appears.
3. Browse to the directory in which you want to save the HTML file.
4. (Optional) In the **File name** text box, enter a file name for the HTML file.
By default, HTML files are named **message-flow.html**.
5. Click **Save**.
6. Press the **ESC** key, which closes the message flow window.

Saving a Call Event Message Flow as a PDF File

You can save a call event message flow as a PDF file.

To save a call event message flow as a PDF file:

1. In the navigation pane under **Operations**, click **Calls**.
The **Calls** page opens in the main display.
2. In the **Recent calls** table, right-click the row for which to create a call event PDF report file and select **PDF report**. The Create Report window appears.

Figure 3-25 Create Report

Create Report

Report Contents

- ☒ Call Information
- ☒ Link Quality Information
- ☒ Voice Quality Information
- ☒ Detailed RTCP Information
- ☒ DTMF Information
- ☐ UCaaS CCaaS information
- ☒ Messages
- ☒ Include Company Logo
- ☒ Include Graph
- ☐ Combine identical
- ☐ Use Device Order
- ☐ Transport protocol
- ☐ IP addresses
- ☐ Codecs
- ☐ Time spans
- ☐ Show Media
- ☐ Unwind messaging
- ☐ SIP URIs
- ☐ VLAN
- ☐ MAC addresses
- ☐ Absolute times
- ☐ Resolve IP addresses
- ☐ Show DTMF Information

Additional Info

Report Comment (optional):

Filename (optional):

CallsPDF

Create Reset Cancel

By default, few of the **Report Content** options are enabled as shown in the screenshot options are selected.

3. In the **Report Content** section, deselect the options you do not require in your report. Do not deselect the **Messages** option.
4. (Optional) In the **Additional Info** section's **Report Comment (optional)** text box, enter information about the report.
5. (Optional) In the **Additional Info** section's, **Filename (optional)** text box, enter a file name for the report.

By default, PDF files are named **CallReport- YMDHMS-callid .pdf**

where

- *YMDHMS* is the syntax for year, month, day, hour, minutes, and seconds that the file was generated.
 - *callid* is the call event's identifier.
6. Click the **Create** button.
The Save As dialog box appears.
 7. Browse to the directory in which you want to save the call event PDF file and click **Save**.
 8. Click the **Cancel** button, which closes the **Create Report** window.

Note

Because the decoded binary ISUP content can be lengthy, only two levels of information are displayed in the PDF report.

BICC Support

You can distinguish between ISUP and BICC messages by the protocol name looking at the Ladder Diagram section.

Currently, Operations Monitor supports BICC calls with only SCTP transport layer protocol. Ensure that you enable the system setting **SCTP quick push** to see BICC calls on the Calls page. To enable the capture of BICC messages, enable SIP/ISUP from the Signaling Protocols page in PSA.

Note

- The platform device type must be STP to correlate BICC and ISUP messages.
- The platform device type must be SGW to correlate BICC and SIP messages.

Operations Monitor supports correlation among BICC, SIP, and ISUP messages. Apps such as Call count, Calls containing keywords, response code search apply to BICC calls in the same way as they apply to ISUP calls. Export of BICC calls is supported.

Limitations: ISUP and BICC protocols have very similar set of messages and hence, in the GUI, there is no way to differentiate ISUP and BICC signaling messages in a correlated call. A distinction between BICC and ISUP calls can be made by looking at the Message Flow information. Here messages are marked as 'ISDN User Part' and 'Bearer Independent Call Control'. There is also a difference in the size of the CIC for a BICC and ISUP message.

System Setting to Enable BICC Support

Support for BICC Protocol is the system setting that allows you to enable or disable the support of BICC signaling messages by Operations Monitor.

You can access this system setting **admin > settings > System Management > System Settings**. This system setting is disabled by default..

Note

The existing system settings which are applicable to ISUP protocol messages are applicable for the BICC protocol messages also. The system settings associated with ISUP messages have similar impact on ISUP and BICC messages.

Viewing BICC Calls in the Recent Calls Page

In the Calls Page You can filter BICC calls based on Originating Point Code (OPC) and Destination Point Code (DPC).

BICC messages along with OPC/DPC values are displayed in **Recent Calls** table. As the payload section of ISUP and BICC frames are very similar and these messages cannot be differentiated by protocol/message name in the GUI, as of now.

Calls page - The format of OPC/DPC supported is either ITUT(3-8-3) or ANSI(8-8-8) format. Currently, Operations Monitor does not support filtering with decimal value equivalent of OPC/DPC configured in ITUT/ANSI format, in the Device settings.

Figure 3-26 Viewing BICC calls in the Recent Calls Page

Recent Calls

Details ...

Type to filter eg- callee=575,caller=115

(None)

☐	Caller	Callee	Start timestamp	End timestamp	Call time	State	OPC	DPC
☐	867526219876	886989946320F	2024/12/23 11:48:30			Setup	4-182-5	4-173-2

Viewing BICC Messages in the Call Info Window

A list of BICC messages along with it's details are shown completely in the **Messages** tab of the Call Info window.

In the ladder diagram, detail of each BICC message is shown.

BICC Advanced Metrics

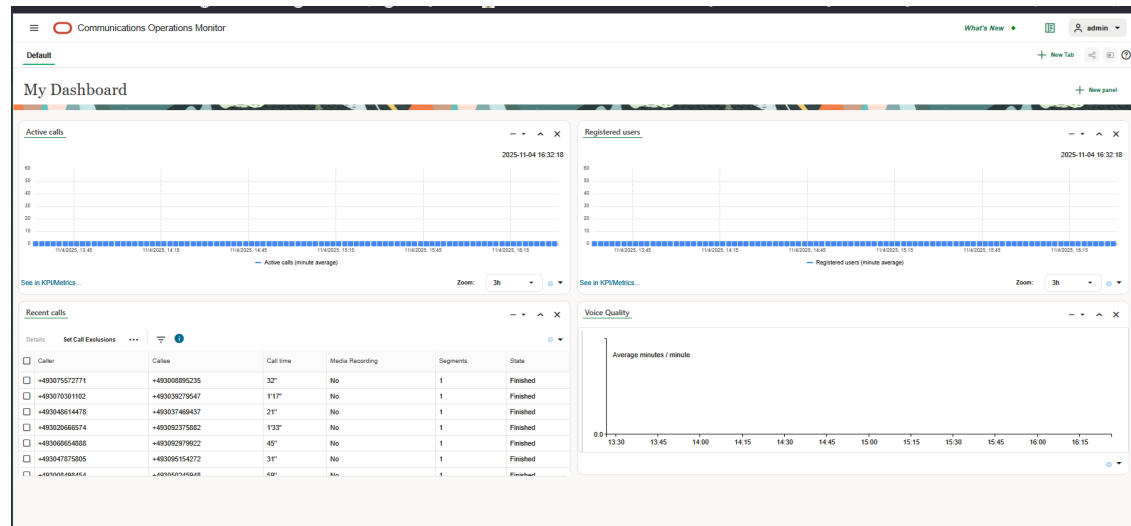
The following is the list of KPIs that are updated when BICC messages are received.

In 'Advanced metrics', the following list of KPIs can be defined with certain range of Q 850 cause codes.

- Number of ISUP Q 850 cause codes
- Number of calls with Q 850 cause codes
- Number of ISUP calls with Q 850 cause codes
- Number of ingress legs with Q 850 cause code
- Number of ISUP ingress legs with a Q 850 cause code

Dashboard

The Dashboard is Operations Monitor's flexible entry page. It allows you to view the information at a glance that is most important to you. Reduced panels are defined for many features of Operations Monitor, and can be displayed on the Dashboard.

Figure 3-27 Dashboard

Types of panels that may appear on your dashboard are:

1. Display a metric/KPI
2. Display recent calls
3. Display registrations
4. Display subscriptions
5. Display alerts
6. Display voice quality data
7. Display user devices chart
8. Display calls by a particular user
9. Display calls passing a platform device
10. Display calls terminated by a platform device
11. Display calls created by a platform device
12. Display registrations of a particular user
13. Display registrations at a particular device
14. Display subscriptions of a particular user
15. Display subscriptions at a particular device
16. Display a device metric/KPI
17. Display voice quality at a particular device
18. Display Top 10 Devices
19. Display Top 5 Negotiated Codecs
20. Display Negotiated Codecs Distribution

Note

Points to Note:

- For the panels, **Display Top 5 Negotiated Codecs** and **Display Negotiated Codecs Distribution**, data is populated only if Platform-wide Negotiated Codec KPIs are created by the respective users.
- These panels come in variants. For example, you can display a **Recent calls** table only for call events passing through a certain platform device.

Understanding the Dashboard Utilities

Starting with Session Monitor Release 6.1, the Dashboard can be organized in the form of multiple Tabs .

The advantages of the new tab-based Dashboard are:

- **Improved Organization:** Tabs help categorize data, making it easier to manage and access different sections.
- **Faster Navigation:** You can switch between tabs quickly, enabling seamless access to different views.
- **Enhanced Focus:** By separating content into tabs, you can focus on one section at a time
- **Space Efficiency:** Tabs maximize screen real estate by reducing clutter.
- **User Experience:** A well-organized tab structure enhances usability
- **Customization:** Tabs allow for easy customization and grouping of related information

What Happens to the Dashboard Panels I had Created Earlier?

A fresh installation or an upgrade to Session Monitor Release 6.1 displays the Default tab. The existing panels are added to the **Default** tab, and the Dashboard functionality remains the same in the **Default** tab. The **Default** tab is always a part of the **Dashboard** page. You cannot delete it, or rename it.

How do I start Creating Tabs on My Dashboard?

To start creating new Tabs, click **+ New Tab** to add a new tab. You can add a maximum of 10 Tabs, including the Default tab.

Configuring Your Default Dashboard Tab

Starting with Session Monitor Release 6.1, the Dashboard can be organized in the form of multiple Tabs.

All existing panels are added to the **Default** tab, and the Dashboard functionality remains the same in the **Default** tab. The **Default** tab is always a part of the **Dashboard** page. You cannot delete it, or rename it.

Each Operations Monitor user can define their own **Default** tab layout. The **Default** tab contains four panels:

- Registrations Counter
- Active Calls Counter

- Recent Calls table
- User Devices Chart

Panels can be added, removed, and rearranged.

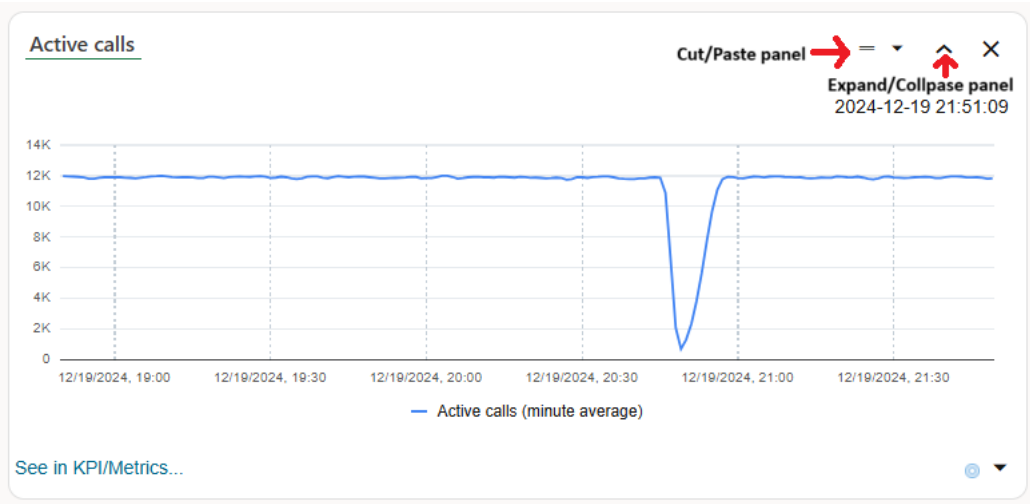
Panels

When you click an element in the navigation pane, a panel appears in the center of the browser window. This panel is a user interface element that displays data.

Many panels can be added to your dashboard for at-a-glance viewing. For more information, see the Dashboard section.

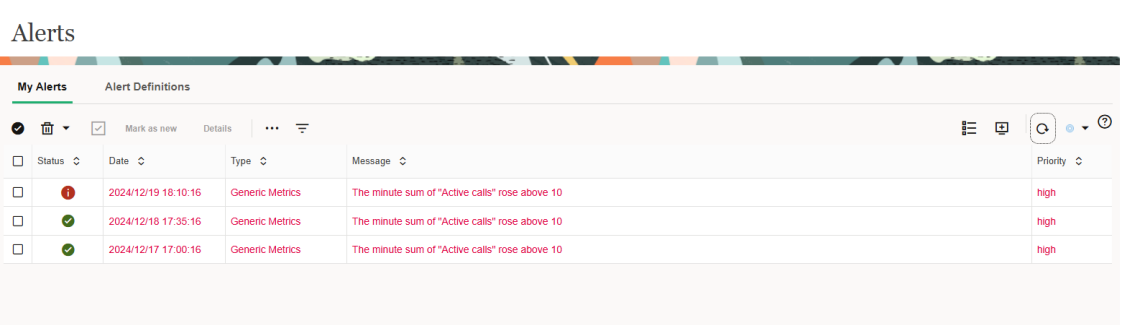
To collapse panels and display titles only, you can click the angle-bracket in the upper-right hand corner.

Figure 3-28 Panels



Another common user interface element is the tab panel.

Figure 3-29 Tabs Panel



Adding a Dashboard Panel to the Default Tab

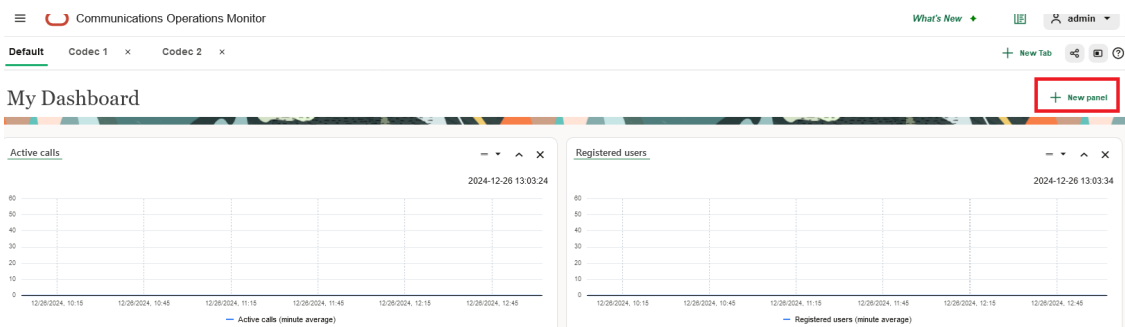
Dashboard panels are individual components or sections within a dashboard that display specific types of data, metrics, or visualizations.

You can add Dashboard panels in the **Default** Tab or from the Operations Monitor pages.

To add a panel directly from the **Default** Tab, click **+ New Panel** button located on the right-side corner of the Dashboard page.

A pop-up window appears that provides a list of pre-existing dashboard panels. Select a panel and click **Finish** to add it to the **Default** Tab.

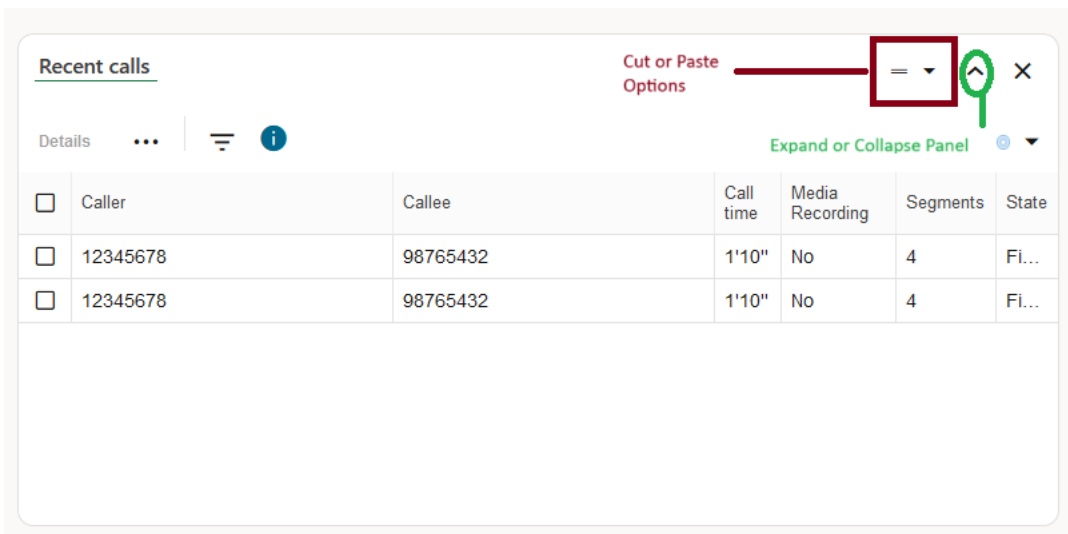
Figure 3-30 Adding a Dashboard Panel to the Default Tab



Many panels can be added to your Default dashboard for at-a-glance viewing.

To collapse panels and display titles only, you can click the angle-bracket in the upper-right hand corner.

Figure 3-31 Panels



To add a dashboard panel from another window in the user interface, click the **Show in Dashboard** icon (shown in following figure). This button is located throughout the Operations

Monitor web user interface. When you click the **Show in Dashboard** icon, a new panel is added in the Default tab of the Dashboard.

Figure 3-32 Show in Dashboard



To display a panel from the **Default** tab in any of your custom tabs, import the desired tab from the Default tab to your custom tab. For more information, see [Adding a Dashboard Tab](#)

Closing, Cutting and Pasting a Dashboard Panel from the Default Tab

- To remove/close a dashboard panel from the **Default** tab:
 1. Click the **x** button in the upper-right corner of the dashboard panel.
 2. A confirmation box appears.
 3. Click **Yes** to continue or **No** to cancel.
- To Cut a Dashboard Panel from the Default tab:
 1. In the Dashboard panel, from the **Cut or Paste Options** drop-down list, click **Cut**.
 2. To paste the dashboard panel in a new location, click the **Cut or Paste Options** on a panel above which you want to paste.
 3. Click **Paste above**.

Note

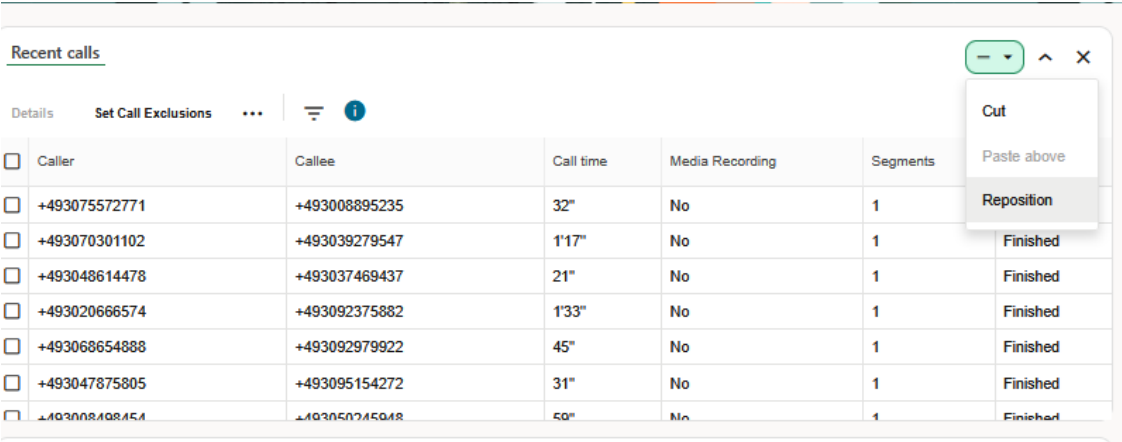
You can also drag and drop to re-order the Tab positions.

Rearranging Dashboard Panels

You can drag and drop dashboard panels to rearrange them. Drag a dashboard panel by its title bar to relocate it on the page.

After adding Panel to dashboard, click on the **Reposition** option. This highlights the panel to be repositioned. Now, click on any other panel. The two panels will swap their positions.

Figure 3-33 Repositioning a Dashboard Panel



Working with Dashboard Tabs

Dashboard tabs are navigation elements within the Operations Monitor dashboard that allows you to switch between different sections or views without leaving the main interface. Tabs enable you to organize data and visualizations into distinct categories or topics, enhancing the dashboard's usability and efficiency

Customizable Dashboard Templates

The ability to add tabs allows you to choose and save customized templates. You can choose any of the following templates when you create a new tab on the Dashboard:

Table 3-4 Available Templates

Template	Description
3 Large cards ¹	1 large panel with 2 adjacent small panels
2 Large cards	2 large panels adjacent to each other
4 cards	4 normal sized panels adjacent to each other
3 cards	3 normal sized panels adjacent to each other
2 cards	2 normal sized panels adjacent to each other
1 card	1 normal sized panel in the entire row
1 Large card	1 Large sized panel in the entire row

¹ Large card indicates that the height is double compared to the normal card

Adding a Dashboard Tab

This section provides information on how to add a Dashboard tab.

The **Default** tab is always a part of the Dashboard page. You cannot delete it, or rename the **Default** tab.

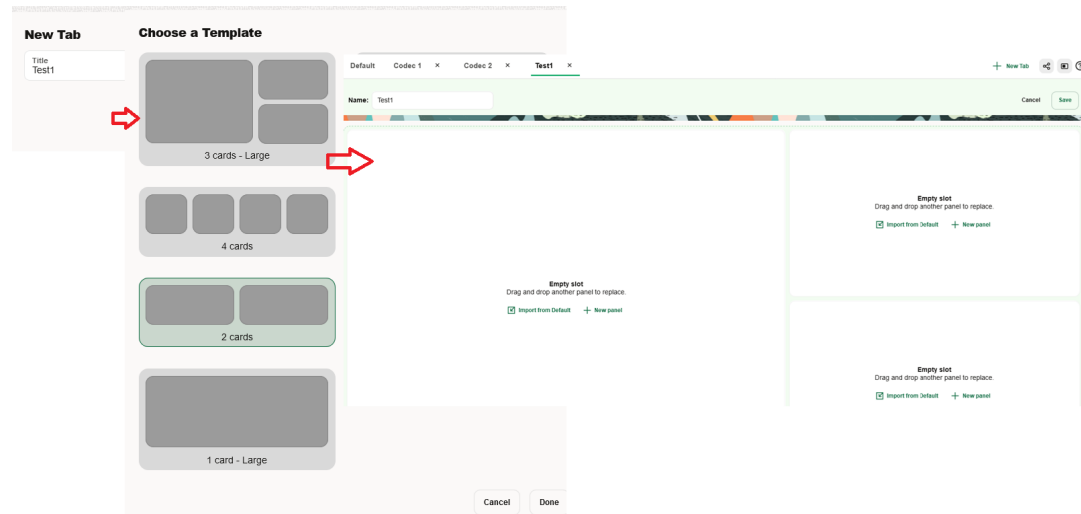
You cannot name any new tab as Default. You can add a maximum of 10 tabs including the **Default** tab. To add a new tab to the Dashboard:

1. In the **Dashboard**, click **+ New Tab**.

2. Provide a name for the Dashboard.
3. In the **Choose a Template** dialog box, select a template that best suits your requirements, and click **Done**. For more information on templates, see [Working with Dashboard Tabs](#).

You can consider a template layout to transform into a single row containing multiple panels in the new tab.

Figure 3-34 Adding a New Tab to the Dashboard

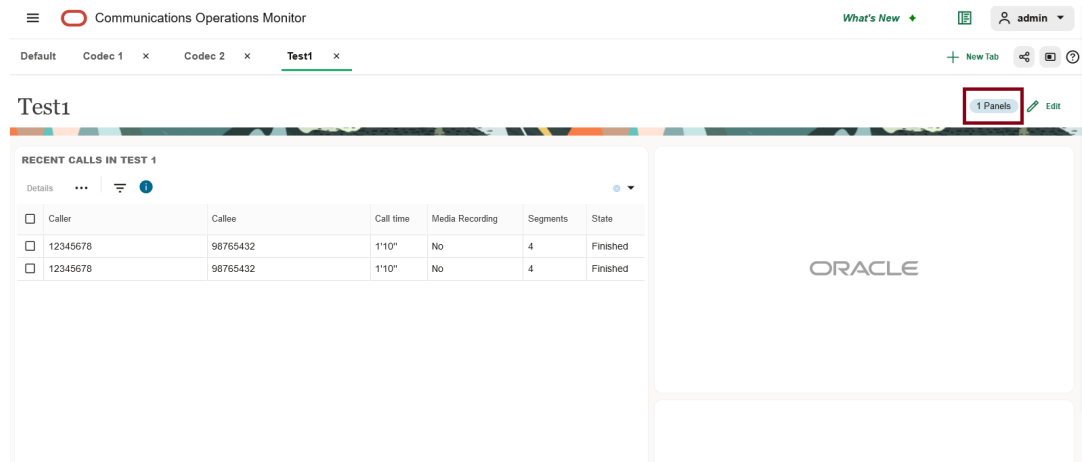


A new tab based on the selected template is created.

4. From this point, you can add panels to the new tab using any of the following methods:
 - Click **Import from Default** to import a panel currently being displayed in the Default tab.
 - Click **+ Add Panel** to add a panel from the list of pre-existing panels.

It is not mandatory to add panels to all slots in a tab. If you do not add a panel, the placeholder text *Oracle* is shown.

5. Click **Add Group Below** to extend the tab layout. For example if you initially chose 2 large cards as the template while adding a new tab Test1, **Add Group Below**, prompts your to choose a template again. This time you can choose 3 Large cards which gets added as a new row to the same tab Test1. Thereby extending the tab layout.
 - To delete a group, click **Delete group**.
6. Click **Save**.

Figure 3-35 A new tab with a panel added

Each tab also displays the number of panels that have been added.

Note

Clicking **X** on the tab header Deletes the tab and does not close it.

Tabs can be dragged and dropped to changed the position and reorder. The order persists across sessions. The tab that is placed in the first position is displayed as the first tab every time the user navigates to the dashboard.

Editing a Dashboard Tab

Each tab has an 'Edit mode'. The edit mode allows you to add new group, configure the group layout, and select additional panels to add within the tab. In the Edit mode you can also delete groups and the newer groups below the current group.

1. For a given tab (not the **Default** tab), click **Edit** in the right-side corner of the Dashboard page.
2. Click any of the following options:
 - Click **Add group below** to add a new group.
 - Click **Import from Default** to import a tab currently being displayed in the Default tab.
 - Click **+ Add Panel** to add a panel from the list of pre-existing panels.
3. Optionally you can also:
 - click the Delete button to delete a panel.
 - Drag and drop panels to change the layout.
4. Click **Save**.

Auto Switch

Session Monitor Release 6.0 provides an innovative feature called - Auto Switch, designed to enhance user experience by automatically navigating between Dashboard tabs. The Auto

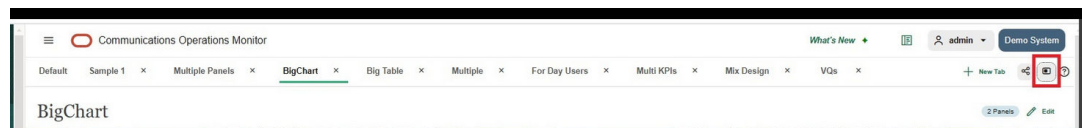
Switch feature enhances efficiency and simplifies the process for managing multiple dashboards simultaneously

The Auto Switch Button is positioned on the right side of the tab navigation menu. You can enable the Auto switch feature by clicking the designated button. When you activate Auto Switch, the dashboard tabs are automatically rotated every 20 seconds, sequentially cycling through each tab. This ensures continuous monitoring of multiple dashboards without requiring manual input.

To enable Auto Switch feature:

- Click the **Auto Switch** button on the right-side of the screen.

Figure 3-36 Auto Switch



Benefits of the Auto Switch

- **Improved Monitoring**
Users can seamlessly track multiple data sets and metrics, making it perfect for real-time monitoring applications
- **Minimized Manual Effort**
Automated tab switching allows users to concentrate on analysis and decision-making without the need for constant manual navigation
- **Optimized Workflow**
Limiting certain operations during auto-switching helps avoid disruptions or errors, ensuring a consistent and smooth experience.

Sharing Dashboard Tabs

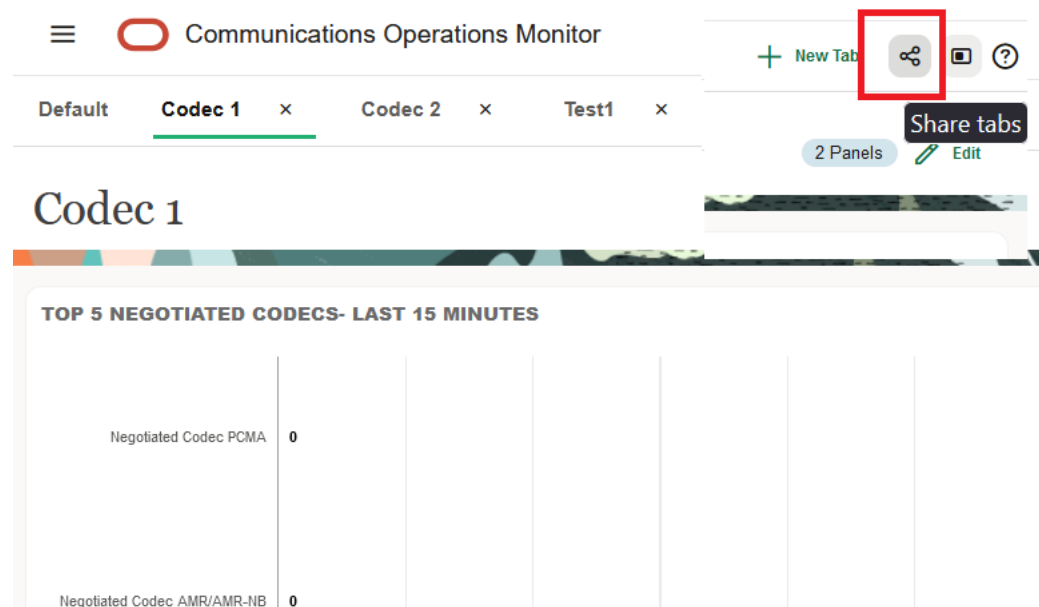
The admin user can share tabs with other users.

The admin user can share tabs with other users. For example, the admin can share a complex tab which took lot of time to configure or a tab that all users must mandatorily have on their dashboard.

This task can only be performed by an admin user. All tabs created by the user will be overwritten by the tabs shared by the admin user. The **Default** tab remains unchanged.

1. As the admin user click the tab that must be shared.
2. Click the Share tabs button.

Figure 3-37 Share Tabs



3. In the Share my tabs to... dialog box, select the user (for example user1) that you want the share the tabs with.
4. Confirm to share the tabs.

Note

- User1 will have to log off and log in again to see the tabs shared by the admin.
- If user1 does not have permission for any component displayed on the shared panels, the placeholder panel *Oracle* is displayed in its place.

Alerts

Operations Monitor has a notification system to warn you of important events called **alerts**. You can prioritize alerts and configure them to trigger certain actions. The **Alerts** page displays all alerts that have been raised.

The following **alert types** are supported:

Table 3-5 Alerts

Alert Name	Description
Generic Metrics	Statistics metrics exceed or fall below certain thresholds.
Device/Tag Metrics	Statistics metrics exceed or fall below certain thresholds.
Synthetic KPIs	Value for a synthetic KPI exceeds or falls below the given threshold.

Table 3-5 (Cont.) Alerts

Alert Name	Description
Metric Baseline Deviation	Allows comparison between a current KPI value and a previously captured KPI value. An alert is generated based on the difference between the two values.
User Devices	A certain user device is detected by the system.
Voice Quality	The quality for a percentage of calls falls beyond a MOS threshold. Voice Quality now allows you to create alerts for MOS, Packet Loss and Jitter.
Device Monitoring (when a device is down)	A device is down.
Oracle Communications Session Monitor messages	Messages sent from Session Monitor
Limits	An internal soft limit within Operations Monitor was passed.
Phone Number	A certain phone number placed or received a call.

The **Alerts** table displays notifications. You can create or edit an **alert definition** in the **Alert Definitions** tab.

Alerts Table

Click **Alerts** in the navigation pane to display the alerts panel, as shown in the following figure.

Figure 3-38 Alerts page

Status	Date	Type	Message	Priority
☐	2024/12/19 18:10:16	Generic Metrics	The minute sum of "Active calls" rose above 10	high
☐	2024/12/18 17:35:16	Generic Metrics	The minute sum of "Active calls" rose above 10	high
☐	2024/12/17 17:00:16	Generic Metrics	The minute sum of "Active calls" rose above 10	high

The following table lists the Alerts panel table columns:

Table 3-6 Alerts Table

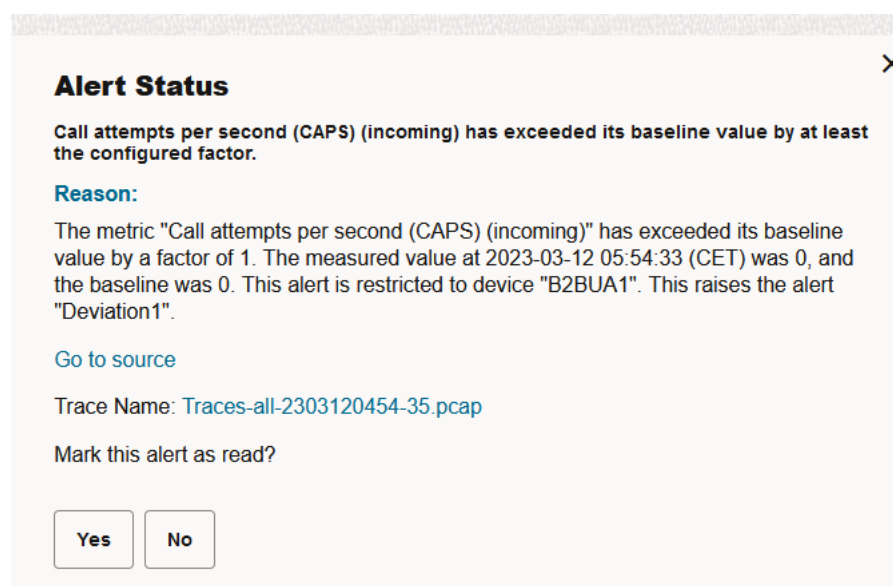
Column	Description
Status	Unread alerts are marked with a red icon. Alerts that have been viewed or read are shown with a green icon. Clicking the icon toggles the status as read/unread.
Date	The date when the alert was raised.

Table 3-6 (Cont.) Alerts Table

Column	Description
Type	The type of the alert. This columns allows for easy filtering.
Message	The alert message explains why the alert was raised.
Priority	Setting priority ranks the alerts. The alert entries with high priority are highlighted by a red background. Low priority alerts are displayed in a lighter color.

When you double-click an alert, the **Alert Status** window appears:

Figure 3-39 Alert Status dialog box



- **Reason:** The reason why this Alert got triggered.
- **Go to Source:** Takes you to the source where this Alert got triggered.
- **Trace Name:** Displays the link for the name of the trace file associated with this alert. Click the link to take you to the Traces page.

Note

You can see the link to the Trace file only if you have set a value for the **Create a trace** field value in the Alert definition. If the **Create a trace** field value is not set in the Alerts definition, you will not see any Trace file name and link in the Alert status dialog box.

- **Mark this Alert as Read:** Click Yes to mark this Alert as read.

In **Alerts** page, the **Mark all as read** button respects table filters, and can be helpful when treating similar alerts. For example, to mark all statistic threshold alerts, enable **Filters** in the

Type column and click **Mark all as read**. The **Delete** drop-down menu allows you to delete either:

- Selected alerts (the check box in the first column is marked).
- Alerts marked as read.
- All alerts.

Upon initial installation of Operations Monitor, the only alerts raised are related to licenses. You must create *Alert definitions* to receive further notifications.

 Note

To avoid being inundated with alerts (for example *Number of active calls exceeded 5000*), Operations Monitor creates duplicate alerts only when the previous one has been deleted, marked as read, or when 1 day has passed.

Alert Definitions Tab

Alert definitions establish which events on the system raise a notification. On the **Alerts** page, click the **Alert Definitions** tab to add a new alert definition. You can also add Alert definitions for the KPIs provided for Non-Call messages such as SUBSCRIBE, NOTIFY, and PUBLISH.

Figure 3-40 Add an Alert Definition

Add an Alert

Alert definition

Select an alert type

- ☒ Generic Metrics
- ☐ Synthetic KPIs
- ☐ Device / Tag Metrics
- ☐ Metric Baseline Deviation
- ☐ User Devices
- ☐ Voice Quality
- ☐ Device Monitoring (when a device is down)
- ☐ Oracle Communications Session Monitor messages
- ☐ Limits
- ☐ Phone Number

Previous Next Finish Cancel

Creating Alert Definitions

To create an alert definition:

1. Click **Add definition**, which starts the Alert Definition wizard.
2. In the **Add an alert** page, select an alert type (see the following figure). This also determines if parameters are required.
3. Optionally, *parameters* have to be provided that tell Operations Monitor when to raise an alert and of that type. Some alert types do not require parameters.
4. If desired, set actions to execute when the alert is raised, for example, to send an e-mail. For more information see, "Actions".
5. Assign an alert name and priority for the notifications raised according to this definition. For more information, see "Alert Name and Priority".
6. Click **Finish** to save the alert definition.

Operations Monitor raises an alert whenever the specified event occurs.

Figure 3-41 Add an Alert

Add an Alert X

Alert definition

Select an alert type

- ☒ Generic Metrics
- ☐ Synthetic KPIs
- ☐ Device / Tag Metrics
- ☐ Metric Baseline Deviation
- ☐ User Devices
- ☐ Voice Quality
- ☐ Device Monitoring (when a device is down)
- ☐ Oracle Communications Session Monitor messages
- ☐ Limits
- ☐ Phone Number

Previous Next Finish Cancel

Alert Actions

For all alerts additional actions can be configured (see the following figure). All actions are optional and can be combined.

Figure 3-42 Actions

Add an Alert [X]

Actions

Specify what should happen when the alert is raised. (Optional)

Send alert email:

Create a trace:

Generate SNMP trap: ☐ Enable this option to send an SNMP trap.

Table 3-7 Fields in the Alerts Definition Table

Fields	Description
Send alert e-mail	Sends an e-mail about the alert to the specified address. SMTP access needs to be configured before. For more information about configuring SMTP, see Configuring SMTP Settings. For most alert types, a deep link to the source of the alert marked as "URL to source" is provided in the alert e-mail. To receive this link, you must first configure the External IP/hostname. For more information, see External IP/hostname. For Traces, if only the Send alert e-mail field has a value, an e-mail notification is sent when an Alert is raised. You can also see the Alert on the Alerts page. The Alert will not have any link to the Trace file.
Create a trace	Creates a trace of the current SIP traffic when the alert is raised. Enter an appropriate time span (in seconds) for packet capture to tell Operations Monitor how far back in time the trace should go. When this field along with Send alert e-mail has valid values, an Alert is raised on the Alerts page, and an e-mail notification is received. Both - the Alert and the e-mail will have the Trace filename and a link maked as URL to trace. If a value is specified only in the Create a trace field, the Alert raised is only visible on the Alerts page. No email notification is sent. The Alert status dialog box has the name and the link to the Traces file.
Generate SNMP trap	Sends an SNMP trap to a configured SNMP target. When this is enabled, Operations Monitor alerts can be tracked and analyzed by an SNMP manager in the network. For more information, see "SNMP Options".

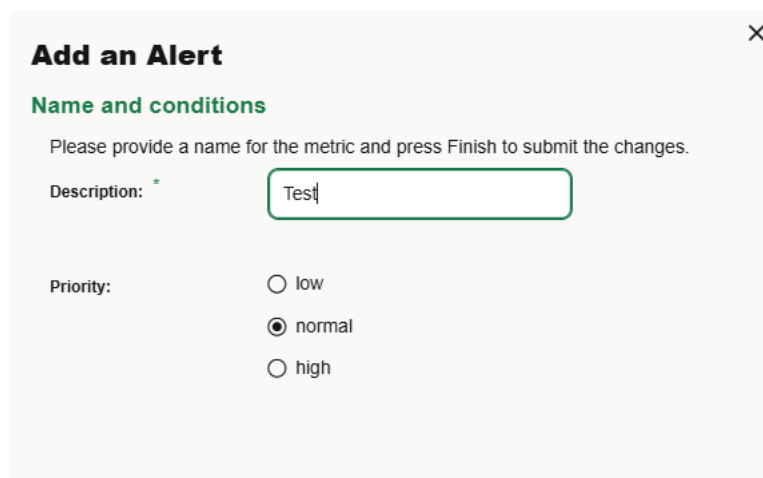
Alert Name and Priority

For all alerts a name and priority needs to be provided (see the following figure). It is also possible to define a minimum number of active calls to trigger the alert. (Optional) To <manage/change/do something>:

Note

The **Minimum active calls** condition is checked at the time of the alert generation, which is (depending on server load) one to several minutes later than the actual alert condition.

Figure 3-43 Alert Name and Priority



Add an Alert [X]

Name and conditions

Please provide a name for the metric and press Finish to submit the changes.

Description: *

Priority:

- ☐ low
- ☒ normal
- ☐ high

Voice Quality Alerts for Individual Platform Devices

Starting with Release 6.1, you can configure voice quality alerts specific to individual platform devices. This allows monitoring of key voice quality parameters such as MOS, Packet Loss, and Jitter on a per-device basis.

You can:

- Create voice quality alert definitions with one or multiple devices in a single alert-definition.
- Configure alert definitions with a maximum of 20 devices per definition.

Note

Irrespective of the number of devices added per alert definition, individual alert is raised for each device, when the threshold defined in the alert definition is met.

- Define threshold values for voice quality parameters (such as, MOS score below a threshold value, Packet-Loss/Jitter above a threshold value). Thresholds are pre-defined and you can only select from any of those predefined values.

Once the alert definition has been created

- An alert is generated when the percentage of calls on a device that do not meet the defined thresholds exceeds the configured limit.
- Calculation is done for the measure and device on both, incoming and outgoing counters.

What happens if you do not add devices to the alert definition

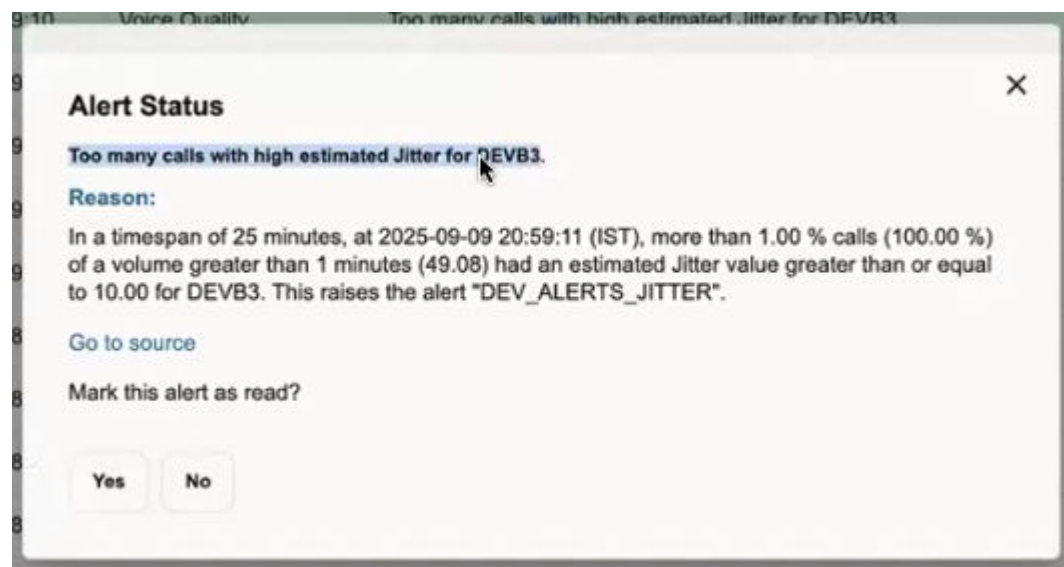
- If you do not add devices to the alert definition, the alert definition is configured on Platform-wide counters for the selected voice quality measure.

Adding Voice Quality Alerts specific to Individual Platform Devices

To create voice quality alerts specific to individual platform devices:

1. On the **Alerts** page, click the **Alert Definitions** tab to add a new alert definition
2. Click **Add definition**, which starts the Alert Definition wizard.
3. In the **Add an alert** page, select Voice Quality.
4. Add **Voice Quality Measures**. Select from MOScqe, Jitter or Packet Loss.
5. In the **Add Voice Quality Devices** dialog, add devices. Only those devices whose VQ Status is set to Full VQ or MOScqe are displayed in the list. For more information, see [Configuring Devices for Voice Quality Measurement](#).
6. In the **Voice Quality Thresholds** dialog, specify thresholds.
7. If desired, set actions to execute when the alert is raised, for example, to send an e-mail. For more information see, [Actions](#).
8. Assign an alert name and priority for the notifications raised according to this definition. For more information, see [Alert Name and Priority](#).
9. Click **Finish** to save the alert definition. Operations Monitor raises an alert whenever the specified event occurs. For example:

Figure 3-44 Device Specific Voice Quality Alert



Editing and Deleting Alert Definitions

To edit a definition, perform one of the following actions:

- Select the entry and click **Delete**.
- Double click the entry.

To delete a definition, select the entry and click **Delete definition**. Once an alert has been deleted, Operations Monitor no longer raises a notification for this definition.

Parameters

The following sections describe the various parameters for each alert type.

Statistics Metrics

Alerts can be defined with either one or two metrics. The metrics are compared to a threshold value using a comparison operator (for example =, <, > or not).

When you input one metric, the alert is triggered if the metric exceeds or falls below the given threshold value, depending on the comparison operator provided. This is suited for alerts such as 'The number of registered users exceeds 20,000.' In this example, an alert is sent when the number of registered users exceeds 20,000. If you would like a second alert to notify you if the value falls below 20,000, you must create a second definition.

When you provide two metrics, Operations Monitor considers the difference of the two metric values to a given threshold value, and therefore allows for more sophisticated alerting scenarios. For example, a statistics metric value deviates too much from its average value.

The example in the following figure shows the metric configuration of the alert scenario 'The number of registered users fell by 1,000 in the last week'. For using this alert definition, you must set the regular value for the metric as well as its average metric. For more information, see "KPI/Metrics".

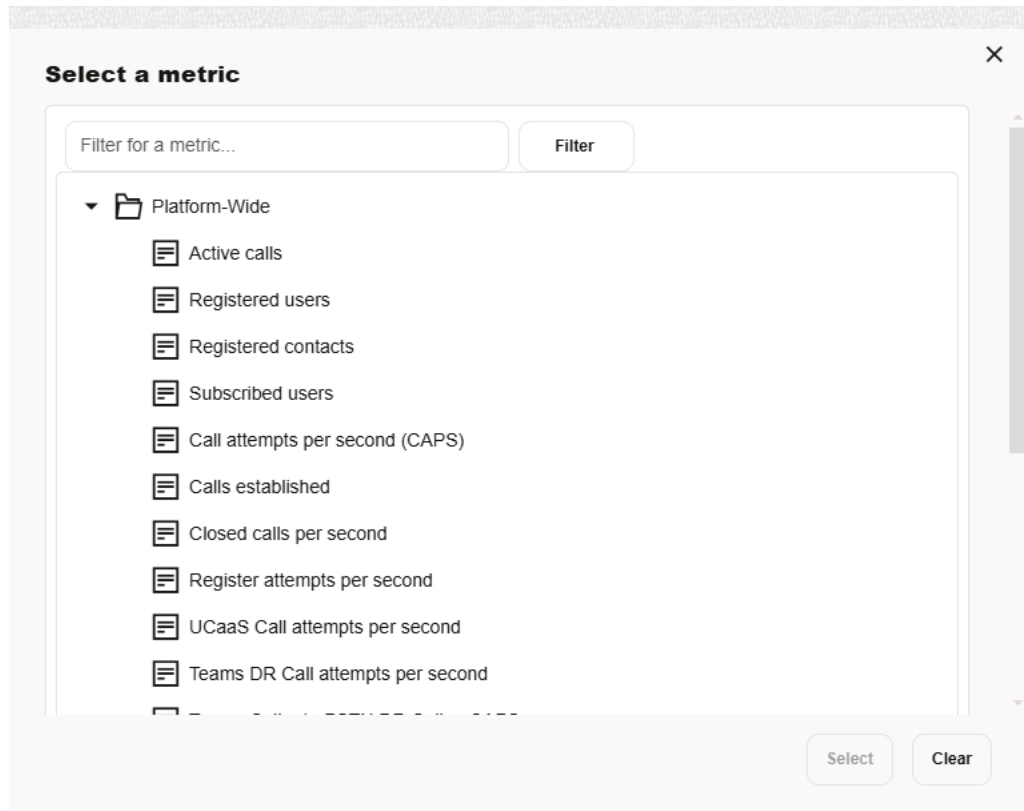
Figure 3-45 Metric Configuration for Alerts

The screenshot shows a web-based configuration window titled "Add an Alert" with a close button (X) in the top right corner. Below the title is a section header "Metric Configuration" in green. A descriptive text states: "Select a metric to monitor and specify a threshold for raising the alert. Optionally, the difference between or the quotient of two metrics can be used." The form contains several fields and options:

- Metric:** A text input field with the placeholder "Select a metric" and a magnifying glass icon. A "Required" label is below it.
- Operation:** A dropdown menu with the placeholder "Select an arithmetic operation".
- Other Metric:** A text input field with the placeholder "Select a metric" and a magnifying glass icon.
- Comparison:** A dropdown menu with the placeholder "Select an operation". A "Required" label is below it.
- Metric threshold:** A text input field with the placeholder "Specify a value". A "Required" label is below it.
- Use value:** A group of four radio button options: "Average", "Sum", "Minimum", and "Maximum". A "Required" label is below the group.
- Time resolution:** A group of three radio button options: "Minute values", "15 minute values", and "Hour values". A "Required" label is below the group.

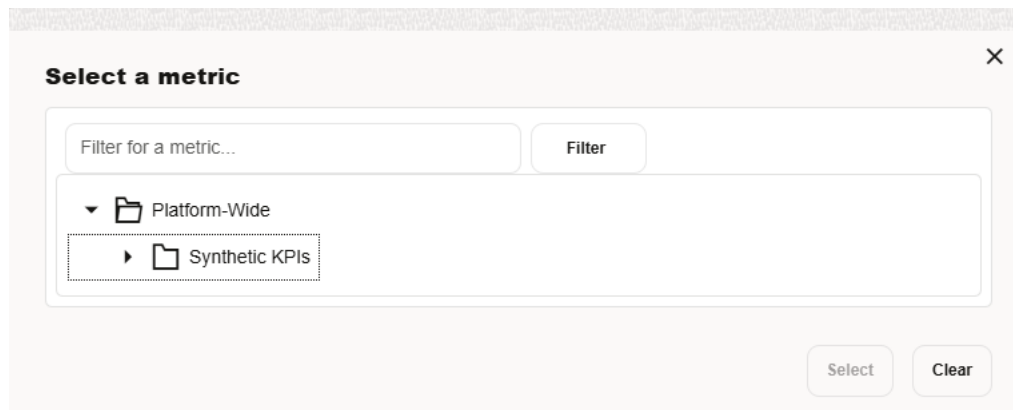
At the bottom of the form are four buttons: "Previous", "Next" (which is highlighted with a dashed border), "Finish", and "Cancel".

Clicking in the **Select a metric** field for a metric displays the metrics dialog box (see the following figure), where you can choose a metric:

Figure 3-46 Select a Metric

Synthetic KPIs

Synthetic KPI alerts comprise a synthetic KPI metric, a comparison operation, and a threshold value as illustrated in the following figure . An alert gets triggered when the value for a synthetic KPI exceeds or falls below the given threshold. For more information on creating synthetic KPI, see "About Synthetic KPIs".

Figure 3-47 Select a Metric

User Agent

Operations Monitor keeps track of all user devices that are registered on the platform and raises an alert depending on the desired option.

Highlighted Devices

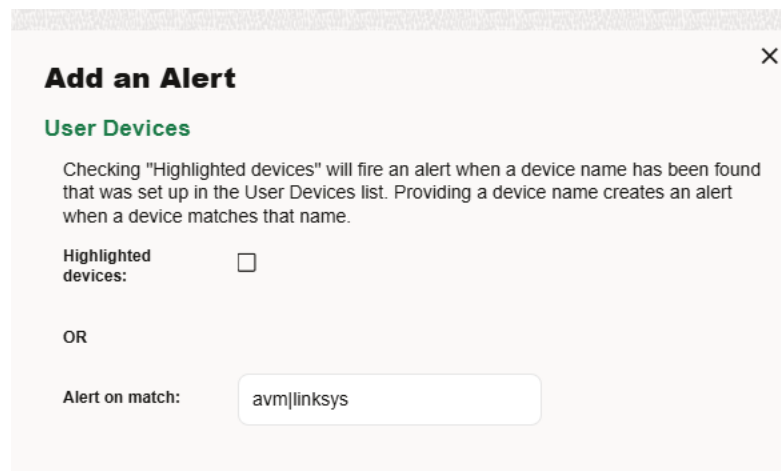
If a list of disapproved devices has been configured in User Devices, and Operations Monitor notices a user device from that list, an alert is sent. This option is recommended if User Devices is frequently updated so that the list can be centrally managed there. For more information, see "User Devices".

Alert on match

This option is intended for a more ad-hoc tracking of user devices. A regular expression can be entered to raise an alert when a matching user device is found. For every expression to track you need to add another alert definition.

The following figure shows an example configuration for detecting any AVM or Linksys devices.

Figure 3-48 Sample configuration for detecting any AVM or Linksys devices



The screenshot shows a dialog box titled "Add an Alert" with a close button (X) in the top right corner. Below the title, the section "User Devices" is highlighted in green. The text inside the dialog explains that checking "Highlighted devices" will fire an alert when a device name is found in the User Devices list. There is a checkbox labeled "Highlighted devices:" which is currently unchecked. Below this, the word "OR" is displayed. At the bottom, there is a label "Alert on match:" followed by a text input field containing the regular expression "avm|linksys".

Device Monitoring

This alert type refers to Device Monitoring and does not need additional parameters. Whenever a monitored device is down, an alert is raised. Only one alert definition of this type is needed. For more information, see "Device Monitoring".

Phone Number Alerting

The Phone Number type provides the possibility to alert on a specific phone number. The alert will be triggered when a call to or from a configured number is detected. To use this alert type the user needs to have the **Number Alerting** permission. Without this permission the **Phone Number** option will not be shown.

Phone numbers are configured in preferred number format. If the Use User Domains system setting is set to **true** then a phone number should be provided as a SIP user, that is, with a domain name: for example, 00403077811-call@example.com. If not, the phone number should

be provided without domain (and without the @ sign). For more information, see "Use User Domains".

Note

Only one number per alert can be defined. No wild cards are allowed.

A good strategy for setting up a number alert is to place a phone call to the desired number and look in the calls grid for the callee to get the exact SIP address/phone number to use for the alert definition.

The search for predefined phone numbers happens two times per minute, with calls that are at least 10 seconds old (in the early stages of a call, not all information needed is available). This means that a call in best case is detected after 10 seconds, in worst case after 40 seconds.

Figure 3-49 Phone Number Alert

The screenshot shows a dialog box titled "Add an Alert" with a close button (X) in the top right corner. Below the title is the section "Number Alerting". A text instruction reads: "Specify the phone number to receive alerts for when call is placed to, or received from, that number. Please note that number is specified in preferred number format." Below this is a form field labeled "Phone Number:" with a red asterisk indicating it is required. The input field contains the text "911". A "Required" label is positioned below the input field.

Traces

The **Traces** page allows you to capture, store and download packet traces of the SIP traffic. Downloads are done in the industry-standard PCAP format, which contains the complete messages as monitored on the network.

The PCAP file format can be interpreted by most of the available protocol analyzers, including open source tools. Any stored message contains TCP/UDP headers, an IP header, and layer 2 headers, as well as the time stamp at which Operations Monitor received it. All messages are written to the disk before any processing is performed. The filter defining, which traffic the traces, can be set in the **Signaling Protocols** section in the Platform Setup Application.

Packets are captured from the moment a trace is started. With Operations Monitor, you can also trace events in the recent past. For more information, see "Packet Buffer".

You can restrict traces to a single SIP user or an IP.

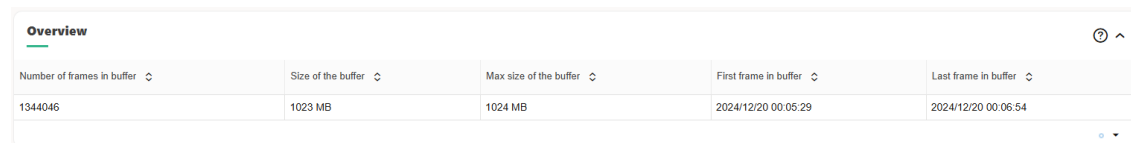
Note

If you restrict the traces to a SIP user, only UDP packets will be captured.

Packet Buffer

In order to create traces with packets received prior to the current time, Operations Monitor keeps an in-memory, rotating raw packet buffer with all the messages captured. The default size of this buffer is 1 GB including the message overhead. The buffer size system option allows you to change the size of this buffer.

Figure 3-50 Traces Info



Overview				
Number of frames in buffer	Size of the buffer	Max size of the buffer	First frame in buffer	Last frame in buffer
1344046	1023 MB	1024 MB	2024/12/20 00:05:29	2024/12/20 00:06:54

The Traces page contains three panels: the first shows information about the raw packet buffer, the second panel can be used for creating a new trace, and the third panel shows the currently running and finished traces.

Traces Info Panel

The Traces Info panel displays details about the state of the raw packet buffer:

- **Number of frames in buffer**
The total number of frames that are currently in the in-memory buffer.
- **Size of the buffer**
The total size in bytes of the raw packet buffer, including the overhead needed for indexing the messages.
- **Max size of the buffer**
The maximum size in bytes to which the buffer can grow. When this limit is reached, old packets are discarded.
- **First frame in buffer**
The timestamp of the oldest packet still in the buffer. Traces cannot capture messages before this point in time.
- **Last frame in buffer**
The timestamp of the newest packet in the buffer. This information is provided in order to approximate the capacity of the buffer in seconds.

Signaling Traffic Capture Panel

The **Signaling Traffic Capture** panel allows you to capture signaling traffic and save the data to a **PCAP** file. If you click **Start Capture** immediately, a trace begins with default settings. This provides a trace for activity in the last five minutes including non-call related messages such as **OPTIONS** and **PUBLISH**.

This panel allows you to configure time ranges, and filter SIP traffic by user or IP.

You can specify the **Start time**, **End time**, and the **Filters** used for a new trace in the **Signaling Traffic Capture** panel. Start and end times can either be set relative to the current time or by using absolute times. If the start time lies before the current time, the trace contains packets from the raw buffer. If the end time lies after the current time, the trace is started and write the packets received until the selected end time or until the user stops the trace.

Note

Traces are limited to durations up to 24 hours. Set traces to a duration shorter than 24 hours. After 24 hours of capturing, no further packets are traced.

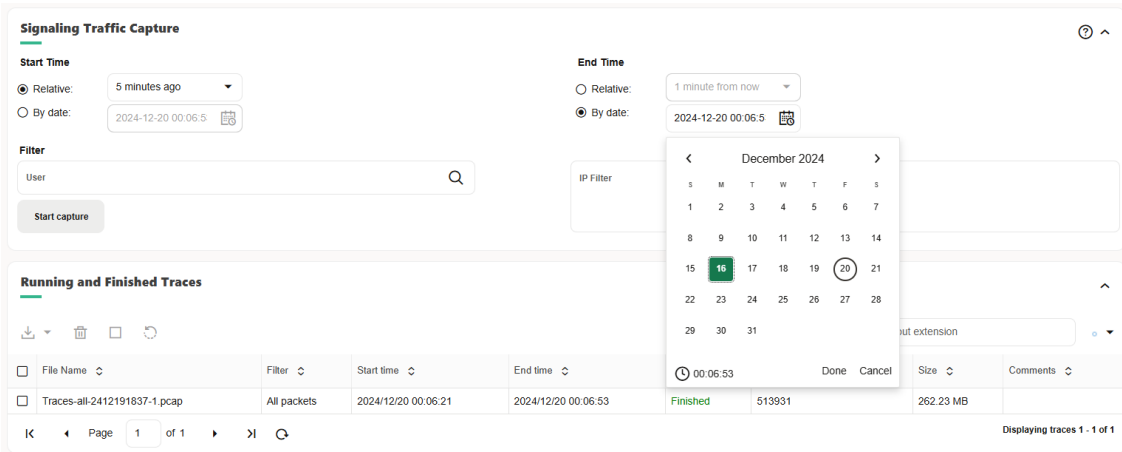
A *Filter* restricts captured messages to a single user, a single Operations Monitor network port, an IP address, or a combination of these. The **User** field has a live auto-complete feature: while typing the first characters of a user name or number, Operations Monitor suggests user names and numbers containing those characters from the set of known users.

The number of traces running simultaneously is limited to 3 by default and are configurable depending on the license. If the limit is exceeded, an error message is displayed.

Examples

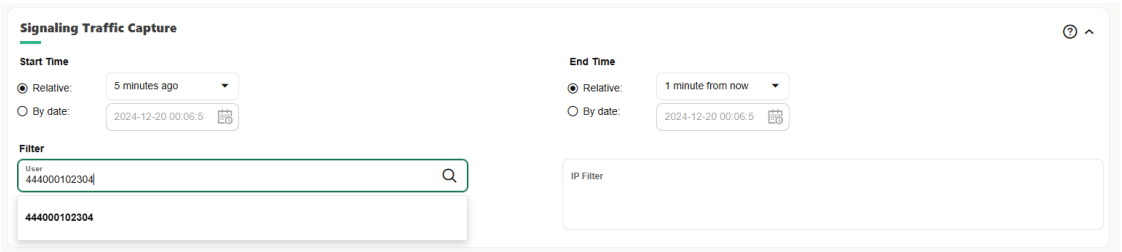
The following figure shows a new trace created for a past transaction using absolute times (from 10:18:56 to 12:24:00). No filter is selected: all messages received by Operations Monitor in the given time interval are included in the trace.

Figure 3-51 New Trace Created for a Past Transaction



In the following figure, a new trace is created for all messages from user '123000020343' from the last 5 minutes. Here, we use a relative start and end time.

Figure 3-52 New Trace Created for all Messages from a User



The following figure illustrates a trace created for all messages, which have either the source or destination IP address in the 62.220.32.0/24 network range. The IP filter field accepts both a host IP address in dotted format (*a.b.c.d*) or a sub-network address with the net mask appended (*a.b.c.d/e*).

Figure 3-53 Trace Created for all Messages with Source or Destination IP Address

The screenshot shows the 'Signaling Traffic Capture' interface. On the left, under 'Start Time', 'Relative' is selected with '5 minutes ago'. Under 'Filter', 'User' is selected. On the right, under 'End Time', 'Relative' is selected with '1 minute from now'. Below this, the 'IP Filter' field contains '62.220.32.0/24'. A 'Start capture' button is visible at the bottom left.

Running and Finished Traces Panel

The last panel on the page lists all traces that are stored on the disk and offered for download. Traces that are currently in progress are also listed and may be stopped before their scheduled end time. The following figure illustrates the panel.

Figure 3-54 Running and Finished Traces

File Name	Filter	Start time	End time	State	Frames captured	Size	Comments
Traces-333003893132-2412191842-11.pcap	333003893132	2024/12/20 00:11:08	2024/12/20 00:12:25	Stopping	0	0 bytes	
Traces-333003893132-2412191842-10.pcap	333003893132	2024/12/20 00:10:59	2024/12/20 00:12:15	Finished	23	12.94 KB	
Traces-333003893132-2412191841-9.pcap	333003893132	2024/12/20 00:10:33	2024/12/20 00:11:49	Finished	15	8.31 KB	
Traces-all-2412191841-8.pcap	All packets	2024/12/20 00:10:12	2024/12/20 00:11:29	Finished	1328715	680.16 MB	
Traces-444000102304-2412191841-7.pcap	444000102304 10.0.1.27	2024/12/20 00:10:04	2024/12/20 00:11:21	Finished	0	0 bytes	
Traces-444000102304-2412191841-6.pcap	444000102304 10.0.1.27	2024/12/20 00:09:45	2024/12/20 00:11:02	Finished	0	0 bytes	
Traces-444000102304-2412191840-5.pcap	444000102304	2024/12/20 00:09:29	2024/12/20 00:10:46	Finished	0	0 bytes	
Traces-all-2412191840-4.pcap	62.220.32.0/24	2024/12/20 00:09:13	2024/12/20 00:10:30	Finished	0	0 bytes	
Traces-all-2412191840-3.pcap	62.220.32.0/24	2024/12/20 00:09:07	2024/12/20 00:11:24	Finished	0	0 bytes	
Traces-all-2412191840-2.pcap	62.220.32.0/24	2024/12/20 00:09:03	2024/12/20 00:11:20	Finished	0	0 bytes	
Traces-all-2412191837-1.pcap	All packets	2024/12/20 00:06:21	2024/12/20 00:06:53	Finished	513931	262.23 MB	

Page 1 of 1

The following information is :

Table 3-8 Information presented for every trace

Column	Description
File name	The name of the PCAP file on disk. This will be also used as the proposed filename when downloading the trace.
Filter	Short description of the filter used for the trace.

Table 3-8 (Cont.) Information presented for every trace

Column	Description
Start time	The date and time the packet trace began. This can lie before the time at which the user has requested the trace.
End time	The date and time when the trace was stopped, or the time it is scheduled to stop in the case of running traces.
State	The current state of the trace is one of the following: • Running: Trace is in progress. • Finished: Trace has finished normally because its end time was reached. • Stopped: Trace was stopped by the user before its end time was reached. • Error: Trace failed to complete, possibly due to an internal error or an Operations Monitor core restart.
Frames captured	The number of packets stored in the trace. For running traces, this value is the number of packets written thus far
Size	The size in bytes of the capture file.
Comments	Remarks on the Trace.

All columns of in the *Running and Finished* Traces can be sorted. For example, you can click the **Size** column to sort the traces by size.

By default, the table is refreshed every five seconds, which can be changed using the **Auto Refresher** drop-down menu at the top right corner of the table.

When you select a trace from the list, the following actions are available from the toolbar above the table:

Download

Downloads the selected trace. This only works when selecting one trace at a time. Traces are compressed in a .gzip format in order to speed up the download.

Delete trace(s)

Deletes the selected traces from Operations Monitor storage.

Stop trace(s)

Stops the selected traces if they are currently running.

Restart trace(s)

Starts a trace with the same parameters as the selected trace, but with the time shifted to present. This only works for traces with relative start and end times.

Set Columns

Click **Set Columns** to hide or display columns in the table.

Note

The total size of storage space, which all traces can use is limited. When the space is full, the oldest trace is automatically deleted. The default value of this limit is set to 40 GB on a standard Operations Monitor server, with the traces being stored in a compressed form.

Search filenames without extension

Type the Trace filename to search for a trace file. This search does not support searching for Trace filenames with the extension.

Packet Inspector

The **Packet Inspector** page allows you to examine and download arbitrary network traffic captured on the probes. Downloads are done in the industry-standard PCAP file format, that contains the complete messages as monitored on the network.

Most of the available protocol analyzers can interpret the PCAP file format, including open-source tools. Any stored message contains the full raw frame including IP and TCP/UDP headers, as well as the timestamp when the message was received.

The filter for Packet Inspector determines the traffic that is captured and available for searching. You set this filter in the **Signaling Protocols** page in Platform Setup Application on the Probe. For increased system performance, it is important that this filter restrict the traffic that is captured and is comparable to the default filter. The Probe captures the packets from the moment the it is set up. See *Session Monitor Installation Guide* for more information about signaling protocol filters.

If you use Packet Inspector for recording media, you need to include media packets in the filter. Media packets are initially stored on the Probe machine until the Probe sends the packets to the Mediation Engine when a user downloads the media to a PCAP file. You need to ensure that there is sufficient disk space on the Probe machine for storing media.

Packet Inspector Page

The Packet Inspector page consists of a form where you specify the search parameters and a panel listing the preview of the results of a search.

Query Panel

The Query panel displays a chart that shows the amount of traffic received every two seconds. You can use the chart for selecting a time range. Operations Monitor searches the packets captured during the selected interval of time.

Time Range Selection

To select a time range, you can select, move, or resize a time range selection in the chart or use the controls to select a specific start and end date or a fixed time range (see the following figure). If you select a start and end date, the selection on the chart changes accordingly. If you select a fixed time range, the start and end dates and the selection on the chart changes accordingly.

Figure 3-55 Packets - Time Range Selection



Filter

To filter the result set further, you can enter filters in the **Filter** text field. On the right of the **Filter** text field (see the following figure) are some filter examples. See "Query Examples" for additional usage examples.

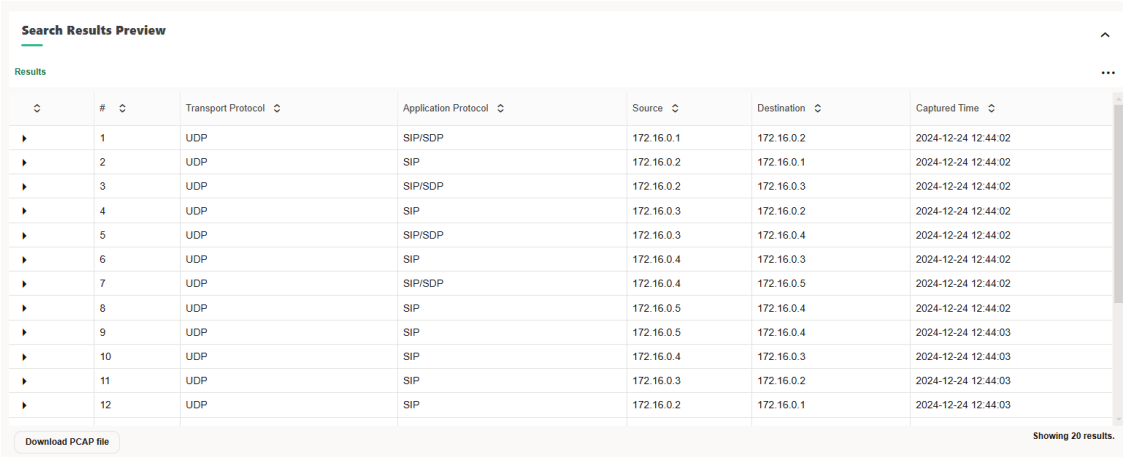
Figure 3-56 Filter



Search Results Preview Panel

The Search Results Preview panel shows a preview of the search results. You can sort the preview using each column. To browse the packet data details, expand its corresponding row. To download the complete set of search results, click the **Download PCAP file** button on the bottom of the panel.

Figure 3-57 Search Results Preview panel



Note

When the traffic sniffing is used with multiple ports and multiple worker threads, the packet sequence in the PCAP file resulting from the Packet Inspector search may not be in the timestamp order. However, if the packets need to be in order based on their timestamp, Wireshark can be used.

Query Examples

Query examples are Wireshark syntax. The following are examples of queries that can be used in the Filter text field:

- **Filter for any IP traffic to or from 192.168.42.70:**

```
ip.addr == 192.168.42.70
```

- **Filter for MEGACO messages to 192.168.1.1 or from 192.168.1.2 with transaction ids in range 2000..2500:**

```
(ip.src == 192.168.1.2 or ip.dst == 192.168.1.1) and megaco.transid > "2000" and megaco.transid < "2500"
```

- **Filter for ISUP to the device with point-code 1111 calling number 1234567:**

```
mtp3.dpc == 1111 and isup and e164.called_party_number.digits == "1234567"
```

Not all filter expressions work with fragmented packets. To get all packets, use an expression like:

```
sip.Call-ID == "910820420140505605616932@172.19.235.6" || ip.flags.mf==1
```

Using a query to filter for media packets can decrease system performance; therefore, it is not recommended.

Note

The total size of the storage space that Packet Inspector can use is limited. The default value of this limit is 81% of the disk space for each configured probe. Furthermore, there is a limit of three concurrent queries for each *product* instance running.

To improve the speed of Packet Inspector queries, use the following syntax to search for IP or ports:

```
tcpdump: [bpf filter]
```

You can use this syntax to search only for IP or ports and without any message content. For examples of BPF filters, see the topic on Filter Syntax in the Oracle Communications Session monitor Installation Guide.

Note

Searches combining tcpdump/BPF and Wireshark filter language are not supported.

Apps

Apps allow you to extend Operations Monitor's reporting capability. You can upload an app to customize the queries and report information provided by Operations Monitor. Operations Monitor provides a number of default apps, which can be accessed on this page. For information on how to develop new extension apps for Operations Monitor, see "Implementing Apps".

Note

Apps searches are not guaranteed to be real-time without advanced hardware sizing.

Figure 3-58 Apps in Session Monitor

Available Apps ?			
	Upload apps	Execute app	View Schedule
☐	Name	Mod.time	Scheduled
☒	Calls count	2024/12/19 12:31:01	Scheduled
☐	Registered users	2024/12/19 12:31:01	Scheduled
☐	Call-Id Search	2024/12/19 12:31:01	
☐	Find calls containing identity	2024/12/19 12:31:01	
☐	Calls containing keyword	2024/12/19 12:31:01	
☐	Calls terminated by a given device	2024/12/19 12:31:01	
☐	INVITEs without SDP	2024/12/19 12:31:01	
☐	INVITEs without SDP by IP	2024/12/19 12:31:01	
☐	Response Code Search	2024/12/19 12:31:01	
☐	Advanced Response Code Search	2024/12/19 12:31:01	
☐	Search leg given state	2024/12/19 12:31:01	
☐	One way audio calls detection	2024/12/19 12:31:01	
☐	User agent / codec statistics	2024/12/19 12:31:01	
☐	Users which register with multiple contacts	2024/12/19 12:31:01	

The **Apps** page (see the figure) is divided into three sections:

- The upper-left area lists *Available Apps*.
- The upper-right area displays outputs of previous *App Runs*.
- The bottom area displays the results of the selected *App Run*. It is empty when you first access the page.

App Descriptions

Apps allow you to extend Operations Monitor's reporting capability. The descriptions for the Apps:

Table 3-9 Apps and Descriptions

App	Description
Call-ID Search	This application takes as input the date and time boundaries such as started before and started after and the ID of the call and finds all calls with the given ID in that time span. The ID of a call can be found in the PCAP or when we expand a call in the Calls page and serves as a unique identifier for each call.
Find calls containing Identity	This application takes as input the date and time boundaries such as started before and started after and the regular expression pattern to search and finds calls which contain that regular expression pattern in any leg in that time span. The regular expression match is done against the Caller and Callee column . For example for a regular expression pattern "123*", "*123" and so on.
Calls containing keyword	This application takes as input the date and time boundaries such as started before and started after and the Searched word for a call and finds all calls with the given searched word in that time span. The searched word can be a definitive word from the message flow like "BYE", "INVITE", "RINGING".
Calls Count	This application takes as input the date and time boundaries only started before and started after and gives the summation of all the calls run in this time frame.
Calls terminated by a given device	This application takes as input the date and time boundaries started before and started after and the name of the device and finds all the calls in which the first BYE message was sent from a given device. The name of the device must be added in the Platform Device in Admin- Settings- Platform Devices .
INVITEs without SDP	This application takes as input the date and time boundaries started before and started after . This app finds calls where the first invite contains no SDP offer (under invite check Accept).
INVITEs without SDP by IP	This application takes as input the date and time boundaries started before and started after . This app finds IP addresses where the first invite contains no SDP offer (under invite check Accept)
Response Code Search	This application takes as input the date and time boundaries started before and started after as well as the Response code . The response code can be from any leg of the call. Response codes include values like 200, 180 and so on.

Table 3-9 (Cont.) Apps and Descriptions

App	Description
Advanced Response Code Search	This application takes as input the date and time boundaries Started before and Started after and Restrict search to final response code (leave empty to match any final code)" and "Filter for the following response code in any leg (leave empty to not filter)", This will search all calls with specified parameters in the given time frame. Response codes include values like 200, 180 and so on.
Search leg given state	This application takes as input the date and time boundaries Started before and Started after and Restrict search state of the leg and filters for the following response code in any leg. State can be Finished or 200,180 etc.
One way audio calls detection	This application takes as input the date and time boundaries Started before and Started after and Restrict search along with another parameter- "Consider no audio as problematic (0 or 1)". This will search all calls having no audio(0) or having one way audio(1) in the given time frame.
Registered users	This application does not take any input parameters but displays the registered users currently present in system.
User agent / codec statistics	This application takes as input the date and time boundaries Started before and Started after . This app gives statistics of the user agent and the codecs used by the user.
Users which register with multiple contacts	This application does not take in any input parameters but outputs the registered users who have registered with multiple contacts in the system.
Voice Quality Statistics	This application takes as input the date and time boundaries only Started before and Started after and returns the Voice Quality Statistics for that duration.
Voice Quality Chunks statistics	This application takes as input the date and time boundaries only Started before and Started after , and returns the Voice Quality statistics for chunks (10 sec interval) in a given time duration.

Available Apps

The **Available Apps** table (see the following figure) contains the columns **Name** and **Mod. time** by default. The first column displays a name for each application, the second column displays each apps modification time. The **Scheduled** column marks apps that are scheduled to run at a certain point in time. Additionally, the **Id** column can be enabled, which displays a unique identifier for each app. This is useful when you want to access the application using the remote procedure call functionality described in section "Remote App Procedure Calls" of this manual.

Figure 3-59 Available Apps

Available Apps ?

Upload apps

Execute app

View Schedule

Name	Mod.time	Scheduled
☒ Call-Id Search	2024/12/16 03:02:34	
☐ Find calls containing identity	2024/12/16 03:02:34	
☐ Calls containing keyword	2024/12/16 03:02:34	
☐ Calls count	2024/12/16 03:02:34	
☐ Calls terminated by a given device	2024/12/16 03:02:34	
☐ INVITEs without SDP	2024/12/16 03:02:34	
☐ INVITEs without SDP by IP	2024/12/16 03:02:34	
☐ Response Code Search	2024/12/16 03:02:34	
☐ Advanced Response Code Search	2024/12/16 03:02:34	
☐ Search leg given state	2024/12/16 03:02:34	
☐ One way audio calls detection	2024/12/16 03:02:34	
☐ Registered users	2024/12/16 03:02:34	
☐ User agent / codec statistics	2024/12/16 03:02:34	
☐ Users which register with multiple contacts	2024/12/16 03:02:34	

App Runs

Show in groups

View Debug Output

Group by

Stop

Run title	App start time	Number of results	Status
☒ Call-Id Search	2024/12/23 09:06:18	1	Finished

Call-Id Search

The app was called with the following parameters:

- title : Call-Id Search
- start_ts : 2024/12/22 00:00:00
- end_ts : 2024/12/24 00:00:00
- callid : 1399557391-30358@172.16.5.2

Caller	Callee	Call time	Setup time	Segments	Code	Min. MOS	Avg. MOS	State
+493026306853	+493088773575	1*19"	1*963ms	1	200	4.41	4.41	Finished

Uploading Apps

You can upload new apps to Operations Monitor in the **Available apps** table. Click **Upload app** to open a dialog box to search for an app archive on your computer and upload it to Operations Monitor. The procedure for creating an archive is described in the section "Implementing Apps".

 Caution

When creating your own applications, or using third-party applications, test your scripts in a test environment to ensure they are safe before uploading them to your production environment. Applications approved by Oracle are safe to use in your environments. However, non-approved applications could cause security and performance issues. Oracle is not responsible for any loss, costs, or damages incurred from using your own applications, or third-party applications.

Running Apps

The **Available apps** section also allows you to start any app that is already present on the system. Starting an app requires you to enter any parameters that the app defines.

To start an app, select it in the table and click on the **Execute app** button. A dialog appears that allows you to enter the app parameters. Every app has a **title** parameter. The sole purpose of the **title** parameter is to distinguish between different app runs of the same app in the **App runs** table. Click **Execute** in the parameter entry dialog to go to the **App runs** table. Execution also starts when a user double-clicks one of the available apps.

There are limits for simultaneous execution of scripts and for the maximum debug output that an script can generate. They are defined by the Maximum Simultaneous Script Runs and the

Maximum Script Output Size system settings. For more information, see "Maximum Simultaneous Script Runs" and "Maximum Script Output Size".

Scheduling Apps

You can also schedule a repeated execution of a given app. For more information, see "Scheduling App Execution".

The table entitled **Available apps** allows you to delete apps from Operations Monitor. To do this, select the app you want to delete in the table and click the **Delete app** button. After confirmation, the selected app is deleted from the system.

The **View Schedule** button displays the scheduling configuration for a given app: the cron expression which determines when this app is triggered, the e-mail address to notify, and the option to attach the result as a **csv** file.

View App Runs

The **App Runs** table (see the following table) displays four columns by default:

- The **Run title** column displays the Run title parameter that was entered when starting the app.
- The **App start time** column displays the start time of the app.
- The **Number of results** column displays the number of results that the app reported. This column updates as the app run proceeds.
- The **Status** column displays either **Starting**, **Running** or **Finished** depending on whether the app run is still in progress or already finished.

Two other columns can be enabled: the **Id** column to display the ID of each app run, and **App name** to show the unaltered name of the app. The **Id** column is useful when you want to access the results of an app using the remote procedure call functionality. For more information, see "Remote App Procedure Calls".

- **Exporting the App Runs to CSV**
The **CSV export** button lets you download the displayed items as a **CSV** file.
- **Debug App Run**
The *View output* action opens a window in which the console output of the selected app is shown.
- **Stopping and Removing App Runs**
The **App Runs** table allows you to stop an app run that is still active. To do this, select the app run you want to stop in the table and click the **Stop** button.

Note

You can only stop an app run when it is in the Running state.

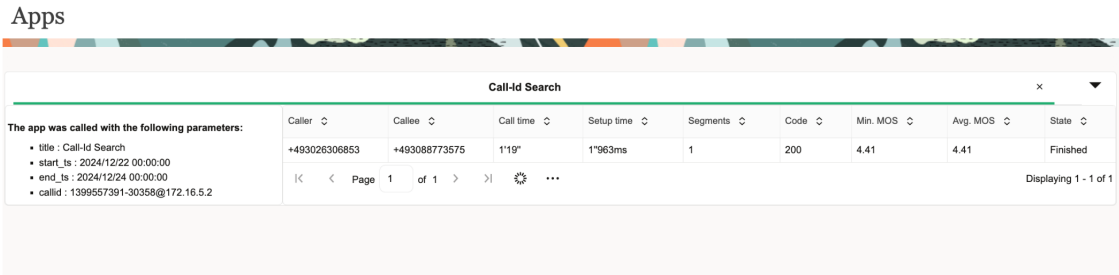
The **App Runs** table can also be used to remove app runs from the system. Select an app run in the table and click the **Delete...** button. You can only delete app runs that are in a **Finished** state.

View App Results

The lower portion of the **Apps** page displays result pages for app runs. The **Apps** page is empty when you first access it. When you double click an app run in the **App Runs** table, a new tab containing an app results view appears in the lower area.

App results view consists of a text display, which shows the parameters provided when starting the app, and a table containing the data rows reported by the app. The information in the table depends on the type of app that generated the results. Apps that search for calls use a similar results table to the calls table described in the section "Calls". Similar to the **Recent calls** table, you can double click on a row to get more detailed call information. This type of results table is shown in the following figure.

Figure 3-60 App Run Results



Expanding the view in the app results section provides a detailed and comprehensive analysis of the output. This improved visualization enhances the ability to analyze data quickly, compare metrics, and validate results.

The results page varies for each app. Multiple app results can be displayed simultaneously, and a new tab is opened in the lower portion for each.

Scheduling App Execution

- Apps can be scheduled to run periodically.
- To set up an app schedule:
1. Select the app from **Available Apps** and click the **Execute App**.
 2. In the **App Parameters** dialog box, click **Execution Schedule** arrow to expand and show the scheduling options (see the following figure):
 - The Schedule itself must be supplied as a cron expression. For more information, see "Cron Expressions".
 - Optionally, an email address can be provided for notification of app completion. The results of the execution may be attached to this email as a CSV file. Each execution of a scheduled app will also always appear in the View App Runs. For more information, see "View App Runs".

Figure 3-61 App Parameters

App Parameters

Title: *

Find calls containing identity

Consider calls after: *

Required

Consider calls before : *

Required

Identity regexp to search for: *

Required

Execution Schedule

Schedule: ⓘ

****2

Email:

admin@admin.com

☒ Attach result as CSV file

Execute

Cancel

Removing an App Schedule

Once a schedule has been set it can be deleted from the schedule list view. Select the app and click the Delete apps button in the Available Apps. Scheduled apps also have the string Scheduled visible in the Scheduled column of this table. For more information, see "Available Apps".

Figure 3-62 Scheduled Apps

Available Apps ⓘ

Upload apps

Execute app

View Schedule

☐	Name ↕	Mod.time ↕	Scheduled ↕
☒	Call-Id Search	2024/12/16 03:02:34	
☐	Find calls containing identity	2024/12/16 03:02:34	
☐	Calls containing keyword	2024/12/16 03:02:34	
☐	Calls count	2024/12/16 03:02:34	
☐	Calls terminated by a given device	2024/12/16 03:02:34	
☐	INVITEs without SDP	2024/12/16 03:02:34	
☐	INVITEs without SDP by IP	2024/12/16 03:02:34	
☐	Response Code Search	2024/12/16 03:02:34	
☐	Advanced Response Code Search	2024/12/16 03:02:34	
☐	Search leg given state	2024/12/16 03:02:34	
☐	One way audio calls detection	2024/12/16 03:02:34	
☐	Registered users	2024/12/16 03:02:34	
☐	User agent / codec statistics	2024/12/16 03:02:34	
☐	Users which register with multiple contacts	2024/12/16 03:02:34	

App Runs

☐ Show in groups

View Debug Output

Group by

Stop

☒	Run title ↕	App start time ↕	Number of results ↕	Status ↕
☒	Call-Id Search	2024/12/23 09:06:18	1	Finished

Call-Id Search

The app was called with the following parameters:

- title : Call-Id Search
- start_ts : 2024/12/22 00:00:00
- end_ts : 2024/12/24 00:00:00
- callid : 1399557391-30358@172.16.5.2

Caller ↕	Callee ↕	Call time ↕	Setup time ↕	Segments ↕	Code ↕	Min. MOS ↕	Avg. MOS ↕	State ↕
+493026306853	+493088773575	1'19"	1'963ms	1	200	4.41	4.41	Finished

Cron Expressions

Operations Monitor supports cron expressions as a means of defining your app schedules. An expression consists of 5 fields separated by white space that represent a set of times. The first field represents minutes, followed by hours, the day of the month, month, and day of the week. For example:

- To run an app every minute use this expression:

```
* * * * *
```

- To run an app every 30 minutes (on the 0th and 30th minute of every hour):

```
0,30 * * * *
```

- And below, every Monday (2nd day of the week) at 1am:

```
0, 1, * * 2
```

Note

App results that include data for calls (result type "calls") remain valid and accessible only as long as the calls are accessible in the system. Once the call(s) fall out of Operations Monitor's scope, the app results which reference them will no longer be available.

4

Operations

This chapter describes how to work with the Operations voice and video monitoring features of Oracle Communications Operations Monitor.

KPI/Metrics

The **KPI/Metrics** page provides standards of measurement by which efficiency, performance, progress or quality of the platform are assessed. Such measurements are called metrics or Key Performance Indicator (KPI).

A metric is a measurement of a numeric property on the monitored platform. Operations Monitor evaluates the metric every second, and aggregates the values into minute and hour averages, minima and maxima. Additionally, it keeps a history of the following increments: one hour, minute and hour averages, and minimum and maximum values.

Operations Monitor offers a wide range of predefined metrics, and allows you to create new ones. Thus, each realm defined in Operations Monitor can have its own personalized list of defined metrics. Operations Monitor users associated to a realm are able to see and change only the metrics defined for that realm. For more information about realms, see "[Realms](#)". Operations Monitor users can save their most used metrics into a **Favorites** list.

You can create an *average* of a metric in Operations Monitor. For example, this is useful if a provider wants to be notified when the number of active calls drops below a certain threshold, but not taking into account the low number of calls during night or weekends. In this case, an average of the active calls during the working days is useful. For information on how to configure this feature, see "[Average Metrics/KPIs](#)".

A KPI is a combination of metrics, and is usually defined as ratio of other metrics. Operations Monitor supports the IETF KPIs defined in the RFC 6067, <https://tools.ietf.org/html/rfc6076>.

The evolution of any metrics or KPI is presented in the chart in the upper area.

KPI/Metrics Monitoring Chart

The **KPI /Metrics Monitoring** chart displays the evolution and history of up to five measurements, including the average values as well as minimum and maximum values.

This chart operates like others in you can zoom out to see the evolution through the past, zoom in and scroll to the present, or pan to a specific time. For more information, on how to use Operations Monitor charts, see "[Charts](#)".

Note

The zoom value on the KPI/Metrics chart page reflects the Zoom value set on the Dashboard panel.

Note

You can view the KPI/Metrics Monitoring chart as a **Line chart** or **Bar chart**. Select the relevant option to see the chart either as a Line Chart or Bar Chart.

Multiple Tabs in the KPI Metrics Page

The KPI Metrics page supports multiple KPI views organized in tabs. Each tab can display up to 8 user-selected KPIs. The **Favorites** section remains common across all tabs. The following get saved per tab:

- Bar or Line Chart
- Selection of the Max 8 metrics
- Min/Max/Avg
- Sum
- Zoom level
- Dual Axis
- Y1 Marker
- Y2 Marker
- Filter in Metrics Library

Figure 4-1 KPI / Metrics Chart

To display the **KPI/Metrics Monitoring** chart, select the metrics from the **Library: Platform-Wide Metrics and KPIs** section. To see the Metrics that have been selected for the chart, click the **Show Selected** check box.

Use the **Expand Chart** toggle option to increase the height of the chart and view it in an expanded view. You can collapse using the same option to return the chart back to its original size.

At the bottom of the KPI Metrics chart:

- Hover the mouse on the chart or hover on the legend below the graph to view the KPI units along with time stamp at each point. This provides a better readability of the charts.
- Click **Show in Dashboard** to add the KPI Metrics Chart as a new panel to the Default tab of the Dashboard. Clicking Show In Dashboard also preserves the current zoom level and the dual-axis configuration of the chart on the Dashboard also. If you want to view it on any another tab other than the Default tab, edit the tab and select the chart panel using the Import from Default option.

Note

When you add a panel from KPI/Metrics to the Dashboard with the bar chart view selected, the same view is displayed on the Dashboard also. This preference is preserved across logouts and page refreshes. Clicking **Show in KPI/Metrics** on the Dashboard, updates the chart view on the KPI page to a bar chart as well.

- Click **Show in Interval** to chart to select Calls, or Registrations, or Subscriptions aligned to the time interval of the chart.
- Click **Export Chart** to export the chart as an .SVG graphic.
- Click **CSV Export of information displayed in the chart** to export the chart data to a .CSV file.
- Click **Clear Chart** to clear the chart and deselect the KPIs selected. This makes the chart area empty.
- Click the **Min/Avg/Max** check box. This check box controls whether minute or hour minima and maxima are displayed for each selected metric.
To display the minimum, average and maximum values of the metrics on the chart, mark the **Show Min/Avg/Max** box at the bottom of the panel. Note that min, average, and max only show meaningful differences when using larger temporal resolutions.
- Click the **Sum** check box to view the sum values of the selected KPI metrics. The Sum values for 1 hour, 3 hours, 6 hours, and 1 day are displayed in minutes, whereas the sum values for 3 days, 7 days, and 30 days are displayed in hours. You cannot view the sum values for 5 minutes and 20 minutes. This table represents the states shown on the UI of the KPI Metrics chart.

Table 4-1 UI States

Option Selected	UI State
None (Default)	The average value of selected KPI is displayed in the chart.
Sum check box selected	The sum value of the KPI is shown on the chart.
Only min/max/avg check box selected	The min/max/avg value of KPI will be shown on the chart.
Sum and min/max/avg check boxes are selected	Both values are shown on the chart.

Note

The metric **Synthetic KPI** cannot be viewed as a sum value.

- The sum values can be exported to .CSV file using the **CSV Export** option.
- While adding a panel in the Default tab, the state of the KPI/metrics chart (with the min/max/avg check box and the Sum check box option is enabled) is carried over in the Dashboard panel too. When you want to view the KPI/metrics graph from the Dashboard > Default tab > panel, and if the sum value of the KPI was already contained in the Dashboard panel, the sum value is reflected in the KPI/Metrics page also.

Creating a KPI/Metrics Chart with Dual Axis

The KPI /Metrics Monitoring chart enables you to select a dual Axis for any KPI chart for all KPIs with markers.

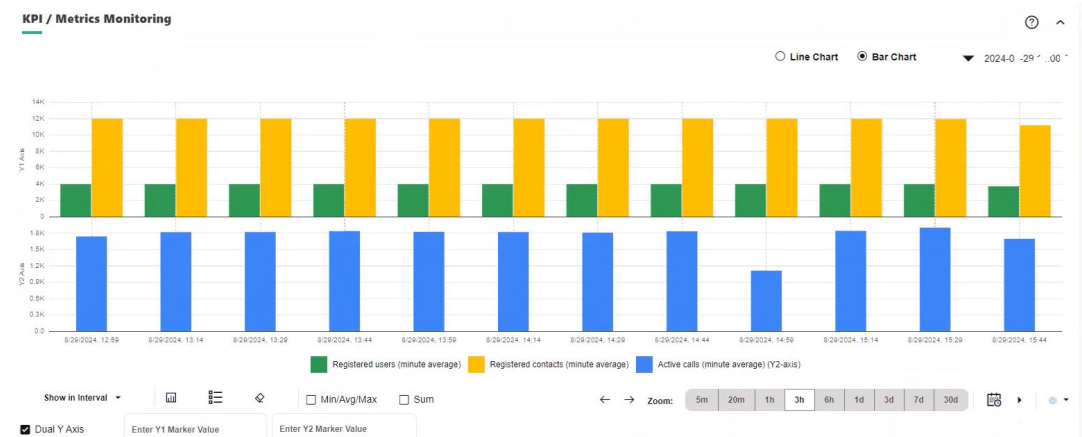
To create a KPI Monitoring Chart with Dual Axis:

1. In the **KPI / Metrics Monitoring** page, select a KPI metric from the **Platform library**. You can add up to five such KPI metrics. The **Dual Axis** check box is enabled only when you select more than one KPI.
2. At the bottom of the chart, select the required duration.
3. Select the **Dual Axis** check box.
 - a. In the pop-up dialog box, select a KPI that you want to view as a secondary KPI on the Y-axis. On selecting a KPI for the dual-Y axis, the KPI and its values are split on the secondary Y axis (Y2 axis). The values for the dual axis are plotted over time along with the primary axis. With the dual axes, you are able to compare the two axes (Y1 and Y2) over time.
 - b. In the **Y1 Marker Value/Y2 Marker Value** fields, provide a numerical marker value. Reference lines indicating the marker value are displayed on the chart.
 - c. Hover the mouse on the chart or hover on the legend below the graph to view the KPI units along with time stamp at each point. This provides a better readability of the charts.
 - d. Use the **Expand Chart** toggle option to increase the height of the chart and view it in an expanded view. You can collapse using the same option to return the chart back to its original size.
 - e. Click **Show in Dashboard** to add the KPI Metrics Dual Axis Chart to the Default tab of the Dashboard. The dashboard panel displays the same zoom level as the original chart. If you want to view it on any another tab, edit the tab and select the chart panel using the Import from Default option

Note

If Any KPI exceeds the marker value, marker is shown in Red line in the chart. The default color is Green.

Figure 4-2 Dual Axis Graph



- Click **Export Graph** to export KPI charts (from a selected view) to a downloadable .SVG format. Provide a name for the SVG file.

Click **Show in Dashboard** to add the KPI dual axis chart as a panel to the Default dashboard Tab. It also preserves the current zoom level and the dual-axis configuration of the chart on the Dashboard. If you want to view it on any another tab, edit the tab and select the chart panel using the Import from Default option

KPI/Metrics Monitoring Grid

The **KPI/Metrics Monitoring** panel contains a **Favorites** list created by the Operations Monitor user that displays the metrics they are most interested. The **Library** provides available metrics and KPIs to select, view, mark as favorite and customize.

Use the **Collapse Library Panel** option to collapse the library panel for a larger and more focused view of their Favorites panel.

You can sort the columns as per the need. The sorting order is saved, and the order persists even if you navigate away and return to this page.

Figure 4-3 KPI/Metrics Monitoring Library and Favorites

★ Favorites							
Active	Name	DeviceTag	Realm	Last Second	Last Minute Avg	Last Hour Avg	SNMP
☐	Active sessions (incoming)	#dev_g1_274	ALL	292	292.42	296.24	Off
☐	SIP requests		ALL	7,839	6,893.29	6,889.89	Off
☐	SIP replies		ALL	7,321	7,184.49	7,181.62	Off
☐	Register attempts per second		ALL	5,401	5,292.35	5,293.66	Off
☐	Session establishment ratio		ALL	76.64	76.39	76.4	Off
☐	Session success ratio		ALL	100	100	100	Off
☒	Call attempts per second (CA...		ALL	106	104.2	103.96	Off
☒	Active calls		ALL	11,912	11,903.65	11,888.78	Off
☐	Closed calls per second		ALL	77	79.66	79.29	Off
☐	Registered users		ALL	40,000	40,000	40,000	Off
☒	Registered contacts		ALL	119,890	119,898.54	119,900.01	Off
☒	Subscribed users		ALL	0	0	0	Off

Library	
☐ Filter metric ☒ Show selected ☐ Custom	☐ Collapse Library Panel
PlatformWide ☒ Active calls ☒ Registered users ☒ Registered contacts ☒ Subscribed users ☒ Call attempts per second (CAPS)	
Devices and Tags Platform-wide	Realm ALL

Library: Platform-Wide Metrics and KPIs

The metrics measured on the entire platform are presented in the *Platform-wide* tree under the following three sections:

- *Defined metrics* is the first, unnamed section and where the most common metrics appear.
- *IETF KPIs and metrics* contains the KPIs as defined in the RFC 6067 (<https://tools.ietf.org/html/rfc6076>).
- *Advanced metrics* is the section where you can configure customized metrics.

Pre-Defined Metrics

Operations Monitor adds the most frequently used metrics at the top of the list:

- Active calls.
- Registered users.
- Registered contacts.
- Call attempts.
- Call established.
- Closed calls per second.

To view a metric from the library in the chart above, you must mark the check box. By default, the *Active calls* metric is displayed.

To see only the selected KPIs, click the **Show selected** checkbox.

Advanced Metrics

Metric types are grouped into the following categories:

Table 4-2 Advanced Metrics Categories

Category Name	Description
Calls	Measures the calls with special properties, such as the number of calls with a call length smaller than 30 seconds.
Codec Statistics	KPIs for supported codecs, lists the statistics of the Codecs that are used over a period. The KPI for the negotiated codec is incremented only if the corresponding negotiated codec is present in the list provided in Supported Codecs. If the codec string does not match this list, then the KPI is not incremented. • Number of Finished Transcoded calls per second. • Number of Finished Calls per Negotiated Codecs with a given codec name. Use the Create New option under this folder to create the specific KPI based on the Codec required. By default, these KPIs are disabled. Codec KPIs will show the graph of negotiated Codec distribution over a period based on the Codec present in the Call. These graphs are available for Platform-wide, Devices, IP Tags, Prefix Tags and Realms. Codec statistics KPIs for Device and IP Tags will be incremented for Source Device only and it will increment for all Codecs KPIs involved in that leg"

Table 4-2 (Cont.) Advanced Metrics Categories

Category Name	Description
Megaco/H.248	Measures the amount of Megaco legs that are active, created, or finished.
MGCP	Measures the amount of MGCP legs that are active, finished, or completed.
Network	Measures transport layer properties, such as the number of TCP streams or the number of SCTP packets.
NONCALL	Measures the failed notifications with special properties, such as the number of failed subscriptions in the last second and number of failed notifications due to timeout or error response.
Number of ISUP Q.850 cause codes	Measures the sniffed ISUP traffic with certain Q.850 cause codes.
Registrations	Measures the registrations with certain properties, such as the number of unauthorized registrations in the last second.
RTCP	Measures the amount of RTCP or RTCP-XR packets and their jitter, delay, and MoScq values.
RTCP Usage	Measures the RTCP or RTCP-XR streams.
SIP NonCall transactions	Measures the SIP NONCALL transactions with properties such as the number of NONCALL transactions with a given method name and the response code or the number of timedout transactions.
SIP traffic	Measures the sniffed SIP traffic, such as the number of SIP requests or the number of certain SIP replies.

Note

The number of completed NONCALL SUBSCRIBE transactions are not directly proportional to the number of Subscribed Users. That is, for a particular user, there could be several completed NONCALL SUBSCRIBE transactions. So, the number of completed NONCALL SUBSCRIBE transactions could be more than the number of Subscribed Users.

Table 4-2 (Cont.) Advanced Metrics Categories

Category Name	Description
SIP transactions	Measures the SIP transactions with certain properties like the number of INVITE transactions that end with an error or the number of failed registrations.
SIP Stir Shaken	VSI updates these counters during header parsing in real time. The KPIs track: • Number of Calls Signed • Number of Calls Unsigned • Number of Calls Bypassed • Number of Calls Verified • Number of calls with verstat = TN-Validation-Passed • Number of calls with verstat = TN-Validation-Failed • Number of calls with verstat = No-TN-Validation • Number of calls with attestation A • Number of calls with attestation B • Number of calls with attestation C
HTTP	• Number of STIR/SHAKEN Requests: Total number of STIR/SHAKEN HTTP requests. • Number of STIR/SHAKEN Requests not answered: Requests without responses (timed out). You can create KPIs dynamically for specific HTTP response code ranges using the KPI Number of HTTP requests answered with a given response code.

Note

These KPIs are also available for PF Device Type across 'B2BUA' and 'Gateway'.

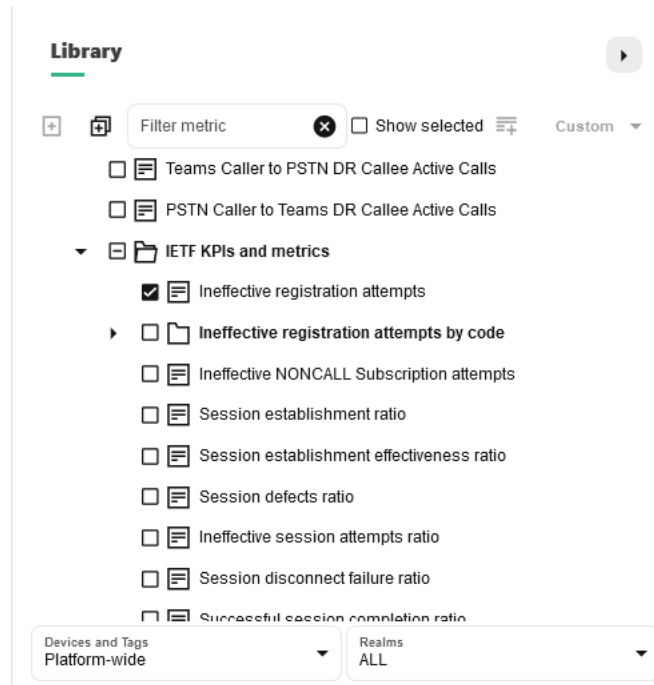
Note

These KPIs are also available for PF Device Type across 'B2BUA' and 'Gateway'.

IETF KPIs and Metrics

In the **IETF KPIs and metrics** section are the KPIs defined in the RFC 6067, <https://tools.ietf.org/html/rfc6076>. A list of IETF KPIs is shown.

Figure 4-4 IETF KPIs and metrics

**Note**

Two KPIs are calculated only on ingress legs.

For example, the IETF KPIs, Session Duration Time and Session Disconnect delay are calculated only on ingress call segments. An ingress call segment is the one where the call enters the system (the destination is a configured platform device but the source is not).

Enabling Metrics

The metrics displayed in *gray* text are *inactive*. Operations Monitor measures these metrics when you activate them. To enable a metric, click on the gray metric.

After a metric is activated, the metric text is displayed in *black*. This signifies that Operations Monitor is providing values for this metric, and you can view its evolution in the chart by marking its check box.

To see the Metrics that have been selected for the chart, click the **Show Selected** checkbox.

Some KPIs will not provide values for users in a realm. These KPIs are calculated on the transport level when the Ethernet frame is decoded. It is not possible to provide these values for users in a realm. These KPIs are:

- Bandwidth of the UDP packets
- Bandwidth of the TCP packets
- Bandwidth of the SCTP packets

These KPIs appear as disabled. Enabling them does not provide any value to a user in a realm.

Configuring KPIs

The **Ineffective registration attempts by code** KPI is configurable. It requires an interval of codes to be specified in order to be activated. Thus, you can customize its own KPI by adding the lower code, the upper code and the name of the new created metric as shown.

Figure 4-5 Define Ineffective Registration Attempts (IRA)KPI

Adding Ineffective registration attempts by code X

Metric Configuration

Name: IRA Error

Export for SNMP: ☒ ?

Parameters

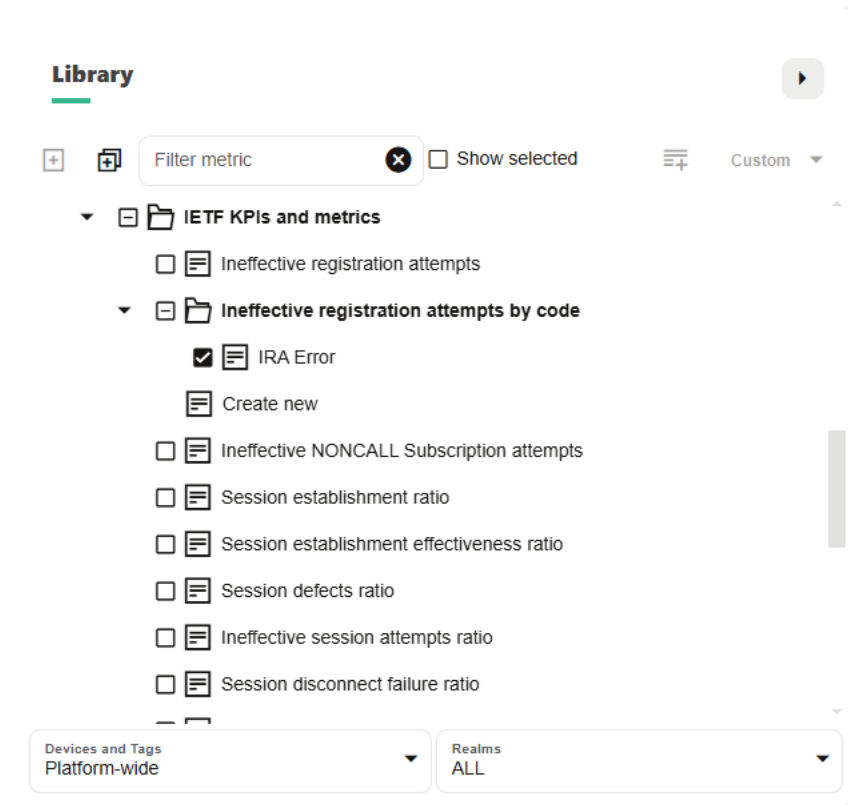
Lower bound for the code: 300

Upper bound for the code: 399

Save Cancel

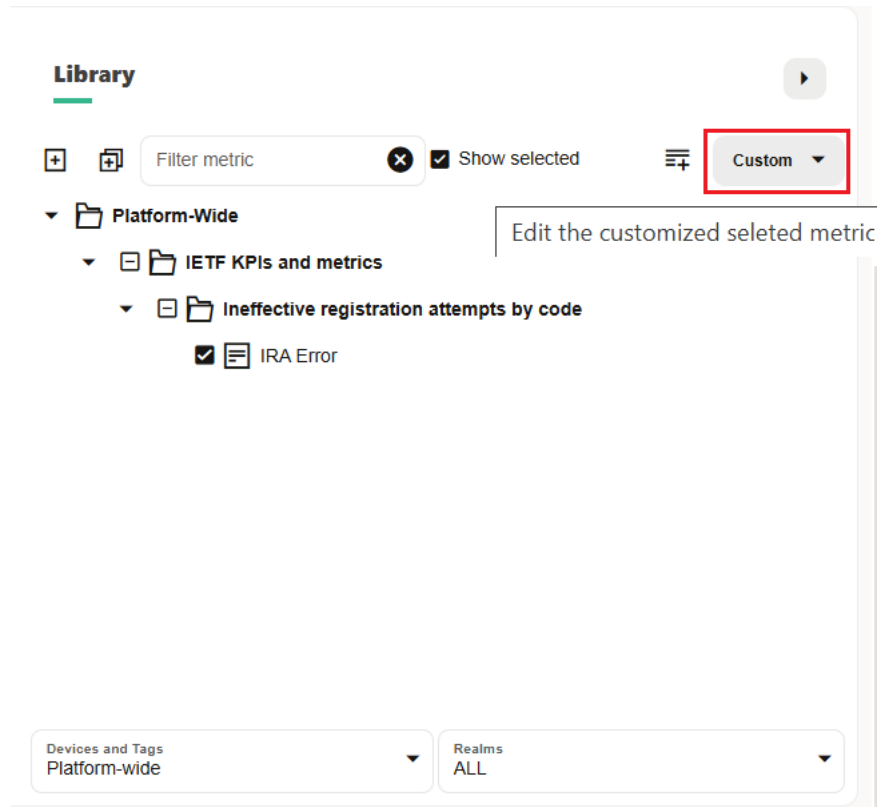
The newly defined KPI is added in the **Ineffective registration attempts by code** folder as shown.

Figure 4-6 Personalized IETF KPI



The user defined metrics can be later edited or deleted by clicking on the **Custom** button as shown.

Figure 4-7 Edit the Customized Selected Metric



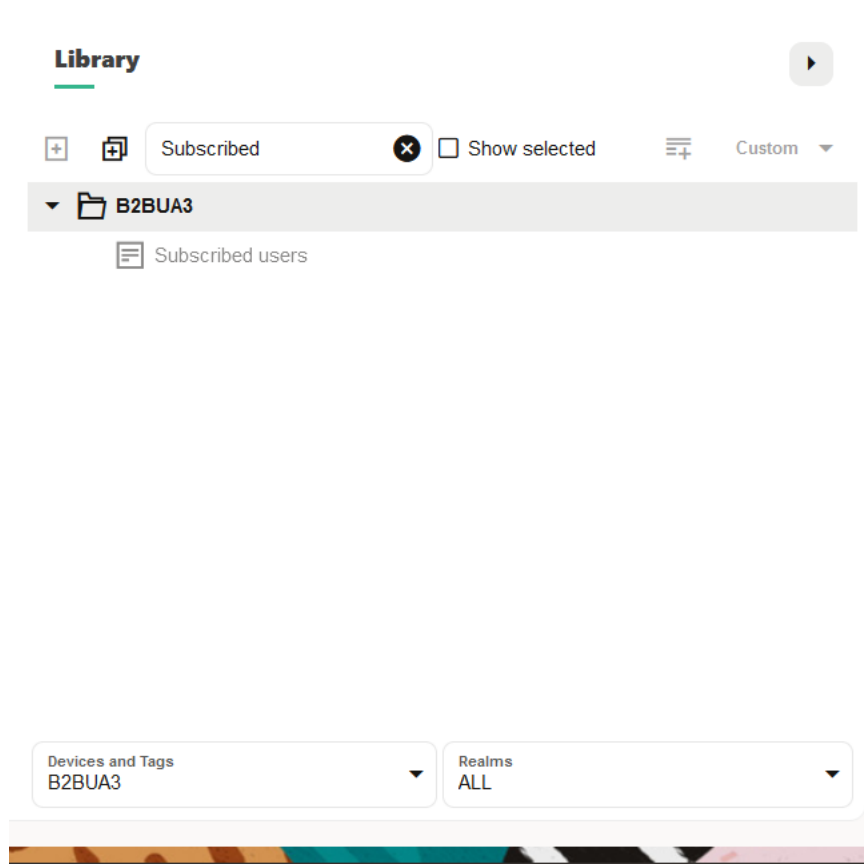
Exporting to SNMP

You can access each core metric through an external application via SNMP. To enable exporting to SNMP, select the metric in the library and click the **Custom** button. Select **Edit custom** and mark the **Export to SNMP** check box. For so-called compound metrics, an export is not possible and the check box is not available.

Library: Per-Device Metrics and KPIs

Operations Monitor can measure metrics for a platform device or specified trunk. In order to enable this feature, you must configure the platform devices (or trunks) in the platform settings. For more information, see "[Platform Devices](#)".

In the **Library** section of the **KPI/Metrics** page, you must select the device or trunk from the **Devices** field below the tree of metrics as shown.

Figure 4-8 Selecting a Device

Once you select a device, the metrics are presented in the Library tree.

Note

Synthetic KPIs appear only when the user selects Platform-wide. This is because Synthetic KPIs are not associated with a specific device.

When you are creating a metric for a device, you must specify whether the metric represents incoming traffic, outgoing traffic, or traversing. For each of the calls metrics, three values are stored:

- *Incoming* counts the call legs which have the IP address of the selected device as a destination.
- *Outgoing* counts the call legs which have the IP address of the selected device as the source.
- *Traversing* counts the calls that are relayed by the selected device. In other words, the calls that have one incoming and one outgoing call leg to/from the device.

If the device is a trunk, *incoming* is replaced by *egress*, and *outgoing* is replaced by *ingress*, as trunks are always viewed from the platform point of view. For more information, see "[Trunks/Prefixes](#)".

Pre-Defined Metrics

Operations Monitor adds the most commonly used metrics at the top of the list:

- Active calls (incoming).
- Active calls (outgoing).
- Active calls (traversing).
- Call attempts (incoming).
- Call attempts (outgoing).
- Call attempts (traversing).
- Registered users.
- Registered contacts.
- Response time (msec).
- Transit time (msec).

Click the check box from the front of metrics name to see the evolution of one of these metrics in the chart.

- **Transit time**

The time difference, in milliseconds, between the first INVITE message from the incoming call leg and the first INVITE message from the outgoing call leg. Only the calls that are relayed by the selected device are counted. To represent these values over time, if more calls are relayed in the same second, the maximum transit time is saved as value for that second. The web interface can then display average and maximum values per minute and per hour.

- **Response time**

The time difference, in milliseconds, between the initial request of a non-INVITE transaction and the final answer. Only the transactions, in which the destination IP address is one of the selected device's addresses, are counted.

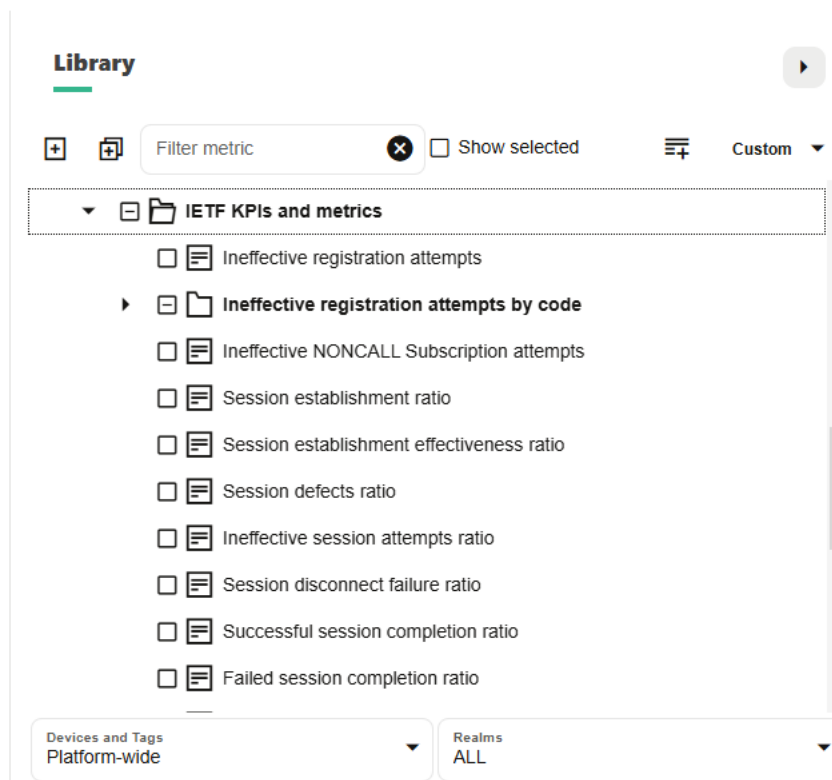
Note

The INVITE transactions are not considered here. The INVITE -> 100 time is always small, while the INVITE ->200 time is irrelevant, because it depends on when the callee answers.

IETF Metrics

A list of per device performance metrics (KPIs) is displayed in the **IETF Metrics** section of the library as shown.

Figure 4-9 IETF Device KPIs



Advanced Metrics

The web user can customize his own metrics under the categories presented in the advanced metrics tree.

Metrics displayed in a *gray color* are inactive and can be activated by clicking on them to bring up a window, as shown.

Once activated, their color becomes *black* and Operations Monitor starts providing measurements for them.

The metrics that share the same properties are grouped in folders and can be easily customized by clicking on the **Create new** link from the folder. An example of this group might be *Number of calls with a given call length*. This metric requires a couple of parameters to be configured, such as name, if it is exported via SNMP, direction of the call and the interval of the reply codes.

Figure 4-10 Configure a New Metric

Adding Number of calls with a given call length X

Metric Configuration

Name: Short calls

Export for SNMP: ☐ ?

Parameters

Call length (milliseconds) >=: 0

Call length (milliseconds) <: 100

Save Cancel

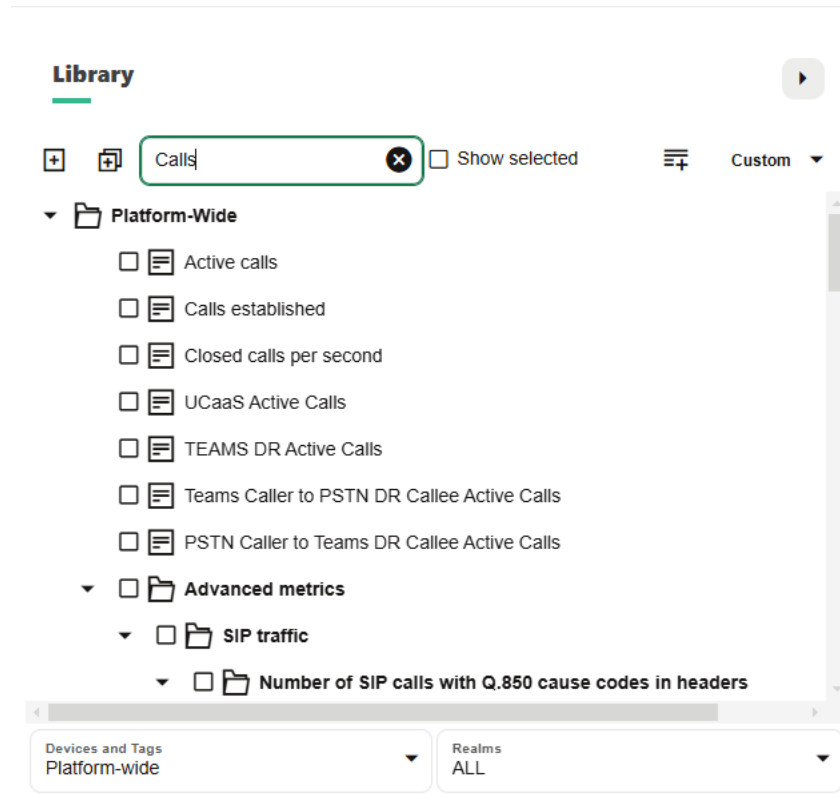
The user defined metrics can be edited or deleted by clicking on the **Custom** button, as shown in the Custom menu.

The same tree of metrics is displayed under the **Devices** page as they are configurable for a platform device (or trunk). For more information, see "[Devices](#)".

Filtering in the Metrics/KPIs List

Operations Monitor offers a search box for filtering the metrics by name. For example, if you want to filter the metrics for those that contain 'calls', enter **calls** into the search box as shown.

Figure 4-11 Filter the Metrics

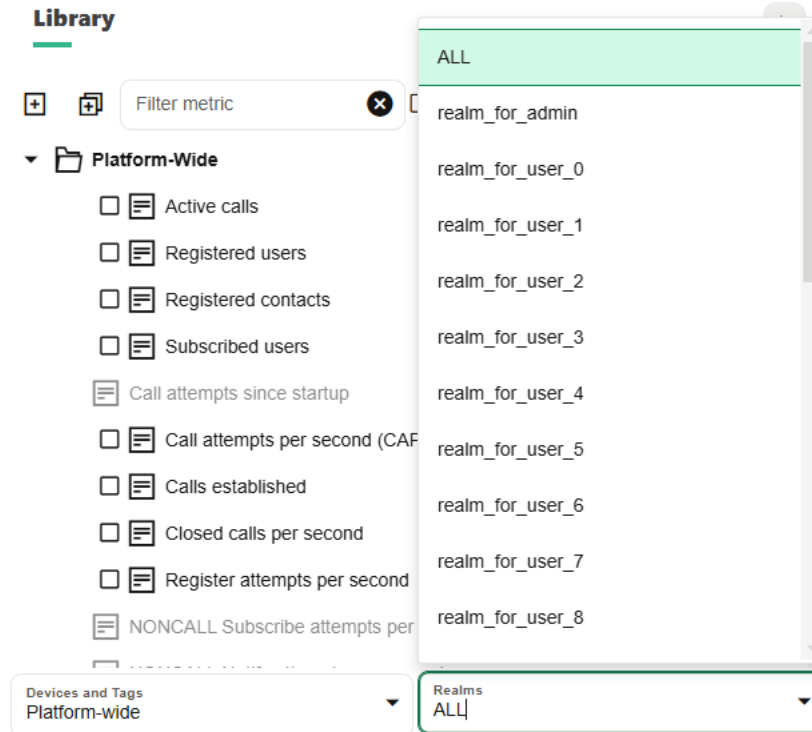


Restricting the Scope of Metrics/KPIs

You can restrict metrics/KPIs to a subset of the subscriber base using **Realms**. User based KPIs are enabled per user and are only visible for the user that has created them. Users in the same realm will not be able to see other users KPIs even they share the same realm. For more information, see "[Realms](#)".

The exception to this rule is the admin user who is able to see all metrics defined for each realm. The admin user can select a realm from the **Realms** list below the metrics tree, as shown.

Figure 4-12 Selecting a Realm



After choosing a realm, the admin user is able to see the metrics tree defined for that realm in the **Library** panel.

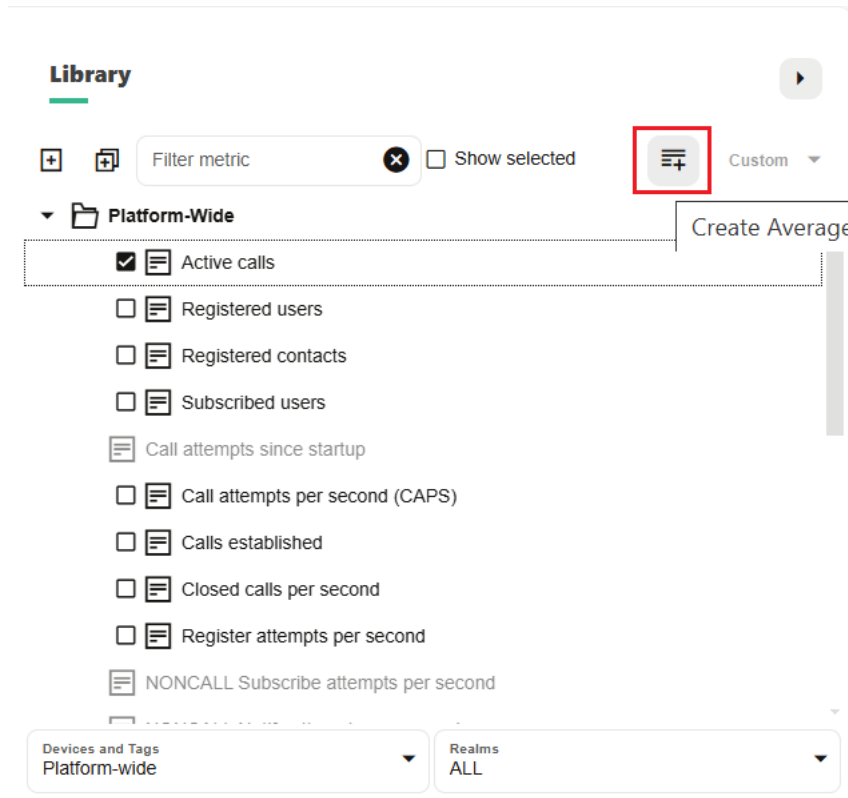
Note

The default Metrics/KPIs for a realm is created first when a user belonging to that realm logs in. For example, a realm bound user that logs in for the first time might be able to see old calls, but the *Active calls* metric only has data from the time the user first logged in and onwards.

Average Metrics/KPIs

An average metric or KPI can be created from any metric or KPI from the **Library** panel. In order to generate the *average metric*, first select the metric or KPI in the **Library** panel and then click on the **Create Avg** button.

Average metrics require configuration parameters such as a name, specifying if it is exported as SNMP, and the period it is calculated.

Figure 4-13 Configure an Average Metric/KPI

As the traffic during the weekends might be significantly lower than during the working days, Operations Monitor offers the ability to calculate the average only for working days as shows. The period of time for which the average has been calculated is given in number of days.

Figure 4-14 Configuring Average

The screenshot shows a dialog box titled 'Adding average metric for Active calls'. It has two main sections: 'Metric Configuration' and 'Average Metric Configuration'. In the 'Metric Configuration' section, the 'Name' field is set to 'Average Active Calls' and the 'Export for SNMP' checkbox is unchecked. In the 'Average Metric Configuration' section, the 'Average calculation' is set to 'over all days in range' (selected with a radio button), and the 'Number of days to calculate average' is set to 28. At the bottom right, there are 'Save' and 'Cancel' buttons.

After the average metric/KPI is created, it is added under the metric or KPI to which it belongs.

Note

The maximum supported limit for the average KPIs is 100.

Favorite Metrics/KPIs

Any metric or KPI from the *Library* can be dragged to the **favorites** list for an at-a-glance view of a small set of metrics. Each Operations Monitor user has their own personalized **Favorites** list as it is saved by user, as shown.

Figure 4-15 Favorite List of Metrics/KPIs

Active	Name	Device/Tag	Realm	Last Second	Last Minute Avg	Last Hour Avg	SNMP
☐	Register attempts per second		ALL	315	318.8	405.31	Off
☐	Call attempts per second (CA...		ALL	299	299.61	300.39	Off
☒	Active calls		ALL	33,665	33,731.06	33,700.68	Off
☐	Calls established		ALL	259	237.22	240.1	Off
☐	Closed calls per second		ALL	239	238.67	240.23	Off
☐	Registered users		ALL	100,000	100,000	100,000	Off
☐	Subscribed users		ALL	22,411	22,006.29	27,503.24	Off
☐	UCaaS Call attempts per sec...		ALL	0	0	0	Off
☐	IRA Error		ALL	0	0	0	On

Table 4-3 Favourites in the KPI Metrics screen

Column	Description
Name	Name of the metric.
Device/Tag	Device it is measured on.
Realm	Realm it belongs to
Last second	Value in the last second.
Last minute avg	Average on the last minute.
Last hour avg	Average on the last hour.
SNMP	Is On if the metric is exported with SNMP. Else it is Off .

Metrics in the Favorites list are displayed with the following information:

Note

In case of a *platform-wide* metric, the **Device** field is empty.

To remove a metric/KPI from the favorites list, first select the metric/KPI, and then click on the **Remove from Favorites** button. In case you want to enable/disable exporting the selected metric/KPI via SNMP click on the **Enable SNMP Export** or **Disable SNMP Export** button.

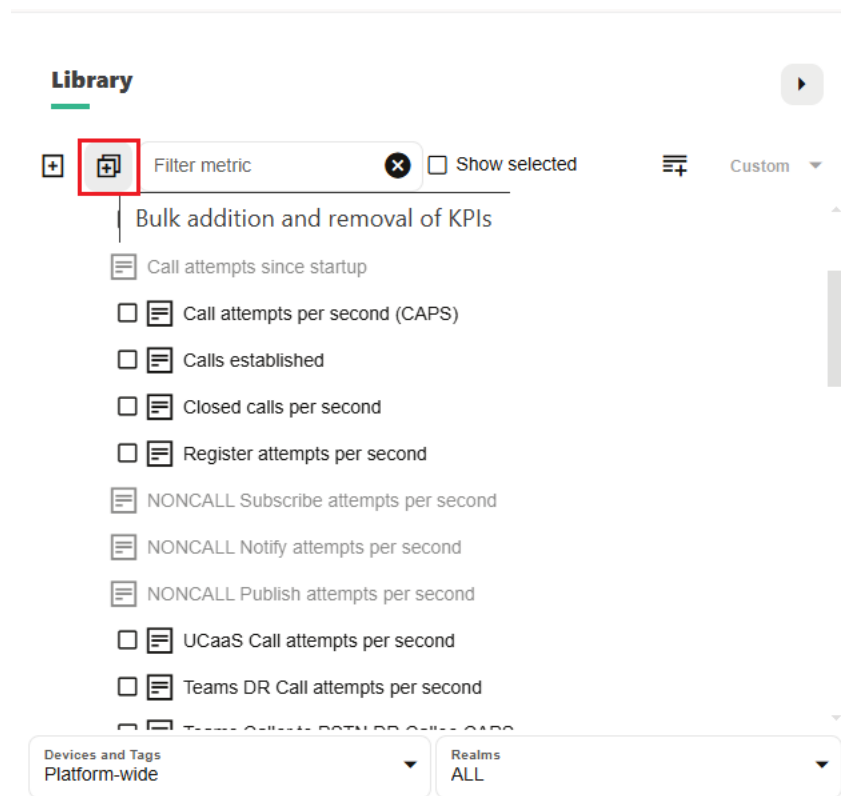
Bulk KPI/Metrics Creation and Removal

Operations Monitor provides the functionality for simplifying the addition and removal of multiple metrics in the **Bulk KPI/Metrics** dialog box. Using this tool, users can add and remove counters for multiple devices and IP Tags in a single operation. It is also useful for providing information about current KPI/counters usage.

Invocation

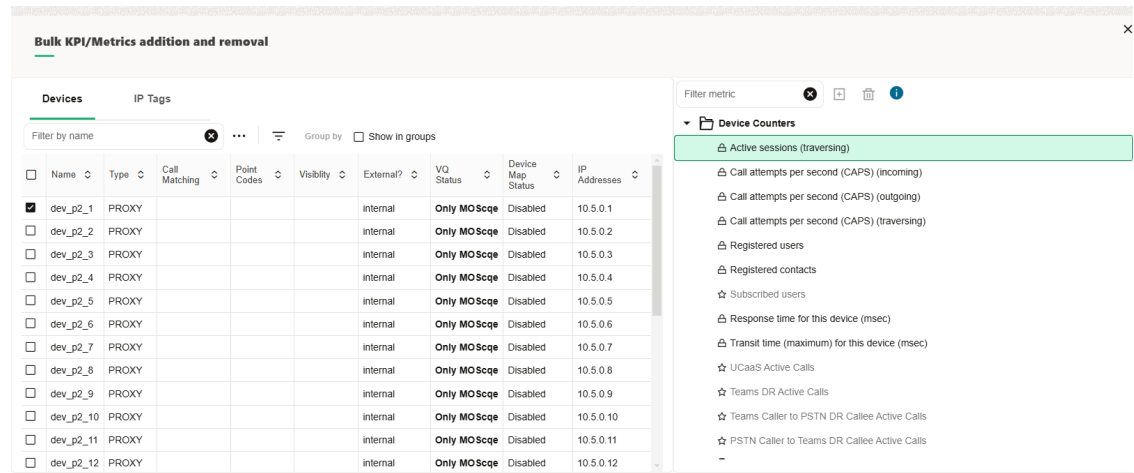
To invoke it, press the corresponding button you will find on the top of the Library toolbar on the **KPI/Metrics** page.

Figure 4-16 Starting Bulk KPI/Metrics



The following dialog appears:

Figure 4-17 Bulk KPI/Metrics Addition and Removal Invocation



Information Shown

The Bulk KPI/Metrics addition and removal dialog window is composed with the following elements:

- **Devices and Ip Tags**

This panel contains two tabs, **Devices** and the **Ip Tags**. Each tab allows users to select different devices/iptags, which are show in their corresponding groups. The same operations can be performed on both tabs.

- **Counters**

Shows a tree with the counters, as in the single device/IPtag widget but showing a symbol notation and a tooltip explains its meaning. These symbols have the following legend:

- Light gray: not existing counter.
- Half dark gray: counter exists for a subset of the selected devices.
- Full dark gray: counter exists for all the selected devices.
- Lock: counter cannot be added or removed.

The top toolbar filter lets users filter by counter name.

- **Progress Bar**

In the top of the dialog, it will show the progress of the bulk action. The process runs in background mode, so other actions can be performed in parallel.

- **Bottom Toolbar**

Shows the current number of counters created and the limit enforced for the bulk counters operations. These limits are not enforced for single counter operations.

Usage

Select one or more devices/IPtags on the device and then select a counter definition in the **KPIs/counters** panel. Adding or removing counters for those devices is implemented using the **Add** and **Remove** buttons on top of the counters tree panel.

Depending on the number of existent enabled counters, the following behavior applies:

- Fully disabled counters are only allowed to be enabled.
- Fully enabled counters (when counter is present for all selected devices) are only allowed to be removed.
- Half enabled counters will be offered two options:
 - Add the ones that are not present in some devices.
 - Remove all the existing ones from all the devices.

Limitations

Some device counters are created by Operations Monitor and cannot be added or removed. They are shown with a **lock** icon. The user is not allowed to add or remove them.

Bulk operations cannot be performed in some critical counters. Those counters will not be shown in the bulk **KPIs/counters** dialog box but they appear in the single device Library widget, in the parent **KPI/counters** page. They cannot be removed.

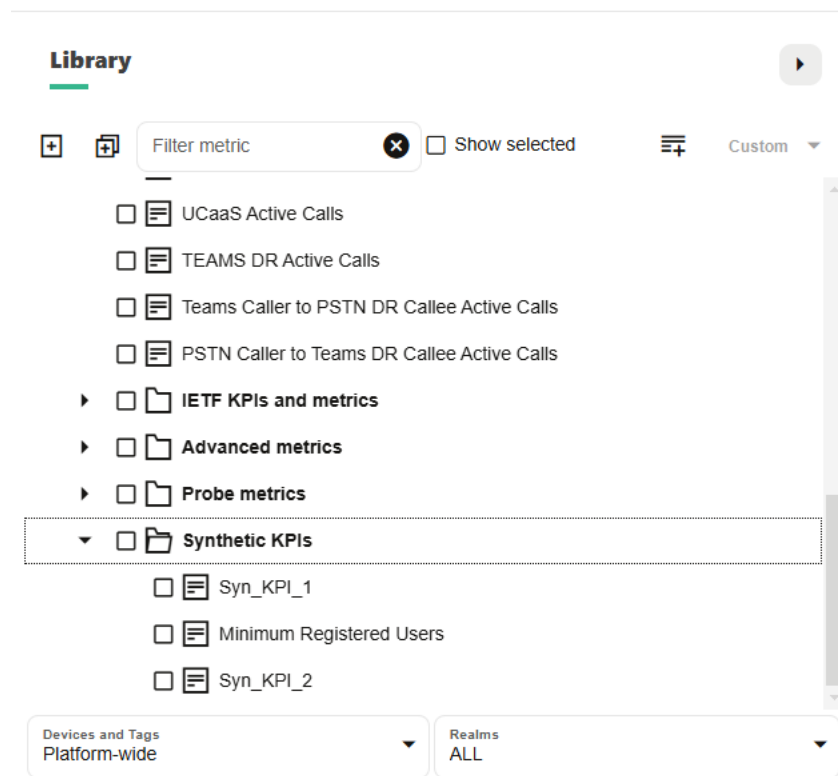
Once the limit for the counters amount is surpassed, users will only be able to perform removal operations.

About Synthetic KPIs

A synthetic KPI is a combination of KPIs. They are shown in the graphs under the **Library: Platform-Wide Metrics and KPIs** section. You can create, edit, and delete synthetic KPIs.

There is a special alert type for synthetic KPIs.

Figure 4-18 Synthetic KPIs Overview



Creating Synthetic KPI

To create a synthetic KPI:

1. In the Operations section of the navigation pane, click **Synthetic KPIs**.
The **Synthetic KPIs** page appears.
2. Click **New**.
The **New Synthetic KPI...** dialog box appears.
3. In the **Name** field, enter a name for the synthetic KPI.
4. In the **Expression** field, enter the arithmetic expression for the synthetic KPI.

You can use the expression tokens to create arithmetic expression. The expression tokens are enabled when you click or enter any value in the **Expression** field. For the syntax of arithmetic expression, see "[Arithmetic Expression Syntax](#)".

5. Click **Save**.

Figure 4-19 New Synthetic KPI Overview

Name	Expression
Syn_KPI_1	.SIP requests.min
Minimum Registered Users	.Registered users.min
Syn_KPI_2	dev_p2_1.Active sessions (incoming).max

Editing Synthetic KPI

To edit a synthetic KPI:

1. From the synthetic KPIs list, select the synthetic KPI.
2. Click **Edit**.
3. The **Edit Synthetic KPI...** dialog box appears.
4. Edit the details, and click **Save**.

Deleting Synthetic KPI

To delete a synthetic KPI:

1. From the synthetic KPIs list, select the synthetic KPI.
2. Click **Delete**.

3. Click **OK**.

Arithmetic Expression Syntax

Operations Monitor uses arithmetic expressions to define synthetic KPIs. An arithmetic expression can contain device, platform-wide KPIs, device KPIs, integer, and so on.

The syntax for arithmetic expression is as follows:

```
@device id #kpi id.Function [Operator][Number] [@device id #.kpi id. Function]...
```

For example,

```
@151#542.min + @151#543.min + @151#546.max - 34 + @151#548.min + 567
```

Parameters

Following are parameters for synthetic KPIs.

Device ID

Each device in the arithmetic expression is represented using numerical ID. For example, @150.

KPI ID

Each platform-wide KPI and device KPI in the arithmetic expression is represented using numerical ID. For example, #123

Operator

The valid operators are +, -, *, and /.

Number

Any number between 9007199254740991 and -9007199254740991.

Function

The **max** and **min** functions return the maximum and minimum values of the expressions respectively.

When you enter the arithmetic expression, the status of the expression is displayed below the **Expression** field. If the expression is valid and complete, the status is displayed as **OK**. If the expression is valid and requires more input, the status is displayed as **Incomplete**.

Calls

The **Calls** page is the central repository for call analysis in Operations Monitor. You can analyze call information by traversing the platform in real-time or historically. This data can be inspected as a high-level overview of all active calls, or a single call and its messages in detail. Operations Monitor can display SIP or ISUP calls together with MEGACO, MGCP, ENUM, and Diameter Cx.

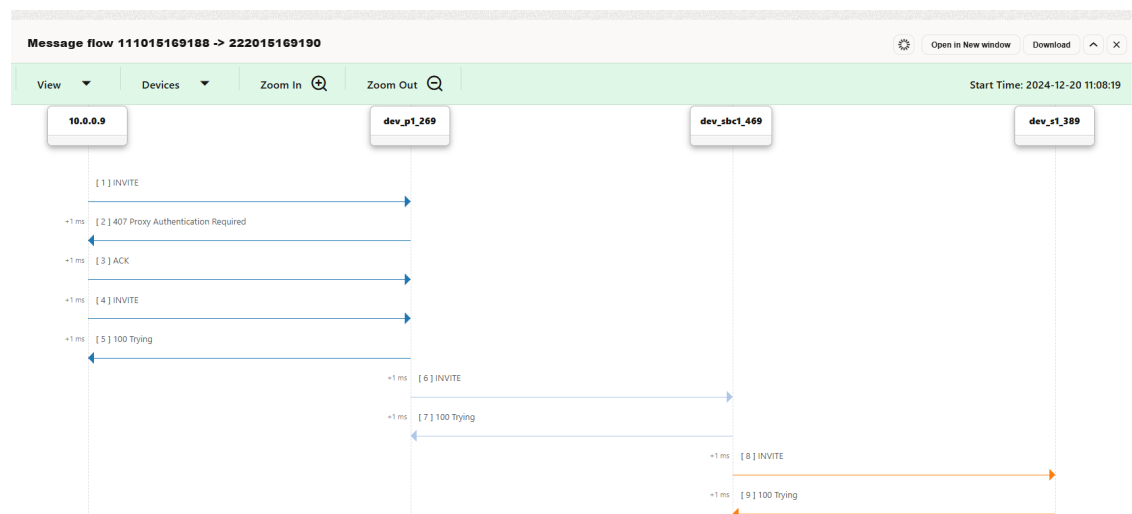
This page contains two panels: the **Calls Chart** displaying the number of calls currently in progress, and **Recent Calls** showing details about recent calls. For more information, see Active Calls Chart and Recent Calls.

Call Legs

A *call leg* is the portion of the call between two platform devices. Operations Monitor gathers messages from multiple points on the network, correlates them into call legs and merges them into *calls*.

1. From the Trunk to the Load Balancer device.
2. From the Load Balancer to the SIP Proxy.
3. From the SIP Proxy back to the Load Balancer.
4. From the Load Balancer to the callee.

Figure 4-20 Example Call Flow

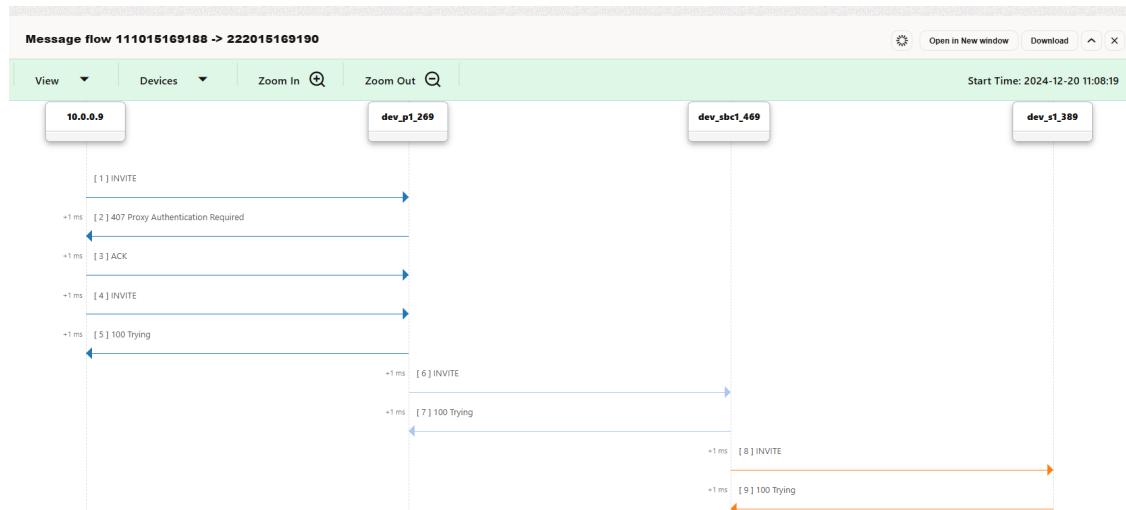


Merging call legs into *call flows* is important for network troubleshooting and gathering accurate statistics. For call merging to work properly, you need to configure the platform devices in the Platform Devices section. For more information about configuring platform devices, see the Initial Configuration section.

DTMF Tones in Call Flow

The call flow shows the DTMF tones. This is subject to certain user permissions.

Figure 4-21 Call Flow with DTMF Tones



Call States

[Table 4-4](#) lists the call states:

Table 4-4 Call States

Call States	Description
Unauthorized	The call was answered with '401' or '407'. The UAC typically sends another INVITE containing the credentials. If these are accepted by the UAS, the state will change to Proceeding or Established .
Proceeding	The call enters this state immediately after the first INVITE is received, and stays in it until an answer changes the state. The State details column may provide extra information (INVITE seen, ACK seen but no final response yet).
Ringing	The call enters this state when the first '180 Ringing' answer is seen.
Established	The call enters this state when the first successful 2xx answer is seen. The State details column mentions if the ACK is not yet received (200 OK seen, waiting for ACK).
Finished	An <i>Established</i> call enters this state when the first BYE message is seen. The State details column mentions if the related 200 OK message is not yet received (BYE seen, waiting for confirmation).
Timed out	An <i>Established</i> call enters this state if it lasts longer than the configured <i>session timeout</i> limit. This limit can be changed from the Session-timeout For Calls system option. For more information, see " Session-Timeout For Calls ".
Error	A call enters this state if Operations Monitor is unable to follow the call, due to an unexpected sequence of message.
Failed	A <i>Proceeding</i> call enters this state if a non-successful final response is seen or the 'INVITE' transaction times out. In the latter case, the State details column shows the 'Timeout during call setup' message. The KPI Number of failed calls per second is incremented for all response codes greater than 300. That is, 3xx,4xx,5xx and 6xx, except for codes 401 and 407.
Not Found	A <i>Proceeding</i> call enters this state if the 404 response code is seen.
Moved	A <i>Proceeding</i> call enters this state if the 301 or the 302 response code is seen.
Off-line	A <i>Proceeding</i> call enters this state if the 480 response code is seen.

Table 4-4 (Cont.) Call States

Call States	Description
Busy	A <i>Proceeding</i> call enters this state if the 486 or the 600 response code is seen.
Canceled	A <i>Proceeding</i> call enters this state if the 487 response code is seen.

If a call has multiple call legs, the call state is computed from the call legs' individual states.

Active Calls Chart

The **Active calls** chart represents the number of established calls at the time of the measure. The minimum, maximum, and average for the sample period are displayed. Zooming and panning are available in this chart. For more information, see "[Charts](#)".

- The **CSV Export of information displayed on the chart** exports the active calls data for the displayed period in a CSV format for post-processing purposes.

Note

The **Timezone Offset Alignment to Hourly Boundary** setting makes exported CSV graph data and metrics line up to the full hour in your local time zone (like 1–2 PM). This is useful if your time zone has a half-hour offset, such as UTC+5:30 or UTC+1:30. When you turn on this setting, time intervals in the exported data will start exactly on the hour in your local time, but there may be a one-time 30-minute gap in the graph data during the switch. Old CSV data is not affected—only new data collected after the setting is turned on (when viewing 3 days or more at a time) is affected.

- The **Show interval in grid** arranges data on a grid according to the time interval of the **Active calls** chart.
- By default, the **Auto Refresh** is set to 30 seconds for this graph. For more information, see "[Refresh Button](#)".

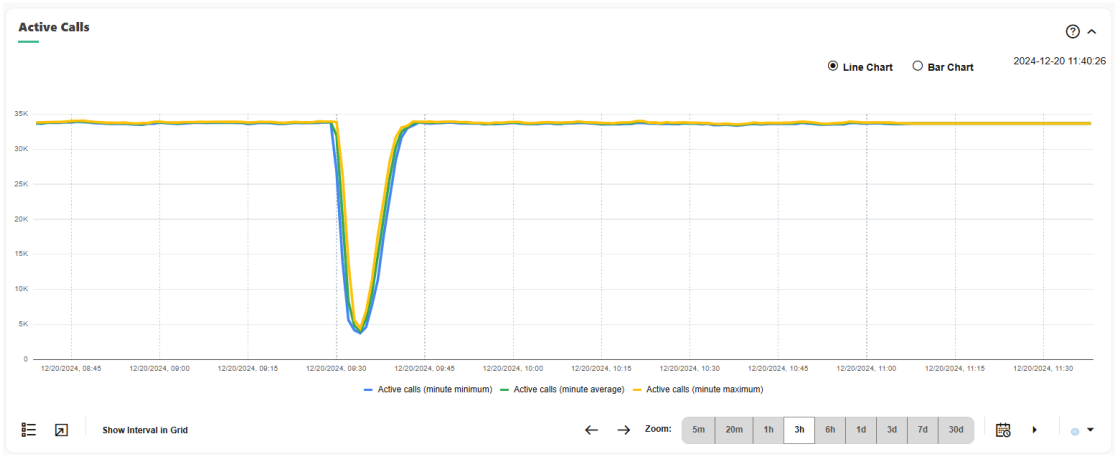
Note

It is observed that Oracle Communications Session Monitor shows a sudden drop in the graphs at least once in a week. It occurs at around 3:45 am and it is a part of the standard cleanup process. This cleanup can not be deactivated.

Example

This example depicts a typical view for one day of the **Active Calls** graph. The number of established calls decreases at night and increases during peak hours.

Figure 4-22 Evolution of Active Calls



Recent Calls

The **Recent Calls** table displays recent and historical information for calls made in the last few days. The calls from this table are updated in real-time as their state changes.

Figure 4-23 Recent Calls Table

Recent Calls																			
Details Set Call Exclusions ...																			
Type to filter eg: caller=575, callee=115																			
Caller	Callee	Start timestamp	End timestamp	Call time	Media Recording	Segments	Code	Ingress device(s)	Egress device(s)	DNMF	Diversion	Diversion Type	Call-Transfer	Min. MOS	Avg. MOS	State	State details	Audio	Identity
☐	+491767020896	+441604603303	2025/10/13 18:18:52	2025/10/13 18:19:27	30"	No	1	200								Finished	No Audio		
☐	+4198259212	+41980101073090920300	2025/10/13 18:17:14	2025/10/13 18:17:22	8"962ms	No	3	200								Finished	Ok		
☐	+4198259212	+41980101073090920300	2025/10/13 18:15:37	2025/10/13 18:15:45	8"962ms	No	3	200								Finished	Ok		

The Recent calls Toolbar

The **Recent calls** table has, in order, the actions as listed here:

Table 4-5 Recent Calls Table Actions

Actions	Description
Details	Opens the Call Details window for the selected call.
Set Call Exclusions	Exclude numbers from the Recent Calls table. Excluding a number from this table hides all rows containing that number, ensuring it does not appear in the current view.
Set Columns	Allows you to toggle hide/view columns in the Recent Calls table.
Select Column	Define a Simple Filter

Table 4-5 (Cont.) Recent Calls Table Actions

Actions	Description
Apply Filters	Apply filters.
Load Filters list box	Select from the list of advanced filters.
Edit Advanced..	Open Advanced Filtering Dialog.
Save	Saves the changes to the advanced filter.
Filters Rename and Delete	Delete or Rename filters.
Clear	Resets any selected filters. The Load Filters list box shows None.
Show Media Recording Window	Shows the media recording window
Show Message flow for selected calls	Shows the <i>message flow diagram</i> for the selected calls. You can select multiple calls in the call grid and show a combined message flow diagram. Use the Ctrl key on Windows/Oracle Linux machines and the Cmd key on Macintosh machines.
Download Message Flow	Enables you to download the message flow as an HTML file to your local hard drive. Note The Download Message Flow button is available on all Calls panels. Except the Dashboard.
Bulk export	Exports the current calls grid contents (with the current set of filters applied) as a zip archive. The archive contains one .csv file which is similar to the one generated with the normal CSV export, but with an additional column named <i>pcap_filename</i>. This references one of the pcap files included in the archive, which contains both SIP and RTP data for the call. If <i>column filters</i> are set, they are also applied to the exported CSV file. It is recommended to filter the calls list to the set of interest before exporting the CSV file.
CSV export	Exports the calls data content in CSV format, for post-processing purposes. If <i>column filters</i> are set, they are also applied to the exported CSV file. The CSV files are set to a maximum of 1 million records. It is recommended to filter the calls list to the set of interest before exporting the CSV file. Note You can set the maximum number of lines to export in a CSV file using the system setting Maximum number of lines exported with CSV export.

Table 4-5 (Cont.) Recent Calls Table Actions

Actions	Description
View saved calls	Shows the list of already saved calls in Operations Monitor. In order to save a call, the Save option from the calls details page must be used.
Show in Dashboard	Adds a reduced version of the Recent calls table to the Dashboard.
Auto-Refresher	From the Refresh menu, the table can be set to auto-update, in order to display the most recent calls and their state changes in real-time. You can set the table to auto-update from the Refresh menu in order to display the most recent calls. The state changes in real-time. The default auto-refresh interval for this table is 5 seconds.

Recent Calls Table

Note

Visibility of fields in the **Calls** table depends on the value of **Calls Field Permission** field under **Settings > User Management > Add (or Edit) User > Permissions for Modules** window.

Table 4-6 Recent Calls Table Columns

Column	Description
Audio	Shows the audio direction of the call. Each call is updated with the audio direction and the value is one of the below values: - No Audio. No RTP packets are exchanged between the end points. Values displayed in Black font. - One way Audio. RTP packets flowed only in one direction. Values displayed in Red font. - OK. RTP packets flows in both the direction. Values displayed in Green font By default, the value of the Audio column is updated once the call is finished. For information on how to enable real-time monitoring of the Audio column, see Audio Status. Note The color of this field depends on the values set in the system settings: Low threshold for Packet Loss Rate and High threshold for Packet Loss Rate. By default, this column is not added to the Recent Calls table, you will need to add this column using the Set Columns feature. You can filter data by applying the different types of filter on this column, can bulk export or export this field data to a .CSV file, and add this column as part of a dashboard panel. Note Starting with Release 6.1, the One Way Audio Addon has been removed from Platform Setup Application and Mediation Engine.
Verstat	Based on the Verstat URI parameter in the From header (or in PAI header). Values can be: - TN Validation Passed - TN Validation Failed - No TN Validation
Identity	Based on the Identity header presence within SIP INVITE (whichever appears first on the leg). 0 - False 1- True - Null - Empty
Certificate	Certificate – based on the 'info' value of the Identity parameter.
Passport	Based on the 'ppt' value of the Identity parameter. Values can be: - div - shaken
Identity Bypass	Based on P-Identity-Bypass header value in the SIP INVITE (the call leg – 1st seen displayed) P-Identity-Bypass: xyz
Attestation Level	Based on Attestation-Info or P-Attestation-Info header value within SIP INVITE (whatever the leg – 1st seen displayed)
Origination ID	The Origination-Id or P-Origination-Id header value is retrieved from the SIP INVITE, using the value found on the first leg that is detected.

Table 4-6 (Cont.) Recent Calls Table Columns

Column	Description
Avg. MOS	The voice quality estimation for Finished calls. If Operations Monitor does not receive RTP traffic, or the RTP module is not loaded, this field is empty. The value is displayed in green, orange, or red depending on the thresholds set in the system options High Threshold for MOS and Low Threshold for MOS. For more information about how Operations Monitor estimates the MOS value of a call, see " Voice Quality ".
Avg Jitter	The average of the measured jitter values of the 10 seconds intervals. By default, this column is not displayed in the Recent Calls table. Add it using the Set Columns feature. You can apply different types of filter on this column, you can bulk export or export this field data to a .CSV file, and add this column as part of a dashboard panel. The color of the values indicates: • Black: Jitter value is within the limits set by the High threshold for Jitter and Low threshold. • Red: Jitter value is greater than the value set in High threshold for Jitter. • Green: Jitter value is less than the value set in Low threshold for Jitter. For more information, see List of System Settings
Avg RTCP delay	The average round-trip delay time reported by RTCP.
Callee	The user to which the call is addressed. This is usually taken from the To header field of the first <i>call leg</i> .
Callee codecs	The comma delineated list of codecs proposed in the SDP body by the UAS. Usually this appears in the responses from INVITE transactions and the UAS includes a single codec in the answer, and this is the codec used in the call. On each <i>re-INVITE</i> from inside the dialog, this field is updated to the last proposed list of codecs. By default, this column is hidden.
Callee Initial codecs	The comma delineated list of codecs proposed in the SDP body by the UAS, usually in the first response from the 'INVITE' transaction. Unlike the Callee codecs , this field is not updated on <i>re-INVITES</i> . By default, this column is hidden.
Callee IP Address	The IP address of the called user that connected first. It is possible to filter this column by IP address or IP address mask. By default this column is hidden.
Callee User Agent	The <i>User-Agent</i> string advertised in the 200 OK message of the last <i>call leg</i> . This string usually contains the brand and the firmware version of the SIP device answering the call. If the User-Agent header is not present, the string is taken from the 'Server' header if present. By default, this column is hidden.
Caller	The user making the call. This is usually taken from the From header field of the first <i>call leg</i> .
Caller codecs	The comma delineated list of codecs proposed in the SDP body by the UAC, usually in the 'INVITE' message. On each <i>re-INVITE</i> from inside the dialog, this field is updated to the last proposed list of codecs. For example, this is useful for detecting T.38 calls. By default, this column is hidden.

Table 4-6 (Cont.) Recent Calls Table Columns

Column	Description
Caller Initial codecs	The comma delineated list of codecs proposed in the SDP body by the UAS, usually in the first 'INVITE' message. Unlike the Caller codecs , this field is not updated on <i>re- INVITEs</i> . This is useful for gathering statistics about the supported codecs. By default, this column is hidden.
Caller IP Address	The IP address of the device initiating the call. It is possible to filter this column by IP address or IP address mask. By default this column is hidden. Call time
Caller User Agent	The User-Agent string advertised in the 'INVITE' message from the first <i>call leg</i> . This string usually contains the brand and firmware version of the SIP device making the call. By default, this column is hidden.
Call time	If the call is <i>Finished</i> , this field represents the call length, measured from the 200 OK message of the INVITE transaction until the first BYE message. If the call is <i>Established</i> , this field represents the time elapsed since the call establishment (the arrival of the 200 OK message of the INVITE transaction) and it is updated on each refresh. If the call is not yet <i>Established</i> , this field is empty. This field has a precision of milliseconds but cannot be filtered for unless the call is <i>Finished</i> .
Call-Transfer	True if this call has been transferred using the call transfer capabilities in SIP.
Code	The <i>SIP response code</i> of the last received message from the 'INVITE' transaction. For <i>Failed</i> calls, this represents the <i>SIP error code</i> .
Diversion	Diversion URI of first Diversion header in call.
Diversion Type	Diversion type of first Diversion header in call. Possible values are: - deflection (CD) - do-not-disturb (DND) - follow-me - no-answer (CFNA) - time-of-day (CFTOD) - unavailable (CFUNV) - unconditional (CFUNC) - unknown: for unknown and all cases that could not be matched to any of the above - user-busy (CFB) - out-of-service
DPC	Destination Point Codes (DPC) contains the address of the destination for the ISUP call. This is always taken from the first ISUP leg seen by Operations Monitor.
DTMF	Displays 'Yes' if there is DTMF information available for this call. Unless the user has the correct rights this field will not be available.
Egress device(s)	This field contains a comma delineated list of the <i>egress devices</i> for the call, that is through which the call leaves the platform.
End timestamp	The timestamp of the message that closes the main leg of the call (usually the first BYE message).

Table 4-6 (Cont.) Recent Calls Table Columns

Column	Description
Gateway Devices	As the MEGACO Gateway column contains the IP address of the MEGACO Gate- way, the Gateway Devices column contains its name.
Ingress device(s)	This field contains a comma delineated list of the <i>ingress devices</i> for the call, that is through which the call enters the platform.
Initiator device	If the call was started from a <i>SIP device</i> of the platform (for example, a media server), this field contains the name of this device. The call must not be relayed by this device, but actually created by it. Otherwise, the field is empty. By default, this column is hidden.
KPI - RTCP Jitter threshold	Defines a threshold for the Jitter KPIs (in ms) based on RTCP. Any Jitter value above this threshold is ignored for the KPI computation. • Default value: 0 • Minimum value: 0 • Maximum value: 2000000 • 0 means no threshold
Max Jitter	The maximum of the measured jitter values of the 10 seconds intervals. You can apply different types of filter on this column, you can export this field data to a .CSV file, and add this column as part of a dashboard panel. The color of the values indicates: • Black: Jitter value is within the limits set by the High threshold for Jitter and Low threshold. • Red: Jitter value is greater than the value set in High threshold for Jitter. • Green: Jitter value is less than the value set in Low threshold for Jitter. For more information, see List of System Settings . By default, this column is not displayed in the Recent Calls table. Add it using the Set Columns feature.
Max RTCP delay	The maximum round-trip delay time reported by RTCP.
Media Bypass	Indicates if the Direct Routing calls has Media bypass “Enabled” or “Disabled” for Direct Routing calls. Shows “NA” for non-Direct Routing calls.
Media Recording	Indicates if RTP recordings were requested for this call.
Media types	Indicates the media types that were negotiated in the call. Multiple media types are separated by a comma (for example: audio, video).
MEGACO Commands	Commands placed by the MEGACO Gateway Controller to the MEGACO Gateway in a transaction. For example, Commands exist to add/modify/subtract Terminations from the Context. See Figure 4-25 .
MEGACO Context ID	Defines an identifier for each MEGACO connection. See Figure 4-25 .
MEGACO Gateway	IP address of the MEGACO Gateway.
MEGACO Gateway Controller	IP address of the MEGACO Gateway Controller.
MEGACO Termination ID	A MEGACO TerminationID is defined for a PSTN line, a channel in a Trunk or rtp stream. Their format is a string like: line/1 or rtp/1 for RTP streams. See Figure 4-25 .
MEGACO Transaction IDs	A MEGACO Transaction is identified by a Transaction ID. See Figure 4-25 .
MGCP Call IDs	Hexadecimal strings of maximum of 32 characters that identify uniquely a call. See Figure 4-26 .
MGCP Capabilities	Defines the capabilities of the endpoints. See Figure 4-26 .
MGCP Connection IDs	The connection identifier is encoded as a hexadecimal string, at most 32 characters in length. See Figure 4-26 .

Table 4-6 (Cont.) Recent Calls Table Columns

Column	Description
MGCP Gateway IP	IP address of the MGCP Gateway.
Min. MOS	The minimum value of the voice quality estimation for Finished calls. If Operations Monitor does not receive RTP traffic, or the RTP module is not loaded, this field is empty. The value is displayed in green, orange, or red depending on the thresholds set in the system options High Threshold for MOS and Low Threshold for MOS . For more information on how Operations Monitor estimates the MOS value of a call, see " Voice Quality ".
Negotiated Codecs	For every call, a codec is negotiated while establishing the media. This Negotiated Codec data for a call is displayed. For more information on supported codecs, see Supported Codecs .
OPC	Originating Point Codes (OPC) contains the address of the originator for the ISUP call. This is always taken from the first ISUP leg seen by Operations Monitor.
Packet Loss Rate (%)	The number of received RTP packets divided by the number of expected RTP packets. By default, this column is not displayed in the Recent Calls table. Add it using the Set Columns feature. You can filter Calls data by applying the different types of filter on this column, you can bulk export or export this field data to a .CSV file, and add this column as part of a dashboard panel.
P-Asserted-ID	The content of the P-Asserted-ID header from the initial INVITE SIP request.
Preferred Callee Number?	The number of the callee determined by the configurable number determination mechanism, if available.
Preferred Caller Number?	The number of the caller determined by the configurable number determination mechanism, if available.
Prefix Group	Prefix Tags matching this call (0 to n tags).
Q.850 Code	Q.850 cause code for the ISUP call.
Q.850 Details	Q.850 Details for the ISUP call.
Q.850 State	Q.850 State for the ISUP call.
Reason	The content of the Reason header from the BYE, CANCEL, SIP request or from a failure SIP reply.
Remote-Party-ID	The content of the Remote-Party-ID or P-Preferred-Identity header from the initial INVITE SIP request.
RTCP streams	The number of RTCP streams belonging to the call.
Segments	The number of <i>call legs</i> in this <i>call</i> . By default, this column is hidden.
Setup Delay	This field represents the time elapsed between the initial 'INVITE' message and the first valid network response, like '180 Ringing', '183 Session in progress', '480 Temporarily Unavailable', etc. It fulfills Session Request Delay for RFC6076. If the call contains ISUP, <i>Setup Delay</i> is computed on the first SIP leg. This field has a precision of milliseconds. By default, this column is hidden.
Setup Delay Type	Shows the type of <i>Setup Delay</i> computed. Can be 'Successful Session Request Delay' or 'Failed Session Request Delay'. By default, this column is hidden.

Table 4-6 (Cont.) Recent Calls Table Columns

Column	Description
Setup time	If the call is <i>Established</i> or <i>Finished</i> , this field represents the time elapsed between the initial INVITE message and the call establishment, marked by the 200 OK answer in the INVITE transaction. If the call is not yet <i>Established</i> , this field is empty. This field has a precision of milliseconds. By default, this column is hidden.
Start timestamp	The timestamp of the first INVITE or IAM message from the call.
State	A short text representation of the call state. For more information on the possible values for this field, see " Call States ".
State details	Extra details about the call state. For example, the state of a call can be <i>Proceeding</i> , and this field adds the information: ACK seen, but no final answer. For more information on the possible values for this field, see " Call States ".
Terminator device	If the call was ended by a <i>SIP device</i> (for example a media server), this field contains the name of the device. The call must not be relayed by this device, but actually terminated by it. Otherwise, the field is empty. By default, this column is hidden.
Transcoded Call	Displays a Yes/No value to indicate if the call was Transcoded or not.
UCaaS CCaaS Originating	This field is populated as "TEAMS_DR" when the call is identified as originated from MS Teams and terminating at PSTN (MS Teams to PSTN call)
UCaaS CCaaS Terminating	This field is populated as "TEAMS_DR" when the call is identified as originated from PSTN and terminating at MS Teams (PSTN to MS Teams call)

Figure 4-24 Recent Calls Table

Caller	Callee	Start timestamp	End timestamp	Segment s	Avg. MOS	State	P-RC-Media-Location	Call-ID	Request-URI	Transcoded Call	Negotiated Codecs	Contact
550015169192	666015169194	2024/12/20 11:08:19		1		Failed	ia001	e776a0@10.0.0.3	sp:66601...			<sp:5500151691
111015169191	222015169193	2024/12/20 11:08:19		1		Failed	ia001	e776a7@10.0.0.2	sp:22201...			<sp:1110151691
333015169190	444015169192	2024/12/20 11:08:19		3		Failed	ia001	e776a6@10.0.0.1,e776a6@10.2...	sp:44401...			<sp:3330151691
550015169189	666015169191	2024/12/20 11:08:19		4		Failed	ia001	e776a5@10.0.0.10,e776a5@10.2...	sp:66601...			<sp:5500151691
111015169188	222015169190	2024/12/20 11:08:19	2024/12/20 11:08:29	3		Off-line	ia001	e776a4@10.0.0.5,e776a4@10.2...	sp:22201...			<sp:1110151691
111015169182	222015169184	2024/12/20 11:08:19		1		Failed	ia001	e7769e@10.4.0.23	sp:22201...			<sp:1110151691
111015169182	222015169184	2024/12/20 11:08:19		1		Failed	ia001	e7769e@10.4.0.23	sp:22201...			<sp:1110151691
333015169187	444015169189	2024/12/20 11:08:19		3		Failed	ia001	e776a3@10.0.0.8,e776a3@10.2...	sp:44401...			<sp:3330151691
111015169182	222015169184	2024/12/20 11:08:19		1		Failed	ia001	e7769e@10.4.0.23	sp:22201...			<sp:1110151691
550015169186	666015169188	2024/12/20 11:08:19		4		Failed	ia001	e776a2@10.0.0.7,e776a2@10.2...	sp:66601...			<sp:5500151691
111015169185	222015169187	2024/12/20 11:08:19		4		Failed	ia001	e776a1@10.0.0.6,e776a1@10.2...	sp:22201...			<sp:1110151691
333015169184	444015169186	2024/12/20 11:08:19		4		Failed	ia001	e776a0@10.0.0.5,e776a0@10.2...	sp:44401...			<sp:3330151691
550015169183	666015169185	2024/12/20 11:08:19		6		Failed	ia001	e7769f@10.0.0.4,e7769f@10.2...	sp:66601...			<sp:5500151691
111015169182	222015169184	2024/12/20 11:08:19		6		Failed	ia001	e7769e@10.0.0.3,e7769e@10.2...	sp:22201...			<sp:1110151691
333015169181	444015169183	2024/12/20 11:08:19		6		Failed	ia001	e7769a@10.0.0.2,e7769a@10.2...	sp:44401...			<sp:3330151691
550015169180	666015169182	2024/12/20 11:08:19		12		Failed	ia001	e7769c@10.0.0.1,e7769c@10.2...	sp:66601...			<sp:5500151691
111015169179	222015169181	2024/12/20 11:08:19		6		Failed	ia001	e7769b@10.0.0.10,e7769b@10.2...	sp:22201...			<sp:1110151691
333015169178	444015169180	2024/12/20 11:08:19		6		Failed	ia001	e7769a@10.0.0.9,e7769a@10.2...	sp:44401...			<sp:3330151691

This graphic shows examples of MEGACO call details in the **Recent Calls** panel.

Figure 4-25 MEGACO Details in the Calls Panel

MEGACO Gateway	MEGACO Gateway Controller	MEGACO Termination ID	MEGACO Context ID	MEGACO Commands	MEGACO Transaction IDs
10.254.12.20	10.254.11.1	rtp/2/0/3702	14172	Request-Add,Reply-Add,Request-Modify,Reply-Modify,Request-Subtract,Reply-Subtract,	2463,2464,2514,257
10.254.12.20	10.254.11.1	rtp/2/0/3702	14172	Request-Add,Reply-Add,	246
10.254.12.20	10.254.11.1	rtp/2/0/3702	14172	Request-Add,Reply-Add,Request-Modify,Reply-Modify,Request-Subtract,Reply-Subtract,	2463,2464,2514,257
10.254.12.20	10.254.11.1	rtp/2/0/3702	14172	Request-Add,Reply-Add,	246

Figure 4-26 MGCP Details in the Calls Panel

MGCP Call IDs	MGCP Gateway IP	MGCP Capabilities	MGCP Connection IDs
193.84.65.202_0001d6b4000000c900000000c,	193.84.65.202		3512013,
193.84.65.202_0001d6b4000000c900000000c,	193.84.65.202		3512013,
193.84.65.202_0001d6b4000000c900000000c,	193.84.65.202		3512013,

Note

To save horizontal space, several columns are hidden by default. To enable the hidden columns, click Set Columns. For more information, see "[Tables](#)".

Recent Calls													
Details ... Type to filter eg- callee=575, caller=115													
	Caller	Callee	Start timestamp	End timestamp	Segment s	Avg. MOS	State	P-RC-Media-Location	Call-ID	Request-URI	Transcoded Call	Negotiated Codescs	Contact
☐	555015169192	666015169194	2024/12/20 11:08:19		1		Failed	lad01	e776a0@10.0.0.3	sp:66601...			<sp:5550151691
☐	111015169191	222015169193	2024/12/20 11:08:19		1		Failed	lad01	e776a7@10.0.0.2	sp:22201...			<sp:1110151691
☐	333015169190	444015169192	2024/12/20 11:08:19		3		Failed	lad01	e776a0@10.0.0.1,e776a0@10.2...	sp:44401...			<sp:3330151691
☐	555015169189	666015169191	2024/12/20 11:08:19		4		Failed	lad01	e776a5@10.0.0.10,e776a5@10.2...	sp:66601...			<sp:5550151691
☒	111015169188	222015169190	2024/12/20 11:08:19	2024/12/20 11:08:29	3		Off-line	lad01	e776a4@10.0.0.9,e776a4@10.2...	sp:22201...			<sp:1110151691
☐	111015169182	222015169184	2024/12/20 11:08:19		1		Failed	lad01	e7769e@10.0.0.23	sp:22201...			<sp:1110151691
☐	111015169182	222015169184	2024/12/20 11:08:19		1		Failed	lad01	e7769e@10.0.0.23	sp:22201...			<sp:1110151691
☐	333015169187	444015169189	2024/12/20 11:08:19		3		Failed	lad01	e776a3@10.0.0.8,e776a3@10.2...	sp:44401...			<sp:3330151691
☐	111015169182	222015169184	2024/12/20 11:08:19		1		Failed	lad01	e7769e@10.0.0.23	sp:22201...			<sp:1110151691
☐	555015169186	666015169188	2024/12/20 11:08:19		4		Failed	lad01	e776a2@10.0.0.7,e776a2@10.2...	sp:66601...			<sp:5550151691
☐	111015169185	222015169187	2024/12/20 11:08:19		4		Failed	lad01	e776a1@10.0.0.6,e776a1@10.2...	sp:22201...			<sp:1110151691
☐	333015169184	444015169186	2024/12/20 11:08:19		4		Failed	lad01	e776a0@10.0.0.5,e776a0@10.2...	sp:44401...			<sp:3330151691
☐	555015169183	666015169185	2024/12/20 11:08:19		6		Failed	lad01	e7769d@10.0.0.4,e7769d@10.2...	sp:66601...			<sp:5550151691
☐	111015169182	222015169184	2024/12/20 11:08:19		6		Failed	lad01	e7769e@10.0.0.3,e7769e@10.2...	sp:22201...			<sp:1110151691
☐	333015169181	444015169183	2024/12/20 11:08:19		6		Failed	lad01	e7769d@10.0.0.2,e7769d@10.2...	sp:44401...			<sp:3330151691
☐	555015169180	666015169182	2024/12/20 11:08:19		12		Failed	lad01	e7769c@10.0.0.1,e7769c@10.2...	sp:66601...			<sp:5550151691
☐	111015169179	222015169181	2024/12/20 11:08:19		6		Failed	lad01	e7769b@10.0.0.10,e7769b@10.2...	sp:22201...			<sp:1110151691
☐	333015169178	444015169180	2024/12/20 11:08:19		6		Failed	lad01	e7769a@10.0.0.9,e7769a@10.2...	sp:44401...			<sp:3330151691

Filtering

You can filter the columns of the **Recent calls** table for specific criteria. When you apply a filter, the **Load Filters** list displays the name of the filter.

Filter Properties

Search on Enter Key

Filter the record after the user presses the Enter key rather than as the user types. This option is checked by default but disabled for Advanced Filter.

Note

The **Search on Enter Key** check box is also available for both the User Calls window in the User Tracking section and the Calls window in the IP Tracking section.

Applying a Simple Filter

To apply a simple filter:

1. From the navigation list, select **Calls**.
2. On the **Recent calls** table, select the list of options on a desired column.
3. Click the **Filters** button.
4. In the Filters dialog box, Enter or select the filter criteria for the filter.
The table is filtered for the criteria and the toolbar displays the label **SIMPLE**.

The following graphic shows an example of a filter applied to the **Call time** column of the **Recent calls** table.

Figure 4-27 Applying a Filter

	Callee	Start timestamp	End timestamp	Call time	Media Recording	Segments	Code	Ingress device(s)	Egre
	444015169153	2024/12/20 11:08:19			No	4	100	dev_p1_272	
	666015169152	2024/12/20 11:08:19							
	222015169151								
	444015169150								
	666015169149								
	222015169148								
	444015169147								
	666015169146								
	222015169145								
	444015169144								
	666015169143								
	222015169142								
	444015169141								
	666015169140								
	222015169139								
	444015169138								
	666015169137								
	222015169136								

Track Caller 111015169134
Create trace with 111015169134
Track Callee 222015169136
Create trace with 222015169136
Record media of caller 111015169134
Record media of callee 222015169136
Call details window
Message flow
Download Message Flow
PDF report
Filter table for ...

Caller : 111015169134
Callee : 222015169136
Call time :
Preferred Caller Number? : No
Caller IP address : 10.0.0.5
Preferred Callee Number? : No
Callee IP address :
Media Recording : No
Setup time :
Setup Delay :
Setup Delay Type :
Segments : 6
Code : 100

Changing a Simple Filter to an Advanced Filter

To change a simple filter to an advanced filter:

1. On the **Recent Calls** table toolbar, click **Edit Advanced**.
The **(Unnamed Filter)** dialog box appears.
2. Click **+**. A list of filter fields appears.
3. Select the fields to include in the advanced filter.
4. Click **Save**.
The **Save filters** dialog box appears.
5. Enter a name for the filter.
6. Click **Save**.
The dialog box now displays the name you assigned the advanced filter.
7. Click **Hide** which closes the dialog box.

Text-Based Filter Fields

Some text-based filter fields can accept queries. In text-based filter fields, you can enter REGEX pattern matching or SQL pattern matching to filter recent calls. REGEX filtering provides slower search times than SQL filtering.

To enter REGEX pattern matching to filter calls, enter the **.*** character combination before the search values.

When regular expressions are filtered, expressions supported are the same as MySQL 5.5.

The following example uses the REGEX filter:

```
.*[0049]
```

To enter SQL pattern matching to filter calls, there are two methods. SQL filtering is faster and more efficient than the REGEX pattern matching. SQL pattern matching is triggered as follows:

- Entering the SQL wildcard character % into the search field. It can be placed in front of or following the filter value.
- Entering ^ at the beginning of a string.

[Table 4-7](#) describes the SQL search filters and provides examples of usage.

Table 4-7 SQL Filter Conditions

Search Filter	Search Example	Description
(none)	0049	Filters for strings that contain 0049.
^	^0049	Filters for strings that begin with 0049.
%	0049% or %0049	Filters for strings that begin with 0049. Filters for strings that end with 0049.

The following graphic shows an example of filtering that selects all finished calls. After the filter is set and the view is refreshed, the total number of finished calls is displayed in the bottom-right corner.

Figure 4-28 Filter All Finished Calls

Caller	Callee	Start timestamp	End timestamp	Call time	Media Recording	Segments	Code	Ingress device(s)	Egress device(s)	DTMF	Diversion	Diversion Type	Call-Transfer	Min. MOS	Avg. MOS	State	State details
333015168866	444015168866	2024/12/20 11:08:18	2024/12/20 11:08:19	0'20ms	No	12	200	dev_p1_267	dev_p2_67, dev_s2_347, dev_s1_387							Finished	
333015168854	444015168856	2024/12/20 11:08:18	2024/12/20 11:08:19	0'20ms	No	12	200	dev_p1_255	dev_p2_55, dev_s2_335, dev_s1_375							Finished	
555015168853	666015168855	2024/12/20 11:08:18	2024/12/20 11:08:19	0'20ms	No	12	200	dev_p1_254	dev_p2_54, dev_s2_334, dev_s1_374							Finished	
111015168840	222015168842	2024/12/20 11:08:18	2024/12/20 11:08:19	0'20ms	No	12	200	dev_p1_241	dev_p2_41, dev_s2_321, dev_s1_361							Finished	
111015168831	222015168833	2024/12/20 11:08:18	2024/12/20 11:08:19	0'20ms	No	12	200	dev_p1_272	dev_p2_32, dev_s2_352, dev_s1_392							Finished	
555015168829	666015168831	2024/12/20 11:08:18	2024/12/20 11:08:19	0'20ms	No	12	200	dev_p1_270	dev_p2_30, dev_s2_350, dev_s1_390							Finished	
555015168805	666015168807	2024/12/20 11:08:18	2024/12/20 11:08:19	0'20ms	No	12	200	dev_p1_246	dev_p2_6, dev_s2_326, dev_s1_366							Finished	

The filtered columns can also be combined to provide more precise answers. For example, to limit the table to all finished calls initiated by a specific device say B2BUA1, set the following filters:

- **State to Finished.**
- **Ingress device to B2BUA1.**
- **End timestamp to before 15:35**

In this table, filtering can be set from the right-click menu. For more information, see [Right-click Menu](#).

Figure 4-29 Filters - Finished Calls by B2BUA1 ending before 15:35

Start timestamp	End timestamp	Call time	Media Recording	Segments	Code	Ingress device(s)	Egress device(s)	DTMF	Diversion	Diversion Type	Call-Transfer	Min. MOS	Avg. MOS	State	State details	Call-ID
2024/12/20 11:08:15	2024/12/20 11:08:16	0*20ms	No	12	200	dev_p1_256	dev_p2_16, dev_s2_336, dev_s1_376							Finished		e7716f@10.0.0.6,e7
2024/12/20 11:08:14	2024/12/20 11:08:15	0*20ms	No	12	200	dev_p1_256	dev_p2_16, dev_s2_336, dev_s1_376							Finished		e7707f@10.0.0.6,e7
2024/12/20 11:08:14	2024/12/20 11:08:15	0*20ms	No	12	200	dev_p1_256	dev_p2_56, dev_s2_336, dev_s1_376							Finished		e77057@10.0.0.6,e7
2024/12/20 11:08:09	2024/12/20 11:08:11	0*20ms	No	12	200	dev_p1_256	dev_p2_16, dev_s2_336, dev_s1_376							Finished		e76b7f@10.0.0.6,e7
2024/12/20 11:08:09	2024/12/20 11:08:10	0*20ms	No	12	200	dev_p1_256	dev_p2_56, dev_s2_336, dev_s1_376							Finished		e76b07@10.0.0.6,e7
2024/12/20 11:08:09	2024/12/20 11:08:10	0*20ms	No	12	200	dev_p1_256	dev_p2_16, dev_s2_336, dev_s1_376							Finished		e76a8f@10.0.0.6,e7
2024/12/20 11:08:06	2024/12/20 11:08:07	0*20ms	No	12	200	dev_p1_256	dev_p2_56, dev_s2_336, dev_s1_376							Finished		e76747@10.0.0.6,e7
2024/12/20 11:08:03	2024/12/20 11:08:04	0*20ms	No	12	200	dev_p1_256	dev_p2_16, dev_s2_336, dev_s1_376							Finished		e763af@10.0.0.6,e7

Filtering for this field is done in seconds. For example, the graphic shows all calls that lasted more than 6 seconds are selected.

Figure 4-30 Filtering By Call Length

Filters Call time

Call

Call time

Call-ID

Call-Transfer

Callee

Callee Codecs

Callee IP address

Callee Initial Codecs

Call time

<

>

Enter Number...

6

Clear

Reset

Apply

Note

When filtering for call length, only the finished calls are considered. Thus, it is not possible to filter for all the established calls with a certain call length.

To filter the calls list for calls that contain RTP streams, use **Media types** filter. You can set the **Media types** filter to list the calls that contain audio, video, text, image, application, message, or other media type.

When Media types filter is used, any call that contains any of the media types is listed. For instance, when the filter is set to **audio**, any call where audio is one of the media types that was negotiated in the call is listed, for example, a call containing audio and video.

When multiple media types are set in the filter, for example **image** and **video**, any call where image or video is one of the media types that was negotiated in the call is listed, for example, a call containing image and audio.

Advanced Filtering

You can create advanced filters to filter the **Recent calls** table for specific combinations of results. Advanced filters enable you to select a specific combination of columns from the **Recent calls** table, then enter criteria against which to filter for matching calls.

See [Table 4-6](#) for details on the metrics available in the **Recent calls** table columns.

Some filter types require that you customize the logic that is applied in the filter. You can customize the logic by toggling options or entering specific criteria to be matched in each advanced filter you create. The logic that can be customized depends on the combination of filters selected.

When an advanced filter has been created, the **Filters** toolbar displays the label **ADVANCED**.

Note

Advanced filtering requires higher resource consumption. Complex advanced filters utilize more system resources and may impact overall system performance.

Working with advanced filters involves the following tasks:

- [Creating an Advanced Filter](#)
- [Adding Criteria to an Advanced Filter](#)
- [Adding Scope to an Advanced Filter](#)
- [Editing an Advanced Filter](#)
- [Applying an Advanced Filter](#)
- [Clearing Advanced Filters](#)

Creating an Advanced Filter

To create an advanced filter:

1. From the navigation list, select **Calls**.
2. On the **Filters** toolbar, click **Clear** which removes any applied filters.
3. On the **Filters** toolbar, click **Edit Advanced**.
The **(Unnamed Filter)** dialog box appears.
4. Click **+**.
A list of filter fields appears.
5. Select fields to include in the advanced filter.
6. Click **Save**.
The **Save filters** dialog box appears.
7. In the **Name** field, enter a name for the filter.
8. Click **Save**.

The **(Unnamed Filter)** dialog box is now named the title you assigned the advanced filter.

9. Click **Hide** which closes the dialog box.

Adding Criteria to an Advanced Filter

To add criteria to an advanced filter:

1. From the **Filters** list, select an advanced filter.
2. Click **Edit Advanced**.

A filter dialog box appears.

3. Click **+**.
4. Select fields to include in the advanced filter.

Repeat this step to add additional fields.

✓ Tip

You can drag column headings from the **Recent calls** table into the dialog box.

5. In the filter dialog box, customize the logic of the filter you choose by entering or selecting logic values to filter for.
6. Click **Save**.
7. Do one of the following:
 - Click **Apply Now** which applies the filter to the **Recent calls** table.
 - Close the dialog box and apply the saved filter at a later time.

Adding Scope to an Advanced Filter

You could create an expression with criteria **a**, **b**, and **c**. You can include brackets in the filter criteria to isolate terms that are dependent on each other, such as:

(a = 2 AND b = 4) OR c = 10

or

a = 2 AND (b = 4 OR c = 10)

To add scope to an advanced filter:

1. From the **Filters** list, select an advanced filter.
2. Click **Edit Advanced**.
The filter dialog box appears.
3. Click **()** in the row you want to add scope to.
4. Click **+** in the same row and insert filter conditions.

① Note

You can move filter criteria within a dialog box by dragging it to a new area.

 Tip

You can drag criteria in to or out of bracketed statements.

5. Click **Save**.
6. Do one of the following:
 - Click **Apply Now** to apply the filter to the **Recent calls** table.
 - Close the dialog box and apply the saved filter at a later time.

Editing an Advanced Filter

To edit an advanced filter:

1. From the **Recent calls** window, select an advanced filter.
2. Click **Edit Advanced**.
The filter dialog box appears.
3. Edit the filter criteria.
4. Click **Save**.
5. Do one of the following:
 - Click **Apply Now** to apply the filter to the **Recent calls** table.
 - Close the dialog box and apply the saved filter at a later time.

Applying an Advanced Filter

To apply an advanced filter:

1. From the **Recent calls** window, select an advanced filter.
2. Click **Edit Advanced**.
A filter dialog box appears.
3. Click **Apply Now** and close the dialog box.

Clearing Advanced Filters

To clear advanced filters:

1. From the **Filters** toolbar, select **Clear**.

Filters - Column Header

Another method of filtering is using the column header search.

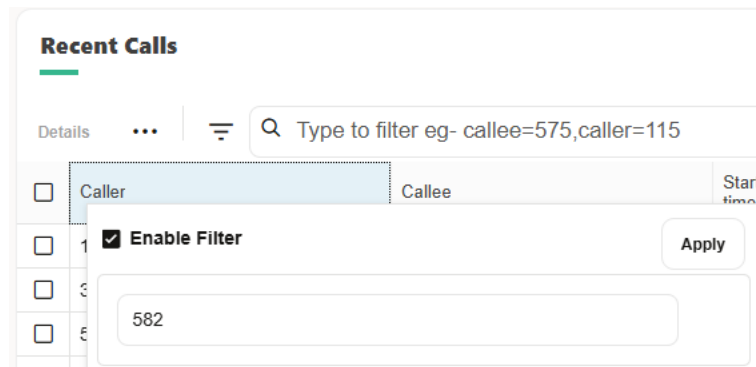
Use the Column Header to filter data.

 Note

You can resize columns, and the adjustments persist even after you navigate away. On returning to the page, the column resizing is saved.

1. Double-click a column header.

Figure 4-31 Creating a Filter - Column Header



2. Add the filter criteria. For example where the caller column contains 582.
3. Select the **Enable Filter** check box.
4. Verify that the search results meets the filter search criteria.
5. You can proceed to perform any of the following tasks:
 - a. Click **Save** to save the filter.
 - b. Click **Clear** to clear the filter.

If you export the filter results to the Dashboard panel, the Dashboard panel displays the filter results. This is also applicable for Bulk Export of Calls, CSV Export.

You can also use this method to filter data in the following pages:

- **Calls**
- **Registrations**
- **Subscriptions**
- **User Calls** section in the User Tracking
- **Calls** section in the IP Tracking
- All Tabs on the **Devices** pages
- Dashboard Panels for Calls, Registrations and Subscriptions

Text-Based Filtering

You can filter data in the Calls page using the Text-based Filter.

To use the text-based filtering:

1. In the **Calls** page, click in the **Filter** text box.
2. Type in the filter criteria. For example: Callee=89.

Figure 4-32 Text-box Based Filter

Recent Calls

Details ...

Q Caller=555,Code=200

ⓧ ⓘ SIMPLE (None)

☐	Caller	Callee	Start timestamp	End timestamp	Call time	Media Recording	Segments	Code
☐	555015168853	666015168855	2024/1...	2024/1...	0'...	No	12	200
☐	555015168829	666015168831	2024/1...	2024/1...	0'...	No	12	200

3. Press the Enter key.
Call details satisfying the filter criteria are displayed.
4. Click X to clear the filter.

ⓘ Note

Placing the cursor in the **Filter** text box lists all previously defined filters.

Right-Click Menu

Right-clicking a row in the **Recent calls** table shows the following contextual options:

Figure 4-33 Right-click menu options

	Start timestamp	End timestamp	Call time	Media Recording	Segments	Code	Ingress device(s)	E
1					Segments : 6			273
}					Code : 100			272
2					Initiator device :			271
					Terminator device :			270
}					Caller User Agent : zmqreplay			269
1					Callee User Agent :			268
}					Caller Codecs : PCMA,PCMU,telephone-event			267
1					Callee Codecs :			266
}					Caller Initial Codecs : PCMA,PCMU,telephone-event			265
1					Callee Initial Codecs :			264
}					Ingress device(s) : dev_p1_260			263
1					Egress device(s) : dev_p2_60			262
}					DTMF :			261
2								260
	2024/12/20 11:08:19			No	6	100	dev_p1_260	d
}	2024/12/20 11:08:19			No	6	100	dev_p1_259	d

Table 4-8 Right-click Context Menu

Menu Option	Description
Track caller	Opens the User Tracking page, pre-filled with the caller user of the selected call. For more information, see " User Tracking ".
Create trace with <caller number>	Opens the Traces page, pre-filled with the caller user of the selected call. For more information, see " Traces ".
Track callee	Displays the User Tracking page, pre-filled with the callee user of the selected call. For more information, see " User Tracking ".
Create trace with <callee number>	Opens the Traces page, pre-filled with the callee user of the selected call. For more information, see " Traces ".
Record media of caller	Record media for a new user window is displayed, with the caller number populated in the User field, for 2 days and Audio as the default options.
Record media of callee	Record media for a new user window is displayed, with the callee number populated in the User field, for 2 days and Audio as the default options.
Call details window	Opens the Call Details Window . For more information, see Call Info or Call Details Window .
Message Flow	Shows the <i>message flow diagram</i> for the selected call. For more information, see Working with Message Flows .
Download Message Flow	Enables you to download the message flow as an HTML file to your local hard drive.
PDF report	Creates a PDF report for the selected call. A dialog appears that allows the user to select the information to include, and to provide a comment to add to the report.
Filter table for ...	Shortcut to <i>column filters</i> . This gives a convenient way of finding calls that are similar with the one selected.

Figure 4-34 PDF Report Creation Dialog

Create Report

Report Contents

☒ Call Information

☒ Link Quality Information

☒ Voice Quality Information

☒ Detailed RTCP information

☒ DTMF information

☒ Messages

☒ Include Company Logo

☒ Include Graph

☐ Combine identical

☐ Use Device Order

☐ Transport protocol

☐ IP addresses

☐ Codecs

☐ Time spans

☐ Show Media

☐ Unwind messaging

☐ SIP URIs

☐ VLAN

☐ MAC addresses

☐ Absolute times

☐ Resolve IP addresses

☐ Show DTMF Information

Additional Info

Report Comment (optional):

Filename (optional):

Create

Reset

Cancel

Exclusion of Numbers

The **Set Call Exclusions** feature enables users to manage the exclusion of caller and callee numbers, with a maximum of five excluded numbers per category (Caller, Callee, or Both).

Users can add numbers to the exclusion list by specifying the exclusion category. If the limit of five excluded numbers is reached in a category, additional numbers can still be added but will be marked as "Not Excluded" until a slot is freed. To exclude a new number after reaching the limit, users must change one of the currently excluded numbers to "Not Excluded." Numbers can also be completely removed from the list using the delete option.

Configuring Set Call Exclusions

Excluding a number from the Recent Calls table hides any rows containing the specified number, ensuring that it is not included in the current view.

To exclude numbers from the **Recent Calls** table view:

1. In the **Recent Calls** table, click **Set Call Exclusions**.

Table 4-9 Reasons

Scenario	Cause
Unable to see Set Call Exclusions menu option.	Ensure that you have added either the Caller or Callee columns to the Recent Calls table using the Set Columns option.

Table 4-9 (Cont.) Reasons

Scenario	Cause
Unable to select the Caller option in the Exclude Number dialog box	- Check that you have added the Caller column using the Set Columns option. - Also check that you have the permission for the Caller column in the Calls Field Permission setting in Settings > User Management.
Unable to select the Callee option in the Exclude Number dialog box	- Check that you have added the Callee column using the Set Columns option. - Also check that you have the permission for the Callee column in the Calls Field Permission setting in Settings > User Management.

2. In the **Exclude Number** dialog box, add the number in the **Enter a Number to be Excluded** box.

- a. Select a category: Caller, Callee, or Both. Click **Apply** to save the changes.
- b. The number is added to the selected category.

The number is now hidden from view in the Recent Calls table.

Points to Note

- A maximum of 5 numbers can be added at a time from the Caller or Callee list.
- If there are already five numbers excluded, you will need to free a slot from an existing excluded number, to add a new number. else the new number moves to a 'Not Excluded' state. "Not Excluded" keeps a number in the list but allows the corresponding rows to be displayed in the table again.
- The X of Y numbers excluded displays the number of entries excluded.

To remove a number from the exclusion list entirely, click the Bin icon next to that number to delete it.

Number Exclusion Using Regex

Information on Number Exclusion Works Using Regex.

When a number (For example, +149302) is added to the exclusion list:

- A Regex pattern uses a negative lookahead to exclude matching numbers.
- The generated Regex pattern looks like: `^(?!\\+49302).*$`
- When you exclude a number like +49302, the system builds a pattern to filter out anything that starts with that number and that number itself if it exists in the table. Hence:
 - +49302 → excluded
 - +493020001 → excluded
 - +4930212345 → excluded
 - +49303 → included
 - +49123 → included
- This approach ensures all numbers that begin with the excluded prefix are filtered out automatically.

- You can exclude broad number patterns by entering only a starting pattern. For example, +49302. or the exact numbers to be excluded.

Paging

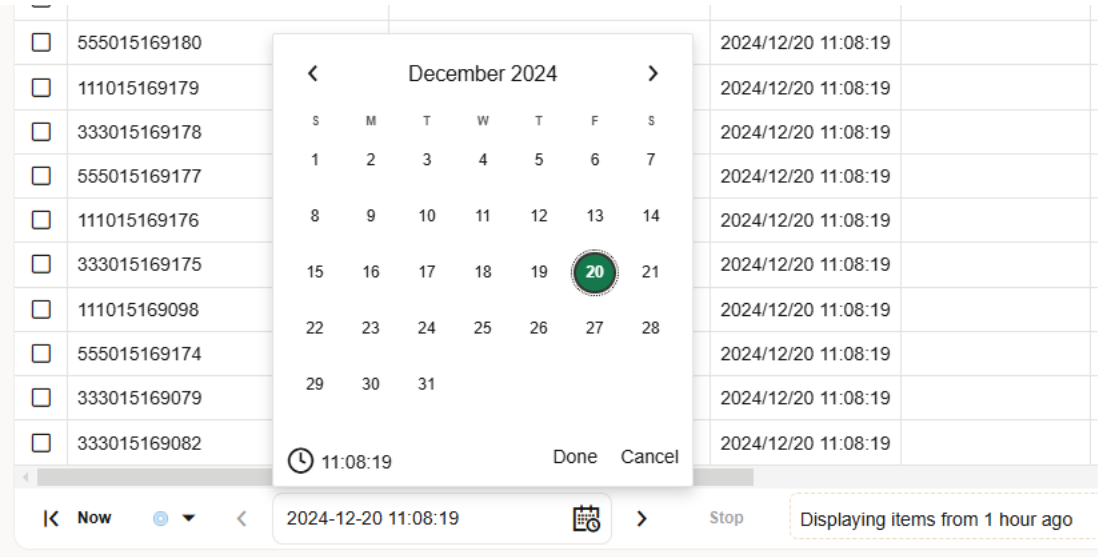
The paging bar allows you to navigate the entries. With the **Newer** and **Older** buttons you can step to the next page of newer respective older entries.

Figure 4-35 The Paging Bar



The **Now** button takes you to the first page, showing the newest entries. The date picker allows you to chose an arbitrary first date and time of the time period you want to view.

Figure 4-36 The Date Picker



The loading bar will show when entries are being fetched. To fill up a page while applying filters, this might require several calls to the server and might take some time. The blue bar in the loading bar shows the range that has been searched.

The **Refresh** button reloads the current entries and shows their updated states.

You can also set the refresh button to auto-refresh mode.

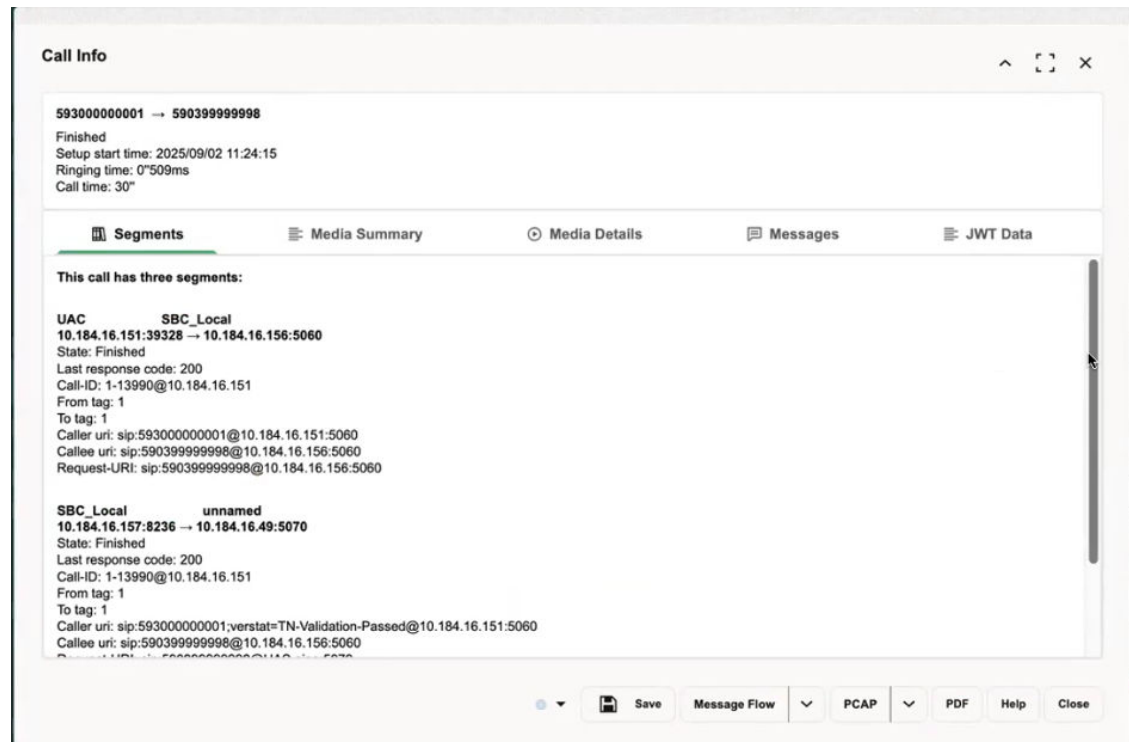
Note

The auto-refresh mode in combination with filtering of a grid can lead to longer refresh times than selected.

Call Info or Call Details Window

To open the call details panel, double-click on a row from the **Recent Calls** table or click the **Details** button from the toolbar. You can also access the call details panel from the **Media Summary** page. For more information, see [Voice Quality](#).

Figure 4-37 Call Info/Details Window



Note

It is possible that the number of segments for a call in the **Call Info** screen are more than the number of calls shown in Recent Calls screen. This is because the information displayed in Call Info screen is obtained by connecting to other nodes in order to retrieve the external segments from other nodes.

The Call Info window contains four tabs:

- **Segments**
- **Media Summary**
- **Media Details**
- **Messages**
- **Meta Data** This tab displays the Meta Data content received from the UCaaS CCaaS service for a correlated Direct Routing call. This is additional information that you can now access with UCaaS CCaaS feature to support end-to-end visibility of a Direct Routing call. This tab is visible only if you have enabled the **UCaaS CCaaS** extension from the Platform Setup Application.

For more information, see [UCaaS CCaaS Monitoring](#).

- **JWT** Displays decoded header and payload for regular JWTs (compact forms not supported).

Note

The JWT tab is seen only when the Stir/Shaken Setting is enabled at PSA.

- **HTTP** Message visibility, which includes Segment info, Request/response Type, and Protocol. Message flow enhancements highlighting HTTP verification and signing.

Call Details Toolbar

You can save the call details for debugging later.

Click the **Save** button to save all the call details, including the raw messages and voice quality information.

Click the **PCAP** button to download the raw signaling messages and the media streams of a call into PCAP file format. See the [Downloading Call Details to a PCAP File](#) for more information.

Click the **PDF** button to create a PDF report for the call with details about segments, raw messages and voice quality information.

Click the **Message flow** button to open the **message flow** diagram.

Segments

The **Segments** tab shows details about each call leg within the call, including:

1. Platform Device name
2. Source and destination devices set with Platform Devices.
3. State
4. Last response code
5. Call-ID
6. From tag
7. To tag
8. Caller uri
9. Callee uri
10. Request-URI
11. Caller device
12. Callee device

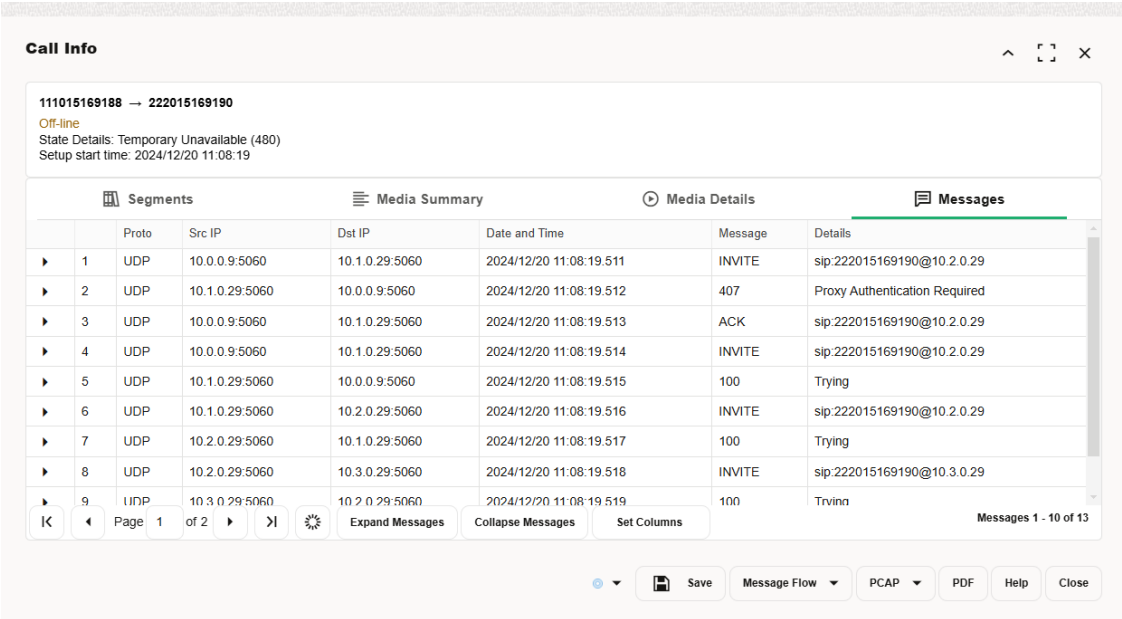
Messages

The **Messages** tab shows a table representation of the messages from the call.

Table 4-10 Messages Table

Column	Description
Date and Time	The absolute time when this message was seen by Operations Monitor.
Details	In case of SIP messages, it is equal to Request-URI for SIP requests, or the reason phrase for SIP replies. In case of ISUP messages, it is equal to point codes. In case of ENUM messages, an example might be 8.4.1.1.7.7.9.7.9.7.4.4.e164.arpa. In case of MEGACO messages, an example might be Add or Modify.
Dst IP	The destination IP address and port number.
Dst MAC	The destination hardware address. This column is hidden by default.
Dst PC	The destination PC address. This column is hidden by default.
Message	In case of SIP messages, it is equal to the SIP method for SIP requests, or the response code for SIP replies. In case of ISUP messages, it is equal to one of the ISUP method types: <i>IAM</i> , <i>ACM</i> , <i>RLC</i> , etc. In case of MEGACO messages, it is equal to either <i>MEGACO Request</i> or <i>MEGACO Reply</i> . In case of ENUM messages, it is equal to either <i>ENUM Query</i> or <i>ENUM Answer</i> .
Proto	The transport layer protocol. The supported transport protocols are <i>UDP</i> and <i>TCP</i> .
Src IP	The source IP address and port number.
Src MAC	The source hardware address. This column is <i>hidden</i> by default.
Src PC	The source PC address. This column is hidden by default.

Figure 4-38 Call Details Messages Tab

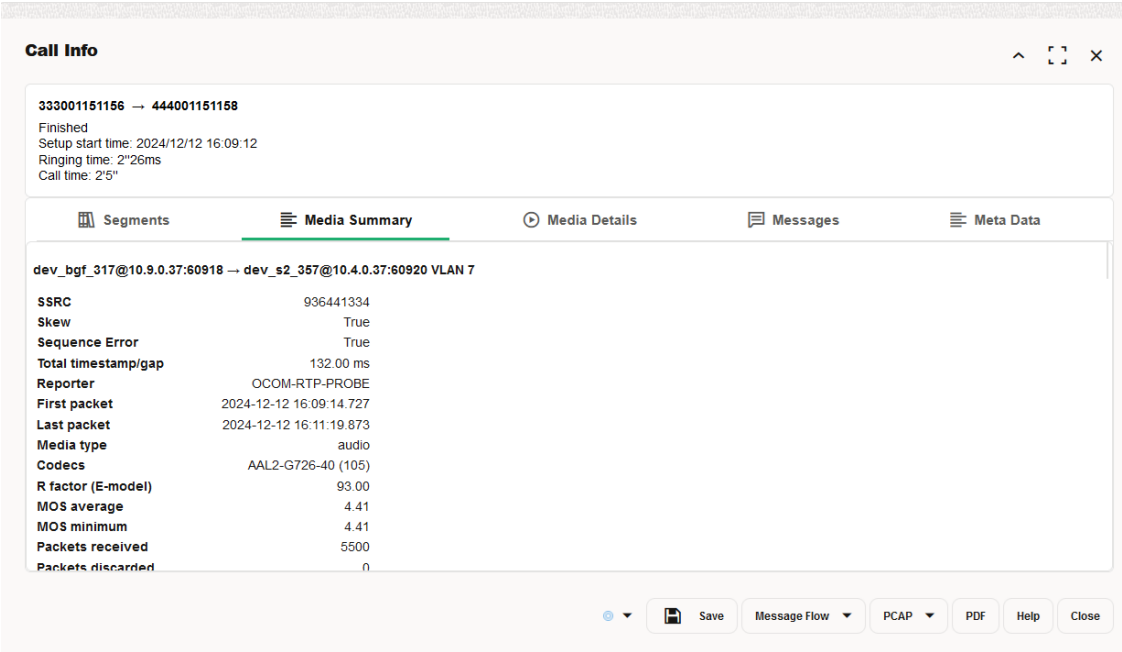


Click the **Expand Messages** button to view the raw messages as seen on the network. The raw messages can be also viewed in context in the **message flow** diagram.

Media Summary

The **Media Summary** and **Media Details** tabs display the voice quality summary of the *finished* calls. It displays the source and destination devices when set in Platform Devices. For a Skype for Business call, along with the other details, the Media Type and the Codec used are also displayed.

Figure 4-39 Media Summary Tab



Downloading Call Details to a PCAP File

You can save the raw signaling messages and the media streams of a call to a PCAP file. When a call has multiple media streams, a single PCAP file is created containing all the streams.

To save the call details to a PCAP file:

1. In the call details panel, click the **PCAP**. Click **Save** or **Save as**.
2. The file is saved as <filename>.pcap.

Device Visibility in Realms

Device visibility in a realm works as a Allowlist for visible devices and a blocklist for hidden devices. By default (if no realm is set in the realm visibility settings for a particular device), realm users will not view the related information (messages/segments) for legs via that device.

If the user belongs to a realm which has limited device visibility (only some devices are visible to the realm):

- Information about call segments between visible devices are shown.
- Information about call segments between visible devices and hidden devices are not shown.
- Information about call segments between visible devices and unknown hosts are shown. An unknown host is a host that does not belong to any device. To hide this information from the realm, create a new device for the respective unknown host and set it as hidden for this realm.

This behavior affects the call information on the **Segments** and **Messages** tabs, in the message flow diagram, PCAP, and PDF generation.

Note

To set a device as visible or hidden to a realm, under **Platform Devices**, click **Realms**. The Realm Assignment dialog box opens. Select the required checkboxes to assign one or more realms to a single device.

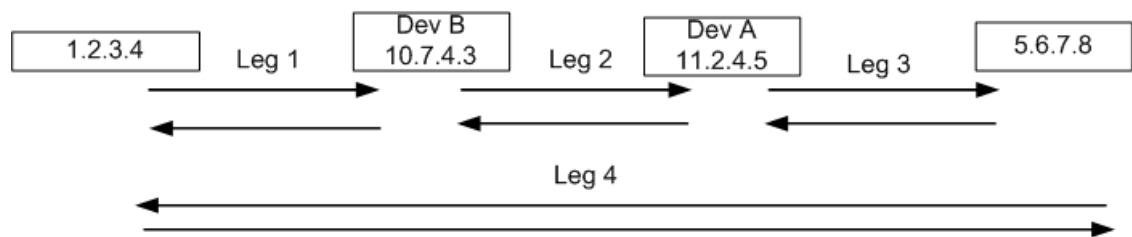
For matching devices, the IP or IP range along with the VLAN information, is considered. As a result, if the VLAN information does not match the device definition, the unmatched device will appear in the diagrams identified by its IP and VLAN. VLAN = 0 implies there is no VLAN, so it matches only the IP of the device.

Following are examples to understand the device visibility:

Example 1

In the following example, User A belongs to Realm A, for which Dev A is shown and Dev B is hidden.

Assume that you will have a call with four legs as shown in the [Figure 4-40](#). There are no VLANs involved in the call.

Figure 4-40 Device Visibility Example 1

In all the possible views that User A could use to see at call flows or call messages (except for the Traces feature and PI (Packet Inspector)):

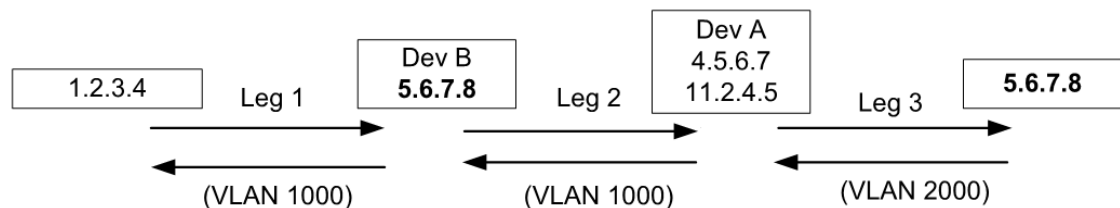
- Leg 1 - Hidden (because Dev B is hidden)
- Leg 2 - Hidden (because Dev B is hidden)
- Leg 3 - Visible (because it is between a visible device and an unknown IP)
- Leg 4 - Visible (because it is between an unknown IP and another unknown IP)

Example 2

In the following example, User A belongs to Realm A, for which Dev A is shown and Dev B is hidden.

Dev B is defined as 5.6.7.8(VLAN=1000) and Dev A is defined as 4.5.6.7(VLAN=1000) 11.2.4.5(VLAN=2000).

Assume that you have a call with three legs as shown in the [Figure 4-41](#) in which Leg 1 and Leg 2 have VLAN=1000, and Leg 3 has VLAN=2000.

Figure 4-41 Device Visibility Example 2

In all the possible views that User A could use to look at call flows or call messages (except for the Traces feature and PI):

- Leg 1 - Hidden (because Dev B is hidden)
- Leg 2 - Hidden (because Dev B is hidden)
- Leg 3 - Visible (because for this leg the VLAN tag is 2000 and not 1000, Leg 3 does not match Dev B (even though it has the same IP address). For this reason, Leg 3 is considered to be a leg between Dev A and an unknown host.)

STIR/SHAKEN Monitoring

STIR/SHAKEN is a framework that integrates two protocol standards—Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted Information Using Tokens (SHAKEN)—to validate the legitimacy of caller identities in SIP-based voice calls.

The STIR/SHAKEN framework prevents caller ID spoofing and reduces unwanted robocalls by verifying caller legitimacy using digital signatures. Starting with the Release 6.1, Session Monitor introduces monitoring and reporting for STIR/SHAKEN-enabled calls.

Enabling STIR/SHAKEN Support

Enable STIR/SHAKEN in two places: In the Platform Setup Application, and under System Settings.

Platform Setup Application (PSA) > **Additional Extensions**. For STIR/SHAKEN monitoring, enable the PSA extension in the Enterprise Operations Monitor.

1. Using the Platform Setup Application:
 - a. In a web browser, go to https://<ip_address>/setup or access the Platform Setup Application using the Mediation Engine GUI by clicking **admin** > **Setup**. The Platform Setup Application Login page appears.
 - b. Login to the Platform Setup Application.
 - c. Navigate to the **Configuration** page. Under the **Additional Extensions** area, select the **STIR/SHAKEN** check box.
 - d. Click **Apply**.

Figure 4-42 Enabling Stir/Shaken

The screenshot shows the 'Configuration' page of the Platform Setup Application. It includes a warning message at the top: 'Please note that you are only allowed to use the products, modules and extensions that you have purchased. For any questions please contact your sales representative.' Below this, there are three main sections: 'Capacity', 'Additional Extensions', and 'Extensions'.

- Capacity:** Contains a text input for 'Concurrent calls' (set to 100000) and a checkbox for 'RTP Recording' (unchecked). Below it is a text input for 'Concurrent RTP streams'.
- Additional Extensions:** A list of checkboxes where 'Non Calls', 'UCaaS CCaaS', and 'Stir/Shaken' are all checked.
- Extensions:** A list of checkboxes where 'App support', 'CDR', 'Diameter', 'ENUM', 'Gateway control protocols', 'REST API', 'SIGTRAN', and 'Media quality' are checked. 'SAU' and 'Skype for Business' are unchecked.

- The STIR/SHAKEN extension, controls if STIR/SHAKEN calls are monitored.
- Enable this extension explicitly. The default setting is false.

 Caution

Enabling/disabling the Stir/Shaken extension will start/stop the HTTP probe process and restart the counters process. It is recommended to perform this action during the maintenance window.

2. System Settings:

a. To view STIR/SHAKEN calls enable the below settings:

- **Support Stir/Shaken calls**

This system setting controls whether STIR/SHAKEN calls are monitored. The default value is false. Enable this system setting after activating the extension in PSA.

- **Stir/Shaken Response Timeout Interval**

Specifies the duration (in seconds) to wait for HTTP responses involved in the STIR/SHAKEN processes. Responses received after the timeout are ignored (default: 3 seconds, maximum: 30 seconds).

b. Enable the system settings

STIR/SHAKEN Call Flow and Verification Process

The STIR/SHAKEN protocols ensures that calls can be traced to their legitimate origin by using digital signatures, allowing service providers and recipients to verify if a caller can rightfully use a given number. This enhances trust in telecommunications, enabling more secure and reliable call flows.

Call Flow for STIR/SHAKEN Calls

Enable the System Setting Support Stir/Shaken Calls *if the calls are to be monitored*.

1. **Call Initiation:** The calling party initiates a call.
2. **Authentication by the Originating Provider:** The provider checks the legitimacy of the call using an authentication service.
3. **Digital Signature Creation:** If the caller's legitimacy is validated, the authentication service generates a digital signature. This signature is attached to the SIP call as an identity header.
4. **Transmission and Verification:** The digital signature (identity header) is included in the SIP INVITE and is transmitted throughout the call path from the originating to the terminating service provider.
5. **Verification at the Terminating End:** Upon SIP call initiation, the originating provider sends an HTTP request as part of the STIR/SHAKEN process to further validate the caller ID. The HTTP response contains the identity header with the digital signature, which is then included in the SIP INVITE.
6. **Reception and Verification by Terminating Provider:** The terminating telephone service provider receives the SIP INVITE with the identity header. It checks the legitimacy of the caller ID by verifying the signature, often referencing a certificate repository.
7. **Outcome Display:** Based on the verification result, the terminating provider flags the call outcome (e.g., verified or spam) on the called party's display.
8. **Process Components:**
 - **Authentication (Signing) Service:** Validates and signs the call at the originating side.

- **Verification Service:** Verifies the signature at the terminating side.

The STIR/SHAKEN process ensures an end-to-end verification by embedding and carrying a digital signature from the originating provider to the terminating provider, who performs the final verification and communicates the result to the called party.

Correlation of HTTP and SIP Traffic

To associate (correlate) HTTP and SIP traffic within Enterprise Operations Monitor the system uses telephone numbers present in the specific protocol headers.

Correlation Method

- **HTTP Side:**
After decoding each HTTP message, Enterprise Operations Monitor extracts two key parameters: the originating and destination telephone numbers (for example, from the origin and dest headers, or TN (phone numbers) values).
- **SIP Side**
The system retrieves the calling and called party numbers from the SIP From and To headers.

Matching Logic

- Correlation occurs by directly matching the originating and destination numbers from the HTTP message with the corresponding caller and callee numbers from the SIP INVITE.
- Only if both numbers match exactly is the HTTP message considered associated with the SIP call.
- This ensures that data (such as STIR/SHAKEN identity information) is correctly tied to its relevant call flow.

Important Notes

Exact Match Requirement: Release 6.1 requires a strict, character-for-character match between HTTP and SIP telephone numbers for a successful correlation.

Voice Quality

Under **Operations** of the main menu, the **Media Summary** page allows you to analyze the transmission effects of the network on the voice quality as perceived by the users of the VoIP platform. It provides a graphical overview for both platform-wide calls and device specific calls.

Voice Quality Source

Operations Monitor gathers voice quality information from four sources:

- [Operations Monitor RTP Probes](#)
- [User Agent Statistics](#)
- [SIP Voice Quality Events \(application/vq-rtcpxr\)](#)
- [Other Voice Quality Monitors](#)

Operations Monitor RTP Probes

Probes monitor the traffic in passive mode and record several measures for each RTP stream:

- The number of lost packets.
- The variance of delays between the received packets (*jitter*).
- The distribution of lost packets inside the stream.
- The *codec* used.

Based on these values, Operations Monitor uses the ITU E-Model to estimate the MOS.

The following restrictions apply:

- MOS is calculated for blocks of 10 seconds (chunks), if a chunk contains more than eight seconds of RTP data and contains only packets of a single audio codec.
- No MOS is calculated if a chunk contains multiple payload types other than the telephone-event (DTMF). That is a change in audio codec or comfort noise packets will prevent MOS computation.
- No MOS is calculated if a gap in a stream is longer than two seconds.

For the following codecs, codec-specific values for the Equipment impairment factor (Ie) and Packet-loss robustness factor (Bpl) are used in the calculation:

- G.711 A-law (PCMA)
- G.711 u-law (PCMU)
- G.722
- G.723.1
- G.726
- G.728
- G.729
- iLBC

For the following audio codecs, default values for Ie and Bpl are used.

- AMR-NB
- AMR-WB (G.722.2)
- iSAC
- OPUS
- Speex

User Agent Statistics

Some SIP devices have the capability to include RTP statistics in a BYE message header, or in the reply to the BYE message. In general, the information provided is not enough to estimate the MOS, with the exception of the 'X-RTP-Stats' *version 3* header.

The user agent statistics data is retrieved from the cache or on demand depending on the system setting. By default, the user agent statistics is always active.

Table 4-11 User Agent Headers Providing RTP Stats

Header Name	Devices	Data Provided
X-RTP-Stats (v2)	AVM	packet loss, jitter, burst lost, codecs.

Table 4-11 (Cont.) User Agent Headers Providing RTP Stats

Header Name	Devices	Data Provided
X-RTP-Stats (v3)	AVM	packet loss, jitter, burst lost, gaps, codecs.
P-RTP-Stats	Cisco, Linksys, Sipura	packet loss, end-to-end latency, burst lost, codecs.
RTP-RxStats	Snom	packet loss.

SIP Voice Quality Events (application/vq-rtcpxr)

Some SIP devices (like: Polycom and Snom) are able to send voice quality information derived from RTCP-XR messages to Operations Monitor's voice quality collector, configurable under *VQ Collector Configuration*. Operations Monitor gets the values of *jitter*, *packet loss*, *burst loss*, and *MOS* from the voice quality collector to display them under the Call details info page.

Operations Monitor only reports data for end of stream statistics (*CallTerm* marker, refer to RFC 6035).

RTCP reports may be generated by endpoints. Such data may not be present or may not be trustworthy. Due to this we do not consider RTCP quality information for our own voice quality metrics. Nonetheless we display RTCP information to complete the view on the voice quality experienced by the users.

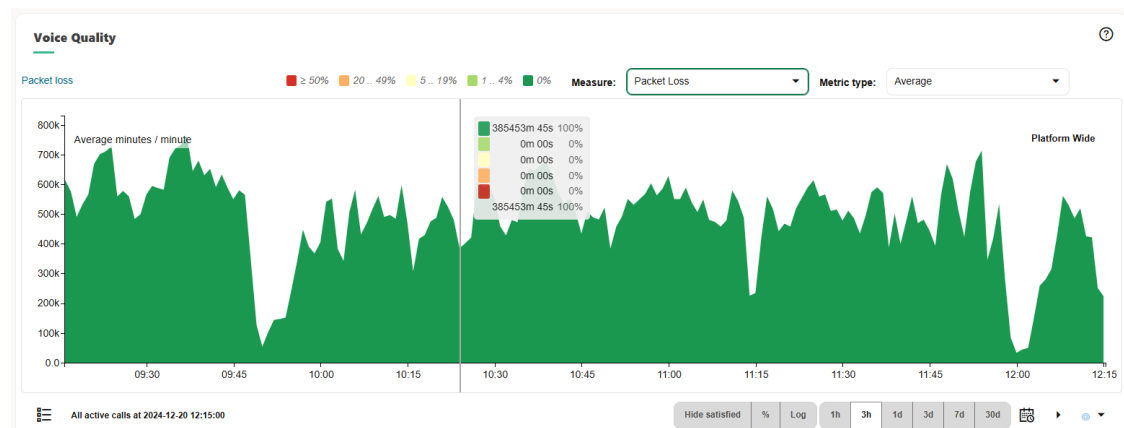
Other Voice Quality Monitors

Oracle Communications SBCs can be configured to forward Voice Quality data to Operations Monitor. Operations Monitor relays this information through its intuitive user interface.

Voice Quality Chart

The Voice Quality page shows device-specific stacked area chart for the MOS, Packet Loss, and Jitter measures. The **Measure** drop-down menu allows you to select either:

- MOScqe
- Packet Loss Rate
- Jitter

Figure 4-43 Voice Quality Overview Chart

Device-Specific Voice Quality Dashboard Panel

The Device-Specific Voice Quality Dashboard panel enables you to view Voice Quality of a specific platform device on the dashboard.

To add a panel directly from the Dashboard page:

1. Right-click on the Dashboard to get a context menu, and choose **Add a panel**. A pop-up window appears that provides dashboard panel options.
2. Click **Display a Voice Quality at a particular device**.
3. Select of measure of the device. The options are MOScqe, Packet Loss Rate, Jitter.
4. Select a Platform Device.

Note

The list of devices shown is dependent of the Measure chosen in the previous step. For example, if you have chosen MOScqe as the measure in Step 3, then in Step 4, the list of devices lists only those devices for which MOScqe or full VQ has been enabled. For more information see [Configuring Devices for Voice Quality Measurement](#)

5. Select Device in/out option to show Incoming or Outgoing data in the Dashboard panel.
6. Provide a name for the panel.
The panel with VQ for the device is added to the dashboard with levels displayed on hovering.

Voice Quality Chart for MOS

The **Voice Quality** page shows a stacked area chart for the MOS measure. Five series are displayed, each based the levels of user satisfaction as specified by ITU recommendation G.107.

- Very satisfied: $MOS \geq 4.34$
- Satisfied: $4.03 \leq MOS \leq 4.33$
- Some users dissatisfied: $3.60 \leq MOS \leq 4.02$
- Many users dissatisfied: $3.10 \leq MOS \leq 3.59$
- Nearly all users dissatisfied: $MOS \leq 3.09$

We analyze the quality of a media stream over a time interval of either one or 15 minutes (determined by the **Voice Quality Chart Scale in Minutes/Minute** system setting) and determine how many minutes and seconds were spent in each of the above MOS ranges. For more information, see "[Voice Quality Chart Scale in Minutes/Minute](#)".

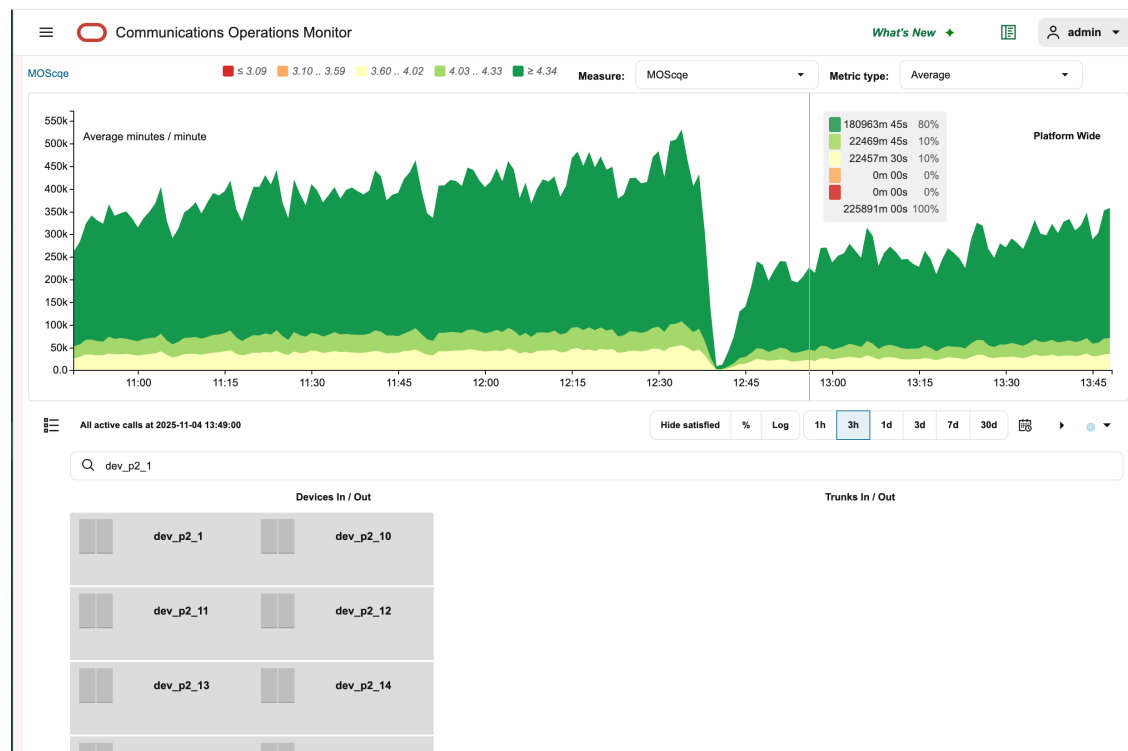
Over a minute a stream may have had 40 seconds with a MOS of ≥ 4.34 , 10s between 4.34 and 4.03, and another 10s between 3.60 and 3.10. If using a 15 minute interval, the values are normalized accordingly to project the average minute and seconds over a 15 minute time period.

In this case, with 40 seconds over one minute of MOS of ≥ 4.34 is 00:40 minutes, but normalized over a 15 minute interval it is 10:00 minutes.

We sum up all the minutes of MOS ≥ 4.34 across all active media streams. This determines the height of the area labeled ≥ 4.34 at T=12:01.

The chart's resolution and range can be controlled with the toolbar directly below it.

Figure 4-44 Voice Quality Chart for MOS



The toolbar offers these options:

- Display the active calls during a period of bad voice quality.
- A Search Filter which is common across both Devices and Trunks.
- Hide statistics about streams with satisfactory quality (do not show the two best categories).
- Switch to a percentage scale.
- Switch to a logarithmic scale.

Additionally, you can select metric with the drop-down in the upper-right corner of the diagram. The metrics are **Average** (default) and **Maximum**.

The reason for using the **Maximum** metric is that for older data only hour resolution is available. A peak that happened during a couple of minutes will then be flattened out when calculating the average over one hour. By preserving the maximum value over a time period, the peaks can still be detected in old data.

When aggregating maximum values from minute to hour resolution, the sum of minutes of all voice quality levels will most likely be greater (at least equal) than that of the minute resolution. This is because the maximum value for each voice quality level over 60 minutes will be chosen.

Voice Quality chart for Packet Loss

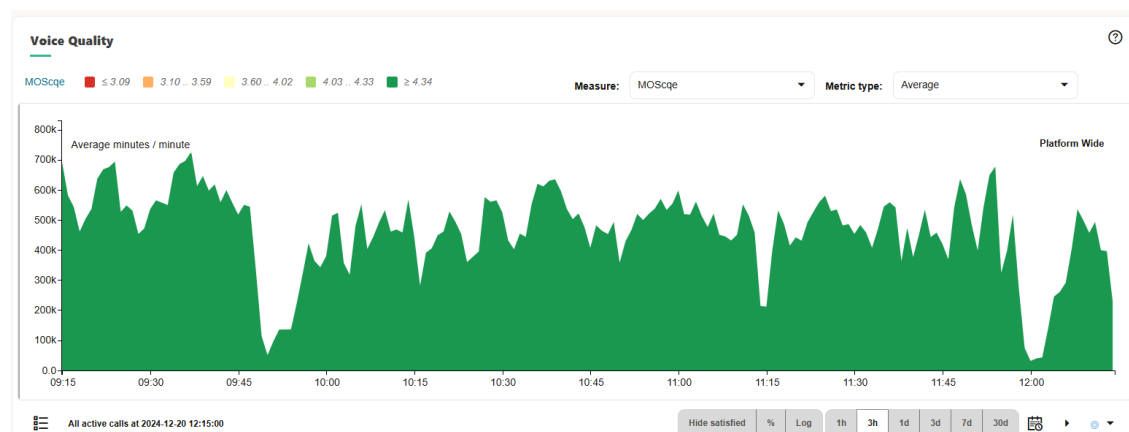
The **Voice Quality** page shows a stacked area chart for the Packet Loss measure. Five series are displayed, each based on the levels of packet loss rated computed based on the raw RTP traffic.

- Very satisfied: PL <=0%
- Satisfied: 1% <= PL <= 4%
- Some users dissatisfied: 5% <= PL <= 19%
- Many users dissatisfied: 20% <= PL <= 49%
- Nearly all users dissatisfied: PL >= 50%

We analyze the quality of a media stream over a time interval of either one or 15 minutes (determined by the **Voice Quality Chart Scale in Minutes/Minute** system setting) and determine how many minutes and seconds were spent in each of the above Packet Loss ranges. For more information, see "[Voice Quality Chart Scale in Minutes/Minute](#)"

The chart's resolution and range can be controlled with the toolbar directly below it.

Figure 4-45 Voice Quality Chart for Packet Loss



The toolbar offers couple of more options:

- Switch to absolute values
- Switch to a percentage scale.
- Switch to a logarithmic scale.

Additionally, you can select metric with the drop-down in the upper-right corner of the diagram. The metrics are **Average** (default) and **Maximum**.

Voice Quality Chart for Jitter

The **Voice Quality** page shows a stacked area chart for the Jitter measure. Five series are displayed, each based the levels of Jitter computed based on the raw RTP traffic.

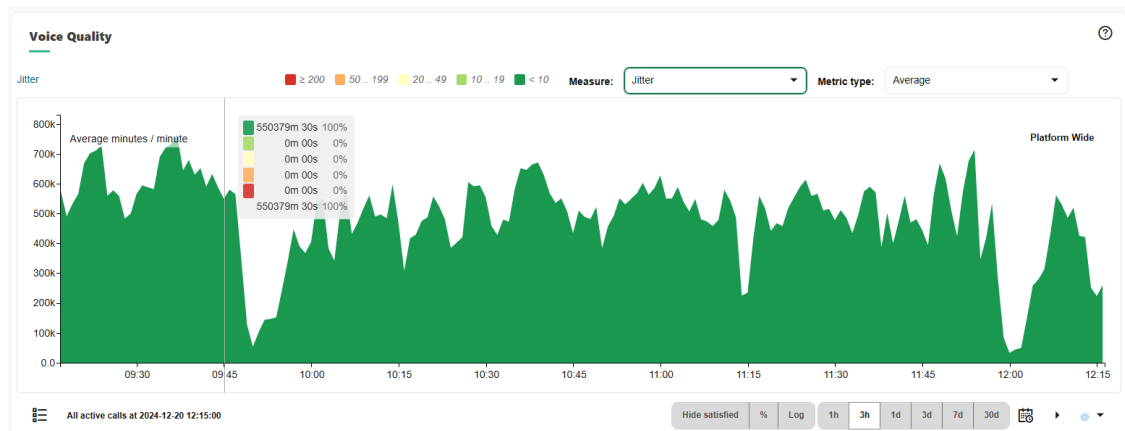
- Very satisfied: Jitter < 10 msec

- Satisfied: 10 msec <= Jitter <= 19 msec
- Some users dissatisfied: 20 msec <= Jitter <= 49 msec
- Many users dissatisfied: 50 msec <= Jitter <= 199 msec
- Nearly all users dissatisfied: Jitter >= 200 msec

We analyze the quality of a media stream over a time interval of either one or 15 minutes (determined by the **Voice Quality Chart Scale in Minutes/Minute** system setting) and determine how many minutes and seconds were spent in each of the above Jitter ranges. For more information, see "[Voice Quality Chart Scale in Minutes/Minute](#)".

The chart's resolution and range can be controlled with the toolbar directly below.

Figure 4-46 Voice Quality chart for Jitter



The toolbar offers couple of more options:

- Switch to absolute values
- Switch to a percentage scale.
- Switch to a logarithmic scale.

Additionally, you can select metric with the drop-down in the upper-right corner of the diagram. The metrics are **Average** (default) and **Maximum**.

Note

Only voice quality measurements calculated by the Operations Monitor probes are shown in this chart. This monitoring has certain limitations:

- Voice quality (MOS, packet loss, and jitter) is calculated for blocks of 10 seconds (chunks), if a chunk contains more than eight seconds of RTP data of a single supported codec. For more information, see "[Operations Monitor RTP Probes](#)".
- Chunks shorter than 10 seconds are normally not shown.
- Streams containing larger gaps (that is due to comfort noise) might be shown as two separate streams.
- Streams that are not matched to calls (no correlation between SDP record received in a SIP message and RTP IP/ports) are not included in Operations Monitor's KPIs.

CSV Export

You can export voice quality data for the displayed period by pressing the CSV export button. The CSV export dialog will open, and when ready provide you with a downloadable CSV file.

Table 4-12 CSV Export Fields

Name	Format	Example
Local timestamps	human readable	7/25/2017 13:42
UTC timestamps	ISO 8601	2014-07-25T11:42:00Z
Interval	integer	60
MOS: 0 .. 3.09	integer	300
MOS: 3.10 .. 3.59	integer	329
MOS: 3.60 .. 4.02	integer	28
MOS: 4.03 .. 4.33	integer	255
MOS: 4.34 .. 5	integer	212

The MOS fields contain the number of seconds of each voice quality level, for the time period given in seconds in the **Interval** field. The interval depends on the available resolution for the time period: either minute or hours. If minute resolution values are available, Interval is typically 60, otherwise 3600. The Interval can in rare cases be less than 60 or 3600, if the machine was rebooted or was down when the measurement period started.

Minute values are only available for the last couple of days.

Active Calls During a Period of Bad Quality

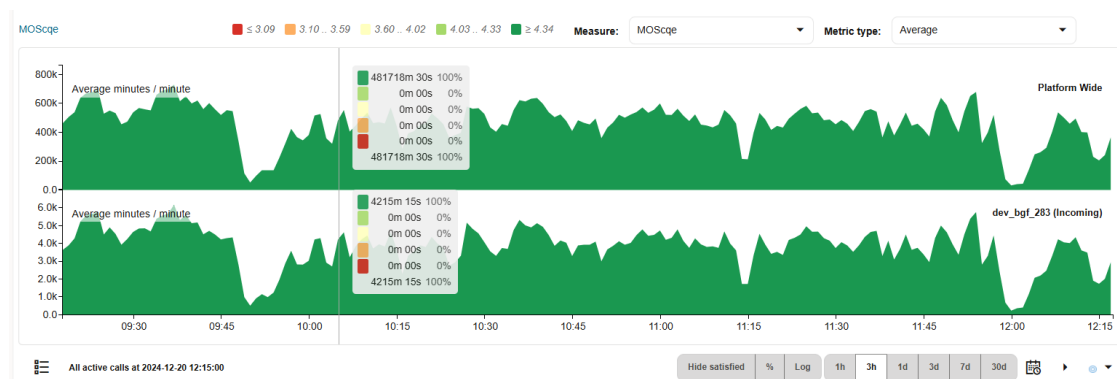
Selecting a time on the main chart will update the **Active calls** button below the chart. This button navigates to the calls page, appropriately filtered to display only calls active at that time.

Voice Quality Charts Per Device

To help diagnose areas of particularly bad MOS, clicking on the main chart at time T loads the Voice Quality data for all platform devices at that time. The MOS stats for a device are displayed next to it. The devices are sorted by MOS quality, those with bad quality at the selected time are listed first.

Clicking on a device augments the main chart with a second chart displaying the Voice Quality for the currently active time resolution and range.

Figure 4-47 Voice Quality per Device



The following two voice quality charts are available for each device, trunk, and IP tag:

- Distribution of incoming calls by MOS ranges, packet loss ranges, and Jitter ranges over the time.
- Distribution of outgoing calls by MOS ranges, packet loss ranges, and Jitter ranges over the time.

Media Summary

You can see the media summary information of any call listed in the **Calls** table.

To view the media summary details:

1. Double-click a row in the **Calls Table**.
The **Call Info** window opens.
2. Click the **Media Summary** tab which opens a textual report of the voice quality data for the call.

Table 4-13 Media Summary Fields

Field	Description
SSRC(Synchronization Source identifier)	Uniquely identifies the source of a stream. For IPFIX calls, if SSRC is sent by Session Border Controller in Interim QoS, only then only SSRC is displayed on the Media Summary tab. If there is no Interim QoS and only End-of-Call, SSRC details does not come from Session Border Controller, and it is not displayed.
Skew	Refers to the difference in arrival times of the packets belonging to the same stream. When the summation of time gap between the RTP packets of a stream is greater than the configured/default jitter_buffer value, then the Skew is updated. . 1. On the Media Summary tab, Skew is displayed as True, if any value present in Media Details tab for Skew. 2. On the Media Details tab, Skew value is displayed in milliseconds(ms).
Sequence Error	• Displays the Sequence Error per stream. • On the Media Summary tab: – Sequence Error is displayed per stream. – Its value is True if there is any sequence error for that stream. If there is no Sequence Error, then this parameter is hidden on the Media Summary tab. • On the Media Details tab, – Sequence Error is displayed per chunk. – The reason for the Sequence Error is shown on hovering over each chunk along with the existing data. – A value of True if there was any sequence error for that stream. If there is no Sequence Error, then the parameter is hidden on the Media Summary tab.

Table 4-13 (Cont.) Media Summary Fields

Field	Description
Total Timestamp	- Total Timestamp is shown as the duration of silence. - It is supported for the following codecs : G.711,G.726, G.727, G.728, and G.722. (This is as per RFC 3389.) - On the Media Summary tab: - the total of all silence durations of all the chunks per stream is displayed - The duration (in Ms) is calculated as the difference between the first Comfort Noise(CN) packet and the corresponding Marker bit packet for a stream. - If multiple occurrences of CN and Marker bit occur in one stream, then the silence duration is a cumulative of all such durations in that particular stream. - Note these two conditions: - If the CN packets starts coming in Chunk 1 and ends with Marker bit packet in Chunk 1 itself. Then that duration will be shown as silence duration in chunk 1 - If CN packets start coming in Chunk 1 but does not end in Chunk 1. For example, if this duration was x seconds. CN packets continue coming in chunk 2 and ends with Marker bit packet in chunk. If this duration was y seconds. The silence duration is shown x and y seconds in chunk 1 and chunk 2 respectively.
VLAN	The VLAN ID (Identifier) indicates which VLAN the RTP packets belong to. This VLAN ID helps in ensuring that RTP packets are correctly routed and managed within the network. In the Message Flow window, VLAN ID is displayed for START RTP and END RTP messages.
Average jitter	The average of the measured jitter values of the 10 seconds intervals.
Average MOS	The average of the estimated MOS values of the 10 seconds intervals.
First packet	The time stamp of the first RTP packet from the stream.
Last packet	The time stamp of the last RTP packet from the stream.
Maximum jitter	The maximum of the measured jitter values of the 10 seconds intervals.
Minimum MOS	The minimum of the estimated MOS values of the 10 seconds intervals.
Packet loss rate	The number of received RTP packets divided by the number of expected RTP packets.
Packets lost	The total number of RTP packets that were lost for this stream. This can have multiple causes: - Packets were dropped by the network - Packets were dropped at sniffing time (visible in PSA Media Signaling page) - Packets were dropped by the internal jitter buffer used for computing Voice Quality stats

Table 4-13 (Cont.) Media Summary Fields

Field	Description
Packets received	The total number of RTP packets that were received in the stream.
Reporter	The source of the report: • <i>OCOM-RTP-PROBE</i>: Operations Monitor probe • <i>VQ-RTCPXR</i>: Voice quality reports received in SIP PUBLISH messages • <i>SBC-RTP</i>: Data based on end-of-call media QoS reports from an SBC • <i>SBC-INTERIM-RTP</i>: Data based on interim media QoS reports from an SBC • <i>SBC-RTCP</i>: Data based on an RTCP summary from an SBC • <i>P-RTP-STAT</i>, <i>X-RTP-STAT</i>, <i>RTP-RXSTAT</i>: Data from one of the supported SIP headers that carry VQ information • <i>SFB</i>: Skype for Business calls.
Total jitter	The sum of the measured jitter values of the 10 seconds intervals.
VLAN	The VLAN tag of the RTP packets

Media Details

The **Media Details** tab displays an estimation of the MOS value for each RTP stream. This data is collected by Operations Monitor RTP probes or may be provided by SBCs in interim media QoS reports. The data is arranged on a grid in 10 second intervals.

You can see the media details grid for any call listed in the **Calls** table.

To view the media details grid:

1. Double-click a row in the **Calls** table.
The **Call Info** window opens.
2. Click the **Media Details** tab which opens a grid report of the media details for the call.
3. Hover over any block on the grid; a tool tip displays data for the interval.

Table 4-14 Media Details Fields

Field	Description
Marker Bit	• Displayed if the Marker Bit is True for a chunk. • Hidden from display if Marker Bit is false. • If the value of Marker bit is True for a chunk, it is for that entire particular chunk. For example, if a chunk has 100 packets and if the Marker Bit for the 50th packet is True, and the Marker bit for the next 50 packets is False, even then the Marker bit is True for that chunk.
Sequence Error	• Displays the Sequence Error per stream. The reason for the Sequence Error is shown on hovering over each chunk along with the existing data. • A value of True if there was any sequence error for that stream.

Table 4-14 (Cont.) Media Details Fields

Field	Description
Skew	Refers to the difference in arrival times of the packets belonging to the same stream. Skew is displayed in milliseconds(ms). , Skew is displayed as True , if any value present in the Media Details tab.
Total Timestamp/gap	- Total Timestamp/gap is shown on the Media Details tab per chunk as the duration of silence. - It is supported for the following codecs : G.711,G.726, G.727, G.728, and G.722. (This is as per RFC 3389.) - The duration (in Ms) is calculated as the difference between the first Comfort Noise(CN) packet and the corresponding Marker bit packet for a stream. - If multiple occurrences of CN and Marker bit occur in one stream, then the silence duration is a cumulative of all such durations in that particular stream. - Note these two conditions: a. If the CN packets starts coming in Chunk 1 and ends with Marker bit packet in Chunk 1 itself. Then that duration will be shown as silence duration in chunk 1 b. If CN packets start coming in Chunk 1 but does not end in Chunk 1. Let's say this duration was x seconds. CN packets continue coming in chunk 2 and ends with Marker bit packet in chunk 2. Let's say this duration was y seconds. Then silence duration will be shown x and y seconds in Chunk 1 and chunk 2 respectively.
VLAN	The VLAN ID (Identifier) indicates which VLAN the RTP packets belong to. This VLAN ID helps in ensuring that RTP packets are correctly routed and managed within the network. It will also be displayed on Message Flow for START RTP and END RTP messages.

Note

Voice quality report intervals may align differently on the grid, depending on the data source. Intervals reported by Session Monitor probes are aligned to a global grid at 10-second boundaries. Intervals reported by SBCs may not be aligned to this grid because they are provided every 10 seconds after the stream began.

Audio Status

The **Audio** column in the **Calls** page reflects the Audio status of a call - both-way, one-way, no-audio.

By default, the value of the **Audio** column is updated once the call is finished. To enable real-time monitoring of the **Audio** column, new parameters have been introduced in the internal Mediation Engine configuration files. Here are the details.

Note

Enable the real-time monitoring of the **Audio** column only during maintenance window as it involves service restarts. Enabling the *interm_MLR* flag can have significant impact on Session Monitor performance. So, it is recommended that you enable this flag only with low traffic profiles. Contact Oracle support for more help.

1. Open the OCOM_home/etc/iptego/vsi.local.conf file.

2. To enable real-time monitoring of the **Audio** column, add:

```
[base]
interim_MLR=1
```

3. Save the file.
4. Restart the pld-vsi service using the command:

```
systemctl restart pld-vsi
```

Once the `interim_MLR` flag is enabled, you can control how often the Mediation Engine must update the **Audio** column in real-time. To modify this timer:

1. Open the `OCOM_home/etc/iptego/meco.local.conf` file
2. Add following line:

```
[mlr]
timeout_sec_for_interim_mlr = 30
```

3. Save the file.
4. Restart `pld-meco` service using the command:

```
systemctl restart pld-meco
```

Media Recording

The Media Recording feature allows you to capture RTP (including DTMF) and RTCP streams of calls, in addition to the signaling messages, to track particular user's calls. You can then download the RTP and RTCP streams to a PCAP file for further analysis in protocol analyzer tools. This is helpful for analyzing voice quality issues and for complying with regulations.

This graphic illustrates the **Media Recording** table, which lists the users that are currently tracked.

Figure 4-48 Users Tracked in Media Recording

Media Recording					
Add Delete Set Column					
☐	User	Tracked since	Tracked until	Media types	Recording content
☐	111015131124	2024/12/20 12:26:38	2024/12/22 12:26:38	audio	RTP Header,RTP Payload
☐	222015131126	2024/12/20 12:26:50	2024/12/22 12:26:50	audio	RTCP
☐	444015131104	2024/12/20 12:27:02	2024/12/22 12:27:02	video,audio	RTCP,RTP Header,RTP Payload
☐	111015131106	2024/12/20 12:27:13	2024/12/20 18:27:13	video	RTCP
Page 1 of 1 (1-4 of 4 items) < < 1 > > ⚙					

To start capturing RTP and RTCP streams, you set up recording rules. A recording rule specifies the subscriber to track, how long to track the subscriber's calls, the media types to record, and the contents to record.

This graphic shows the dialog box for specifying a media-recording rule.

Figure 4-49 Media Recording Rule Configuration

Media Recording allows you to record calls with multiple media types, for example, a call containing audio and video or audio and image.

Note

To record audio using Media Recording, you must enable the **RTP Recording** feature on both the Mediation Engine and the Probe. To record all other media types, including video and image, you must enable the **Packet Inspector extension** on both the Mediation Engine and Probe. All media types will display even when **Packet Inspector extension** is not enabled. Packet Inspector is not required for recording audio. See *Session Monitor Installation Guide* for more information about enabling these features.

The content that is available for recording depends on the user permissions. For example, the user may have permissions to download RTP header but not RTP payload.

When the recording content is restricted to RTP Headers only, the system records the following:

- RTP headers for RTP traffic (audio, video, text, T.38 over RTP)
- UDP headers plus the first two bytes (sequence number) for T.38 over UDPTL
- TCP headers only for TCP-based media

Operations Monitor saves the RTP and RTCP packets for all calls made or received by the subscribers that are tracked in Media Recording. For example, if the expiration time is **2 days**, then for two days the system tracks all calls made or received by the subscriber and records the calls that match the rule.

The **Tracked until** column in the **Media Recording** table shows the expiration time. After the expiration time, the recording rule is deleted. This prevents the recording rules list from becoming too long.

All users with the same realm assigned can share a recording job. Users in the realm **ALL** can view all the recordings in the system.

Recording RTP Streams

To start recording the RTP streams for a subscriber:

1. In the **Recent calls** panel of the **Calls** page, click the Recording icon in the menu bar:

Figure 4-50 Media Recording



The **Media Recording** table appears. The table shows the subscribers that are currently tracked.

2. Click the **Add** button.

The Record media for a new user dialog box appears.

3. In the **User** field, enter the phone number or the SIP user name to track.

Operations Monitor records for all the SIP user names that match the given pattern as a suffix. This is useful when the same subscriber uses various prefixes. For example, if a subscriber uses both *0123456* and *+49123456* phone numbers, enter *0123456*, so that both numbers are matched.

4. In the **Expiration time** section, select the time interval until when the subscriber is tracked.
5. In the **Media types** section, select one or more media types to record.
6. In the **Recording content** section, select one or more content to record.

The content available for recording depends on the user permissions.

7. Click **OK**.

To stop the recording for a particular subscriber, select the user in the **Media Recording** table and click **Delete**.

Downloading Recorded RTP Streams

RTP streams are downloaded in the industry-standard PCAP file format. When a call has multiple media streams, you can select the media streams that you want to download. The content available for downloading depends on the user permissions. A single PCAP file is created containing all the streams.

Figure 4-51 Download the Signaling and Recorded Media Streams

PCAP download

For this session, multiple signaling and media streams may be available. Please select the streams to be included in the PCAP file. You will receive a single file containing all streams.

☒ Include signaling messages

☒ Include Media payload from all streams

172.31.1.2:20001 → 172.31.2.1:10001 (audio)
1 recorded stream
☒ Media payload

172.31.2.1:10001 → 172.31.1.2:20001 (audio)
1 recorded stream
☒ Media payload

Download Close

To download the recorded RTP streams for a call:

1. In the **Recent calls** panel on the **Calls** page, double-click a call that is made or received by the tracked user.
The Call Info dialog box appears.
2. In the Call Info dialog box, click the **PCAP** button.
The PCAP download dialog box appears.
3. Select the recorded streams you want to save.
4. Click the **Download** button.
The Export status dialog box appears, which contains a link to the PCAP file that is generated for the call.
5. Click the PCAP file link.
6. Select the option to save the file, and click **OK**.

Registrations

The **Registrations** page allows you to examine the registration events detected on the monitored platform. Examples of these events are: a SIP device tries to publish itself as an on-line entity willing to engage itself in communication with other devices, changes this status to off-line, or queries a central authority about this status. Registration events are generated using the SIP protocol method 'REGISTER'.

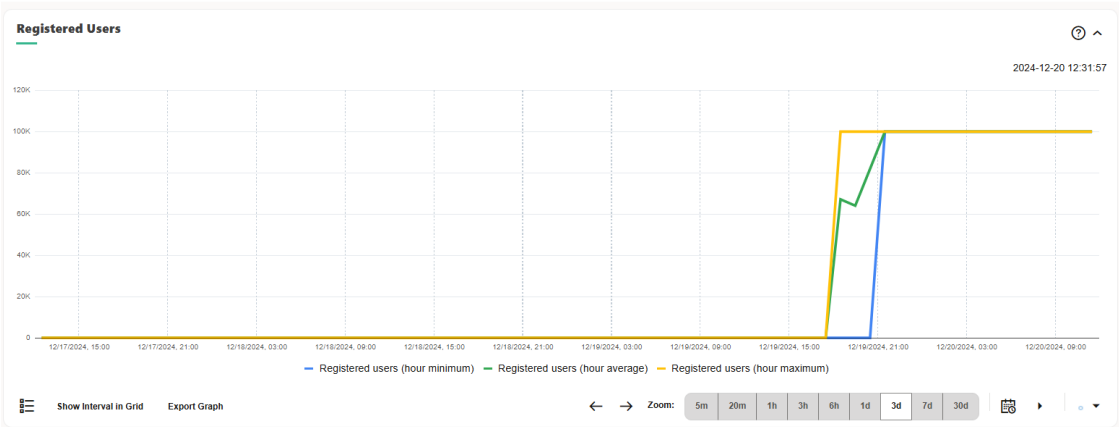
The **Registrations** page contains two panels: the first is the **Registered Users** panel, which provides an overview of the number of registered devices and the fluctuation over time, and the **Registrations Table**, which groups the events for one subscriber (one AOR in SIP terminology) and gives more details.

Registered Users Panel

The top panel contains a chart that traces the total number of registered users over time. The sampling interval is 1 minute for drawing the sample's minimum, maximum, and average values.

By default, a window of three hours is presented. The time frame can be adjusted and the chart allows for panning. For more information on using charts, see "[Charts](#)".

Figure 4-52 Registered Users Panel While Dragging Time Window



Note

If Operations Monitor has no registration information over a period of time (due to factors like recent start up, downtime, or lack of traffic), that interval is indicated in the chart by a gray area.

Registrations Table

The **Registrations** panel contains a table of the registrations events, grouped by SIP user. The list is ordered chronologically, presenting the latest event as the first entry by default. Table columns can be resized, and the size adjustments persist even after navigating away from the page and returning back to the page. The table can be sorted and/or filtered. For more information on creating Filters, see "[Filtering](#)".

Note

If the system setting *Group New Registrations from the Same User* is true, duplicate registration events in state 'New' from the same users are grouped together. However, since the grouping is done on each requested chunk, duplication removal over different chunks does not work.

Figure 4-53 Registration Table

Registrations							
Registration Details		Message Flow			(None)		
User	Contacts	Source IP Address	Timestamp	Registrar	Event	Code	User Device
444000056395	slp:333000056395@10.2.0.34:5060;transport=UDP	10.2.0.34	2024/12/20 12:16:37	dev_s1_394	Expired	0	
222000032939	slp:111000032937@10.2.0.18:5060;transport=UDP	10.2.0.18	2024/12/20 12:11:47	dev_s1_378	Expired	0	
666000012360	slp:555000012356@10.2.0.39:5060;transport=UDP	10.2.0.39	2024/12/20 12:07:27	dev_s1_399	Expired	0	
222000040298	slp:555000057016@10.0.0.7:5060;transport=UDP		2024/12/20 11:58:17	dev_sbc1_457	Expired	0	
222000019826	slp:111000084984@10.0.0.5:5060;transport=UDP		2024/12/20 11:53:57	dev_sbc1_465	Expired	0	
666000040260	slp:111000046698@10.0.0.9:5060;transport=UDP		2024/12/20 11:53:17	dev_sbc1_459	Expired	0	
666000013791	slp:555000015229@10.0.0.10:5060;transport=UDP		2024/12/20 11:53:07	dev_sbc1_470	Expired	0	
666000009603	slp:555000060001@10.0.0.2:5060;transport=UDP		2024/12/20 11:52:27	dev_sbc1_442	Expired	0	
444000008434	slp:555000080872@10.0.0.3:5060;transport=UDP		2024/12/20 11:51:47	dev_sbc1_473	Expired	0	
444000005482	slp:111000008040@10.0.0.1:5060;transport=UDP		2024/12/20 11:51:37	dev_sbc1_441	Expired	0	
222000093512	slp:333000097310@10.0.0.1:5060;transport=UDP		2024/12/20 11:50:08	dev_sbc1_471	Expired	0	
444000064339	slp:555000066097@10.0.0.8:5060;transport=UDP		2024/12/20 11:38:38	dev_sbc1_458	Expired	0	
222000088895	slp:111000088893@10.2.0.14:5060;transport=UDP	10.2.0.14	2024/12/20 11:33:48	dev_s1_374	Expired	0	
666000078291	slp:555000078289@10.2.0.10:5060;transport=UDP	10.2.0.10	2024/12/20 11:31:07	dev_s1_370	Expired	0	
Search limit reached Search next period Search entire history							
IK Now 2024-12-20 11:16:07 Stop Displaying items from 1 hour ago							

Here is a list of column descriptions for the **Registrations** table:

Table 4-15 Registration Table

Column	Description
User	Both admin and non-admin users belonging to a Realm defined by a custom pattern header can view Registrations and the associated KPIs. For more information, see Custom Patterns (Optional) Contains the user part of the AOR; if the system setting Use users domains is enabled, the domain part is also included in this field. When specifying a filtering token, all users that contain that token (position independent) will be shown.
Contacts	Filtering is done by matching a given string. All the contacts provided by the registering device are listed here, each as a SIP URI.
Source IP address	The IP address of the network device that initiated the registration event. Filtering is done by matching a given string.
Destination IP address	The IP address of the network server targeted by the registering device. Filtering is done by matching a given string.
Timestamp	The moment in time when the event occurred. Filter by specifying an interval (between <i>Before</i> and <i>After</i>) or a Date (the <i>On</i> date selector).
Registrar	The device configured in <i>Settings/Platform Devices</i> that was targeted by the subscriber's device when registering. When trying to filter by a certain device, a list of configured devices is presented out of which one or more can be selected.

Table 4-15 (Cont.) Registration Table

Column	Description
Event	The type of registration event; the table below is detailed on each defined type. For filtering one can choose to filter the presented list to only include some of the possible events.
Code	The SIP code that the registration message exchange finished with. Filter by specifying any valid SIP reply code.
User Device	Displays the user agent (User device) used in the Registration process.

Registrations Table Actions

The **Registrations** table provides a few action buttons.

- Click the **Registration details** button when a row is selected in the table, and a window appears containing *more details* for individual registration events; this window can be also opened by simply double-clicking on the selected row in the table.
- Click the **Message flow** button to open a **SIP message flow diagram** window that depicts the network entities involved and message exchange of the registration event.
- Click the **Set Columns** button hide/unhide the columns from the display.
- Click the **Filters** button to define filters and to see the required information in the table. For more information, see [Filters](#) section.
- The **CSV export** button allows to have all table entries exported into a CSV file. If the contents of the table have been filtered, the contents of the exported CSV file will only contain the filtered results.

Note

You can set the maximum number of lines to export in a CSV file using the system setting **Maximum number of lines exported with CSV export**.

Note

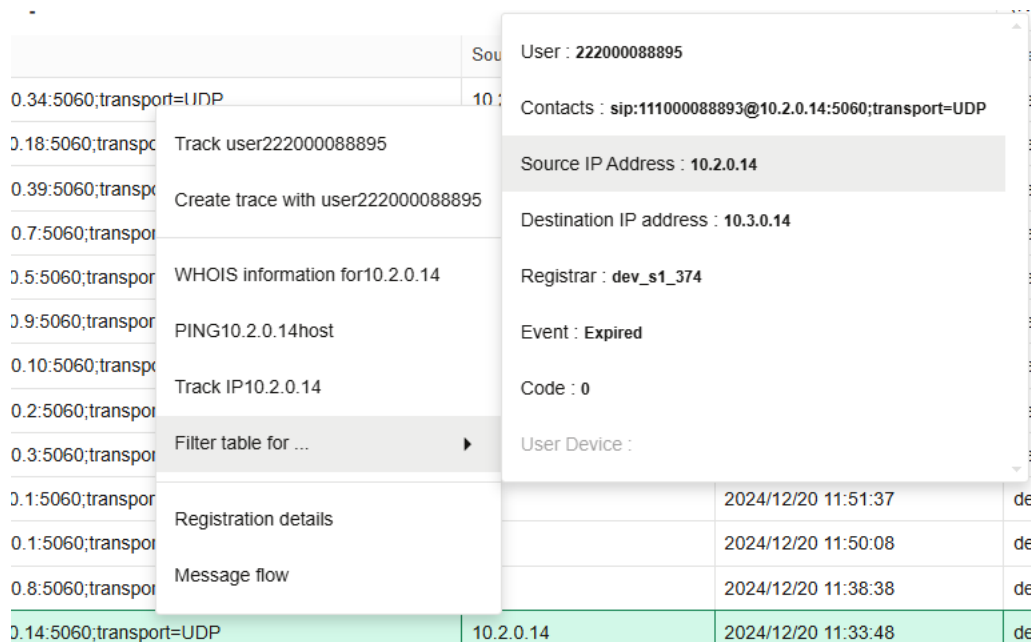
Many of these actions are available by right-clicking on a row.

Right-Click Contextual Menu - Registrations

Right-click menu actions are as follows:

Table 4-16 Right-click menu options

Menu option	Description
Track user <user name>	Loads the User Tracking page with the User field pre-filled in the search panel taken from the event
Create Trace with user <user name>	Loads the Traces page with the User field pre-filled with the value taken from the corresponding registration event.
WHOIS	Allows you to inquire who is the owner of the IP used as the source of the registration. A window appears that contains the record stored into the WHOIS database for the given address
PING	Pings the source IP address.
Track IP	Redirects you to the IP tracking page to get the details about the specific IP. For more information, see IP Tracking
Filter Table for...	<i>Filter table for ...</i> allows you to filter for: - Other registration events of the same user or contact. - All registrations involving the same address or device. - The same code or event type.
Registration Details	Opens the Registration Details window
Message Flow	Opens the Message Flow window

Figure 4-54 Registrations Table - right-click contextual menu

Paging

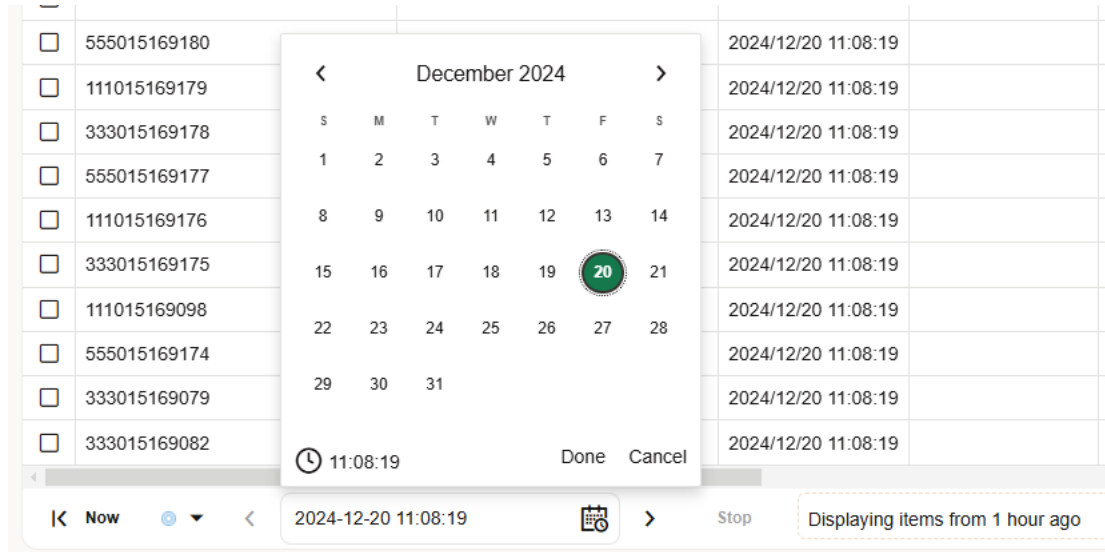
The paging bar allows you to navigate the entries. With the **Newer** and **Older** buttons you can step to the next page of newer respective older entries.

Figure 4-55 The Paging Bar



The **Now** button takes you to the first page, showing the newest entries. The date picker allows you to choose an arbitrary first date and time period.

Figure 4-56 The Date Picker



The loading bar will show when entries are being fetched. To fill up a page while applying filters, this might require several calls to the server and might take some time. The blue bar in the loading bar shows the range that has been searched.

You can set the **Refresh** button to auto-refresh mode. Please note that auto-refresh mode in combination with filtering of a grid can lead to longer refresh times than selected.

Registration Details

The details window for a registration event contains the following information:

- The user of full AOR (subjected to settings).
- The timestamp when the event occurred.
- The network entity of the platform having received the registration request (the ingress device).
- The IP address used to originate the requests.
- The type of registration event.
- A table that contains details about the exchanged messages in this event, listed in chronological order.

The table lists the columns in Registration Details window.

Table 4-17 Registration Details Window

Column	Description
Proto	The network transport protocol used to carry the SIP messages from client to the platform. This field can be either UDP or TCP.
Src IP	The IP address of the device that generated the message; can be either the client's or one of platform boxes, depending on the direction.
Dst IP	The IP address of the device that received the message; just as with <i>Source</i> , it can be either the client's or platform's.
Date and Time	The moment in time when the mirrored network packet was received by Operations Monitor.
Message	SIP message which caused the particular event
Details	Details about a event.

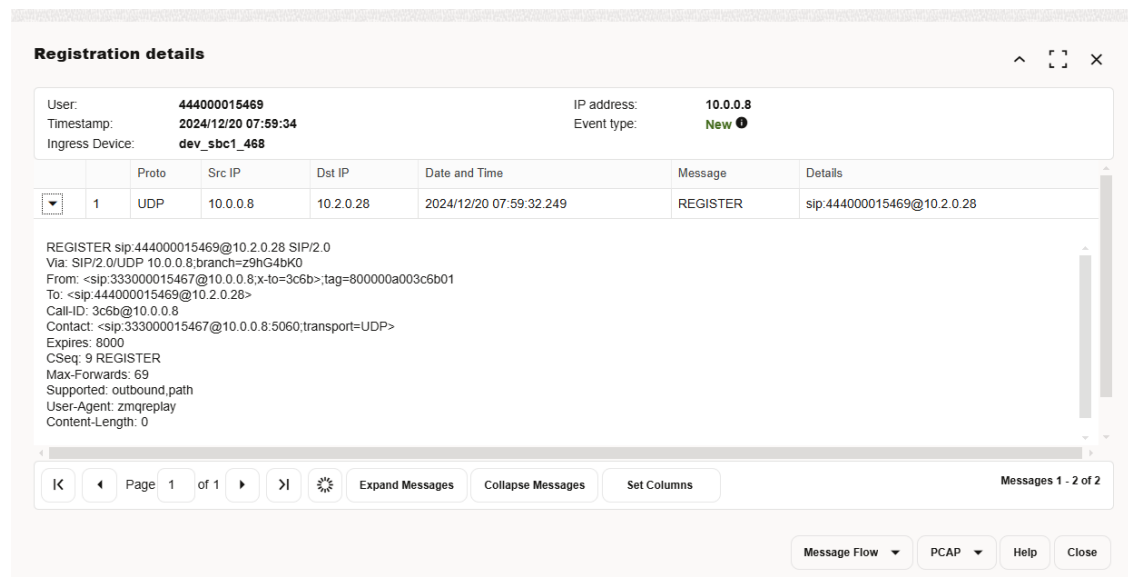
Registration Details Actions

In the Registration Details window, Click **Expand messages** to view all the raw SIP message as seen on the network. You can click **Collapse Messages** to display the brief view of the messages.

Note

You can view one raw message at a time by clicking the Triangle button on any of the table's entries, as shown.

Figure 4-57 Registration Details Window with One Expanded Raw Message



Beside the **Help** and **Close** buttons, the details window contains a **Message flow** button and a **PCAP** button. The **Message flow** button creates a *SIP message flow diagram*, and the **PCAP** button allows you to save the shown network packets into a PCAP file.

Registration Event Categories

Registration events are categorized as follows:

- **Failed**
Final response code is bigger than 299.
- **Unauthorized**
Two consecutive transactions are answered with 401, or when one 401 transaction is not followed by another REGISTER request in the next 5 seconds.
- **New**
A new contact binding was created for this user.
- **Gone**
Another registration request was answered by the registrar, and the binding was not found in the response.
- **Expired**
A binding is considered expired when the time interval specified in the 'expires' parameter from the registrar's answer is over. No messages are associated with this type of event.

Skype for Business Registration Events

You can view Skype for Business Registration events in the Registrations table under **Registrations**.

To View Details for a Skype for Business Registration Event:

1. Click **Registrations**.
The page displays two panels: **Registered Users** and **Registrations**.
2. In the **Registrations** panel, select the Skype for Business event. For example, an event where the **Registrar** displays the value **sfb**, and the **Source IP address** column displays the IP address of an SfB server.

Figure 4-58 Skype for Business Registration Event

User	Contacts	Registrar
tdomingos	sip:tdomingos@192.168.1.14;transport=tcp	
bureau1erd4	sip:bureau1erd4@192.168.33.17;transport=tcp	sfb

- a. Select the event, and click **Registration Details** to view more details of the event. You can see that the source IP address of the 200 OK message is the SfB server, and the destination IP address of the 200 OK message is the SfB endpoint.

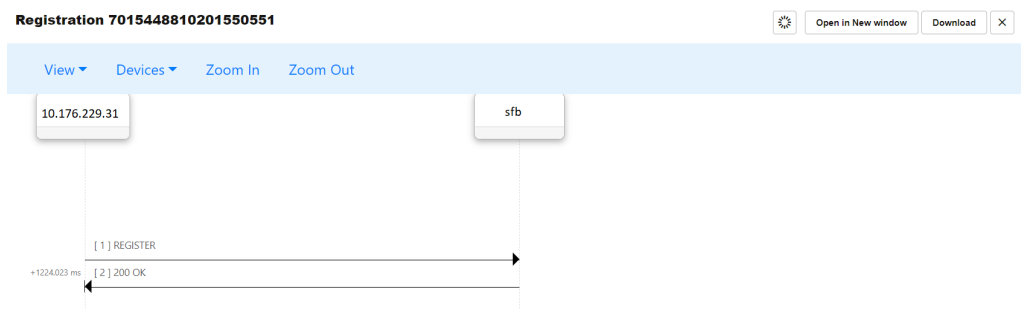
Figure 4-59 Registration Details for Skype for Business Event

Registration details ^] x

User:	anwasha1	IP address:	10.176.229.31
Timestamp:	2021/10/12 15:47:09	Event type:	New i
Ingress Device:	sfb		

	Proto	Src IP	Dst IP	Date and Time	Message	Details
	TCP	10.176.229.31:54389	10.176.227.231:5061	2020-02-26 6:18:15.069	REGISTER	sip:vm.sfb
	TCP	10.176.227.231:5061	10.176.229.31:54389	2020-02-26 6:18:15.075	200	OK

- b. Click **Message flow** to see the message flow for the registration event.

Figure 4-60 Message flow for Skype for Business Registration Event

You can also view Skype for Business Registration events and other SIP traffic from an Sfb Endpoint in the User Search view. For more information, see [User Search Panel](#).

User Devices

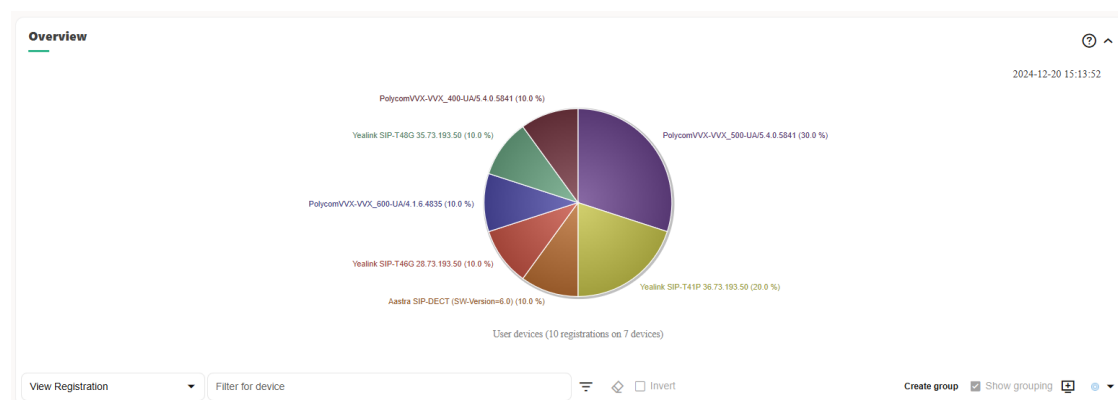
Operations Monitor provides statistics for user agents (user devices) registered on the monitored platform. These statistics are based on the **User-Agent** header of the REGISTER request. Alternatively, Operations Monitor can also evaluate the **User-Agent** headers of INVITE requests and replies in order to provide statistics about the callers and callees of the user device.

The **User Devices** page is located under the **Voice/Video Operation** section of the main menu. The **User Devices** panel displays a pie chart of the found user agents. The **Devices List** table contains detailed information about each user device in the lower area.

User Devices Chart

The **User Devices** chart displays the relative frequency of user agents as shown.

Figure 4-61 User Devices Chart



Operations on User Devices

You can filter and group user devices with the following actions in the **User Devices** chart:

- **Select data source**

You can select whether the statistics displayed on the **User Devices** page is based on registrations, callers, callees, or subscriptions. To choose a display, select one of these from the drop-down menu to the left below the chart:

- **View Registration**
- **View Callers**
- **View Callee**
- **View Subscriptions**

The information stored for callers and callees is based on the list of calls that Operations Monitor keeps in memory.

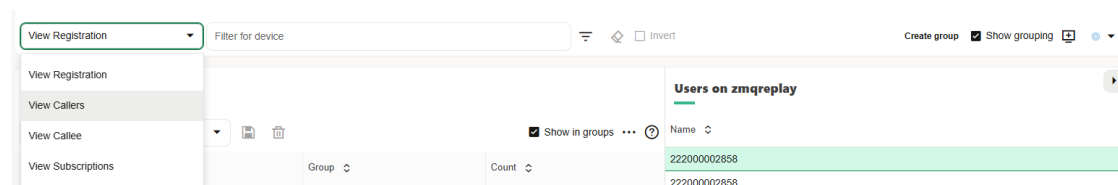
- **Restrict the User Devices page**

You can specify the statistics on the **User Devices** page to match or not match a certain regular expression. Enter a regular expression into the text field to the left of the filter button below the chart. Click **Filter**. If you want to invert the match, mark the **Invert** check box below the chart.

- **Group devices**

To create a new group of user devices, enter a regular expression in the **Filter for device** field and click the **Create group** button. The new group rule is applied to the **Device List** panel (below the chart). If the **Show grouping** check box below the chart is marked, the groupings are also applied to the pie chart.

Figure 4-62 Operations on User Devices



Note

When you create filter or group user devices, this is applied to the **User Devices** chart and the **Devices** list.

The **User Devices** chart also contains the **Show in Dashboard** icon button in the bottom-right corner. Click this button to add the panel, with the current filter settings applied, to the dashboard.

Devices List Panel

The **Devices List** panel contains two tables. The left table lists the devices by group, and the right table displays callers and callees for any device that is selected in the devices table.

Figure 4-63 Devices List Panel

Devices Name	Group	Count
▼ Non-grouped devices (28 users on 8 devices)		
Yealink SIP-T41P 36.73.193.50	Non-grouped devices	12
Yealink SIP-T46G 28.73.193.50	Non-grouped devices	6
Aastra SIP-DECT (SW-Version=6.0)	Non-grouped devices	3
Yealink SIP-T48G 35.73.193.50	Non-grouped devices	3
Panasonic-KX-TGP600CE/05.000 (bcc342a7125a)	Non-grouped devices	1
Yealink SIP-T46S 66.82.0.21	Non-grouped devices	1
Yealink SIP-T48S 66.82.0.21	Non-grouped devices	1
Panasonic-KX-TGP600CE/05.000 (bcc34200b8e5)	Non-grouped devices	1

The user devices table columns:

Table 4-18 User Device Table

Column	Description
Device name	Displays the full user agent string for each device.
Group	Indicates the group to which the device belongs.
Count	Shows the number of users per device.

Right-Click Menu

Right clicking on any of the user devices provides the following options:

- **Delete group user devices**

Removes a group definition from the system. This only effects the **User Devices** page.

- **Highlight a group**
Highlights all the devices from a group.
- **Highlight a user device name**
Highlights all the user devices with a specific name.
- **Filter by a user device name**
Filters the statistics displayed on the page by the selected user device name.

Figure 4-64 Right-Click Menu

Devices Name ↕	Group ↕	Count ↕
▼ Non-grouped devices (28 users on 8 devices)		
Yealink SIP-T41P 36.73.193.50	Non-grouped devices	12
Yealink SIP-T46G 28.73.193.50	Non-grouped devices	
Aastra SIP-DECT (SW-Version=6.0)	Non-grouped devices	
Yealink SIP-T48G 35.73.193.50	Non-grouped devices	
Panasonic-KX-TGP600CE/05.000 (bcc342a7125a)	Non-grouped devices	
Yealink SIP-T46S 66.82.0.21	Non-grouped devices	
Yealink SIP-T48S 66.82.0.21	Non-grouped devices	1

Users Using a Specific User Device

The right-side table only contains the **Name** column. An identifier is displayed for each user. If you right-click on a row in the Users table, a context menu appears with the following actions:

- **Track**
Brings you to the **User Tracking** page with the selected user entered.
- **Trace**
Brings you to the **Traces** page, where a new trace is started and filtered for the selected user.

Subscriptions

The **Subscription** page allows you to view and analyze non-call messages and notifications of presence events. Currently, only subscribe, notify, and publish messages are supported.

The **Subscription** page contains two panels:

- **Subscribed Users** panel: Displays the number of subscribers and the fluctuation over time, and
- **Subscriptions** table: Displays subscriber event information. The Subscriptions table contains a table of subscription events. The list is ordered chronologically, presenting the latest event as the first entry by default. You can resize the table columns, and the adjustments will persist even after navigating away from the page and on returning to the page.

System Settings for Subscription

These are the system settings for the Subscription feature:

Allow Number of Refresh subscription

Flag to limit the number of Refresh SUBSCRIBE entries to be seen in the ladder diagram. (Initial Subscription not included)

- Default value: 10
- Maximum value: 20
- Minimum value: 0. '0' means none of the Refresh Subscribe messages can be seen in the ladder diagram.

Allow regeneration of subscription events for user updates

If a user has Subscribed in the core once, it's realm is not re-checked till the Subscription expires and gets renewed. If realms are changed continuously and/or the customer needs to have subscriptions always matched to the current realms configuration, enable this option. Doing so, has some performance impacts on the core subscription processing.

Default value: False

Group Non-Call Subscriptions from the same user

This setting enables you to group Non-Call Subscriptions from the same user and event type. The default value is True.

Match Subscription events by comparing the username suffix

The Mediation Engine matches the related subscription attempts by the SIP username. If this value is zero, then the whole username is used. If more than zero, the number defines how many digits/characters must match.

- Default value: 0
- Maximum value: 50
- Minimum value: 0

Search for matching Non-Call subscription segments

When viewing the diagram of a Non-Call Subscription event, the Mediation Engine searches for other Non-Call subscription events that are related. This option controls the time span in which it searches, in seconds. If set to 0, the searching of related Non-Call subscription events is disabled. The default value is 10, the maximum value is 25, and the minimum value is 0.

Subscriptions expired events

If enabled, an *Expired* event is generated when a subscription binding expires.

Default value: True

Platform Setup Application Initial Log In

All Session Monitor application interfaces are accessed through encrypted HTTPS connections. At the initial login, your web browser may not recognize the server and displays the warning: This Connection is Untrusted. Click **Confirm Security Exception** to proceed.

For information about how to protect connections to the system and avoid the untrusted certificate warning in the future, see Oracle Communications Session Monitor Security Guide.

This section describes how to configure Session Monitor using the Platform Setup Application.

To configure Session Monitor:

1. In a web browser, go to `https://<ip_address>/setup`.
The **Platform Setup Application Login** page appears.
2. In the **Username** field, enter **sysadmin** and in the **Password** field, enter **oracle**.
The License Terms agreement page appears.
3. Accept each Session Monitor application license terms agreement, by selecting the **I agree to the license terms** check box.
4. Click **Proceed**.
The **Change Password** dialog box appears.
The **Platform Setup Application** page appears.
5. Change the password by doing the following:
 - a. In the **Set password** field, enter a new password.

Note

The password must have at least 8 characters. The password must contain at least one uppercase character. The password must contain a number. The password must contain a special character (@, #, -, _, .).

- b. In the **Repeat password** field, re-enter the password used in the previous step, which verifies that the password value was entered correctly.
 - c. Click **Change**.
The **Machine Type** page appears.
6. On the Machine Type page, select the machine type on which to install your licensed Session Monitor applications and components:
 - To install an Operations Monitor probe, select **Probe**.
 - To choose different Session Monitor applications, select the **Mediation Engine** and then select the required product (or applications) as per the license:
 - To install Operations Monitor, select the **Operations Monitor** check box.
 - To install Oracle Communications Control Plane Monitor, select the **Control Plane Monitor** check box.
 - To install an Operations Monitor embedded probe, select the **Probe (embedded)** check box.
 - To install Mediation Engine Connector, select the **Mediation Engine Connector** check box.

Only the checked items are included in the installation.

Note

The Machine Type page only appears the first time you configure Session Monitor prior to the products installation. Machine type cannot be changed after the PSA installation is completed.

You can select only one machine type for each installation process.

Packet Inspector probe is not supported on a Session Monitor probe with SIP/RTP sniffing for the calls and VQ analysis.

The products are machine-type specific and cannot be interchanged between machine types.

For example, the Probe machine type requires a probe product, and the Mediation Engine machine type requires the Operations Monitor product.

The machine type Mediation Engine Probe (embedded) must be chosen either with Operation Monitor or with Control Plane Monitor option selected.

7. Click *Continue*.

The machine type and application information appear in the status panel located on the right under the navigation list.

The **Configuration** page appears.

8. Configure the Session Monitor settings for the machine type you chose in step 5 in accordance with the terms of your license as follows:

- a. From the Capacity section in the Concurrent calls field, enter the number of concurrent calls printed on your license.
- b. If you have licensed RTP recording, select the RTP Recording check box.
- c. From the Capacity section in the Concurrent RTP streams field, enter the number of concurrent RTP streams printed on your license.

Note

The number entered in the Concurrent RTP streams field can cause performance and stability issues if it is set higher than what your network hardware supports. Values above 20 are not recommended. Changes to the RTP recording setting take effect only after restarting the system.

- d. In the Additional Extensions section, select the **Non Calls** check box to see the Subscription panels in the user interface. You can edit this check box even after the installation is done.
- e. From the Extensions section, select all the product extensions you have licensed.

Note

You cannot change the configured extensions after the installation. All Oracle Communications Session Monitor Enterprise users should select Media quality .

9. Click *Continue*.

The Disk Usage page appears.

10. On the Disk Usage page, specify the maximum disk usage partition for the Packet Inspector.

Note

On the Disk Usage page, specify the maximum disk usage partition for the shared file system containing the database/data storage (single raid systems). For systems with two raid arrays you can select the usage independently for both filesystems. For Probes with Packet Inspector feature you would be able to select the maximum storage capacity.

The Mediation Engine Connection List page appears.

Note

The **ME Connection List** page appears only if you have selected machine type as Probe or Mediation Engine with Probe.

11. (Optional) If you selected Probe on the Machine Type page, set which mediation engines are connected to the Operations Monitor probe.
 - a. Click **Add a new ME**.
 - b. In the Hostname or IP field, enter the IP address of the machine that hosts the mediation engine.
 - c. In the Port field, enter the port number of the mediation engine. For a Cleartext transmission enter 4741 and for TLS enter 4742.
 - d. In the Name field, enter a name for the mediation engine.
 - e. In the TLS field, select the check box for TLS transmissions or leave the check box unchecked for Cleartext.

The Operations Monitor Probe can transmit data to one or more mediation engines with either transport layer security (TLS) encryption, or with un-encrypted Cleartext. A mediation engine can connect to more than one Operations Monitor Probe or more than one Session Border Controller Probe.

Note

Oracle recommends using TLS for connections between Standalone Probes and the Mediation Engine.

12. Click **Continue**.

The Trusted Certificate page appears.

13. In the **Upload a trusted certificate** field, select **Browse** and locate the signed certificate file. Click **Continue**.

(Optional) By default, the mediation engine machine accepts only encrypted transmissions, (unless the mediation engine and probe are on the same machine); for Cleartext transmissions select the **Accept insecure connections from remote probes** check box.

Click **Continue**.

The Server Certificate page appears.

14. All Session Monitor interfaces are accessed through encrypted (secure) HTTPS connections. Each Session Monitor machine uses a unique certificate to establish secure connections and to guarantee its authenticity and protect users' data.

Do one of the following:

- To use the self-signed certificate, click **Continue**.
- To sign the server certificate with your organization's Public Key Infrastructure (PKI):
 - a. Select **Download request**.
 - b. Sign the certificate with the X.509 format.
 - c. In the **Upload signed certificate** field, select **Browse** and locate the signed certificate file.
 - d. Click **Continue**. The SMTP Configuration page appears.

Note

- To regenerate a key and certificate on install, select **Regenerate key and self-signed certificate on install** and click **Continue**.
- (Optional) Click **Download current certificate** to download the current self-signed certificate.

15. Session Monitor can send notifications and alerts directly to a user's email address. If you require notifications or alerts, select the Enable SMTP check box and fill in the relevant fields with your SMTP server details.

16. Click **Continue**.

The Capture Settings page appears.

17. The **Capture Settings** page contains a list of configured network interfaces. Monitoring can be enabled and disabled. You should have configured network devices while installing Oracle Linux 8.

18. Click **Continue**.

The Data Retention page appears. If you have enabled the **Non Calls** check box in the Configuration > Additional Extensions section, only then the Subscription Data - Subscriptions is enabled.

19. Click **Continue**.

The Install page appears.

20. (Optional) Click **Download Configuration**, which downloads your configuration settings file in the default download location of your system.

21. Open the **psa_conf.json** configuration file and verify your settings.

22. Click **Install**.

The **Did you select the right applications** dialog box appears.

23. Verify that you have chosen the correct Session Monitor applications and components for installation; after installation is complete, the selected applications and components cannot be changed.

Click **OK**.

The Platform Setup Application initiates the installation and reports its progress.

The Installation Complete dialog box appears.

24. Do one of the following:

- To go back to the Platform Setup Application, click **Back to Setup**.
- To go to a Session Monitor application dashboard, click **Go to Application**.

25. The credentials for logging in to Session Monitor are:

- For Platform Setup Application, enter the user name provided by Oracle and the password you set up in step 5.
- For Operations Monitor and Control Plane Monitor, enter the login credentials provided by Oracle Sales Consultant.

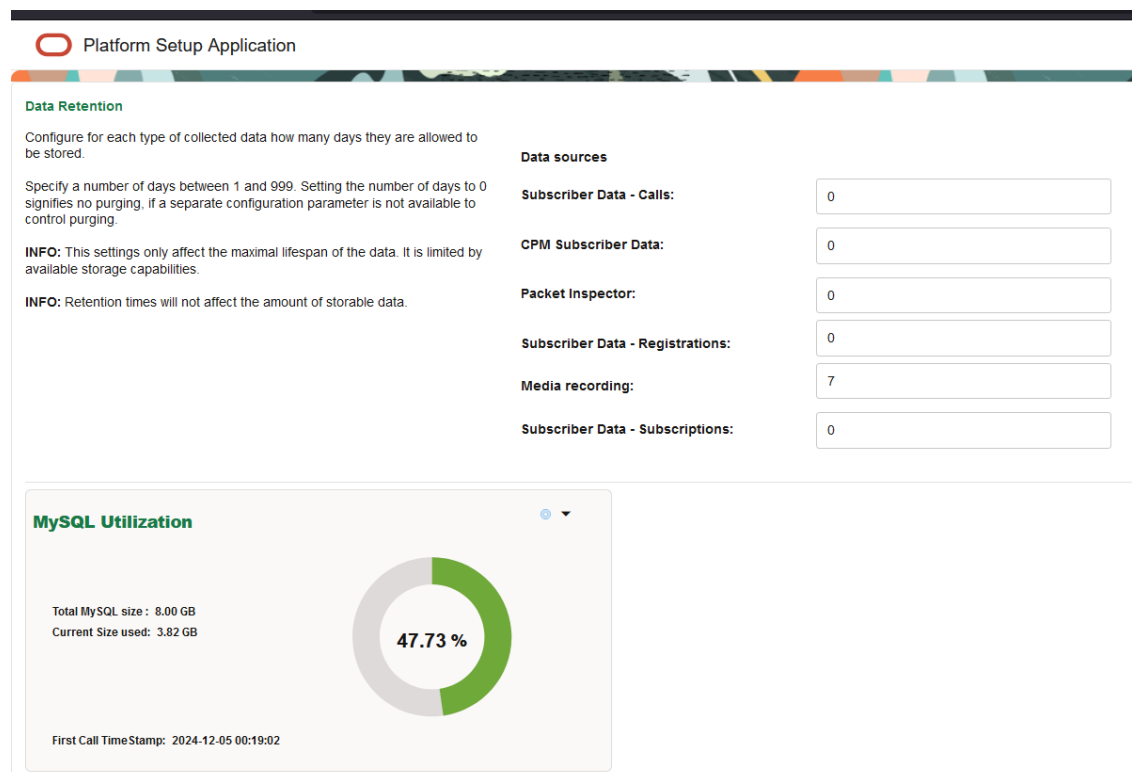
Data Retention

Data Retention allows you to get information on the utilization of MySQL. This feature is available for machine types of Mediation Engine + Probe or Mediation Engine.

Data Retention provides a graphical representation of the MySQL storage utilization. It provides an intuitive, and real-time insights into MySQL storage utilization. The Data Retention option in the Platform Setup Application, provides information on: :

- Total MySQL size
- Current size
- First call timestamp

Figure 4-65 Data Retention



You can view the graphical representation (a meter gauge) for the current size used against the total MySQL size. Session Monitor appropriately formats the size. The amount of storage used is displayed in GB if the database is smaller than 1 TB. Any database instance that is configured with more storage than 1 TB is displayed as an absolute value in TB. The meter gauge also indicates the percentage of the current MySQL size that is being used out of the total capacity. If there is no data available (when installed for the first time), the GUI displays "No data available" instead of the meter gauge. The interface provides a data refresh feature that includes options such as:

- 30 seconds
- 1 minute
- 2minutes
- 5 minute

Configuring Data Retention

Configure the Data Retention policy for different types of data collected. Set the duration for retaining the stored data.

1. Click the **Data Retention** menu option in the Platform Setup Application.

Note

The **Data Retention** feature is available only for machine types of Mediation Engine or Mediation Engine + Probe.

2. Provide the following details

Table 4-19 Data Retention Fields

Field	Description
Subscriber Data - Calls	Set the duration in days for Calls data retention. • Provide a numerical value between 1 and 999 • Set to 0 to disable.
CPM Subscriber Data	Set the duration in days for CPM Subscriber data retention. • Provide a numerical value between 1 and 999 • Set to 0 to disable.

Note

If you have set the Calls retention value as non-zero, then set a non-zero value for Media recording retention. The Calls retention value must always be greater than or equal to the Media recording retention value.

Table 4-19 (Cont.) Data Retention Fields

Field	Description
Packet Inspector	Set the duration in days for Packet Inspector data retention. - Provide a numerical value between 1 and 999 - Set to 0 to disable.
Subscriber Data - Registrations	Set the duration in days for Subscriber Data - Registrations data retention. - Provide a numerical value between 1 and 999 - Set to 0 to disable.
Media recording	Set the duration in days for Media recording data retention. If Calls retention duration has been set to a non-zero value, then set the Media recording retention duration between 1 and the value set for Calls retention. If Calls retention duration is set to 0 then you can set the Media retention duration can be set to any value between 0 and 999.
Subscriber Data - Subscriptions	Set the duration in days for Subscriber Data - Subscriptions data retention. - Provide a numerical value between 1 and 999 - Set to 0 to disable.

Subscribed Users Panel

The top panel contains a chart that traces the total number of subscribed users over time. The sampling interval is 1 minute for drawing the sample's minimum, maximum, and average values.

By default, a window of three hours is presented. The time frame can be adjusted and the chart allows for panning.

Figure 4-66 Subscribed Users Panel



Note

If Operations Monitor has no subscription information over a period of time (due to factors like recent start up, downtime, or lack of traffic), that interval is indicated in the chart by a gray area.

Subscriptions Table

The **Subscriptions** panel contains a table of the subscription events. The list is ordered chronologically, presenting the latest event as the first entry by default. The table can be resorted and/or filtered. For more information, see "[Filtering](#)".

Note

If the system setting *Group New Subscriptions from the Same User* is true, duplicate subscription events in state 'New' from the same users are grouped together. However, since the grouping is done on each requested chunk, duplication removal over different chunks does not work.

This table lists the column descriptions for the **Subscriptions** table:

Table 4-20 Subscriptions Table

Column	Description
User	Contains the user part of the AOR; if the system setting Use users domains is enabled, the domain part is also included in this field. When specifying a filtering token, all users that contain that token (position independent) will be shown.
Event Type	Event-type(SIP header Event of SUBSCRIBE) the User is Subscribing for. Filtering is done by matching a given string.
Source IP address	The IP address of the network device that initiated the subscription event. Filtering is done by matching a given string.
Destination IP address	The IP address of the network server targeted by the subscribing device. Filtering is done by matching a given string.
Timestamp	The moment in time when the event occurred. Filter by specifying an interval (between <i>Before</i> and <i>After</i>) or a Date (the <i>On</i> date selector).
Notifier	The device configured in Settings> Platform Devices that was targeted by the subscriber's device when subscribing. When trying to filter by a certain device, a list of configured devices is presented out of which one or more can be selected.
Method	Sip Message in this subscriptions.
Subscription State	State of this subscription as per the "Subscription-State" header in NOTIFY Message
User Device	The User-Agent header of the SUBSCRIBE request.

Table 4-20 (Cont.) Subscriptions Table

Column	Description
Subscribe Count	Indicates the total number of SUBSCRIBE messages received for this subscription including initial and refresh
Notify Count	Indicates the total number of NOTIFY messages received for this subscription
Publish Count	Indicates the total number of PUBLISH messages received for this subscription
Event State	The state of the Subscription Event. For filtering one can choose to filter the presented list to only include some of the possible event states.
Code	The SIP code that the subscription message exchange finished with. Filter by specifying any valid SIP reply code.

Right-Click Contextual Menu - Subscriptions

Right-click menu actions are as follows:

Table 4-21 Right-click menu options

Menu option	Description
Track subscription user <user name>	Loads the User Tracking page with the User field pre-filled in the search panel taken from the event
Create Trace with user <user name>	Loads the Traces page with the User field pre-filled with the value taken from the corresponding subscription event.
WHOIS	Allows you to inquire who is the owner of the IP used as the source of the subscription. A window appears that contains the record stored into the WHOIS database for the given address
PING	Pings the source IP address.
Track IP	Redirects you to the IP tracking page to get the details about the specific IP. For more information, see IP Tracking
Filter Table for...	<i>Filter table for ...</i> allows you to filter for: • Other subscription events of the same user • All subscription involving the same address or device. • The same SIP response code or event type.
Subscription Details	Opens the Subscription Details window
Message Flow	Opens the Message Flow window

Figure 4-67 Subscriptions Table

Devices Name ↕	Group ↕	Count ↕
▼ Non-grouped devices (28 users on 8 devices)		
Yealink SIP-T41P 36.73.193.50	Non-arouped devices	12
Yealink SIP-T46G 28.73.193.50	Non	
Aastra SIP-DECT (SW-Version=6.0)	Non	
Yealink SIP-T48G 35.73.193.50	Non	
Panasonic-KX-TGP600CE/05.000 (bcc342a7125a)	Non	
Yealink SIP-T46S 66.82.0.21	Non	
Yealink SIP-T48S 66.82.0.21	Non-arouped devices	1

Subscription Table Actions

The **Subscription** table provides a few action buttons.

- Click the **Subscription Details** button when a row is selected in the table, and a window appears containing *Subscription details* for individual Subscription events; this window can be also opened by simply double-clicking on the selected row in the table.
- Click the **Message Flow** button to open a **SIP message flow diagram** window that depicts the network entities involved and message exchange of the Subscription event.
- Click the **Set Columns** button hide/unhide the columns from the display.
- Click the **Filters** button to define filters and to see the required information in the table. The Filters selection list, **Save**, **Delete**, **Rename**, and **Clear** are all options related to Filters. For more information, see [Filters](#) section.
- The **CSV export** button allows to have all table entries exported into a CSV file. If the contents of the table have been filtered, the contents of the exported CSV file will only contain the filtered results.

Note

You can set the maximum number of lines to export in a CSV file using the system setting **Maximum number of lines exported with CSV export**.

- The **Show in Dashboard** button allows you to add the panel, with the current filter settings applied, to the dashboard.

Note

Many of these actions are available by right-clicking on a row.

Subscription Details

The details window for a Subscription event contains the following information:

- The user of full AOR (subjected to settings).

- The timestamp when the event occurred.
- The network entity of the platform having received the subscription request (the ingress device).
- The IP address used to originate the requests.
- The type of subscription event.
- A table that contains details about the exchanged messages in this event, listed in chronological order.

This table lists the columns in Subscriptions Details window.

Table 4-22 Subscription Details Window

Column	Description
User	The user of full AOR
Proto	The network transport protocol used to carry the SIP messages from client to the platform. This field can be either UDP or TCP.
Src IP	The IP address of the device that generated the message.
Dst IP	The IP address of the device that received the message.
Date and Time	The moment in time when the mirrored network packet was received by Operations Monitor.
Details	The device that received the message; just as with <i>Source</i> , it can be either the client's or platform's.
Message	SIP message which caused the particular event.

Subscription Details Actions

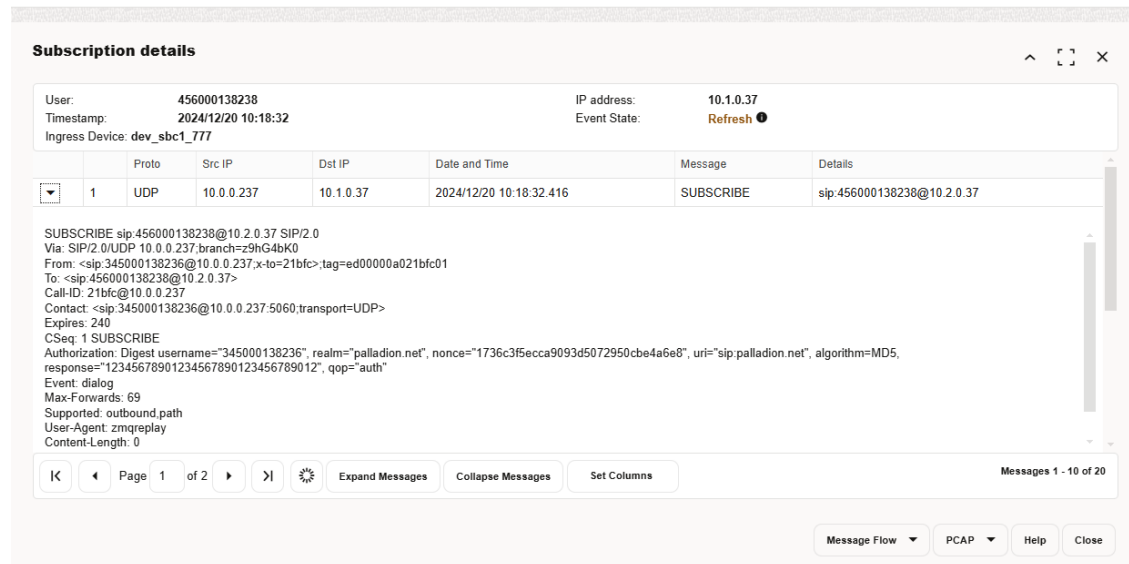
In the **Subscription Details** window:

- Click **Expand Messages** to view all the raw SIP message as seen on the network. You can click **Collapse Messages** again to display the brief view of the messages.
- Click Set columns to Hide or Unhide columns from display.

Note

You can view one raw message at a time by clicking the Triangle button on any of the table's entries, as shown.

Figure 4-68 Subscription Details Window with One Expanded Raw Message



The **Message flow** list box has the following options:

- **Message Flow**
Creates a *message flow diagram*
- **Open in new window**
Opens the message flow diagram in a new window.
- **SVG**
Opens the message flow diagram in a SVG window from which you can save the message flow as a .png graphic.

The **PCAP** option allows you to save the shown network packets into a PCAP file.

Subscription Event Categories

Subscription events are categorized as follows:

- **Failed**
Final response code is greater than 299.
- **Unauthorized**
Two consecutive transactions are answered with 401, or when one 401 transaction is not followed by another SUBSCRIBE request in the next 5 seconds.
- **New**
A new Subscribe binding was created for this user.
- **Refresh**
Subscription event of type 'Refresh' is created for a successful SUBSCRIBE or NOTIFY transaction with 200 response when the Subscription of the user is refreshed.
- **Gone**
Subscription event of type 'Gone' is created when there is Un-subscribe (expire value is '0' in SUBSCRIBE/NOTIFY transaction) for the Subscribed user.

- **Expired**

A binding is considered expired when the time interval specified in the 'expires' parameter from the Notifier's answer is over. No messages are associated with this type of event. For each Subscribed user, timer_expired is initialized with expires value agreed for the subscription. When the subscription of the user is not refreshed and if the subscription duration exceeds the 'expires' value.

Subscriptions Panel in User Tracking

The Subscriptions Panel contains two tables where the first displays the current subscriptions and the second panel displays history of the subscription events for the tracked user.

Figure 4-69 Subscriptions Panel in User Tracking

Current Subscriptions							
Event	IP Address	Expires	Expires In	Refreshed	First Seen	Link	User Device
dialog	10.0.7.239	360	265	2024/12/20 10:22:32	2024/12/20 10:18:32		zmqreplay

History Subscriptions						
User	Event Type	Source IP Address	Timestamp	Notifier	Event State	Code
456000023032	dialog	10.0.7.239	2024/12/20 10:18:32	dev_p1_481	Refresh	200
456000023032	dialog	10.0.7.239	2024/12/20 10:06:32	dev_p1_481	Expired	200
456000023032	dialog	10.0.7.239	2024/12/20 09:54:32	dev_p1_481	Expired	200
456000023032	dialog	10.0.7.239	2024/12/20 09:44:32	dev_p1_481	Expired	200
456000023032	dialog	10.2.0.31	2024/12/20 09:44:32	dev_s1_641	Expired	200

Table 4-23 Current Subscribed Contacts Table

Column Name	Description
Event	Event the User is Subscribing for. Filtering is done by matching a given string
IP address	The IP address from where the Subscribe request originates.
Expires	The expiration interval set by the server.
Expires In	The remaining time until expiration.
Refreshed	The last time the registrations was refreshed.
First Seen	The first time the tracked user subscribed successfully.
Link	An indicator for the link quality to the tracked user which is displays in the Link Quality section. This column remains blank unless the particular users subscribed source IP address is set to be tracked for the Link Quality. The indicator is of LED diode icon with coloring based on the quality measured.
User Device	The User-Agent header of the SUBSCRIBE request.
Suggested Expires	It contains the value of the Expires header sent with the SUBSCRIBE request.

Table 4-23 (Cont.) Current Subscribed Contacts Table

Column Name	Description
VLAN	VLAN of the device.

The lower table contains the history of subscription events for the tracked user.

Subscribed Users Panel in IP Tracking

In the **IP Tracking** page, select the **Subscribed Users** toggle check box to display or hide the **Subscribed Users** panel

The **Subscribed Users** panel displays the users that are currently subscribed with the searched IP address(es). The results include the user, the IP address, and the subscribed event of the user.

You can jump to the **Subscribed Event** page using the right-click menu.

Figure 4-70 Subscribed Users Panel

User	IP Address	Subscribed Event
234000058049	10.1.0.48	dialog
234000125249	10.1.0.48	dialog
234000115649	10.1.0.48	dialog
234000173249	10.1.0.48	dialog
234000221249	10.1.0.48	dialog
234000182849	10.1.0.48	dialog
234000240449	10.1.0.48	dialog
234000278849	10.1.0.48	dialog
234000288449	10.1.0.48	dialog
67800029349	10.1.0.48	dialog

Subscriptions Tab in Devices Page

The **Subscriptions** tab aggregates information about each device where the Subscribe message originated from.

Figure 4-71 Subscriptions Tab

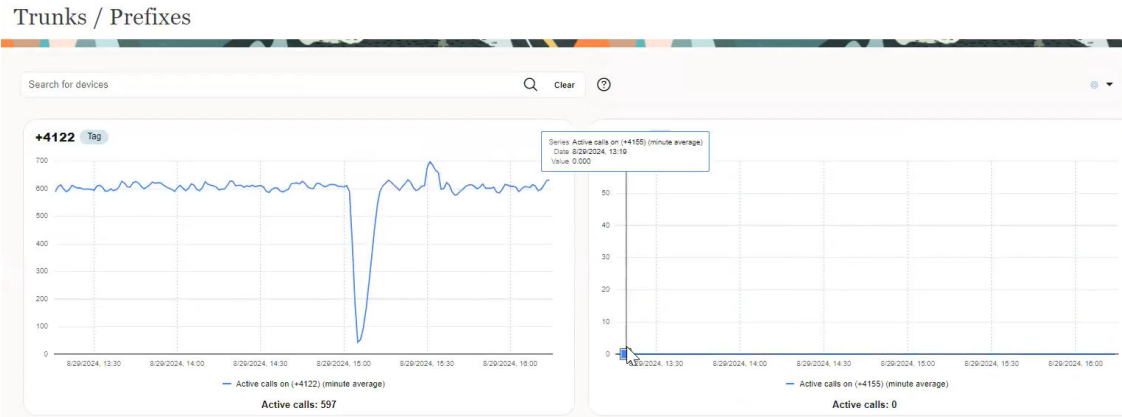
Calls going through this Device			Terminated Calls		Originated Calls		Registrations		Subscriptions										
Subscription Details		Message Flow						(None)				Save		Delete Rename		Clear			
User	Event Type	Source IP Address		Timestamp		Notifier		Subscription State		User Device		Event State		Code					
444000119887	dialog	10.0.0.6		2024/12/20 11:08:19		dev_p1_246				zmqreplay		Expired		200					
666000119847	dialog	10.0.0.6		2024/12/20 11:08:18		dev_p1_246				zmqreplay		Expired		200					
222000119807	dialog	10.0.0.6		2024/12/20 11:08:18		dev_p1_246				zmqreplay		Expired		200					
444000119767	dialog	10.0.0.6		2024/12/20 11:08:17		dev_p1_246				zmqreplay		Expired		200					
666000119727	dialog	10.0.0.6		2024/12/20 11:08:17		dev_p1_246				zmqreplay		Expired		200					
222000119687	dialog	10.0.0.6		2024/12/20 11:08:16		dev_p1_246				zmqreplay		Expired		200					
444000119647	dialog	10.0.0.6		2024/12/20 11:08:16		dev_p1_246				zmqreplay		Expired		200					
666000119607	dialog	10.0.0.6		2024/12/20 11:08:15		dev_p1_246				zmqreplay		Expired		200					
444000119527	dialog	10.0.0.6		2024/12/20 11:08:14		dev_p1_246				zmqreplay		Expired		200					
666000119487	dialog	10.0.0.6		2024/12/20 11:08:14		dev_p1_246				zmqreplay		Expired		200					
222000119447	dialog	10.0.0.6		2024/12/20 11:08:14		dev_p1_246				zmqreplay		Expired		200					

Trunks/Prefixes

The **Trunks/Prefixes** page presents an overview of the status of all configured trunks and prefixes on the monitored platform. The **Active sessions** chart displays the number of inbound (ingress) and outbound (egress) sessions for each trunk or prefix.

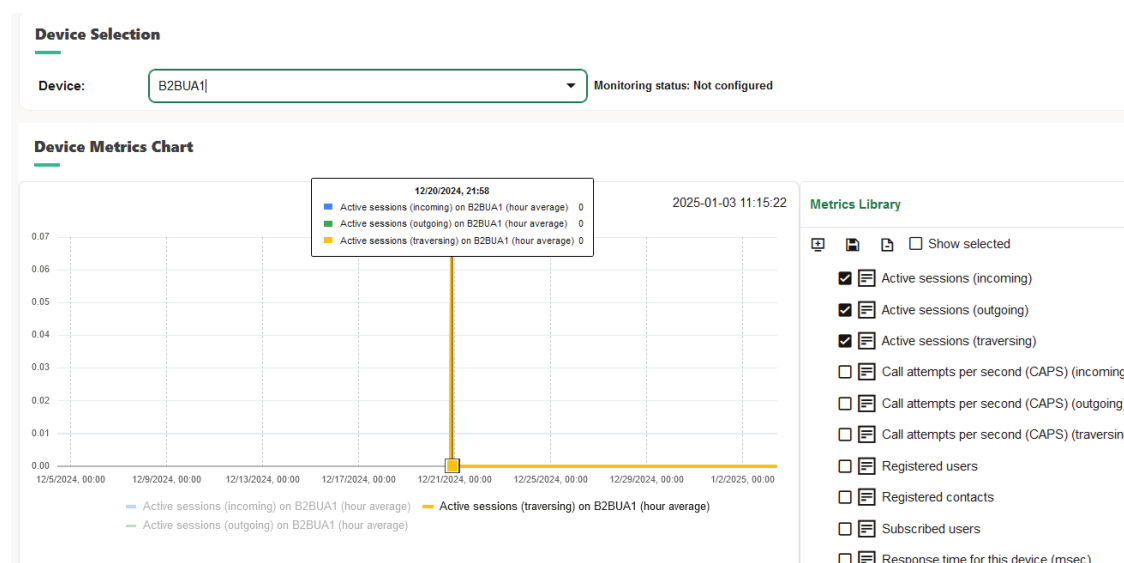
The chart name for prefixes includes a tag, and the chart name for trunks includes a device. This provides clear identification and organization for trunks and prefixes.

Figure 4-72 Trunks/Prefixes Page



The metric displayed in the chart can be configured in the **Device** page. To change the metric to display for a trunk, select the metric from the *Metrics Library* and click **Save selection**.

Figure 4-73 Configuring the Metric to Display for a Trunk



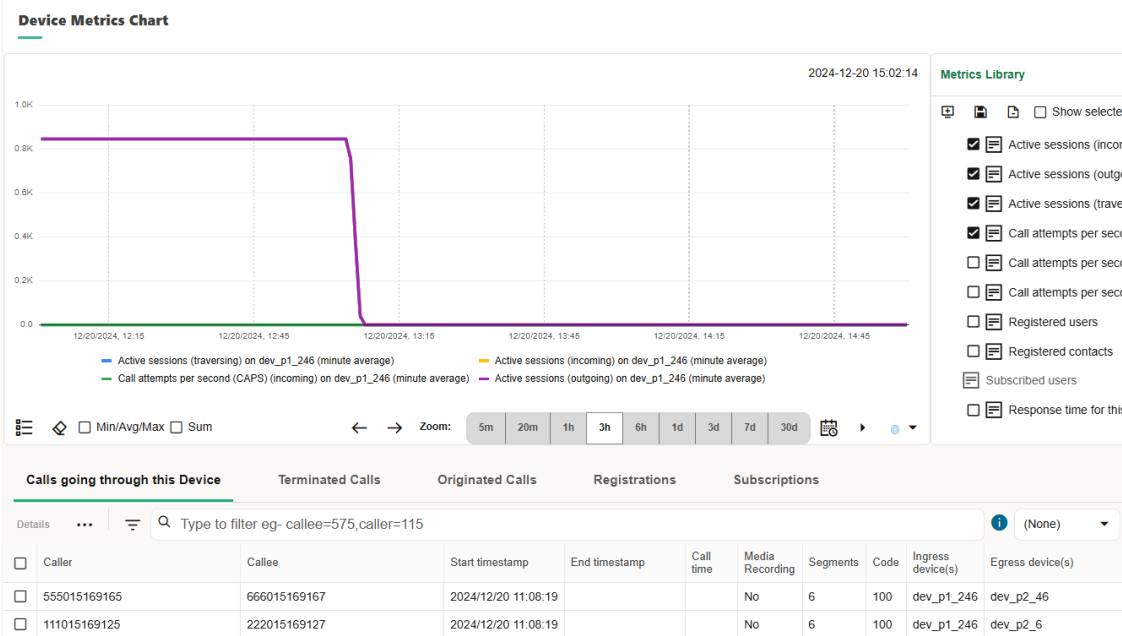
After the change, the **Call attempts** chart is displayed for the *SuperTrunk*.

When you click on a trunk, you are taken to the **Devices** page for this trunk. Clicking on a prefix has no effect. The **Trunks/Prefixes** page also features a **Refresh** button, which can be used to control the update interval for the textual information contained on the page.

Devices

The **Devices** page shows not only an overview of all configured platform devices, but it also aggregates information about each individual platform device. To use it, the platform devices (or trunks) have to be configured in the platform settings. For more information, see "[Platform Devices](#)". This page contains a device selection drop-down menu, a device metrics chart, and a tab panel providing details about calls, registrations, and voice quality for the selected device.

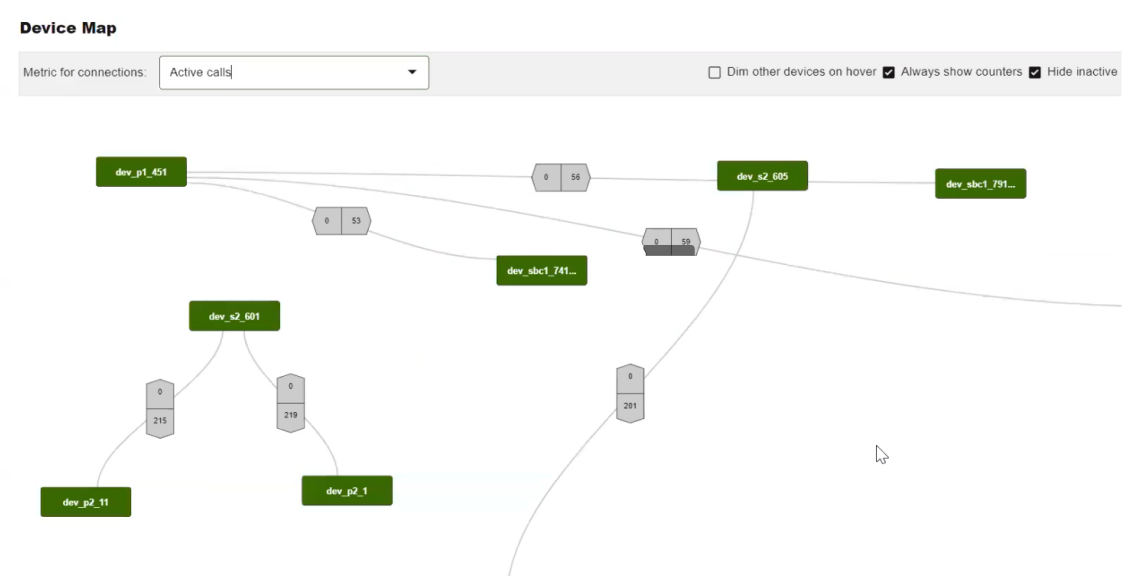
Figure 4-74 Devices Page



Device Map

You can display a map of devices by clicking on **Device Map** button. It shows an overview of the status and activity for all configured devices on the monitored platform. The devices are displayed as nodes on a topological graph; activity between nodes is shown in the lines connecting them. From this page it is easy to monitor platform activity and status.

Figure 4-75 Device Map



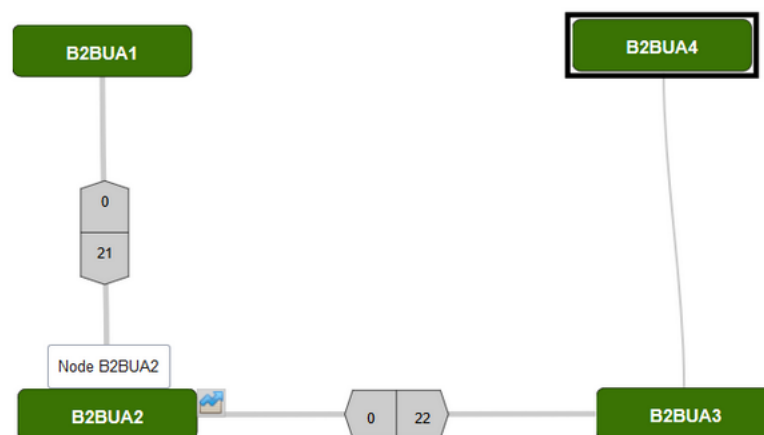
Note

With Session Monitor 4.4 enables the displays of Trunk Devices on the **Device Map** page.

Once added, you can drag and drop devices around the page to best represent the local network topology. There is a **Reset Layout** button on the toolbar to reset the page.

Hover over the node with the mouse cursor to show the inbound and outbound value of the displayed metric of a node.

Figure 4-76 Hovering Over a Device to Display the Active Metric

**Note**

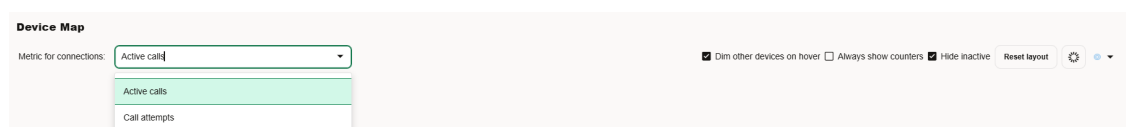
A maximum of 50 devices can be enabled for the Device Map.

Device Map Toolbar

The Devices page has view display options, which are configurable through controls on the toolbar.

shows the display options that are available on the Device page toolbar.

Figure 4-77 Device Map Toolbar

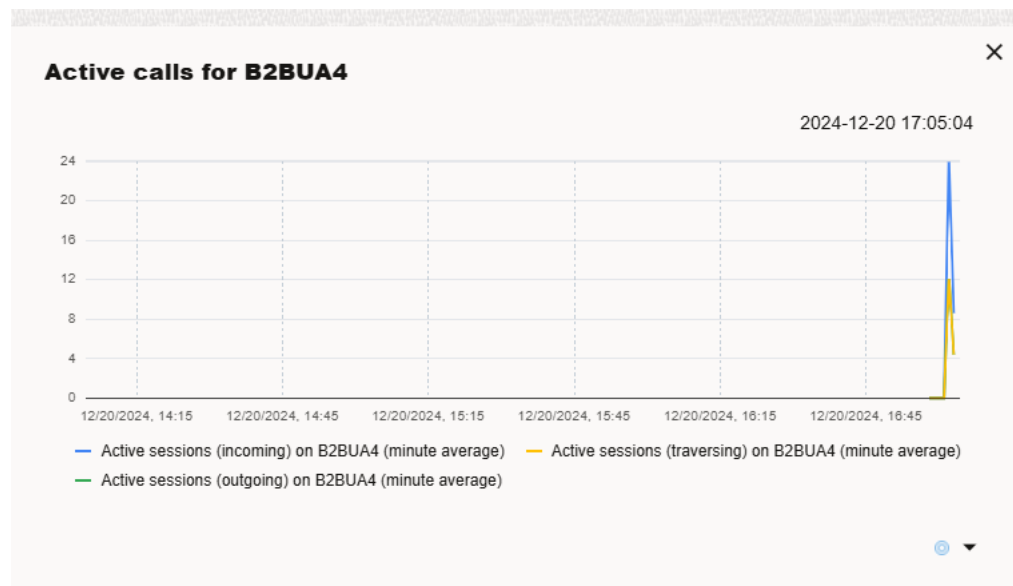


The display options are as follows:

- **Metric for Connections**
Select the metric to be displayed.
- **Dim other devices on hover**
Select this option to dim other devices when you hover over a specific device.
- **Always show counters**
Select the **Always show counters** check box to change the above device hovering behavior so that Operations Monitor always shows metric data.
- **Hide inactive**
Select the **Hide inactive** check box to hide devices that are not interacting with others. This can often help de-clutter the display. When the page data is refreshed all devices are checked to see whether they have become active.
- **Reset layout**
Applies the default layout if the configuration by the user via dragging and dropping becomes unmanageable.
- **Refresher**
The **Devices** page features a **Refresh** button to control the update interval for the metric data contained in the page. For more information, see "[Refresh Button](#)".

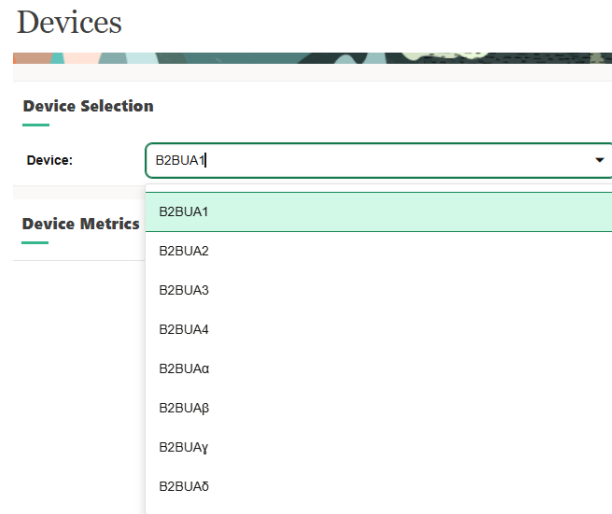
More detailed information about the selected metric can be displayed per-device by clicking on the **Details** button that appears overlaid on a device while hovering:

Figure 4-78 Click on a Device to Display Detail Information About the Active Metric



Device Selection Panel

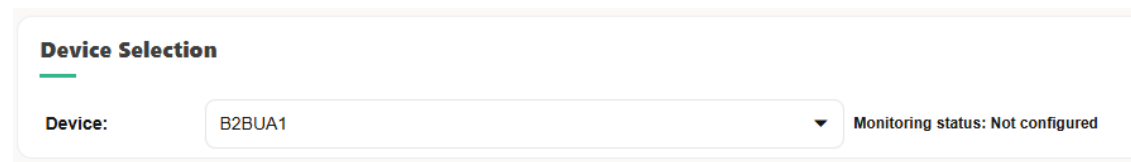
The **Device Selection** panel determines the device whose details are displayed on the page. Select a device from the drop-down menu.

Figure 4-79 Device Selection Panel

Device Monitoring Status

The **Device Selection** panel displays the monitoring status for the current device. This information is available only if device monitoring is configured for that specific platform device.

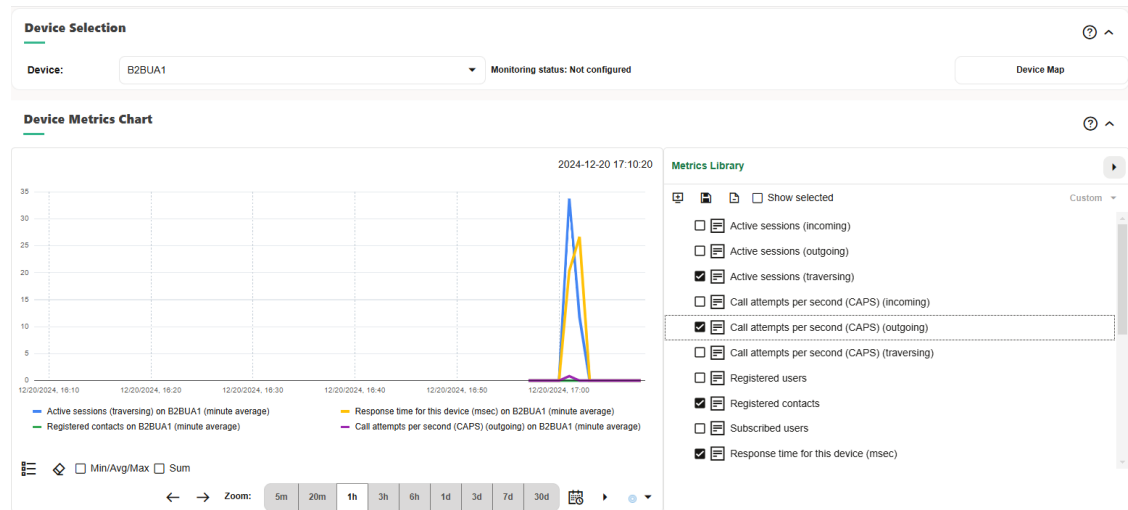
To configure device monitoring, refer to "[Platform Devices](#)" and "[Device Monitoring](#)".

Figure 4-80 Device Monitoring Status

Device Metrics Chart

The **Device Metrics Chart** displays the evolution of the selected device metrics from the **Metrics Library**. For more information about the Metrics Library, see "[KPI/Metrics](#)". Device metrics are special as they measure properties connected to a certain platform device.

Figure 4-81 Device Metrics Chart

**Note**

You can select up to five metrics by marking the check box of the desired metric.

Click the **Expand/Collapse Metric Library** option to collapse the Metric Library panel to be for a larger view of the chart.

- In the **Metrics Library** section:
 - Click **Show in Dashboard** to add the **Device Metrics Chart** to the **Dashboard** by
 - Click **Save Selection** to save the current set of selected metrics for the specific device in the **Device Metrics** chart.
 - Click **Clear Selection** to clear the current set of selected metrics for the specified device in the **Device Metrics** chart.
 - Click **Show Selected** to display only those metrics in the Metric Library section, which have been selected for the chart.
 - At the bottom of the Device Metrics chart:
 - Click **CSV Export information displayed in the chart** to export the chart metrics to .CSV file.
 - Click the **Show Min/Avg/Max** check box, this check box controls whether minute or hour minima and maxima are displayed for each selected metric.
 - Click the **Sum** check box to view the sum values of the selected KPI metrics. The Sum values for 1 hour, 3 hours, 6 hours, and 1 day are displayed in minutes, whereas the sum values for 3 days, 7 days, and 30 days are displayed in hours. You cannot view the sum values for 5 minutes and 20 minutes. The sum values can be exported to .CSV file using the **CSV Export** option.
- This table represents the states shown on the UI of the Device Metrics chart.

Table 4-24 UI States

Option Selected	UI State
None (Default)	The average value of selected KPI is displayed in the chart.
Sum check box selected	The sum value of the KPI is shown on the chart.
Only min/max/avg check box selected	The min/max/avg value of KPI will be shown on the chart.
Sum and min/max/avg check boxes are selected	Both values are shown on the chart.

Note

The metric **Synthetic KPI** cannot be viewed as a sum value.

The other controls are described in the section on chart panels. For more information, see "[Charts](#)".

Calls Going Through This Device Tab

The **Calls going through this device** tab is similar to the *Recent calls* panel described in the "[Calls](#)" section. The table displays only the calls that have an inbound leg to the current device and an outbound leg from the current device.

Figure 4-82 Calls Going Through This Device Tab

Calls going through this Device																
Terminated Calls																
Originated Calls																
Registrations																
Subscriptions																
Details	...	Type to filter eg- callee=575, caller=115	(None) Edit Advanced													
Caller	Callee	Start timestamp	End timestamp	Call time	Media Recording	Segments	Code	Ingress device(s)	Egress device(s)	DTMF	Diversion	Diversion Type	Call-Transfer	Min. MOS	Avg. MOS	State
☐ 555015169165	666015169167	2024/12/20 11:08:19			No	6	100	dev_p1_246	dev_p2_46							Failed
☐ 111015169125	222015169127	2024/12/20 11:08:19			No	6	100	dev_p1_246	dev_p2_6							Failed
☐ 333015169085	444015169087	2024/12/20 11:08:19			No	12	100	dev_p1_246	dev_p2_46, dev_s2_326, dev_s1_366							Failed
☐ 555015169045	666015169047	2024/12/20 11:08:19			No	6	100	dev_p1_246	dev_p2_6							Failed
☐ 111015169005	222015169007	2024/12/20 11:08:18			No	6	100	dev_p1_246	dev_p2_46							Failed
☐ 333015168965	444015168967	2024/12/20 11:08:18			No	6	100	dev_p1_246	dev_p2_6							Failed
☐ 555015168925	666015168927	2024/12/20 11:08:18			No	6	100	dev_p1_246	dev_p2_46							Failed
☐ 111015168885	222015168887	2024/12/20 11:08:18			No	6	180	dev_p1_246	dev_p2_6							Failed
☐ 333015168845	444015168847	2024/12/20 11:08:18			No	4	180	dev_p1_246								Failed

Terminated Calls Tab

The **Terminated calls** tab is exactly like the **Recent calls** panel described in "[Calls](#)". The table displays only the calls which have an inbound leg to the current device. Terminated calls do not have an outbound leg from the current device.

Figure 4-83 Terminated Calls Tab

Calls going through this Device																
Terminated Calls																
Originated Calls																
Registrations																
Subscriptions																
Details	...	Type to filter eg- callee=575, caller=115	(None) Edit Advanced													
Caller	Callee	Start timestamp	End timestamp	Call time	Media Recording	Segments	Code	Ingress device(s)	Egress device(s)	DTMF	Diversion	Diversion Type	Call-Transfer	Min. MOS	Avg. MOS	State
☐ 555015086605	666015086607	2024/1...	2024/1...	2'5"	No	6	200	dev_p...	dev_p...					4.41	4.41	Fl...
☐ 111015004365	222015004367	2024/1...	2024/1...	2'5"	No	6	200	dev_p...	dev_p...							Fl...
☐ 555015002005	666015002007	2024/1...	2024/1...	2'5"	No	6	200	dev_p...	dev_p...					4.41	4.41	Fl...
☐ 555014980885	666014980887	2024/1...	2024/1...		No	6	487	dev_p...	dev_p...							Ca...
☐ 111014921085	222014921087	2024/1...	2024/1...	2'5"	No	6	200	dev_p...	dev_p...					3.95	4.26	Fl...
☐ 111014843325	222014843327	2024/1...	2024/1...	2'5"	No	1	200	dev_p...						4.41	4.41	Fl...
☐ 111014602725	222014602727	2024/1...	2024/1...	0'...	No	1	200	dev_p...								Fl...

Originated Calls Tab

The **Originated calls** tab is exactly like the **Recent calls** panel described in "[Calls](#)". The table displays only the calls which have an outbound leg from the current device. Originated calls do not have an inbound leg to the current device.

Figure 4-84 Originated Calls Tab

Calls going through this Device

Terminated Calls

Originated Calls

Registrations

Subscriptions

Details

...

🔍

Type to filter eg- callee=575,caller=115

(None)

Edit Advanced

<

Registrations Tab

The **Registrations** tab is similar to the **Registrations** panel described in "[Registrations](#)". However, it only displays registrations which are handled by the current device.

Figure 4-85 Registrations Tab

Calls going through this Device			Terminated Calls	Originated Calls	Registrations	Subscriptions			
Registration Details		Message Flow	...						
					(None)			Rename	
User	Contacts			Source IP Address	Timestamp	Registrar	Event	Code	User Device
444000009646	sip:333000009644@10.0.0.5:5060;transport=UDP			10.0.0.5	2024/12/20 13:21:57	dev_sbc1_445	Expired	0	
444000033646	sip:333000033644@10.0.0.5:5060;transport=UDP			10.0.0.5	2024/12/20 13:21:57	dev_sbc1_445	Expired	0	
444000057646	sip:333000057644@10.0.0.5:5060;transport=UDP			10.0.0.5	2024/12/20 13:21:57	dev_sbc1_445	Expired	0	
444000081646	sip:333000081644@10.0.0.5:5060;transport=UDP			10.0.0.5	2024/12/20 13:21:57	dev_sbc1_445	Expired	0	
666000009606	sip:555000009604@10.0.0.5:5060;transport=UDP			10.0.0.5	2024/12/20 13:21:57	dev_sbc1_445	Expired	0	
666000033606	sip:555000033604@10.0.0.5:5060;transport=UDP			10.0.0.5	2024/12/20 13:21:57	dev_sbc1_445	Expired	0	
666000057606	sip:555000057604@10.0.0.5:5060;transport=UDP			10.0.0.5	2024/12/20 13:21:57	dev_sbc1_445	Expired	0	
666000081606	sip:555000081604@10.0.0.5:5060;transport=UDP			10.0.0.5	2024/12/20 13:21:57	dev_sbc1_445	Expired	0	
222000009566	sip:111000009564@10.0.0.5:5060;transport=UDP			10.0.0.5	2024/12/20 13:21:47	dev_sbc1_445	Expired	0	
222000033566	sip:111000033564@10.0.0.5:5060;transport=UDP			10.0.0.5	2024/12/20 13:21:47	dev_sbc1_445	Expired	0	
222000057566	sip:111000057564@10.0.0.5:5060;transport=UDP			10.0.0.5	2024/12/20 13:21:47	dev_sbc1_445	Expired	0	
222000081566	sip:111000081564@10.0.0.5:5060;transport=UDP			10.0.0.5	2024/12/20 13:21:47	dev_sbc1_445	Expired	0	
666000081486	sip:555000081484@10.0.0.5:5060;transport=UDP			10.0.0.5	2024/12/20 13:21:47	dev_sbc1_445	Expired	0	

Note

The **Registrations** tab is not available for gateway devices and trunks.

Subscriptions Tab in Devices Page

The **Subscriptions** tab aggregates information about each device where the Subscribe message originated from.

Figure 4-86 Subscriptions Tab

Calls going through this Device										Terminated Calls		Originated Calls		Registrations		Subscriptions				
Subscription Details		Message Flow	...									(None)		Save	Delete	Rename	▼	Clear		
User	Event Type		Source IP Address		Timestamp		Notifier		Subscription State		User Device		Event State		Code					
444000119887	dialog		10.0.0.6		2024/12/20 11:08:19		dev_p1_246				zmqreplay		Expired		200					
666000119847	dialog		10.0.0.6		2024/12/20 11:08:18		dev_p1_246				zmqreplay		Expired		200					
222000119807	dialog		10.0.0.6		2024/12/20 11:08:18		dev_p1_246				zmqreplay		Expired		200					
444000119767	dialog		10.0.0.6		2024/12/20 11:08:17		dev_p1_246				zmqreplay		Expired		200					
666000119727	dialog		10.0.0.6		2024/12/20 11:08:17		dev_p1_246				zmqreplay		Expired		200					
222000119687	dialog		10.0.0.6		2024/12/20 11:08:16		dev_p1_246				zmqreplay		Expired		200					
444000119647	dialog		10.0.0.6		2024/12/20 11:08:16		dev_p1_246				zmqreplay		Expired		200					
666000119607	dialog		10.0.0.6		2024/12/20 11:08:15		dev_p1_246				zmqreplay		Expired		200					
444000119527	dialog		10.0.0.6		2024/12/20 11:08:14		dev_p1_246				zmqreplay		Expired		200					
666000119487	dialog		10.0.0.6		2024/12/20 11:08:14		dev_p1_246				zmqreplay		Expired		200					
222000119447	dialog		10.0.0.6		2024/12/20 11:08:14		dev_p1_246				zmqreplay		Expired		200					

5

Customers

This chapter describes how to work with the customer experience and troubleshooting features of Oracle Communications Operations Monitor.

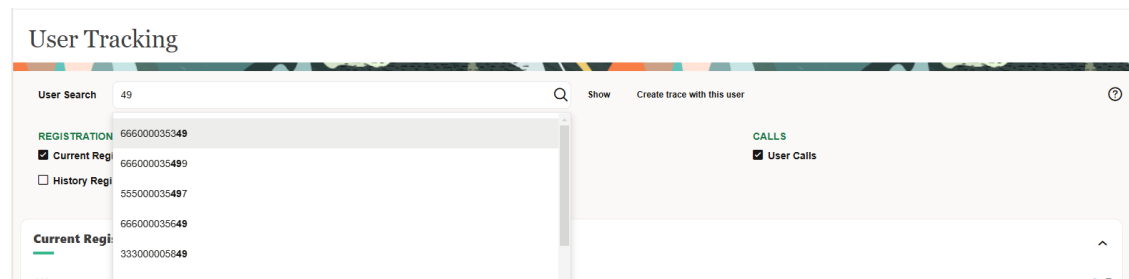
User Tracking

The **User Tracking** page can be accessed under the **Customers** section of the main menu. This page aggregates information for each user of the monitored platform and displays the history of the user's registrations and the calls. A *user* in Operations Monitor is identified by the user name part and optionally by the host name part of a SIP URI.

User Search Panel

The **User Search** panel allows you to specify the user that needs to be tracked on the **User Tracking** page. It is enabled with *live search* functionality. As soon as you type an identifier in the text field, a background search for users containing the text you entered in the field is performed. A maximum of 30 found users is displayed in the drop down selection.

Figure 5-1 User Search Panel



Registrations Panel in User Tracking

The Registrations Panel can be activated by selecting a set of two checkboxes - **Current Registrations** and **History Registrations** which you can toggle to view or hide the current registered contacts and history of the registration events for the tracked user.

Note

By default, the **Current Registrations** and **User Calls** check boxes are enabled.

Figure 5-2 Registrations Panel

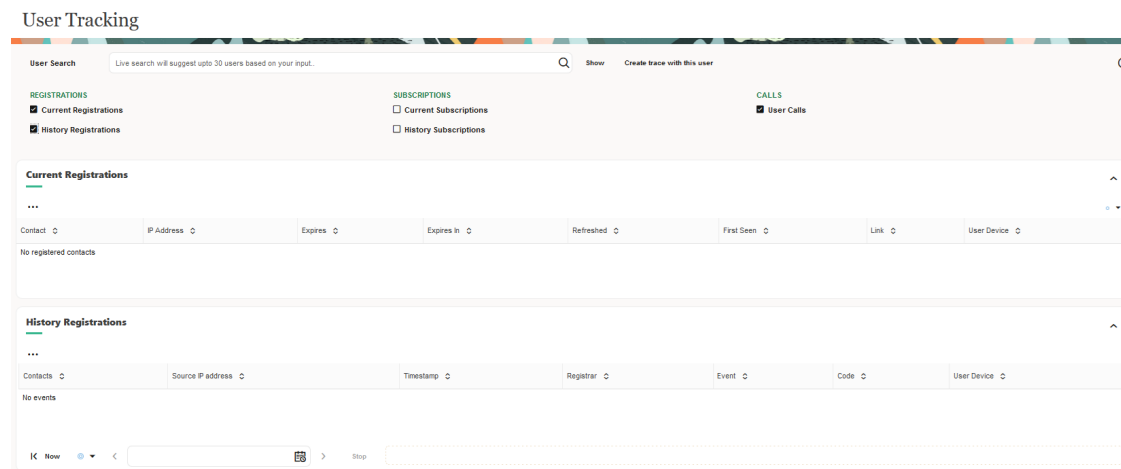


Table 5-1 Current Registered Contacts Table

Column Name	Description
Contact	The Contact header of the REGISTER request.
IP address	The IP address the REGISTER request originates from.
Expires	The expiration interval set by the server.
Expires In	The remaining time until expiration.
Refreshed	The last time the registration was refreshed.
First Seen	The first time the tracked user registered successfully.
Link	An indicator for the link quality to the tracked user which is displays in the Link Quality section. This column remains blank unless the particular users registered source IP address is set to be tracked for the Link Quality. The indicator is of LED diode icon with coloring based on the quality measured.
User Device	The User-Agent header of the REGISTER request.
Suggested Expires	It contains the value of the Expires header sent with the REGISTER request.
VLAN	VLAN of the device.

The lower table contains the history of registration events for the tracked user.

Subscriptions Panel in User Tracking

The Subscriptions Panel can be activated by selecting a set of two checkboxes - **Current Subscriptions** and **History Subscriptions** which you can toggle to view or hide the current subscribed contacts and history of the subscription events for the tracked user.

Figure 5-3 Subscriptions Panel

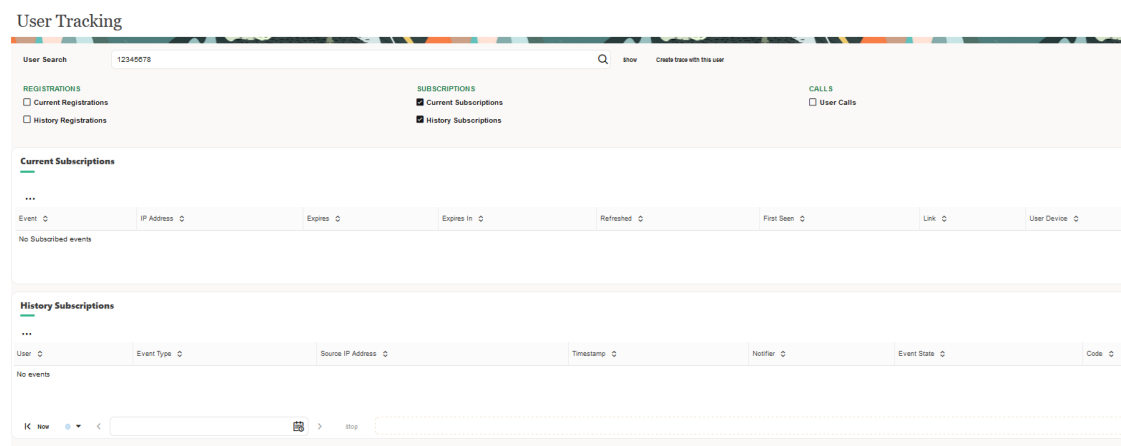


Table 5-2 Current Subscriptions Table

Column Name	Description
Event	The Contact header of the Subscribe request.
IP address	The IP address the Subscribe request originates from.
Expires	The expiration interval set by the server.
Expires In	The remaining time until expiration.
Refreshed	The last time the Subscription was refreshed.
First Seen	The first time the tracked user subscribed successfully.
Link	An indicator for the link quality to the tracked user which is displays in the Link Quality section. This column remains blank unless the particular users subscribed source IP address is set to be tracked for the Link Quality. The indicator is of LED diode icon with coloring based on the quality measured.
User Device	The User-Agent header of the SUBSCRIBE request.
Suggested Expires	It contains the value of the Expires header sent with the SUBSCRIBE request.
VLAN	VLAN of the device.

The lower table contains the history of Subscription events for the tracked user.

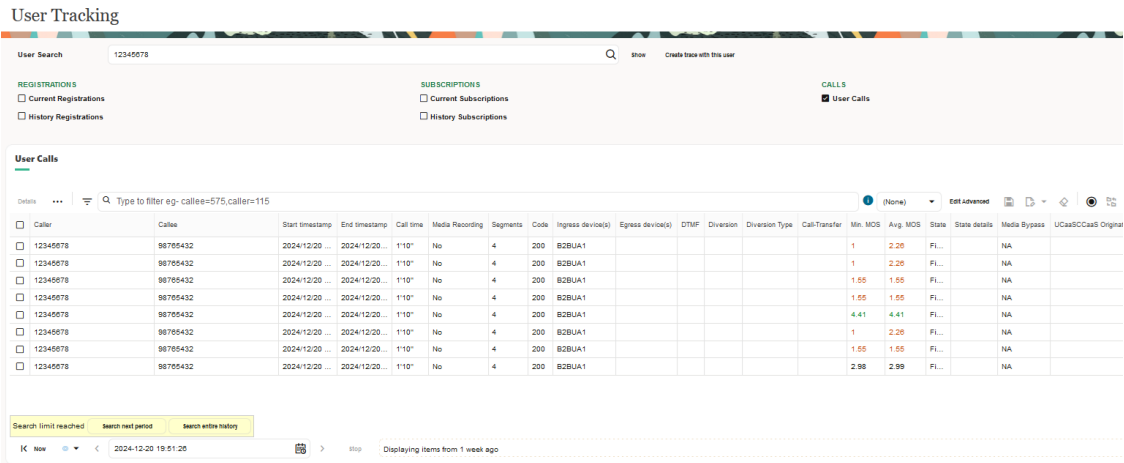
User Calls Panel

The **User Calls** panel can be activated by selecting the **User Calls** checkbox, which you can toggle to display or hide the history of calls that the tracked user participated in either as a caller or a callee.

Note

By default, the **Current Registrations** and **User Calls** check boxes are enabled.

Figure 5-4 User Calls Panel

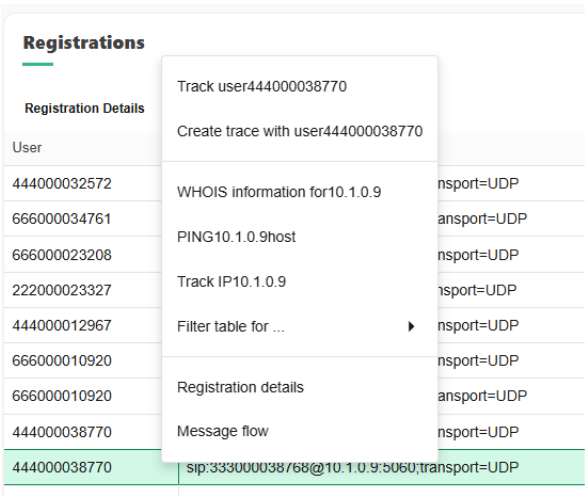


You can double-click or select a call in the **User Calls** table, and click on **Details** to get to the **Call Info** dialog box. Click on the **Message flow** to display a diagram of the underlying SIP messages of a call. You can also download the message flow in HTML format, to your local hard drive. For details on the usage of the **User Calls** table refer to "[Calls](#)".

User Actions

The graphic shows the actions that can be performed on the tracked user.

Figure 5-5 Right-Click On the Registration Event



Right clicking on a register event from the second table of the **Registrations** panel shows the following actions you can perform on the tracked user:

- **Track User username**
Displays the User Tracking page for the specific user where you can see information for this user on Registrations, Subscriptions, and Calls.
- **Create trace with this user**

Redirects you to the **Traces** page and starts a trace that is filtered for the tracked user. For more information, see "[Traces](#)".

- **WHOIS information**

Gives the result of a WHOIS query for the IP address of the user.

Figure 5-6 WHOIS Results for an IP

WHOIS Information

```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf
%
% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.
%
% Information related to '62.220.31.128 - 62.220.31.255'

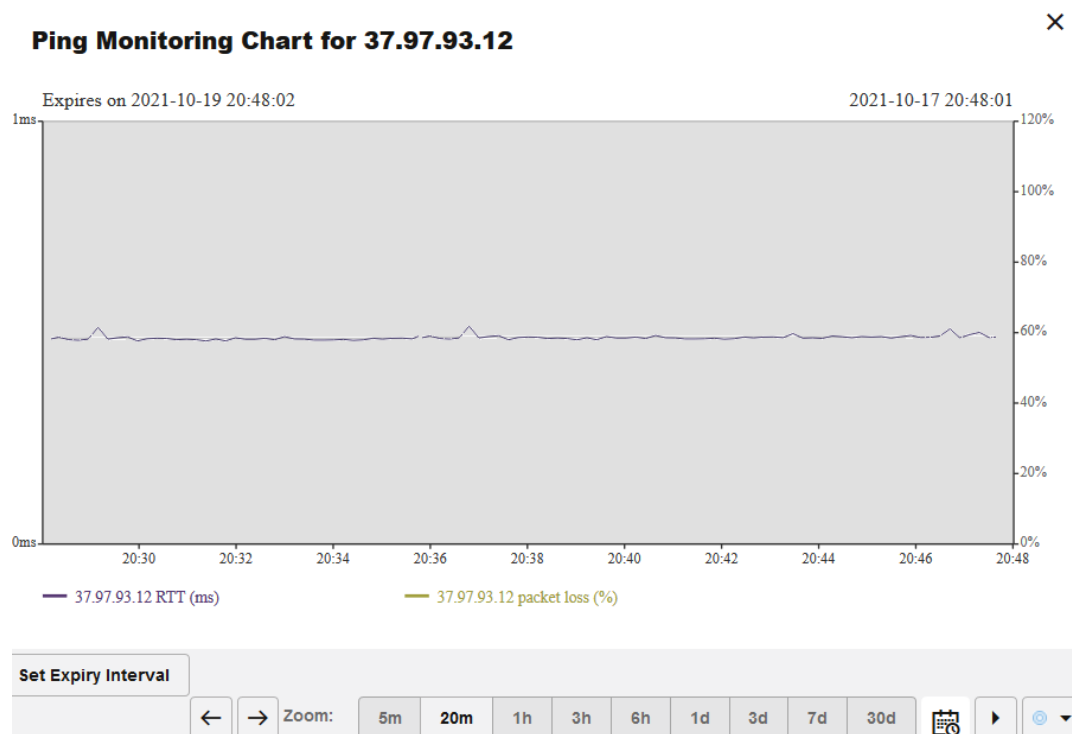
inetnum:        62.220.31.128 - 62.220.31.255
netname:        DE-IPTRGO-GmbH-01
descr:          VT Internet DSL
country:        DE
admin-c:        VTB-RIPE
tech-c:         VTB-RIPE
status:         ASSIGNED PA
remarks:        customer network
mnt-by:         VT-MNT
source:         RIPE # Filtered

role:           Versatel Hostmaster
remarks:        Internet Engineering
address:        Versatel West GmbH
address:        Unterte-Wilms-Strasse 29
address:        44143 Dortmund
address:        Germany
phone:          +49 (0) 231 399 0
abuse-mailbox:  abuse@versatel.de
admin-c:        DMS66-RIPE
admin-c:        AD8661-RIPE
admin-c:        NL1054-RIPE
```

- **PING host**

Checks the quality of the link between the provider and subscriber's host by pinging the host periodically.

Figure 5-7 Link Quality with the host



- **Track IP**

Redirects you to the **IP tracking** page to get the details about the specific IP. For more information, see "[IP Tracking](#)".

Right-click on a registered contact gives you a similar menu as the previous one.

IP Tracking

The **IP Tracking** page aggregates information about a single IP address. It displays all users registered with the given IP address, and provides links to the **User Tracking** page for each user. Either IPv4 or IPv6 addresses may be supplied.

Note

Pinging an IPv6 address is not supported.

IP Search Panel

The **IP Search** panel contains the text input field where you can enter the IP address you want to track. This field accepts network ranges. If a range is entered, Operations Monitor displays the available information for the IP addresses from the range. For example, entering 62.220.31.0/24 displays all the users that are registered from an IP address within that network range.

Figure 5-8 IP Search Panel

IP Tracking

IP Search

172.16.0.1

Show

☐ Registered Users

☐ Subscribed Users

☒ Calls

Calls

Details

...

☰

🔍 Type to filter eg- callee=575,caller=115

i

(None)

▼

Edit Advanced

☐	Caller	Callee	Start timestamp	End timestamp	Call time	Media Recording	Segments	Code	Ingress device(s)	Egress device(s)
☐	12345678	98765432	2024/1...	2024/1...	1'...	No	4	200	B2BUA1	
☐	12345678	98765432	2024/1...	2024/1...	1'...	No	4	200	B2BUA1	

Registered Users Panel

In the **IP Tracking** page, select the Registered Users toggle check box to display or hide the **Registered Users** panel. This panel displays the users that are currently registered with the searched IP address(es). The results include the user, the IP address, and the number of registered contacts of the user are included in the results.

Note

By default, the **Registered Users** and **Calls** check boxes are enabled.

You can jump to the **User Tracking** page using the right-click menu.

Figure 5-9 Registered User's Panel

User	IP Address	Registered Contacts
222000008426	10.0.0.5	1
444000001756	10.0.0.5	1
222000008546	10.0.0.5	1
222000009236	10.0.0.5	1
222000033536	10.0.0.5	1
222000009146	10.0.0.5	1
444000000856	10.0.0.5	1
222000009956	10.0.0.5	1
222000009806	10.0.0.5	1
222000008726	10.0.0.5	1

Subscribed Users Panel in IP Tracking

In the **IP Tracking** page, select the **Subscribed Users** toggle check box to display or hide the **Subscribed Users** panel

The **Subscribed Users** panel displays the users that are currently subscribed with the searched IP address(es). The results include the user, the IP address, and the subscribed event of the user.

You can jump to the **Subscribed Event** page using the right-click menu.

Figure 5-10 Subscribed Users Panel

User	IP Address	Subscribed Event
234000058049	10.1.0.48	dialog
234000125249	10.1.0.48	dialog
234000115649	10.1.0.48	dialog
234000173249	10.1.0.48	dialog
234000221249	10.1.0.48	dialog
234000182849	10.1.0.48	dialog
234000240449	10.1.0.48	dialog
234000278649	10.1.0.48	dialog
234000288449	10.1.0.48	dialog
678000029349	10.1.0.48	dialog

Calls Panel in IP Tracking Page

In the **IP Tracking** page, select the **Calls** toggle check box to display or hide the **Calls** panel

The **Calls** panel displays recent and historical information for calls made in recent days. Calls displayed in this panel were made from or to the searched IP address(es). Calls to the searched address are only listed if they were completed. The calls from this table are updated in real-time as their state changes.

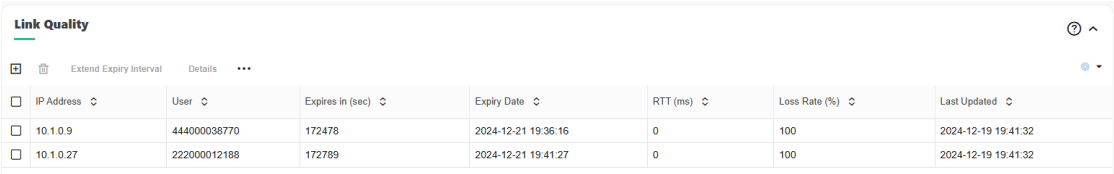
For a description of the columns in the **Calls** panel, refer to [Table 4-6](#):

Link Quality

Operations Monitor has the ability to ping the public IP of a subscriber or ping the IP of a proxy. You can access Link Quality under the *Customer Experience & Troubleshooting* section of the main menu. It sends out 10 *ICMP Echo Request* packets every minute with a 500 milliseconds delay between successive packets to an individual target. Based on the incoming responses and elapsed time for the requests, it reports on the target's reachability, packet loss and round trip delay.

For every pinged address, Operations Monitor measures an average value of round-trip time (RTT) and **loss rate**. The loss rate is the percentage of ICMP Echo Replies lost for a remote target as shown.

Figure 5-11 Link Quality Table



☐	IP Address	User	Expires In (sec)	Expiry Date	RTT (ms)	Loss Rate (%)	Last Updated
☐	10.1.0.9	444000038770	172478	2024-12-21 19:36:16	0	100	2024-12-19 19:41:32
☐	10.1.0.27	222000012188	172789	2024-12-21 19:41:27	0	100	2024-12-19 19:41:32

Check Link Quality to a Subscriber

To check the quality of the link between the provider and the subscriber, the provider can start pinging the user's IP from the **User Tracking** page. This is usually helpful to track voice quality problems. For more information, see "[User Tracking](#)".

Check Link Quality to a Proxy

To start pinging a new address, you must add the IP address to the **Network Link Quality** page by clicking on the **Add** button. IP address is added and is configured to be pinged for 2 days. Once you add a pinged address, the interval is extended by pressing the **Extend Expiry Interval** button of the **Link Quality** panel.

Figure 5-12 Add a Target to Ping

To stop pinging a target, you can delete the address by selecting it and pressing the **Delete** button of the **Link Quality** panel.

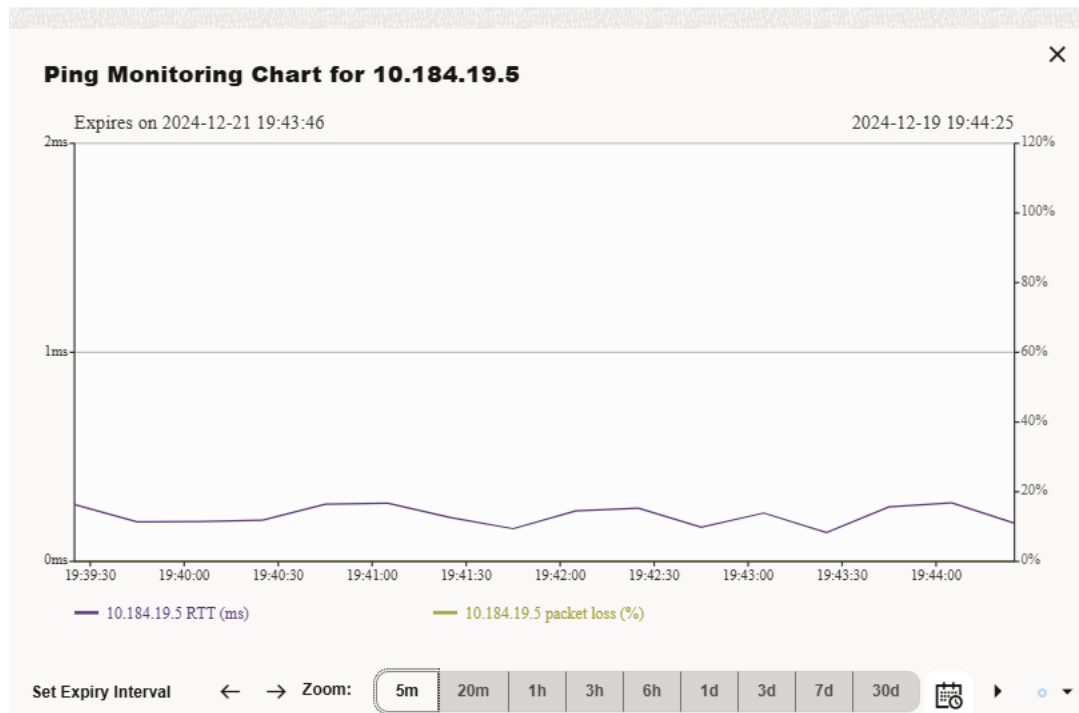
The **Link Quality** panel describes the quality of a link through its columns.

Table 5-3 Link Quality Panel

Column Name	Description
IP Address	Uses the IPv4 address of the target to ping either the subscriber or a proxy.
User	In case of a subscriber, the User field provides the username.
Expiry Date	Define the time when Operations Monitor ceases to ping the target.
Expires in (sec)	Define the pinging interval period in seconds.
RTT (ms)	Takes the average value of the <i>round trip time</i> in milliseconds.
Loss Rate (%)	Takes the average value of the <i>loss rate</i> in percentage.
Last Updated	Describes when the link quality values were last updated.

As an example, displays link quality results with three particular targets. The first two targets have a good link quality as their medium loss rate is equal to 0% and the average value of the RTT is 0.04ms and 11.95ms. The last target is unreachable as it doesn't respond at all to ping requests. Thus its average loss rate is equal to 100%.

Figure 5-13 Good Link Quality



A time chart of positive link quality presents RTT and Loss Rate values over one hour. The dark blue wave defines the RTT values, and the light green wave defines loss rate. On a scale of 0ms up to 1ms from the left side of the graph, RTT values slightly vary around the medium value of 0.04ms. As the loss rate value stays constant at 0%, it overlaps with the horizontal axis with 2 exceptions where is 100%.

Figure 5-14 Poor Link Quality



A poor link quality evolution is shown in the graphic.

6

Control Plane Monitor

This chapter describes how to work with Oracle Communications Control Plane Monitor, which has advanced monitoring and troubleshooting features for Diameter transactions.

Oracle Communication Operations Monitor supports the IMS Cx interface. The Cx Diameter messages are correlated with SIP calls and appear in the Operations Monitor **Calls** user interface and not in the Control Plane Monitor user interface. The following Diameter interfaces are supported:

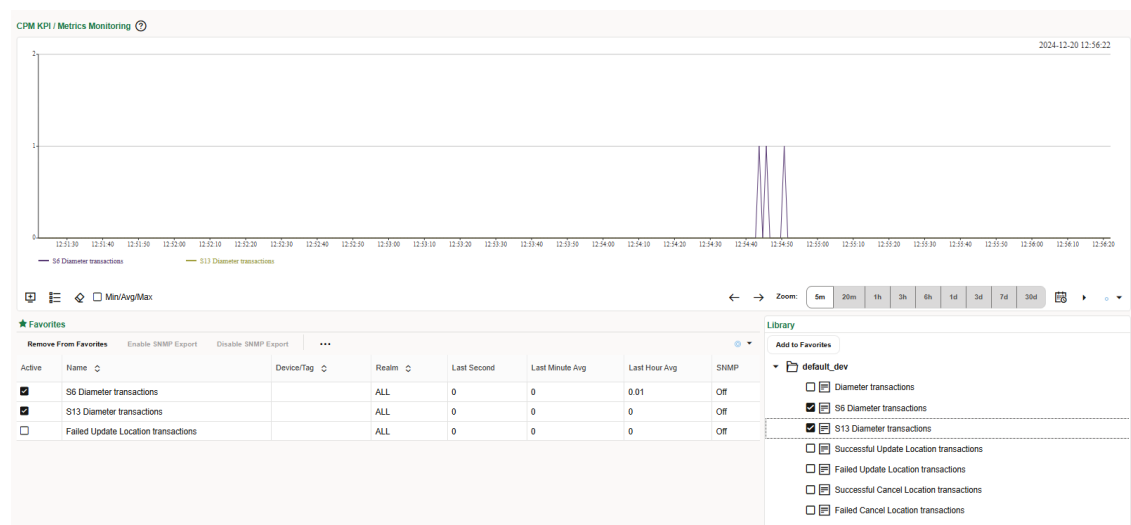
- S6a
- S6d
- S13
- S13

KPI/Metrics

The Control Plane Monitor **KPI/Metrics** page offers similar functionality as the **KPI/Metrics** page from the Operations Monitor product. The difference is that only Diameter specific KPIs are available, and they are not editable.

This is the Control Plane Monitor KPI/Metrics page.

Figure 6-1 Control Plane Monitor KPI/Metrics Page



Currently, the following Platform Wide KPIs are available:

Table 6-1 Platform Wide KPIs

Platform Wide KPIs	Description
Diameter transactions	Number of new hop-by-hop Diameter transactions per second that pass the filter configured in the Platform Setup Application, regardless of Application ID.
S6 Diameter transactions	Number of new hop-by-hop Diameter transactions per second that have the Application ID 16777251 (3GGP S6a/S6d).
S13 Diameter transactions	Number of new hop-by-hop Diameter transactions per second that have the Application ID 16777252 (3GGPS13/S13').
Successful Update Location transactions	Number of completed hop-by-hop Diameter transactions per second that have the Diameter command 316 (Update Location) and the result code 2001 (Success).
Failed Update Location transactions	Number of completed hop-by-hop Diameter transactions per second that have the Diameter command code 316 (Update Location) and a result code different from 2001 (Success).
Successful Cancel Location transactions	Number of completed hop-by-hop Diameter transactions per second that have the Diameter command 317 (Cancel Location) and the result code 2001 (Success).
Failed Cancel Location transactions	Number of completed hop-by-hop Diameter transactions per second that have the Diameter command code 317 (Cancel Location) and a result code different from 2001 (Success).
Probe Metrics - Local Probe (OCSM)	
Synthetic KPIs	

The following KPIs are available on a per-device basis:

- Incoming S6 Diameter transactions**
 Number of new Diameter transactions per second that are received by the given device and have the Application ID 16777251 (3GGP S6a/S6d).
- Outgoing S6 Diameter transactions**
 Number of new Diameter transactions per second that are created by the given device and have the Application ID 16777251 (3GGP S6a/S6d).
- Successful incoming Update Location transactions**
 Number of completed Diameter transactions that are received by the given device and have the Diameter command 316 (Up- date Location) and the result code 2001 (Success).
- Failed incoming Update Location transactions**
 Number of completed Diameter transactions that are received by the given device and have the Diameter command 316 (Update Location) and a result code different from 2001 (Success).
- Successful incoming Cancel Location transactions**
 Number of completed Diameter transactions that are received by the given device and have the Diameter command 317 (Cancel Location) and the result code 2001 (Success).

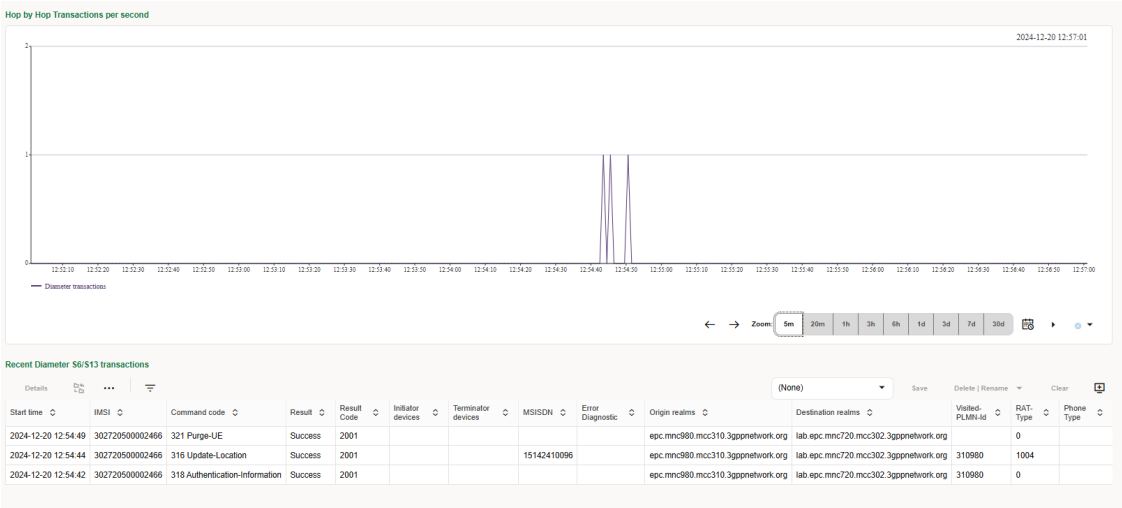
- **Failed incoming Cancel Location transactions**
Number of completed Diameter transactions that are received by the given device and have the Diameter command 317 (Cancel Location) and a result code different from 2001 (Success).

Transactions

The **Transaction** page is the central repository for transaction analysis in Control Plane Monitor. You can analyze the transaction traversing the platform in real-time or historically. Control Plane Monitor automatically correlates the transactions into End-to-End transactions.

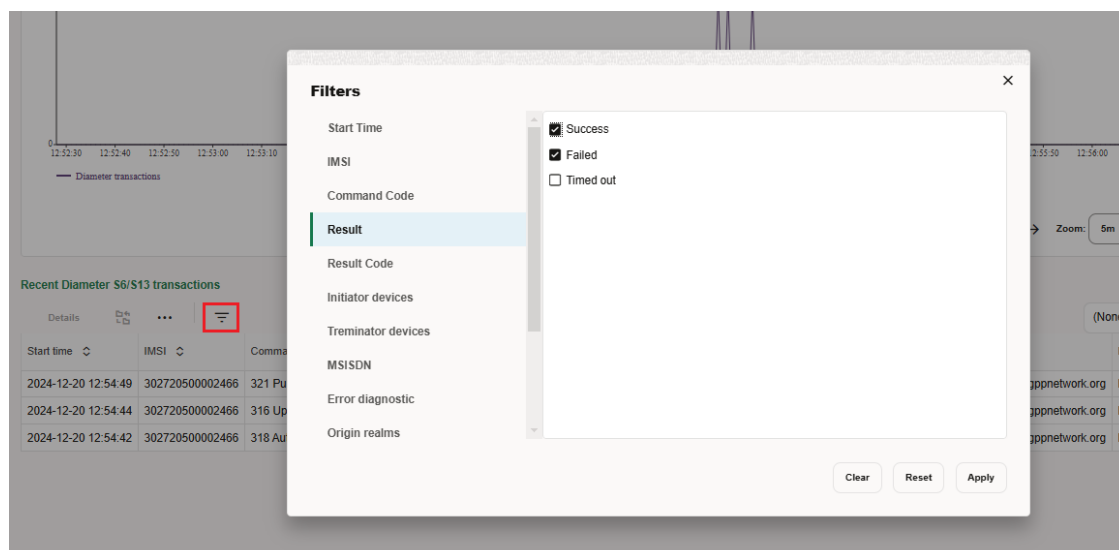
This page contains two panels: the top one shows the Diameter transactions KPI while the bottom one contains the recent S6/S13 transactions.

Figure 6-2 Control Plane Monitor Transactions Page



Filtering Columns

The **Transactions** table supports Filtering for all columns. For more information, see [Filtering](#)

Figure 6-3 Control Plane Monitor Filtering

Transaction Details

To open the **Transaction details** window, double-click on a row from the **Recent S6/S13 transactions** table or select the transaction and click the **Details** button.

The upper portion for the window contains brief identification information of the transaction: the IMSI, the Diameter realms, the MSISDN and so on.

The bottom portion of the window contains the list of messages composing the transaction. You can drill down in the details of each message by expanding the tree.

Click the **Message flow** button to open a *message flow diagram* with the messages involved in this transaction.

To save the raw messages of the transaction into a PCAP file, click the **PCAP** button.

Figure 6-4 Transaction Details

Transaction Details

IMSI
302720500002466

MSISDN
15142410096

Start
2024-12-20 12:54:44

Id
2

Origin Realm
epc.mnc980.mcc310.3gppnetwork.org

Destination Realm
lab.epc.mnc720.mcc302.3gppnetwork.org

Initiator Devices
n/a

Terminator Devices
n/a

Command Code
316 Update-Location

Result
Success

Result Code
2001

Error Diagnostic
n/a

Visited-PLMN-Id
310980

RAT-Type
1004

Software Version
01

Messages

Set Columns

		Code	Type	Error	Src IP	Dst IP	Hop.Id	End.Id	Date and Time
▶	1	316	Request	No	10.13.101.12:11111	173.209.219.135:3868	1352461500	348807	2024-12-20 12:54:44
▶	2	316	Answer	No	173.209.219.135:3868	10.13.101.12:11111	1352461500	348807	2024-12-20 12:54:44

◀ ◻ ▶

Page 1 of 1

⌂ ⚙

Expand Messages

☐ Plain Text View

Messages 1 - 2 of 2

⚙

Message Flow

PCAP

Close

Message Flow

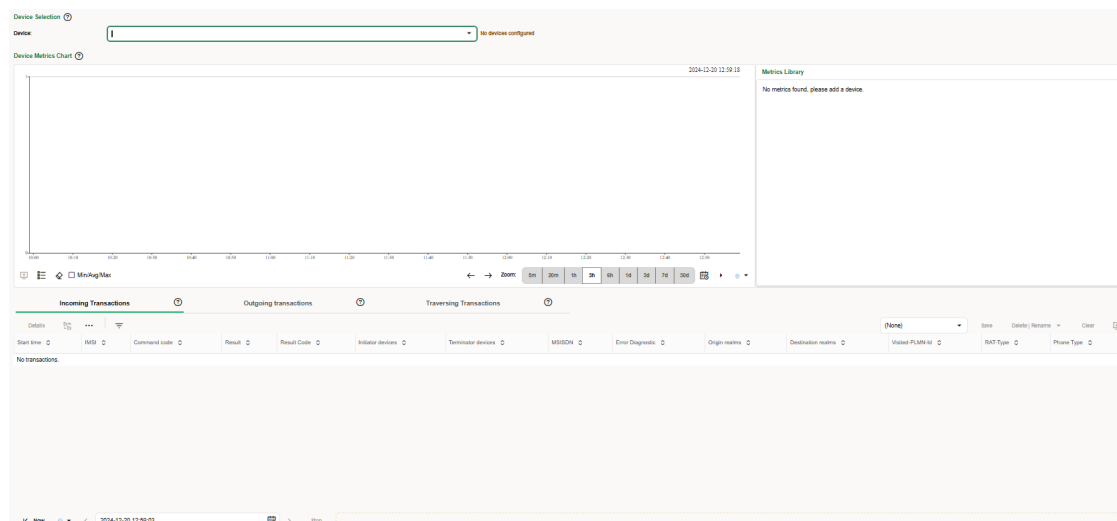
You can generate a *message flow diagram* by two means:

- Select one or more transactions from the **Recent S6/S13 Transaction** list and click the **Draw Diagram** button from the top toolbar. To select more transactions, hold the Shift key while selecting.
- Open the Transaction details window for a given transaction and click the **Message Flow** window.

Devices

The **Devices** page offers a device centric view of the Diameter transaction and KPIs.

Figure 6-5 Control Plane Monitor Devices Page



The **Device Selection** panel determines the device whose details are displayed on the page. Only configured diameter devices are available in this drop down. For example, HSS, Diameter agent, and Diameter proxy. For more information on the diameter devices, see [Table 7-9](#).

The **Device Metrics Chart** displays the evolution of the selected device metrics from the *Metrics Library*.

You can add the **Device Metrics Chart** to the **Dashboard** by clicking the **Show in Dashboard** icon button.

At the bottom of the chart, the **Show Min/Avg/Max** check box controls whether minute or hour minima and maxima are displayed for each selected metric. For more information on the chart panel controls, see "[Charts](#)".

Incoming Transactions

The **Incoming Transactions** tab is similar with the **Recent S6/S13 Transactions** panel, which is described in "[Transactions](#)". The table displays only the transactions which have an inbound leg to the current device.

Outgoing Transactions

The **Outgoing Transactions** tab is similar with the **Recent S6/S13 Transactions** panel, which is described in "[Transactions](#)". The table displays only the transactions which have an outbound leg from the current device.

IMSI Search

The **IMSI Search** page displays information about a particular IMSI. To choose the IMSI you can either enter it in the search box from the top of the page or use the right-click menu from the **Transactions** list.

Figure 6-6 Control Plane Monitor IMSI Search Page

IMSI Search

IMSI Search ?

Search IMSI

302720500002466

Search

Summary:

IMSI:
302720500002466
Phone Number:
15142410096
Phone Type:
n/a

State:
attached
Location:
n/a

Attached Since:
Fri Dec 20 2024 18:24:44 GMT+0530 (India Standard Time)
Last Seen:
Fri Dec 20 2024 18:24:42 GMT+0530 (India Standard Time)

Details

...

(None)

Save

Delete | Rename

Clear

Start Time	Command Code	Result	Result Code	Initiator devices	Terminator devices	MSISDN	Error diagnostic	Origin realms	Destination realms	Visited-PLMN-Id
2024-12-20 12:54:49	321 Purge-UE	Success	2001					epc.mnc980.mcc310.3gppnetwork.org	lab.epc.mnc720.mcc302.3gppnetwork.org	
2024-12-20 12:54:44	316 Update-Location	Success	2001			15142410096		epc.mnc980.mcc310.3gppnetwork.org	lab.epc.mnc720.mcc302.3gppnetwork.org	310980
2024-12-20 12:54:42	318 Authentication-Information	Success	2001					epc.mnc980.mcc310.3gppnetwork.org	lab.epc.mnc720.mcc302.3gppnetwork.org	310980

<

Now

>

2024-12-20 12:54:42

Stop

Displaying items from 5 minutes ago

The **Summary** section provides high-level information about the selected IMSI number, including the current attachment state and the phone number.

The transactions list from the bottom is similar with the one from the **Transactions** page, but it is pre-filtered by the selected IMSI.

7

Settings

This chapter describes how to work with the **Settings** features of Oracle Communications Operations Monitor.

General Settings

The **General Settings** section of the **Operations Monitor Settings** dialog box allows you to view the status of the Operations Monitor server, configure date and time, update the Operations Monitor software or license, view properties of the currently installed license and execute some system-wide actions.

Status

The **Status** page allows you to view some important information about the Operations Monitor server at a glance. To access the **Status** page, from the **Settings** menu, select **General Settings**, and then select **Status**. The **Status** page has the following areas, **Network**, **Date and Time**, and **Software**, and **HTTPS** as shown.

Figure 7-1 Status Page

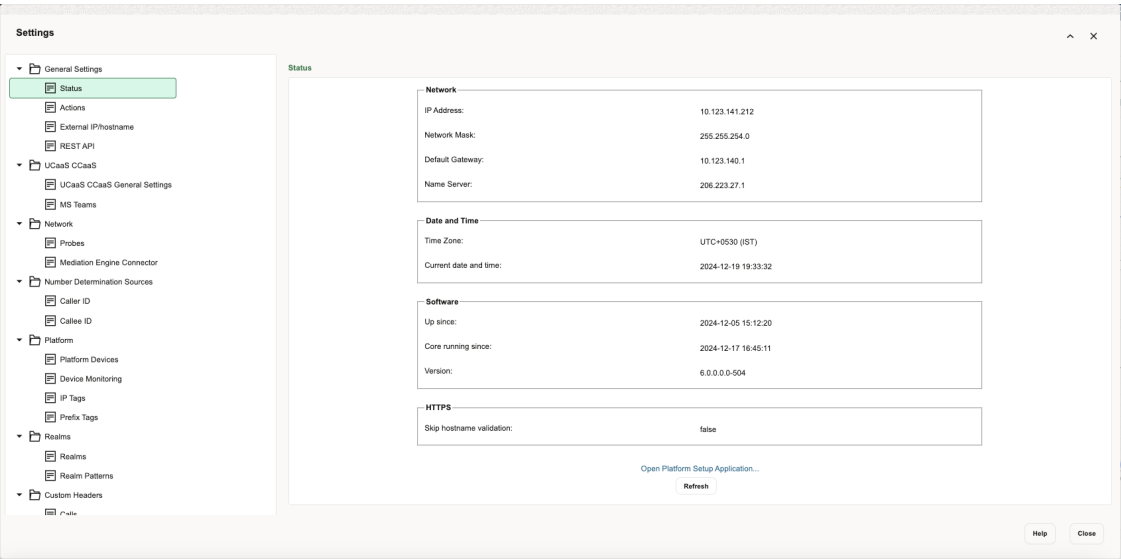


Table 7-1

Area	Description
Network	Displays information about the configuration of the primary network interface (IP Address, Network Mask, Default Gateway, and Name server).

Table 7-1 (Cont.)

Area	Description
Date and Time	Displays information about the configured Time Zone and the Current date and time settings on the Operations Monitor server.
Software	Displays the time since the Operations Monitor software has been up and the time since core has been running. Version: Software version being used. Version History Option: Detailed log of previous software versions, enabling users to track updates and changes over time.
HTTPS	Set the Skip hostname validation to True/False. Skip Hostname Validation is a configuration setting that bypasses the process of verifying whether the hostname (domain name or IP address) in a certificate matches the hostname of the server being connected to.

Actions

The **Actions** page allows you to block alerts and reset the browser UI state. To access the **Actions** page, from the **Settings** menu, select **General Settings**, and then select **Actions**. To execute one of these actions, click the corresponding button on the **Actions** page. A confirmation dialog box appears. Click **OK** to continue.

Figure 7-2 Actions Page

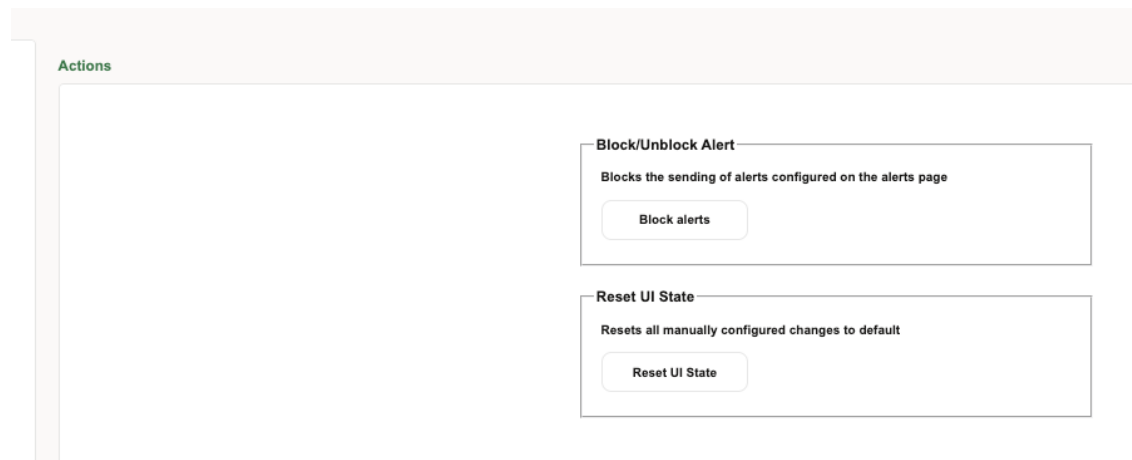


Table 7-2 Action Page Fields

Field	Description
Block alerts	Blocks the sending of alerts configured on the alerts page.

Table 7-2 (Cont.) Action Page Fields

Field	Description
Reset UI state	For the user's convenience, Operations Monitor stores state information about the tables in HTTP cookies. The state information contains the hidden columns and the filtering criteria. This way the filters are kept even if the web page is refreshed or the browser is restarted. You can drop this UI state by using this action. It will delete all HTTP cookies used for state persistence.

External IP/hostname

The External IP/hostname is used as base for deep links in alerting emails. Typically, this is the hostname you see in the address field of your browser.

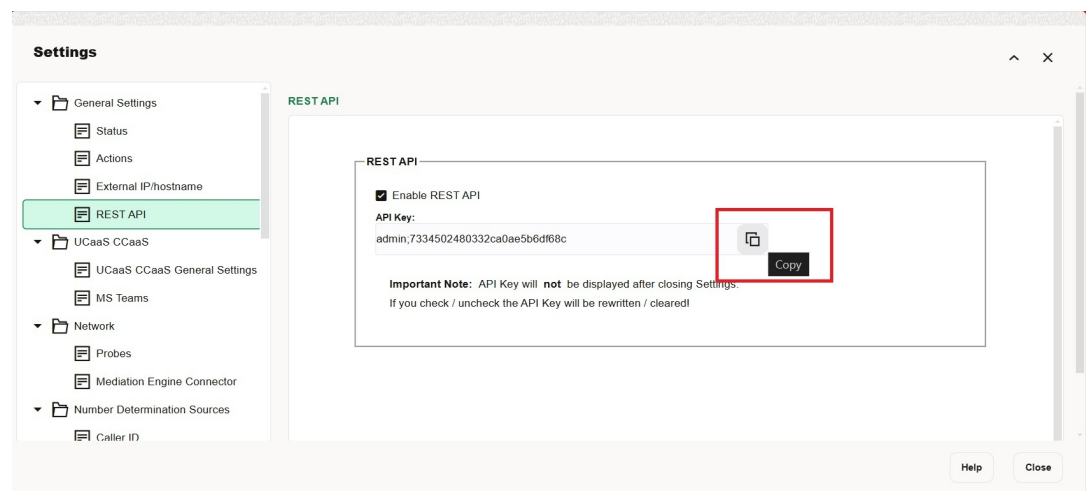
This page allows you to view and update the External IP/hostname. To access the page, from the **Settings** menu, select **General Settings**, and then select **External IP/hostname**. The **External IP/hostname** page contains one field in which you can enter new text. Enter text in the field and click **Update** to save the External IP/hostname.

REST API

The new API Key is used to authenticate the user when using the new REST API.

1. From the **Settings** menu, select **General Settings**, and then select **REST API**.
2. Select the **Enable REST API** option, which generates a new API Key.

Figure 7-3 API Key



Note

After closing the **Settings** dialog box the API Key will no longer be displayed. The API Key is displayed only once when it is first created.

UCaaS CCaaS Monitoring

UCaaS CCaaS Monitoring enables you to view the correlated calls made from PSTN to UCaaS CCaaS applications and conversely too.

Currently, we support only Microsoft Teams such as, correlation of Direct Routing (DR) calls received from SBC with the call record received from Microsoft Teams (using Microsoft Graph Service). Correlation is done based on a unique correlation ID which is present in the SIP call received from SBC and the call records details received from Microsoft Teams (MS Teams). The call records also contain information of media details that are displayed in the **Calls Info** window of a correlated Direct Routing call. The message flow includes a new leg which refers to the UCaaS CCaaS leg for a correlated Direct Routing call.

Identifying MS Teams Direct Routing Calls in Operations Monitor

Mediation Engine process identifies a call as a Direct Routing call if the *x-i* parameter in the contact header of the SIP message is present and the *X-MS-TenantId* is absent.

If the contact header has the *x-i* parameter and *X-MS-TenantId* header is not present in the SIP message, then the call is considered as a Direct Routing call, and the value of the *x-i* parameter is saved and used for correlating the SIP call with the Graph data received from Microsoft graph.

The *x-i* parameter in the contact header is used as a correlation ID to correlate the Direct Routing call record information from Microsoft graph with the SIP calls. The *x-i* parameter is present in the contact header of the Invite message if the call is initiated from the MS Teams. If call is initiated from the PSTN then the *x-i* parameter is present in the contact header of the response messages 1xx (except 100 trying)/2xx/3xx/4xx/5xx/6xx responses.

To enable this feature follow the instructions provided in the section [UCaaS CCaaS Activation](#).

UCaaS CCaaS Monitoring Activation

Follow the steps given in this section to activate UCaaS CCaaS Monitoring:

Activation of the UCaaS CCaaS Monitoring involves:

- [Enabling the UCaaS CCaaS Extension](#)
- [Enabling UCaaS CCaaS System Settings](#)

Enabling the UCaaS CCaaS Extension

To activate UCaaS CCaaS monitoring, enable the UCaaS CCaaS Extension.

To enable the UCaaS CCaaS Extension:

The flag **UCaaS CCaaS** has been introduced in the Configuration section of the Platform Setup Application page to enable the UCaaS CCaaS Monitoring feature. This flag is disabled by default.

You can enable this flag during a fresh installation or even after the installation.

To activate the UCaaS CCaaS feature for upgraded systems, you need to enable this flag from the Platform Setup Application page after the upgrade.

Figure 7-4 UCaaS CCaaS Check Box

Configuration

Please note that you are only allowed to use the products, modules and extensions that you have purchased. For any questions please contact your sales representative.

Capacity

Please check the license and enter the capacities that were licensed to you:

Concurrent calls: *

☐ RTP Recording

Concurrent RTP streams: *

Extensions

☒ App support

☒ CDR

☒ Diameter

☒ ENUM

☒ Gateway control protocols

☒ REST API

☐ SAU

☐ Skype for Business

☒ SIGTRAN

☒ Media quality

Additional Extensions

☒ Non Calls

☒ UCaaS CCaaS

☒ Stir/Shaken

After enabling this flag, you can view the following on the user interface:

- **UCaaS CCaaS Settings**
- **Metadata** tab in the Call Info page
- **UCaaS CCaaS** columns in the **Calls** Page
- **UCaaS CCaaS Legs** in message flow

Note

To view correlated DR calls, enable the System Setting **Support UCaaS CCaaS Calls**.

The UCaaS CCaaS Monitoring feature is available only for Nodes installed as Mediation Engine and Mediation Engine + Probe. For more information, see the section Configuring Session Monitor in the Oracle Communications Session Monitor Installation Guide.

Enabling UCaaS CCaaS System Settings

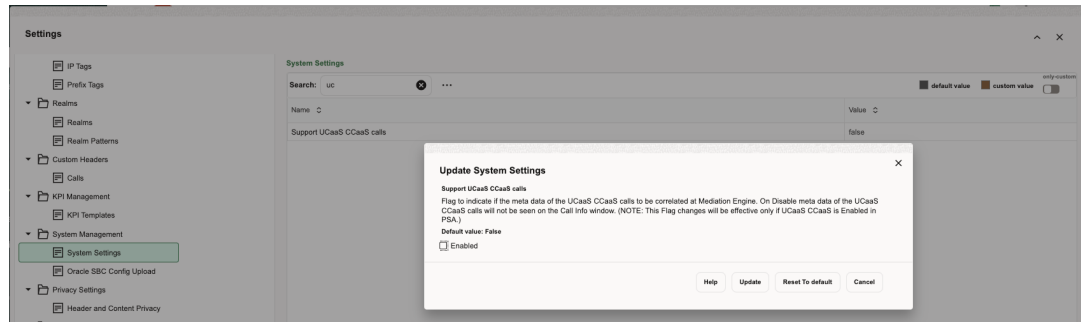
The **Support UCaaS CCaaS calls** system setting in the Mediation Engine handles the correlation of UCaaS CCaaS Calls. This setting comes into effect only if the UCaaS CCaaS extension is enabled from the Platform Setup Application. By default this setting is disabled.

- If the **admin > Settings > System Settings > Support UCaaS CCaaS calls** is true, then UCaaS CCaaS Calls are correlated at Mediation Engine and you can see the Meta Data information
- If **admin > Settings > System Settings > Support UCaaS CCaaS calls** is false, then UCaaS CCaaS Calls are not correlated and you will not see Meta Data information.

To enable the UCaaS CCaaS system setting:

1. Click **admin > Settings > System Settings**.

Figure 7-5 System Settings for UCaaS CCaaS



2. Search for **Support UCaaS CCaaS calls**.
3. Double-click **Support UCaaS CCaaS calls** settings.
4. Check the **Enabled** check box.
5. Click **Update**.

The value is updated and is set to true.

Configuring UCaaS CCaaS Settings

The two setting options found under the folder: **admin → Settings → UCaaS CCaaS** are used for configuring the UCaaS CCaaS application.

The configuration involves two parts -

- Configuring Microsoft Teams
- Configuring the Proxy server (optional task)

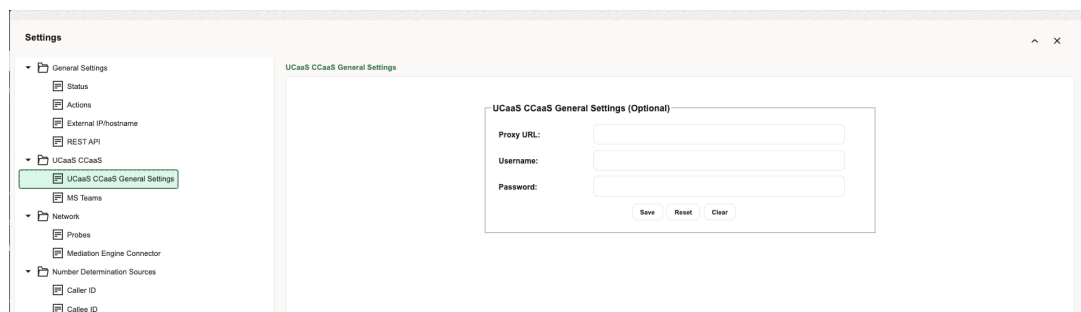
UCaaS CCaaS General Settings

This feature requires the Mediation Engine to connect to the Internet as the Mediation Engine needs to call the Microsoft Graph APIs. If it is not possible, there is an option to configure the proxy server to be able to call the Graph APIs using the proxy server. The proxy server that you configure here is *only* used to call the MS Graph APIs and is not used for any other internet URL. Configuring the proxy server is an optional task. This needs to be done if a direct connection to the Internet is not available on the Mediation Engine.

To configure the proxy details:

1. Provide the HTTP(S) proxy URL in the **Proxy URL** field.

Figure 7-6 UcaaS CCaaS Settings



2. Provide the user name and password for the proxy server, if applicable.

Note

The Username and Password fields are optional. However, if you specify a password is then the username field is mandatory.

3. Click **Save**.

Configuring Microsoft Teams

Operations Monitor needs to connect to the Microsoft Identity platform to fetch the Direct Routing Call information from the Microsoft Graph API.

There are two steps to complete this configuration:

1. Register an application with the Microsoft identity platform
2. Configure relevant parameters, obtained as part of Step 1, in the MS Teams Settings page in Operations Monitor user interface.

Note

Ensure that you read the information provided in this section before proceeding to execute both steps. Also, note that names of particular sections mentioned in Step 1 can be changed by Microsoft at any point. For example, *Microsoft Entra ID* was earlier named as *Azure Active Directory*.

Registering the Microsoft Teams App

This section provides information on how to register the Microsoft Teams App.

Follow the steps mentioned in <https://learn.microsoft.com/en-us/entra/identity-platform/quickstart-register-app> to register the app.

Here are some guidelines for easy reference. For more information on the specific screens displayed, refer to the above link.

1. Sign in to the Microsoft Entra admin center.
2. Navigate to **Identity > Applications > App Registrations**, and select **New Registration**.
3. Enter a display **Name** for your application.
4. Specify who can use the application, As Operations Monitor supports only a single Client ID/Tenant ID as of now, it is recommended that you select **Single Tenant** as an option.
5. Ignore the **Redirect URI** configuration, as it is not required.
6. Select **Register** to complete the initial app registration.

Note

After the app is registered, note down the Application (client) ID and Directory (tenant) ID values - these are required later. Ignore **Configure Platform Settings** as it is not required.

The next step is to Add Authentication Credentials in the registered app.

Add Authentication Credentials

Authentication Credentials are used by Operations Monitor.

There are two main ways to authenticate with the application registered in Microsoft Entra:

1. Client Secret
2. Certificate Credentials

As per Microsoft guidelines, it is recommended that you choose the option **Certificate Credentials**, as this option is more secure than the Client Secret option. Certificate Credentials are ONLY supported by the Operations Monitor.

To add Certificates:

1. In the Microsoft Entra admin center, in **App registrations**, select your application.
2. Select **Certificates & secrets > Certificates > Upload certificate**.
3. Select the certificate file you want to upload. The certificate must be any one of the following file types: .cer, .pem, .crt.

After the certificate is uploaded, note down the *Thumbprint* value - this will be required later.

Adding API Permission

After uploading the certificates, add permission for the API *CallRecords.Read.All* so that Operations Monitor can fetch Direct Routing call record information.

To add the API permission:

1. In the **Microsoft Entra admin center**, in **App registrations**, select your application.
2. Select **API Permissions > Add a permission > Microsoft APIs > Microsoft Graph**.
3. Select **Application permissions**.
4. Type **CallRecord** in the search box and select **CallRecords.Read.All**.
5. Select **Add permissions**.
6. Select **Admin consent required** as **Yes** if not done by default.

Note

Ensure that the status for CallRecords.Read.All permission is Green as shown in the image below.

Figure 7-7 Add permissions

API / Permissions name	Type	Description	Admin consent req...	Status
▼ Microsoft Graph (2)				
CallRecords.Read.All	Application	Read all call records	Yes	Granted for [redacted] ***

App registration is complete now. Proceed to Step 2 to configure MS Teams settings in the Operations Monitor user interface.

Configuring MS Teams Settings in Operations Monitor User Interface

Once the MS Teams App is registered, follow the instructions in this section to configure the information in the Operations Monitor User Interface:

Configuring MS Teams Settings in the Operations Monitor User Interface:

1. Provide the Application (client) ID and Directory (tenant) ID retrieved from Microsoft Entra where your app is registered.

Figure 7-8 MS Teams Configuration

The screenshot shows the 'Configure MS Teams' configuration window. The left sidebar has 'Settings' expanded, with 'MS Teams' selected. The main configuration area includes the following fields and controls:

- Application (client) ID:** Text input field.
- Directory (tenant) ID:** Text input field.
- Scope:** Text input field.
- Thumb print:** Text input field.
- MSGraph API Version:** Dropdown menu with '1' selected.
- Private Key:** File upload button labeled 'Choose File' and a text field showing 'No file chosen'.
- Data Source Latency (minutes):** Input field with a value of '20' and an information icon.
- Display Null Values:** A checkbox that is currently unchecked.
- Buttons:** 'Save', 'Reset', and 'Clear' buttons at the bottom right.

2. In the **Scope** field, provide the Microsoft graph service URL. The default value is *https://graph.microsoft.com/.default*
 3. In the **Thumb print** field, provide the thumbprint generated after uploading certificates as part of app registration.
 4. In the **MSGraph API Version** field, select the version available from the drop down.
 5. In the **Private Key** field, upload the private key file generated while creating the certificate, same certificate was uploaded while registering the app.
 6. In the **Data Source Latency (minutes)** field, enter the maximum number of minutes Session Monitor waits to receive the teams call correlation data from MS Graph API. The default value is 20 (minimum limit: 5 and maximum limit: 60).
- The **Data Source Latency** field reflects the time delay after which the MS Teams Direct Routing call data is available using the MS Graph API, once the call is finished. The value of this field should be set to a value more than the maximum delay observed in the receiving call data, to ensure that no DR calls are dropped/not correlated.
7. Select the **Display Null Values** check box to view null values in the **Meta Data** tab of Call Info. By default null values are not shown.
 8. Click **Save**.

Note

Operations Monitor recommends a default value of 20 minutes based on the observations in the lab test of fetching data from Microsoft Graph. The minimum value of 5 minutes helps if Microsoft starts providing call data early, so that users also get 'correlated' data in Session Monitor early.

UCaaS CCaaS Monitoring - Additions in the Calls Page

UCaaS CCaaS Monitoring - Additions in the Calls Page will be available only if you have enabled the UCaaS CCaaS extension from the Platform Setup Application page.

Recent Calls Table

The UCaaS CCaaS Monitoring Feature introduces three columns to the Recent Calls table in Calls Page:

- **Media Bypass:** Indicates if the call has Media bypass “Enabled” or “Disabled” for MS Teams Direct Routing calls. For non- UCaaS CCaaS calls, this column displays value as “NA”.
- **UCaaSCCaaS Originating:** This field is populated as “TEAMS_DR” when the call is identified as originated from MS Teams and terminating at PSTN (Teams to PSTN Calls)
- **UCaaSCCaaS Terminating:** This field is populated as “TEAMS_DR” when the call is identified as originated from PSTN and terminating at MS Teams (PSTN to Teams Calls)

These columns are enabled by default, if the corresponding Platform Setup Application extension is enabled, in all Calls Panel including Devices Page, IP Tracking page, User Tracking page except for the Dashboard Panels.

Figure 7-9 UCaaS CCaaS Monitoring - Recent Calls

Caller	Callee	Start timestamp	End timestamp	Call time	Media Recording	Segments	Code	Ingress device(s)	Egress device(s)	DTMF	Diversion	Diversion Type	Call-Transfer	Min. MOS	Avg. MOS	State	State details	Media Bypass	UCaaSCCaaS Originating	UCaaSCCaaS Terminating
49300000001	59300000001	2025/01/06 07:48:14	2025/01/06 07:50:44	2'29"	No	2	200	SBC						4.4	4.4	Finished		Enabled	TEAMS_DR	

To view the columns on the Dashboard calls panel, add these columns manually using the **Set Columns** feature.

UCaaS CCaaS - Filtering

All the three columns of UCaaS CCaaS can be filtered and have the below filter options:

Table 7-3 Columns of UCaaS CCaaS - Filtering

Column	Filter Option
Media Bypass	- Enabled - Disabled - NA
UCaaSCCaaS Originating	TEAMS_DR
UCaaSCCaaS Terminating	TEAMS_DR

These columns are available across all filtering options such simple filter, Advanced Filter, Text-Based Filter Search. Refer [Filtering](#) Section for more details.

Figure 7-10 Media Bypass Simple Filter

The screenshot shows a configuration window titled "Filters" with a "State" tab. The "media bypass" filter is selected. The "Media Bypass" section contains three checkboxes: "Enabled", "Disabled", and "NA", all of which are currently unchecked. At the bottom of the window are "Clear", "Reset", and "Apply" buttons.

Figure 7-11 UccaaS CCaaS Originating Simple Filter

The screenshot shows a configuration window titled "Filters" with a "State" tab. The "Uca" filter is selected. The "UCCaaS Originating" section contains one checkbox: "TEAMS_DR", which is currently unchecked. Below this section, the text "UCCaaS Terminating" is visible. At the bottom of the window are "Clear", "Reset", and "Apply" buttons.

Figure 7-12 UCaaS CCaaS Columns in Advanced Filter

(Unnamed Filter)

() +

UCaaS CCaaS Originating in TEAMS_DR and () + -

Media Bypass in Enabled, Disabled () + -

Use the + and - to add or remove filters, () for brackets.

Rename Save Hide Apply Now

Figure 7-13 UCaaS CCaaS Columns in Text-based Filter Search

Recent Calls

Details ...

UCaaS CCaaS Originating=TEAMS_DR

SIMPLE (None) Edit Advanced

Recent Filters

- Filter 1 => UCaaS CCaaS Originating=TEAMS_DR
- Add new filter

	DTMF	Diversion	Call-Transfer	Min MOS	Avg MOS	State	Media Bypass	UCaaS CCaaS Originating	UCaaS CCaaS Terminating
59300000001				4.4	4.4	Fl...	Enabled	TEAMS_DR	

UCaaS CCaaS – Changes in Calls Info

Meta Data is the new tab in the Calls Info dialog box introduced by UCaaS CCaaS. This tab displays the Meta Data received from the UCaaS CCaaS service for a correlated Direct Routing call.

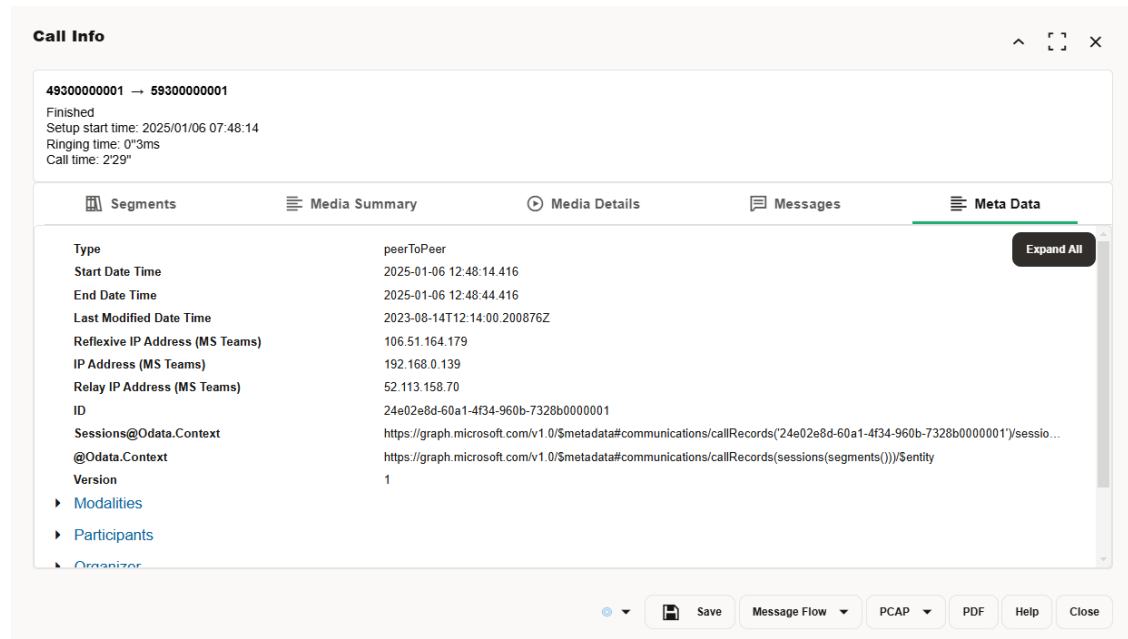
This is additional information that you can now access to support end-to-end visibility of a Direct Routing call. The Meta Data is represented in a tree structure and by default is shown in a collapsed state.

Click **Expand All** or expand each node in the tree structure to view the Meta Data in detail. On expanding, you can see the option to Collapse again.

The Call Information received from MS Teams may contain many fields where values are unavailable, which are marked as null. In the Meta Data tab such fields are not shown by

default, if you want to view the null value fields, then enable the **Display Null Values"** check box from **Settings > UCaaS CCaaS > MS Teams Settings**.

Figure 7-14 Meta Data tab in Call Info window



UCaaS CCaaS - Changes in the Message Flow Window

In the Message flow window, for a MS Teams to PSTN DR Call, Operations Monitor now supports the ability to see the signaling and media information for the MS Teams/ UCaaS. Similarly, for a PSTN to MS Teams Direct Routing call as well.

UCaaS CCaaS introduces 2 new messages in the Message Flow based on the Meta Data received from UCaaS CCaaS Service (MS Teams) - UCaaS_CCaaS Media and UCaaS_CCaaS Signalling:

- **UCaaS_CCaaS Signalling:** All contents of Meta Data except "Segments" data part is considered as UCaaS_CCaaS Signalling data.
- **UCaaS_CCaaS Media:** "Segments" data part of Meta Data is considered as UCaaS_CCaaS Media data.

These messages are displayed as a separate leg in the Message Flow. The device IP value of this leg in the Message Flow can be any of the following based on a valid IP address found in this order:

Reflexive IP Address >> IP Address >> Relay IP Address >> 1.1.1.1(Static IP)

These 2 UCaaS CCaaS messages are available in all Message Flow options like SVG, PDF and Message Flow Download.

Note

These 2 new flows in Message Flow do not correspond to any raw SIP message but only are representative of the leg between MS Teams client and MS Teams proxy.

Figure 7-15 PSTN to MS Teams Message Flow

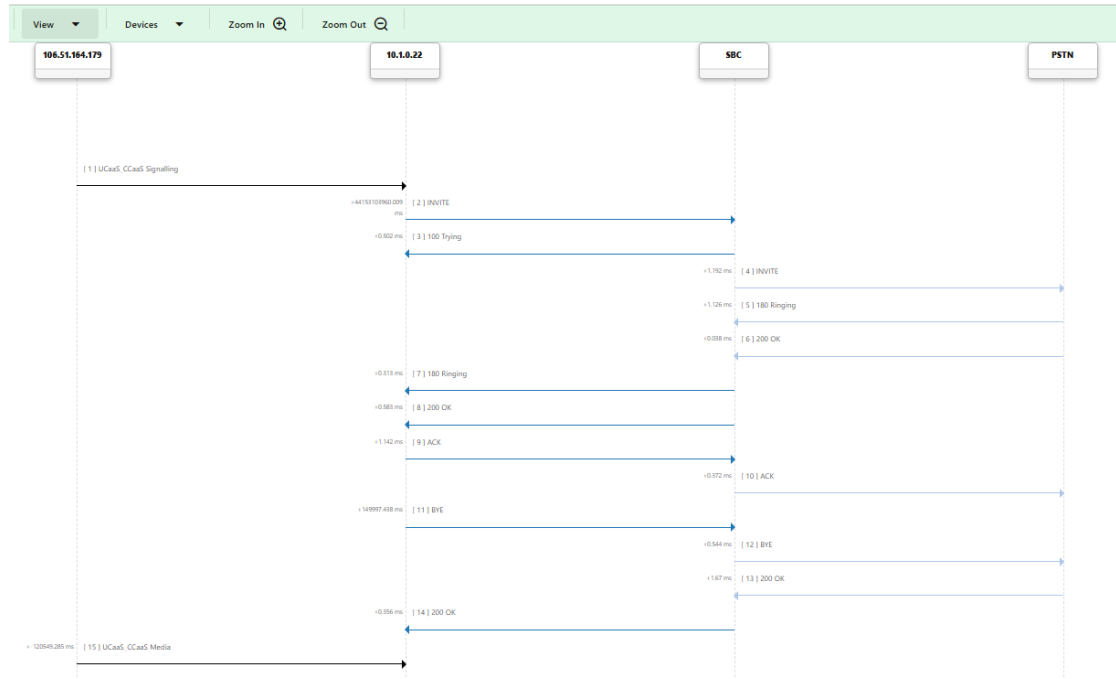


Figure 7-16 UCaaS_CCaaS Signalling Leg

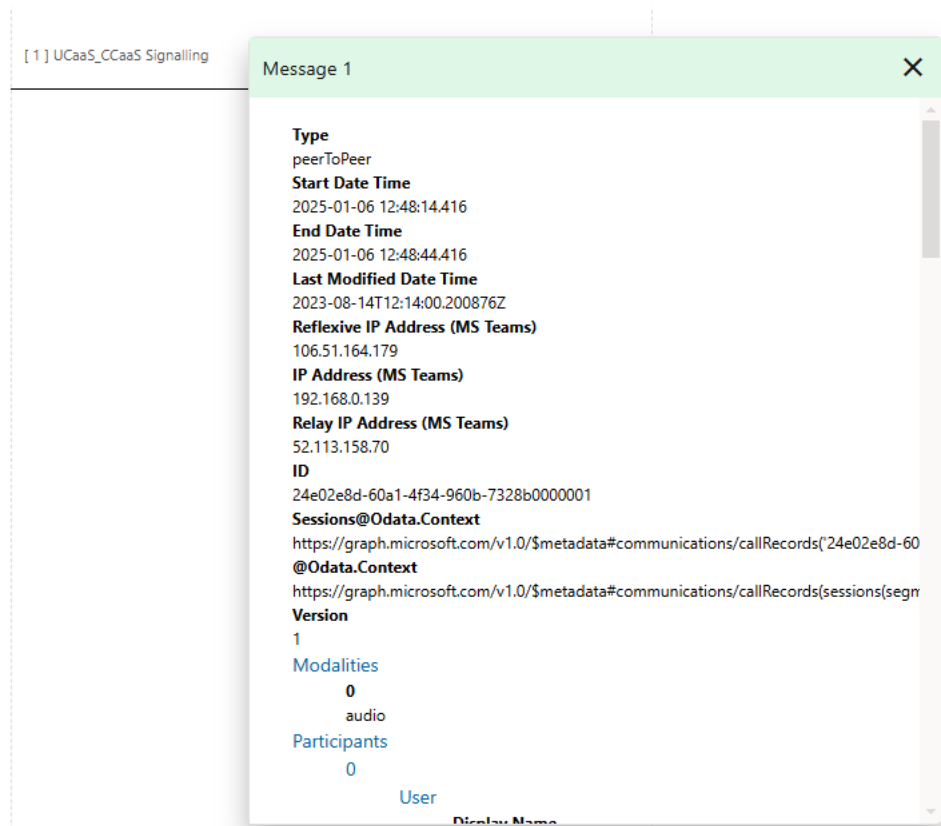
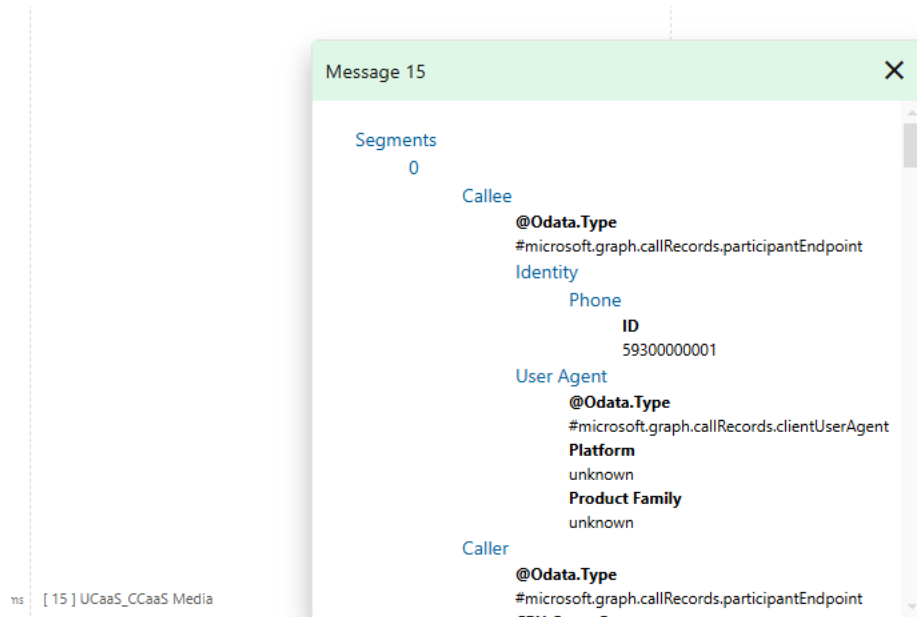


Figure 7-17 UCaaS_CCaaS Media Leg



Exporting UCaaS CCaaS Data - PDF Format

While exporting the PDF, you can include UCaaS CCaaS data in the export. Select the **UCaaS CCaaS Information** check box to do so.

By default, the **UCaaS CCaaS Information** check box is not selected. When you select the **UCaaS CCaaS Information** check box, Meta Data and UCaaS CCaaS messages are exported in the PDF. The **UCaaS CCaaS Information** check box is available if you have enabled the UCaaS CCaaS extension from the **Platform Setup Application** page.

Figure 7-18 Export PDF

The 'Create Report' dialog box contains the following elements:

- Report Contents:**
 - ☒ Call Information
 - ☒ Link Quality Information
 - ☒ Voice Quality Information
 - ☒ Detailed RTCP information
 - ☒ DTMF information
 - ☐ UCaaS CCaaS information (highlighted with a red box)
 - ☒ Messages
 - ☒ Include Company Logo
 - ☒ Include Graph
 - ☐ Combine identical
 - ☐ Use Device Order
 - ☐ Transport protocol
 - ☐ IP addresses
 - ☐ Codecs
 - ☐ Time spans
 - ☐ Show Media
 - ☐ Unwind messaging
 - ☐ SIP URIs
 - ☐ VLAN
 - ☐ MAC addresses
 - ☐ Absolute times
 - ☐ Resolve IP addresses
 - ☐ Show DTMF Information
- Additional Info:**
 - Report Comment (optional): [Text area]
 - Filename (optional): [Text field]
- Buttons:** Create, Reset, Cancel

UCaaS CCaaS - CSV Export

The UCaaS CCaaS fields Media Bypass, UCaaS CCaaS Originating and UCaaS CCaaS Terminating are available in the CSV file downloaded using the CSV Export and Bulk Export options.

Table 7-4 CSV Export

Column Header	CSV Header	Displayed Values (UI)	CSV Values
Media Bypass	uccc_media_bypass	NA	-1
-	-	Enabled	1
-	-	Disabled	0
UCaaS CCaaS Originating	uccc_originating	TEAMS_DR	1
UCaaS CCaaS Terminating	uccc_terminating	TEAMS_DR	1

UCaaS CCaaS - CDR

The fields - **UCaaS CCaaS Originating** and **UCaaS CCaaS Terminating** fields has been added in CDR. These fields are updated based on the presence of the *x-i* parameter in a SIP message of a Direct Routing call. This is not dependent on MS graph data.

The fields **ucaas_ccaas_org** and **ucaas_ccaas_term** can be found in the CDR.

Table 7-5 UCaaS CCaaS CDR Fields and Values

Column Header	CDR Header	CSV Values
UCaaS CCaaS Originating	ucaas_ccaas_org	TEAMS_DR
UCaaS CCaaS Terminating	ucaas_ccaas_term	TEAMS_DR

Note

In CSV Export, UCaaS CCaaS Originating and UCaaS CCaaS Terminating fields are updated only after Graph Data is received from MS Teams unlike in CDR where it is updated based on the presence of “x-i” parameter in SIP message as soon as call finishes. In situations where Mediation Engine fails to receive Graph Data from MS Teams, you will notice CSV Export data not matching with the CDR data due to this reason.

UCaaS CCaaS - REST API

These 3 UCaaS CCaaS fields are available in the /me/getPagedCalls REST API response also.

Figure 7-19 /me/getPagedCalls REST API response sample

```
{
  "predicate": "older_than",
  "next_value": "7280513081946406915",
  "first_page": false,
  "last_page": false,
  "success": true,
  "calls": [
    { "uccc_media_bypass": "0", "uccc_terminating": 1, "uccc_originating": null, "aud
    { "uccc_media_bypass": "0", "uccc_terminating": 1, "uccc_originating": null, "aud
  "search_range": 900
}
```

Note

PCAP that is downloaded does not contain any information about Meta Data and UCaaS CCaaS Messages as the raw SIP messages are not received from MS Graph APIs.

UCaaS CCaaS - KPI Page

The UCaaS CCaaS feature introduces eight Platform-wide KPIs to monitor DR call traffic. These KPIs will be available by default, but will come into effect only if you have enabled the UCaaS CCaaS extension from the Platform Setup Application.

These KPIs are incremented only for MS Teams DR Call. Further, the KPIs are incremented immediately when call is identified as a Direct Routing call by parsing the *x-i* parameter and the *X-MS-TenantId* header (will not wait for graph data to increment the KPIs).

To view the UCaaS CCaaS KPIs, navigate to the **KPI/Metrics** page, and select **Platform-wide** under the **Library** section. These KPIs are visible under the default path. They will not be available for Device, Prefix Tag and IP Tag KPIs.

List of UCaaS CCaaS KPIs and their description:

Table 7-6 UCaaS CCaaS KPIs

Serial Number	Counters	Description
1	UCaaS Call attempts per second	Number of UCaaS CCaaS call attempts for each second
2	Teams DR Call attempts per second	Number of Teams DR call attempts for each second
3	Teams Caller to PSTN DR Callee CAPS	Number of Teams DR call attempts for each second made from Teams Caller to PSTN Callee
4	PSTN Caller to Teams DR Callee CAPS	Number of Teams DR call attempts for each second made from PSTN Caller to Teams Callee
5	UCaaS Active Calls	Number of established UCaaS CCaaS concurrent calls

Table 7-6 (Cont.) UCaaS CCaaS KPIs

Serial Number	Counters	Description
6	Teams DR Active Calls	Number of established Teams DR concurrent calls
7	Teams Caller to PSTN DR Callee Active Calls	Number of established Teams DR concurrent calls made from Teams Caller to PSTN Callee
8	PSTN Caller to Teams DR Callee Active Calls	Number of established Teams DR concurrent calls made from PSTN Caller to Teams Callee

Note

For now, as Mediation Engine is monitoring only MS Teams DR Calls, so values of generic KPI such as "UCaaS Call attempts per second" will be equal to specific KPI like "Teams DR Call attempts per second". However, in the future when Operations Monitor adds support for other vendors then value of the KPIs will differ

UCaaS CCaaS - User Management

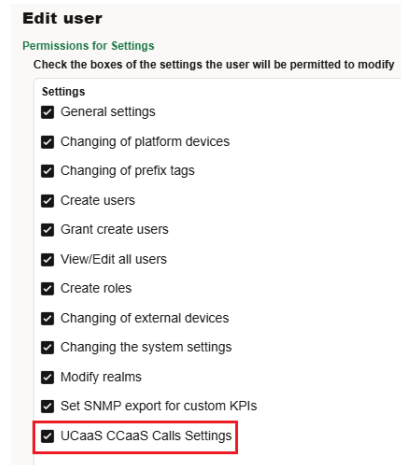
To manage the UCaaS CCaaS settings a new permission **UCaaS CCaaS Calls Settings** has been introduced to user management as a part of this feature.

You can find the new permission under **admin > Settings > User Management > Permission** for the **Settings** page. The admin user can enable or disable this permission for a user. By default, this permission is disabled.

- If **UCaaS CCaaS Calls Settings** is true, then the users can view and modify the **UCaaS CCaaS** section in the Settings Page (user->Settings).
- If **UCaaS CCaaS Calls Settings** is false, then the users cannot view and modify the **UCaaS CCaaS** section in the **Settings** Page (user->Settings).

Note

These permissions are available in user roles also.

Figure 7-20 'UCaaS CCaaS Calls Settings' permission

UCaaS CCaaS Header Notification

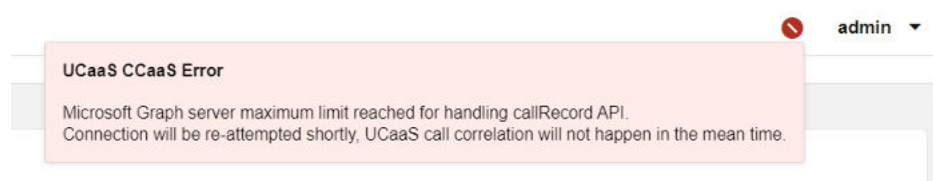
This section describes about the notifications displayed by Operations Monitor if an error occurs with Microsoft Graph.

429 Error Notification:

Microsoft Graph can send 429 error response for the call records REST query. On receiving the response all pending REST queries are dropped and the Teams Process waits until the time mentioned in Retry-After header of 429 error response and then proceeds with a new query from the current timestamp.

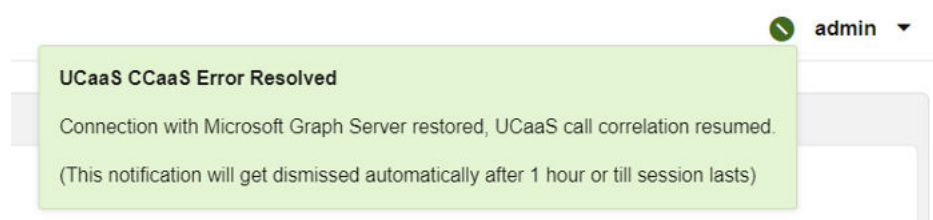
429 error response may occur if the call record threshold limit is crossed which is 1500 request per 20 second per application per tenant defined by the MS Graph services. If this threshold is crossed then, and there is 429 error response, then the calls cannot be correlated from this point on till the retry timer. A red notification icon pops up in the application header once a 429 error is received from the MS Graph API which indicates that the API limit was reached because too many requests were sent.

On hovering over the icon, the exact error can be viewed. This notification icon is displayed continuously until the 429 error is not resolved.

Figure 7-21 429 Error Notification

Once the 429 error is resolved i.e., after the retry-timer if the call records are fetched successfully from the Teams process, then a message is sent GUI to indicate the same. The error icon changes its color to green and the success message can be viewed upon hovering over it. This message will be dismissed automatically after 1 hour or till the session lasts.

Figure 7-22 429 Error Resolved Success Notification



MS Teams Configuration Error Notification

If there are any Teams configuration errors in the MS Teams page (**admin > Settings > UCaaS CCaaS > MS Teams**), then following error is displayed on the GUI as shown here. For a detailed description of this error, check the `/var/log/messages` file. Once the error is fixed a green icon with message "UCaaS CCaaS Error Resolved" is displayed same as above, and error message is cleared.

Figure 7-23 Teams configuration error Notification

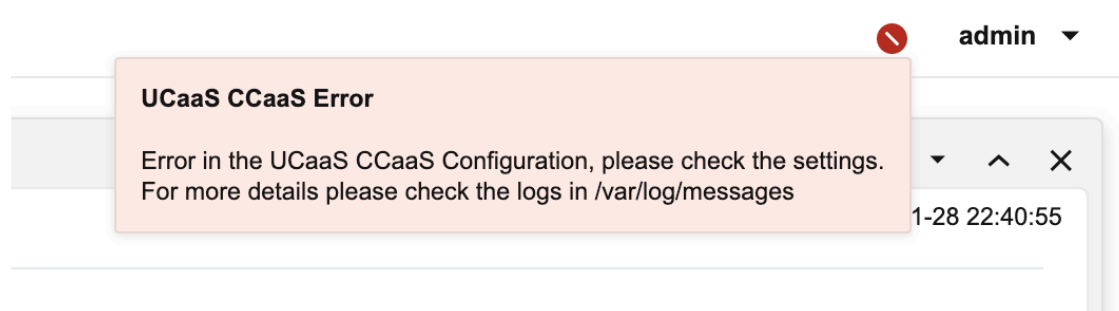
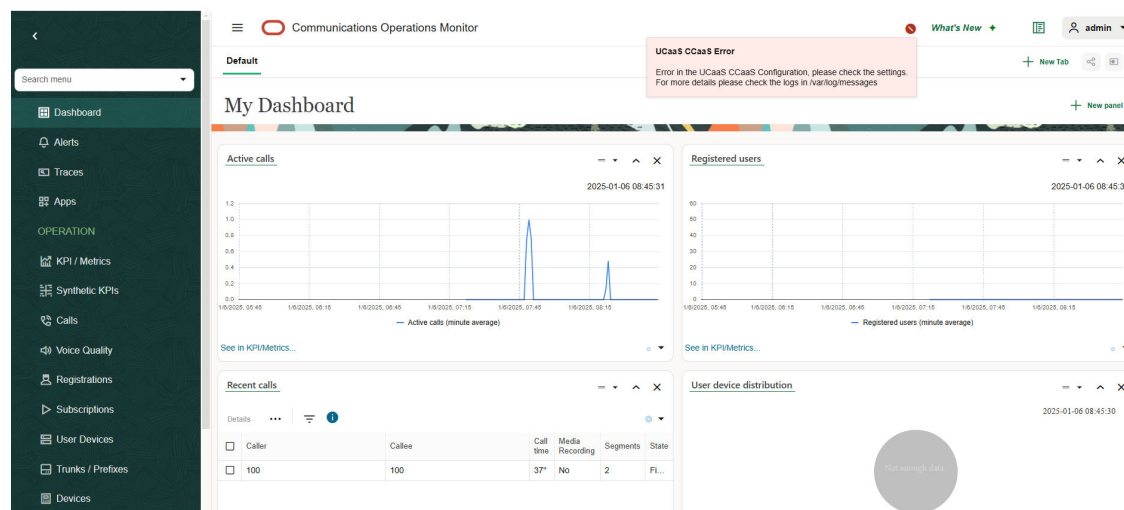


Figure 7-24 Teams configuration error Notification



Disabling UCaaS CCaaS Monitoring

Users who prefer to not to use UCaaS CCaaS Feature can disable it by following below steps. Once disabled DR Calls will not longer be correlated with MS Teams Data.

Disabling UCaaS CCaaS after installation or upgrade:

1. In a web browser, go to https://<ip_address>/setup or access Platform Setup Application using the Mediation Engine GUI by clicking **admin > Setup**. The Platform Setup Application Login page appears.
2. Navigate to the **Configuration** page. The **UCaaS CCaaS** check box appears under **Additional Extensions** option.
3. Uncheck the **UCaaS CCaaS** checkbox
4. Click **Apply**.

On disabling this flag, the **UCaaS CCaaS Settings, Metadata** Tab in the **Call Info** and **UCaaS CCaaS** columns in the **Calls** page will not be visible to user. If you make any changes to the System Setting **Support UCaaS CCaaS calls** will no longer come into effect.

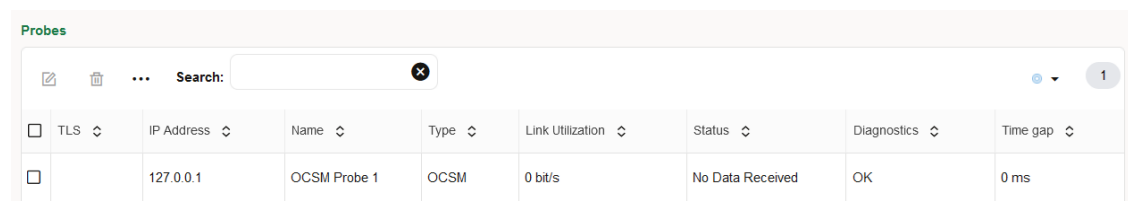
Network

The **Probes** page helps you define the remote agents that are pushing the data to the Mediation Engine of Operations Monitor. To access the **Probes** page, from the **Settings** menu, select **Network**, and then select **Probes**.

Probes

If your Operations Monitor installation has been configured to use probes on remote machines for traffic sniffing, you may view or edit those probes using this panel. By default, Operations Monitor treats the local machine as its one and only probe.

Figure 7-25 Probes



	TLS	IP Address	Name	Type	Link Utilization	Status	Diagnostics	Time gap
☐		127.0.0.1	OCSM Probe 1	OCSM	0 bit/s	No Data Received	OK	0 ms

SBC probes are not configured using Operations Monitor, but it is possible to edit their names and IP addresses using the **Probes** panel. You can remove probes using the **Remove** button in the probes list dialog box, but if a probe still exists, it will eventually reappear in the list of probes. Use the column **Status** to verify if your settings are correct and Operations Monitor can connect to the probes.

There is a process that searches for new probes at a given time interval. If they are correctly configured they will appear in the **Probes configuration** panel. When a probe is removed from the network, it should also be removed from the list.

[Table 7-7](#) lists the columns in the **Probes** panel and the information that is shown for each probe:

Table 7-7 Probe Panel Columns

Column	Description
TLS	A lock appears if the connection with this machine is encrypted.
IP address	The IP address of the probe that will be used.
Name	A name to identify the probe. Can be edited by the user.
Type	Two types of probes are shown: • OCSM. Oracle Communications Session Monitor (Session Monitor) probes are either standalone probes or embedded probes in a Session Monitor Mediation Engine. • SBC. These kind of probes are configured on the SBC side by adding the IP of the Mediation Engine to the configuration. SBC probes will thus automatically connect to the Mediation Engine. An internal process is triggered every 60 seconds for embedded probes auto-discovery. This process runs in the background and the refresh button will not trigger the auto-discovery process. There is a "System Setting" for modifying the refresh interval. It is not recommended to alter the default value so as not to overload the system. If there is an embedded probe that has the same IP address as the Session Monitor probe, its configuration in Operations Monitor will be overwritten.
Link Utilization	This column shows the traffic volume in bits per second if the probe is reachable.
Status	The value of this cell depends of the data received. If no received data is shown, that may indicate a potential problem.
Diagnostics	Shows information about possible errors that can appear in probes configuration, such as IP conflicts and counters mis-configuration. In the latter case, a button will let the Administrators manually create the missing counters.
Time Gap	Absolute time difference between the Operations Monitor instance and the probe in milliseconds. If the difference is bigger than the established maximum value, the value will appear in red color and an alert symbol will appear in the dashboard, noticing that there is a significant time difference. The setting name for the time difference probe value alert is <i>Time difference in probes that will trigger an alert</i> .

Searching for and Filtering Probes

Using the **Search** option, you can search for and filter probes with ease, allowing for faster diagnostics and system monitoring. This feature helps you locate specific probes by filtering based on search keywords such as IP address, Name, Type and so on.

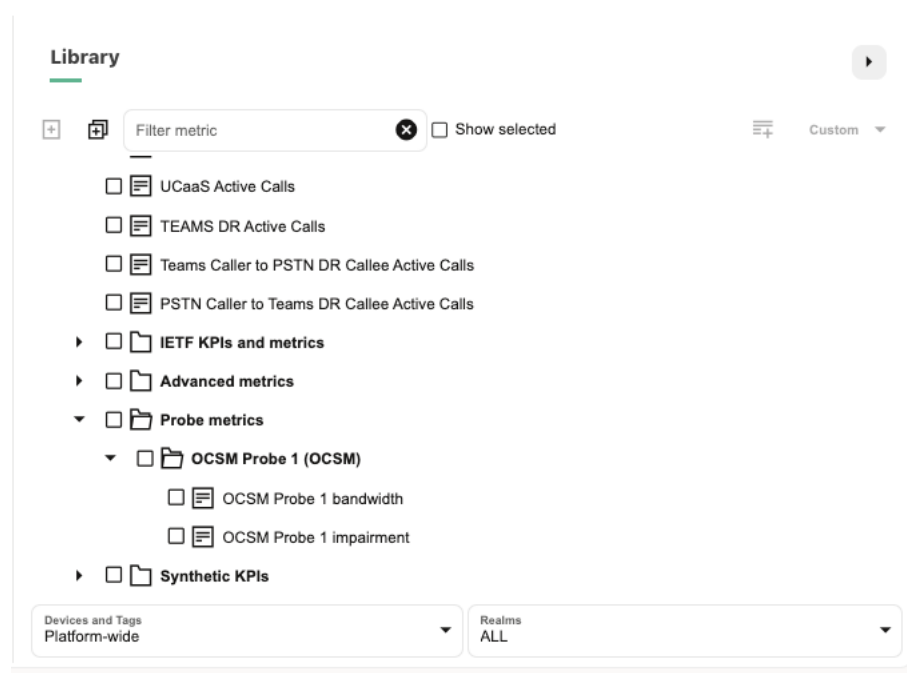
KPIs associated with each added probe

There are two KPIs that are associated with each added probe:

- **Bandwidth**, which is the amount of traffic, both forwarded by the probe in bits/second. Includes signal and also voice if it was recorded and forwarded to the Mediation Engine.
- **Impairment**, which is a Boolean value. Has the value of 1 for each minute that a problem has been detected with the probe. For more information on the problem the system log should be consulted.

Probe metrics are shown in the **KPI/Metrics** page, inside its own folder, as shown.

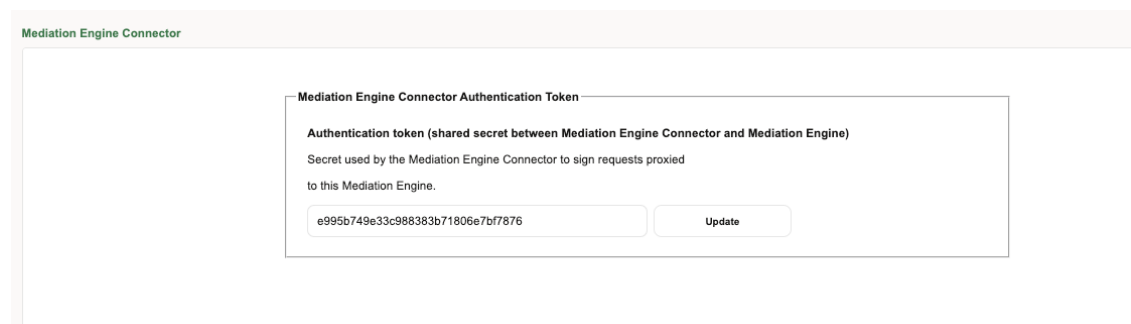
Figure 7-26 Library View of the Probe metrics Folder Metrics



Mediation Engine Connector

If Operations Monitor installation has been configured to use a Mediation Engine Connector, the authentication token, which this Mediation Engine uses to authenticate itself to the Mediation Engine Connector, can be configured on this page as shown here:

Figure 7-27 Authentication Token Configuration



To configure Mediation Engine Connector:

1. Log into Operation Monitor.
2. Click **Admin** and then click **Settings**.
3. Click **Network**.

4. Click **Mediation Engine Connector**.
5. In the **Authentication Token** field, enter your choice of token details for the Mediation Engine, and click **Update**.

Result: Mediation Engine connects with the Mediation Engine Connector.

Note

You must note down the token details for future reference.

6. (Optional) Perform the following steps if you have disabled the Mediation Engine.
 - a. Log into Mediation Engine.
 - b. Under **Settings**, click **ME Management**.
 - c. Select the node and double-click the disabled column field select **yes** from the drop-down list.

Note

If a node is marked as **Disabled**, the devices do not propagate to other Mediation Engines and the other Mediation Engine Connector controlled node Mediation Engines do not query for retrieving information about calls.

- d. Click **Save**.

Result: Mediation Engine is added.

Disconnecting Mediation Engine from Mediation Engine Connector

To disconnect Mediation Engine from Mediation Engine Connector:

1. Log into Operation Monitor.
2. Click **Admin** and then click **Settings**.
3. Click **Network**.
4. Click **Mediation Engine Connector**.
5. Click **Unlink from MEC...**

Result: The Mediation Engine is disconnected from Mediation Engine Connector.

Note

Though, Mediation Engine disconnected from Mediation Engine Connector, Mediation Engine details appears in the mediation engine list in the **ME Management** screen. To remove the Mediation Engine from the list, navigate to **ME Management**, select the mediation engine, click **Delete Selected** and then click **Save**. If you click **Replicate Configuration**, the mediation engine will connect back to the Mediation engine connector. Make sure to note down all the fields of this entry before disconnecting for future reference.

Number Determination Sources

This section of the configuration enables the definition of prioritized lists of trusted devices, from which phone number information may be taken for the caller and callee, along with the headers to be used (for example, From/To).

Note

Only data leaving a device via the Trusted IP ranges is considered for number determination purposes.

Figure 7-28 Enabling and Adding Prioritized Lists

Add new config [X]

Device:

Header:

Priority	Enable	Header
1	☐	SIP To header
2	☐	SIP request URI
3	☐	SIP P-Called-Party-ID header
4	☐	ISUP called party number from IAM/SAM
5	☐	ISUP generic number, ported number
6	☐	Custom SIP header name (custom header)

[Add] [Cancel]

Platform

The **Platform** section of the **Settings** window contains configuration options for defining the monitored SIP network. Operations Monitor requires this information for accurately mirroring SIP messages.

Platform Devices

The **Platform Devices** section is used to define the topology of the monitored network. This section defines the SIP devices and how they behave in order for Operations Monitor to properly merge calls and provide accurate overall and per-device statistics.

Figure 7-29 Platform Devices Settings

Platform Devices

Choose Template

Import

Export

Device Map

Group by

Filter

Toggle External

Realms

Diagram Order

VQ Status

Search:

☐ Show in groups

565

☐	Name	Type	Call Matching	IP Addresses	Point Codes	Visibility	External?	VQ Status	Device Map Status	Assigned Template
☐	dev_p2_1	PROXY		10.5.0.1		realm_for_admin	internal	Only MOScqe	Disabled	No Template
☐	dev_p2_2	PROXY		10.5.0.2		realm_for_admin	internal	Only MOScqe	Disabled	No Template
☐	dev_p2_3	PROXY		10.5.0.3			internal	Only MOScqe	Disabled	No Template
☐	dev_p2_4	PROXY		10.5.0.4			internal	Only MOScqe	Disabled	No Template
☐	dev_p2_5	PROXY		10.5.0.5			internal	Only MOScqe	Disabled	No Template
☐	dev_p2_6	PROXY		10.5.0.6			internal	Only MOScqe	Disabled	No Template
☐	dev_p2_7	PROXY		10.5.0.7			internal	Only MOScqe	Disabled	No Template
☐	dev_p2_8	PROXY		10.5.0.8			internal	Only MOScqe	Disabled	No Template
☐	dev_p2_9	PROXY		10.5.0.9			internal	Only MOScqe	Disabled	No Template
☐	dev_p2_10	PROXY		10.5.0.10			internal	Only MOScqe	Disabled	No Template
☐	dev_p2_11	PROXY		10.5.0.11			internal	Only MOScqe	Disabled	No Template
☐	dev_p2_12	PROXY		10.5.0.12			internal	Only MOScqe	Disabled	No Template
☐	dev_p2_13	PROXY		10.5.0.13			internal	Only MOScqe	Disabled	No Template
☐	dev_p2_14	PROXY		10.5.0.14			internal	Only MOScqe	Disabled	No Template
☐	dev_p2_15	PROXY		10.5.0.15			internal	Only MOScqe	Disabled	No Template
☐	dev_p2_16	PROXY		10.5.0.16			internal	Only MOScqe	Disabled	No Template

Table 7-8 Columns and Descriptions in the Platform Devices page

Columns	Descriptions
Add	A wizard guides you through to add additional platform devices options.
Edit	To edit a device, double click its table row, or select the device and click the Edit button. A wizard dialog box opens, pre-filled with the current values for the selected device.
Delete	To delete a device, select it and click the Delete .
Import	Import a device configuration
Export	Export a selected device configuration as a .csv file or JSON file.

Device Types

Operations Monitor supports the device types shown in Device Type Settings figure, and described in the table below. The **Show in groups** check box in the Platform Devices page, groups devices of the same type in a group.

Figure 7-30 Add a New Platform Device

Add a new platform device

Device Type

Select the device type you would like to add

- ☐ SBC/B2BUA
- ☐ Proxy
- ☐ Non-Record-Route Proxy
- ☐ Gateway
- ☐ Trunk
- ☐ L2 Balancer
- ☐ STP
- ☐ SGW
- ☐ Diameter agent
- ☐ HSS
- ☐ Diameter proxy

Required

Previous Next Finish Cancel

Table 7-9 Device Types

Device Type	Description
SBC/B2BUA	Select this option for devices that terminate an incoming leg and originate one or more independent outgoing legs from the same call (creating at least two SIP sessions). Examples include, session border controllers (SBCs), application servers (AS), and private branch exchanges (PBX). Because a B2BUA works by accepting the incoming call leg as a UAS, and creating a new leg as a UAC, it is difficult to determine whether two call legs are part of the same call. Therefore, on selecting this option, the wizard displays more configuration options for merging the call legs. For more information Choose the 3PCC option for SBC/B2BUA devices that work as 3PCC servers. These servers create a call between two parties using two outgoing call legs. The configuration options are available in the 3PCC Options page. When the 3PCC option is enabled on a SBC/B2BUA device type, the Operations Monitor must determine whether two outgoing legs are part of the same call. On selecting this option, a wizard displays more configuration options for 3PCC legs. If the device is capable of originating two outgoing legs with a common header in the context of the same call, only select the 3PCC option to configure. For Skype for Business calls, ensure that you configure the SfB Server as a B2BUA device. This is required for the outbound and inbound messages to be correlated and for the SfB calls to be shown as two distinct calls in the Calls page. This is shown in the Active Calls KPI.
Proxy	Select this option for devices that route calls without creating a new SIP dialog. The Call-ID in the outgoing call leg is usually left unchanged and SIP soft-switches and SIP layer load balancers are usually implemented as proxies.

Table 7-9 (Cont.) Device Types

Device Type	Description
Non-Record-Route Proxy	Select this option for devices that route INVITE messages but are skipped by the next messages in the dialog. These devices usually keep the Call-ID and the tag in the From SIP header field, as well as the URIs in the From and To headers unchanged.
Gateway	A SIP gateway is a device that connects the SIP platform to other types of networks (for example, PSTN, H.323). Operations Monitor only monitors the calls terminated and created by the gateway on the SIP side. Call merging is not created for gateway devices. If you need SIP/ISUP call merging, use an SGW (Signaling Gateway) device.
Trunk	This is not a physical device, but a peering with other carriers in which the peering IP addresses are known. Operations Monitor can display the calls going to and from this peer, as well as statistics about them. In addition to static IP addresses, the trunks can be defined using the OTG and DTG URI parameters.
L2 Balancer	A SIP load balancer acts at Layer 2 (of the OSI stack), keeping the IP addresses untouched and only modifying the hardware addresses. Operations Monitor supports these setups by identifying the devices by their hardware addresses in addition to the IP addresses.
STP	A Signaling Transfer Point (STP) monitors SS7/Sigtran routers and supports call merging for these protocols.
SGW	A Signaling Gateway (SGW) transfers between different types of protocols. These multi-protocol signaling routers convert between ISUP and SIP and allow call merging between different types of call signaling protocols. For more information, see. Note: A simple (or SIP) GATEWAY is always seen as a terminating device.
Diameter agent	Select this option if you are monitoring Diameter devices in Control Plane Monitor. For example, Mobile Management Entity (MME).
HSS	Select this option if you are monitoring Diameter messages exchanged with a Home Subscriber Server (HSS) in Control Plane Monitor.
Diameter proxy	Select this option if you are using an intermediate device to monitor a proxy that relays Diameter transactions in Control Plane Monitor.

SBC/B2BUA Call Merging

Call merging across B2BUA devices is a crucial point for SIP troubleshooting. Operations Monitor can use a large set of criteria for matching the calls, has several easy-to-use presets, and can also combine the criteria in a very flexible way by using custom algorithm expressions.

For STP devices, a similar choice of options applies. For SGW devices, the only options are the default or custom matching algorithm.

The wizard panel offers the high-level options:

image

Figure 7-31 Choosing the Call Matching Type for a B2BUA Device

Add a new platform device [X]

B2BUA Options
Select the method by which the call legs of this B2BUA (SBC etc.) can be matched.

☐ Use generic Oracle Communications Operations Monitor/Enterprise Operations Monitor algorithm (recommended)

☐ by Call-ID
Match if a common suffix of this many characters exists (optional):

☐ by From username
Match if a common suffix of this many characters exists (optional):

☐ by From and To username
Match if a common suffix of this many characters exists (optional):

☐ Use custom algorithm
Required

Previous Next Finish Cancel

Table 7-10 B2BUA Device Options

Option	Description
Use generic Oracle Communications Operations Monitor/Enterprise Operations Monitor algorithm (recommended)	The algorithm was developed to accurately detect which call legs belong to the same call for the most common SBC/B2BUA configurations. The algorithm takes into account the time difference between the calls, the <i>session-id</i> from the SDP, the From and To users, the P-Asserted-Identity header, the Diversion header, etc. Oracle recommends using this option and to adjust if necessary. For more information about the generic algorithm, see " Call Merging Algorithms ".
by Call-ID	To be used if the SBC/B2BUA is configured to copy the Call-ID header from the incoming <i>call leg</i> to the outgoing <i>call leg</i> . If the <i>suffix</i> parameter is given, then only the last <i>suffix</i> characters are compared. This is useful, for example, if the SBC/B2BUA only prepends a string to the <i>Call-ID</i> to make it unique.
by From username	To be used if the SBC/B2BUA is configured to keep the same From user between <i>call legs</i> , and this does not lead to false positives in most cases. If the <i>suffix</i> parameter is given, only the last <i>suffix</i> characters are compared. This is useful if the SBC/B2BUA only changes the prefix of the numbers (for example, from +49 to 0049).

Table 7-10 (Cont.) B2BUA Device Options

Option	Description
by From and To username	To be used if the SBC/B2BUA is configured to keep the same From user and To user between <i>call legs</i> . If the <i>suffix</i> parameter is given, only the last <i>suffix</i> characters are compared. This is useful if the SBC/B2BUA only changes the prefix of the numbers (for example, from +49 to 0049).
Use custom algorithm	This allows flexible combining available criteria for matching, ordered tests, and nested tests, as well as matching on arbitrary SIP headers. For more information on how to write a custom algorithm, see "Call Merging Algorithms" . If this is selected, another wizard panel will be shown for entering the algorithm. The Operations Monitor generic algorithm is pre-filled as a starting point.

Figure 7-32 Entering a Custom Match Algorithm

Add a new platform device ×

Custom call matching script for B2BUA

Enter the call matching script:

```
(cond
  ((call_id 0) #t)
  ((sdp_media_ip_port) #t)

  ; custom header
  ((hf_equals "session-id") #t)

  ((time_diff 15000 2000) #f)

  ; Matching by from and to
  ((uri_user 6 ("from" "pai" "rpid" "ppid"))
    (cond
      ((uri_user 6 ("to" "ruri" "diversion")) #t)
      (## #f)
    )
  )
)

; If nothing matches, return false (default)
```

Previous Next Finish Cancel

3PCC Options

Third-Party Call Control (3PCC) servers initiate two outgoing legs to establish a single call between two parties. Session Monitor correlates the two SIP sessions using a custom header that is common to both outgoing legs. This feature is configurable per SBC/B2BUA device. The default value is disabled.

Figure 7-33 Configuring 3PCC Options

Add a new platform device [X]

3PCC Options

Select this option only if the selected device functions as 3PCC (3rd Party Call Correlation) server. Select the strategy to identify defining call between the matching legs and configure call matching script by which 3PCC outgoing legs are matched.

3PCC mode: ON/OFF button

☒ Enable 3PCC ⓘ

Triggering Leg Identification:

Please select [v] Required

Custom call matching script for 3PCC: ⓘ

[] Required

Previous Next Finish Cancel

Identifying the Triggering Leg

The *triggered leg* or Callee leg is the leg that defines the call state. The other leg is the *triggering leg* or Caller leg. For example, a 3PCC server originates a call to both a SIP User Agent and a PSTN user. The outgoing leg towards the User Agent is the triggering leg and the outgoing leg towards the PSTN user is the triggered leg.

There are two ways to identify the triggering leg:

1. **Hostname in FROM and TO Headers being the same in INVITE:** The INVITE in the triggering leg contains the same hostname in the From and To headers.
2. **Provisional Response:** The triggering leg generates a provisional response (18x) relatively faster than that of the triggered leg.

Select one of the strategies to identify the triggering leg.

Call Matching Script

The call matching script correlates the two outgoing legs in the context of 3PCC calls.

The following is the basic template for a call matching script.

```
(cond
  ((hf_equals <any 3PCC custom header>) #t)
  ((time_diff 2000 0) #f)
  ; If nothing matches, return false (default)
)
```

If the 3PCC header is X-Genesys-CallUUID, the script looks like the following.

```
(cond
  ((hf_equals "X-Genesys-CallUUID") #t)
  ((time_diff 2000 0) #f)
  ; If nothing matches, return false (default)
)
```

The functionality of `hf_equals()` is explained in the Call Merging Algorithms chapter, but the `time_diff()` method varies slightly in a 3PCC call matching script. The syntax is `time_diff(interval1, interval2)`.

- `interval1` - The maximum time difference between the initial INVITE message of one outgoing call leg and the initial INVITE of another outgoing call leg. The maximum value is 5 seconds.
- `interval2` - Since there won't be any matching incoming call legs for outgoing call legs in 3PCC calls, this value has no significance and is not used. Use the default value of 0.

 Note

The algorithm configured, in this 3PCC options page, will not be used to correlate incoming calls and outgoing calls.

Enable the 3PCC option only when a device functions as a 3PCC server by originating two outgoing legs in the context of the same call. Because 3PCC is more resource intensive, choose this option only when needed.

Device Identification

The devices are usually identified by only their IP addresses. Exceptions are the *trunk* devices, which can be also identified by the *OTG* and *DTG* parameters, and the set-ups in which the hardware addresses are significant. Either IPv4 or IPv6 addresses may be supplied. IP ranges with bitmasks smaller than 24 (for IPv4) or 120 (for IPv6) might impact performance significantly.

In the **Device identification by address** wizard panel, specify the identification addresses for the device you create. Enter the IPs used by the device in a list separated by spaces. If multiple devices share an IP address, but are in different VLANs, you can also specify the VLAN IDs.

You can specify VLAN IDs in multiple ways. You can enter:

- **IP(VLAN=x)** with $x \geq 0$, which matches packets with VLAN ID x .
- **IP** without a specified VLAN. The IP matches any packets, with or without a VLAN.
- **IP(VLAN=0)** or **IP(VLAN=off)** which only matches packets with no VLAN. This restricts the IP to only non-VLAN packets.

Figure 7-34 Device Identification Settings

Add a new platform device [X]

Device identification by address

Select the identification addresses for this device.

IPs used by this device (space separated). If more devices are sharing the same IP address, but are in different VLANs, you can specify the VLAN IDs here. If left out, all VLAN IDs are matched.
Example: "172.23.12.0/24 172.43.34.1 172.43.23.3/24(vlan=60) 172.3.2.4(vlan=50) 74dc::2ba":

Trusted IPs. Often internal IPs, used by Number Determination Sources:

Required

Previous Next Finish Cancel

Identifying Trunk Devices

For *trunk* devices, there is also the option of identifying by using the *OTG* and *DTG* parameters, offered by an extra wizard panel.

Figure 7-35 Trunk Identification Settings

Add a new platform device [X]

Device identification strategy

Select the device identification strategy.

☐ Use IP addresses

☐ Use DTG/OTG URI parameters

Required

Previous Next Finish Cancel

The parameters *OTG* and *DTG* are the originating and destination trunk identifiers found in the **From** header field of the *URI*, respectively, *Request-URI*.

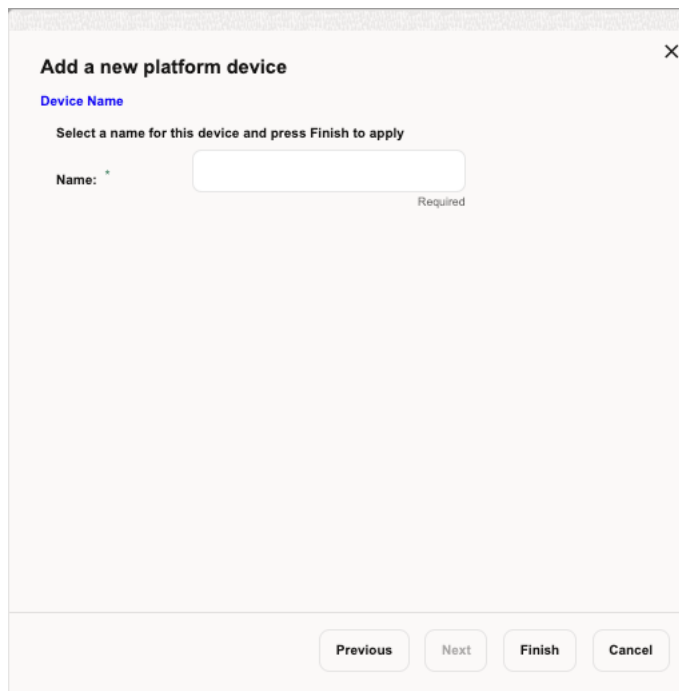
Trusted IP Ranges

For the Number Determination algorithm, only these IPs (or point codes) on each device are considered when identifying a call. Set this field to the source IPs for messages that you wish to take number information from.

Providing a Name

The last step in the creation wizard is to set a name for the device. The name may contain spaces, but it is recommended to keep the name short in order to fit in the table columns and SIP diagrams.

Figure 7-36 Device Name Settings



Add a new platform device X

Device Name

Select a name for this device and press Finish to apply

Name: * Required

Previous Next Finish Cancel

Visibility Configuration

You can configure a device or trunk to be visible or hidden for each realm. Click the **Realms** button in the toolbar to list the current defined realms as illustrated. If one or more realms are checked, the device/trunk is visible only to the users belonging to those realms.

Figure 7-37 Device Visibility Settings

Select in which realms the device is visible

Realms
☒ realm_for_admin
☐ realm_for_user_0
☒ realm_for_user_1
☐ realm_for_user_10
☐ realm_for_user_11
☐ realm_for_user_12
☐ realm_for_user_13
☐ realm_for_user_14
☐ realm_for_user_15
☐ realm_for_user_16
☐ realm_for_user_17

Close

Configuring Devices for the Mediation Engine Connector

A Mediation Engine Connector allows a user to monitor multiple Mediation Engines that are located in separate geographic locations.

If a call is sent through a device monitored by two Mediation Engines, the Mediation Engine Connector sees the call flow through both Mediation Engines. In order for the Mediation Engine Connector to correlate the call, you must designate one Mediation Engine as internal, and the second Mediation Engine as external. The Mediation Engine Connector consolidates the data from both Mediation Engines and presents the single call flow.

The **Toggle external** button allows you to select a device and determine if the device is visible to the associated "internal" Mediation Engine, or visible to other "external" Mediation Engines in the Mediation Engine Connector platform.

For more information on correlation, see "Understanding Call Correlation" in "Configuring Mediation Engines" in *Mediation Engine Connector User's Guide*.

For more information regarding the Mediation Engine Connector, consult your Oracle representative.

Enabling or Disabling Device Map for a Device

A Device Map shows an overview of the status and activity for all configured devices on the monitored platform. You can enable or disable the display of a device in device map for a specific device in the **Platform Devices** page.

After upgrading to 4.4 from a previous release, with the Device Map Limit set to any value outside of the supported range, the **Enabled device map** flag is set to **False** and the individual **Device Map Status** for all devices in Platform Devices is set to **Disabled**. This is also applicable to the savepoint configuration from older releases that are restored in 4.4.

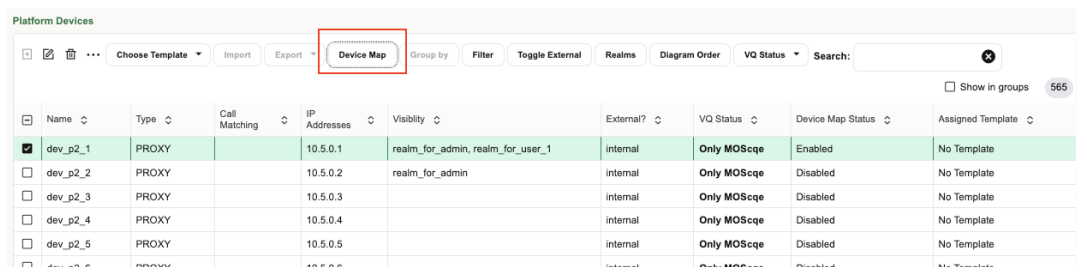
To enable Device Map for a device and to set the limit:

1. Click **admin**, and then click **Settings**.
2. In the **Settings** page, click **Platform**, and then click **Platform Devices**.
3. Select the device for which you want the device map to be enabled.
4. Click **Device Map** to enable or disable.

Note

If the **Device Map** button is not enabled, set the **Enabled Device Map** flag to **True**. You can find this under **System Settings**.

Figure 7-38 Enabling Device Map



The screenshot shows the 'Platform Devices' interface. At the top, there are buttons for 'Choose Template', 'Import', 'Export', and 'Device Map'. The 'Device Map' button is highlighted with a red rectangle. Below the buttons is a table with columns: Name, Type, Call Matching, IP Addresses, Visibility, External?, VQ Status, Device Map Status, and Assigned Template. The table contains five rows of device data. The first row, 'dev_p2_1', has 'Device Map Status' set to 'Enabled'. The other rows have 'Device Map Status' set to 'Disabled'.

Name	Type	Call Matching	IP Addresses	Visibility	External?	VQ Status	Device Map Status	Assigned Template
dev_p2_1	PROXY		10.5.0.1	realm_for_admin, realm_for_user_1	internal	Only MOScqe	Enabled	No Template
dev_p2_2	PROXY		10.5.0.2	realm_for_admin	internal	Only MOScqe	Disabled	No Template
dev_p2_3	PROXY		10.5.0.3		internal	Only MOScqe	Disabled	No Template
dev_p2_4	PROXY		10.5.0.4		internal	Only MOScqe	Disabled	No Template
dev_p2_5	PROXY		10.5.0.5		internal	Only MOScqe	Disabled	No Template

Note

If you set the **Enabled Device Map** flag under **System Settings** to **True**, then for a selected Platform device, setting the **Device Map Status** to **Enabled** creates device-to-device counters for that specific device. Setting **Device Map Status** to **Disabled**, deletes those counters.

Configuring Devices for Voice Quality Measurement

The **Voice Quality** page lets you to view voice quality statistics based on the MOS, Packet Loss, and Jitter measures. For more information on voice quality, see "[Voice Quality](#)".

You can configure a device or trunk to be associated with either of the following voice quality (VQ) statuses.

If a device has no templates applied, then the VQ Status button is enabled for all such devices. If you have upgraded to Session Monitor Release 6.1, all devices can still use this VQ Status button if no templates are applied. This ensures that you can apply VQ statuses for all the devices post upgrade.

If a device is associated with a template then the VQ Status button is disabled. You can still add VQ counters as part of a custom template for a device. For more information on custom templates, see [KPI Templates](#).

- No VQ: None of the VQ counters is enabled.
- Only MOScqe: Only the MOS VQ counter is enabled and the other VQ counters gets disabled.
- Full VQ: All three kinds of the VQ counters (MOS, Packet Loss, and Jitter) are enabled.

Note

When you change the **VQ status** for a device from "Full VQ" to "No VQ" or "Only MOScqe", and from "Only MOScqe" to "No VQ", the existing VQ data of the "Full VQ" status and the "Only MOScqe" status is lost.

Figure 7-39 Platform Devices Settings - VQ Status

Platform Devices

Choose Template Import Export Device Map Group by Filter Toggle External Realms Diagram Order VQ Status Search: 565

Name	Type	Call Matching	IP Addresses	Visibility	External?	VQ Status	Device Map Status	Assigned Template
Trunk1	TRUNK		1.2.2.33		internal	No VQ	Disabled	Default
Test Device 11	SBC/B2BUA	Using generic ...	2.2.2.23		internal	No VQ	Disabled	No Template
Test Device 1	SBC/B2BUA	Using generic ...	2.2.2.22		internal	No VQ	Disabled	Default
10_A_SBC	SBC/B2BUA	Using generic ...	1.1.1.11		internal	No VQ	Enabled	Default
Dev_test1	SBC/B2BUA	Using generic ...	2.3.2.1		internal	No VQ	Disabled	No Template
dev_stp_520	STP	Using generic ...	10.13.0.40		internal	Only MOScqe	Disabled	No Template
dev_stp_519	STP	Using generic ...	10.13.0.39		internal	Only MOScqe	Disabled	No Template
dev_stp_518	STP	Using generic ...	10.13.0.38		internal	Only MOScqe	Disabled	No Template
dev_stp_517	STP	Using generic ...	10.13.0.37		internal	Only MOScqe	Disabled	No Template

Note

If the **VQ status** displays the word "**Partial**" in red while associating a device with the VQ status, it implies there has been an issue causing the device counters to not match the VQ status. To resolve this issue, try setting **VQ Status** back to "No VQ" for the device using the **Platform Device Settings** page, and then again to "Full VQ" to re-add the VQ counter.

Searching for Platform Devices

Using the **Search** option, you can search for and filter platform devices quickly and efficiently.

The Search feature allows you to narrow down results based on keyword such as device name, Type and so on. This helps you locate the exact platform device you need. If you are managing a large list of platform devices or troubleshooting individual devices, this tool simplifies the process.

Figure 7-40 Searching for Platform Devices

Platform Devices

Choose Template Import Export Device Map Group by Filter Toggle External Realms Diagram Order VQ Status Search: 21

Name	Type	Call Matching	IP Addresses	Point Codes	Visibility	External?	VQ Status	Device Map Status	Assigned Template
B2BUA1	SBC/B2BUA	Using generic ...	172.16.0.2 17...		realm1	internal	No VQ	Disabled	SBC1
B2BUA2	SBC/B2BUA	Using generic ...	172.16.0.3 17...		realm1	internal	No VQ	Disabled	SBC1
B2BUA3	SBC/B2BUA	Using generic ...	172.16.0.4 17...		realm1	internal	No VQ	Disabled	SBC1
B2BUA4	SBC/B2BUA	Using generic ...	172.16.0.5 17...		realm1	internal	No VQ	Disabled	SBC1

Click **X** to clear the Search keyword.

Device Monitoring

The **Devices Monitoring** page is used for starting monitoring a device defined in "[Platform Devices](#)". Monitoring is realized by counting the number of requests that remain unanswered.

Figure 7-41 Devices Monitoring Settings



SIP Device	Monitoring Type	Failure Limit	Wait Period	Enabled?
dev_p2_1	PASSIVE	20	5	Disabled

Operations Monitor uses the following algorithm for monitoring SIP devices:

- A counter is kept with the number of *incoming* SIP requests to the monitored device, which have received no answer. These requests are *not* sent by Operations Monitor, but are regular requests from the SIP network.
- Whenever the monitored device sends a message (regardless of what type of message), the counter is set to zero, because the device must be *up*.
- If the counter exceeds a configurable threshold, a timer is started to fire after a configurable time interval.
- If the monitored device sends a message before the timer fires, the timer is canceled and the counter is set to zero again.
- If the timer fires, the monitored device is marked as *down*.

Enabling Device Monitoring

In the **Device Monitoring** table, each line represents a device being monitored. To enable or disable the monitoring of any device, select the device in the table and click the **Toggle Enabled** button in the toolbar. The **Enabled?** column from the table shows the current status.

Adding and Editing Monitored Devices

Before you add a device to be monitored, you must configure the device in the **Platform Devices** settings section.

To add a new monitoring configuration, click the **Add** button from the upper toolbar. A wizard dialog guides you through the monitoring options.

To edit an existing monitoring configuration line, select the device and click the **Modify** button in the toolbar. A wizard dialog opens pre-filled with the current values for this monitoring configuration. If you want to permanently delete a configuration type for a device, select it from the table and click **Delete**.

Note

Device monitoring does not affect the performance or stability of the monitored device. It is immune to connectivity problems between the monitoring and the monitored device, reducing false positives.

Device Monitoring Parameters

To configure a device monitoring, a couple of parameters are requested:

- Device name to be monitored.
- Expiry interval of the timer.
- Number of unanswered requests needed to start the timer.

Additionally, you can enable device monitoring immediately, or leave it disabled until toggled from the list of monitored devices.

Figure 7-42 Device Monitoring Parameters

Add new device monitoring entry X

Device to monitor

Choose the device to monitor

Device: dev_p2_1

Expiry interval. The time in seconds (floats accepted) after to declare a request as not answered: 5

The number of consecutive inbound requests marked as not answered needed to declare the device as down: 20

Select this checkbox if you want to enable monitoring now. You can toggle this option later without changing the other options: ☒

Finish Cancel

IP Tags

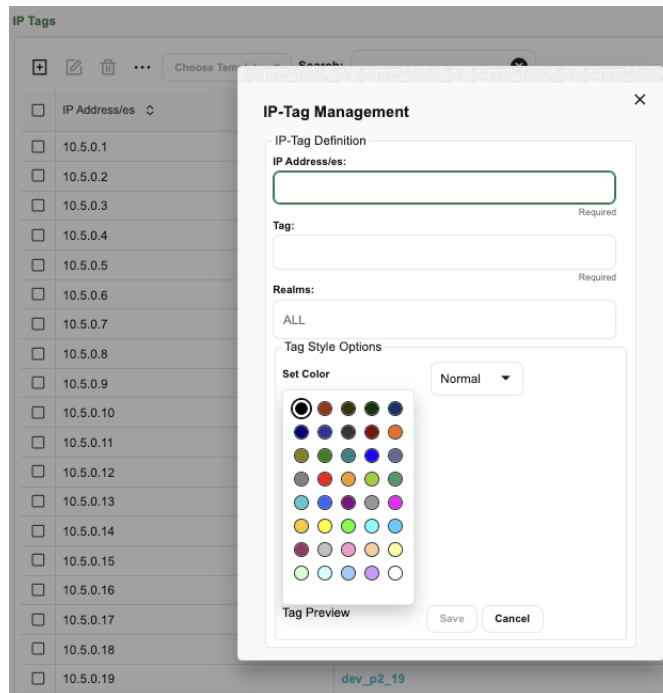
IP tags are a way of assigning friendly names to *IP* addresses or *IP subnets* (either IPv4 or IPv6). The IP tag's name appears in brackets in the **Call Details** window. The color and font style of the tags can be customized. IP tags are visible and editable by all users.

You can assign KPI templates to IP Tags. For more information on Choose Template, and Assigned template, see [KPI Templates](#).

Adding a New IP Tag

The New IP Tag Management window is used to add new IP addresses.

Figure 7-43 Adding a New IP Tag



Searching for IP Tags

You can search for IP Tags previously created using a keyword in the Search text box.

Prefix Tags

Prefix tags allow assigning a friendly name to phone *prefixes*. Once the prefix tag is created, the user can create a KPI or metric on. You can, like with devices, configure a prefix tag to be visible or hidden for each realm, with the difference that prefixes in the *ALL* realm won't be visible for the user in another realm. For more information, see ["KPI/Metrics"](#).

When a prefix tag KPI is created in a realm, the value of the KPI is sourced from the calls matching both the prefix and the realm pattern. If you create a prefix tag in one realm and a KPI in a different realm, the KPI will not be visible to users who are restricted to one of the two realms.

The **Platform: Prefix Tags** window is used to add new Prefix tags.

Figure 7-44 Adding a New Prefix Tag

The screenshot shows the 'Prefix Tags' management interface. A modal dialog titled 'Add new Prefix Tag' is open, allowing the user to create a new tag. The dialog contains three input fields: 'Name' (with the value 'Prefix +1'), 'Prefixes' (with the value '+111' and a 'Required' label), and 'Realms' (with the value 'ALL'). 'Save' and 'Cancel' buttons are at the bottom right of the dialog. In the background, a table lists existing prefix tags with columns for 'Name' and 'Prefixes'.

Name	Prefixes
+4158	+4158 058 58 4158 004158
+4161	
+4171	
+4177	
+4178	
+4179	
+4181	
+4191	
+4121	
+4122	
+4143	
+4144	
+4141	
+4131	
+4152	
+4155	+4155 055 55 4155 004155
+4133	+4133
+4132	+4132 032 32 4132 004132
+4126	+4126 026 26 4126 004126
+4127	+4127 027 27 4127 004127

You can apply KPI templates to Prefix tags. For more information on **Choose Template**, and **Assigned Template**, see [KPI Templates](#).

Note

You can create a prefix tag using a maximum of 6 characters (including the "+" character if it is needed). For example, 493080.

Searching for IP Tags

You can search for Prefix Tags previously created using a keyword in the **Search** text box.

Automatic Realm Pattern Import

You can create an external list of realm patterns and import the list into Operations Monitor. You can compose a list as a CSV file, upload the file by using FTP, and configure Operations Monitor to have the CSV file processed at a defined interval to import the realm patterns.

This is an alternate method of adding realms to Operations Monitor. Importing realm patterns from an external CSV file may be preferable if you have a large number of entries to add or if you make frequent changes to the realm definitions. See [Realms](#) for more information on adding realms using the Operations Monitor interface.

 Caution

Importing new realm patterns overwrites existing realm patterns. The import feature is not additive; rather, all numbers for all realms should always be present in the CSV file.

About Formatting the CSV File

Each line in the CSV file contains the realm name and the number pattern separated by a comma.

For example:

RealmName, NumberPattern

Assign each realm name and number pattern a unique value and order the list alphabetically. Only enter single number entries (even if there are number ranges belonging to the realm). Do not include duplicate entries. The import function of Operations Monitor compacts the numbers to the least possible amount of patterns by grouping them into the ranges.

Following is an example of a list of realm names and number patterns:

```
03940394, 444333222111
40404044, 404040404040
realmone, 133334444555
realmone, 133334444666
second, 12224444333
```

Sorting Realms

If you are unsure of the uniqueness or ordering of realm names and number patterns, you can use the UNIX **sort** function on the file you have created.

From the command line, enter:

```
/var/vsi/ftp/realms# cat list.csv | sort -u > ordered_list.csv
```

The listing of users can be sorted on name, email, or realm.

When sorting on realm, **ALL** comes first (or last, respectively), even if there is an entry coming alphabetically before **ALL**. Similar logic applies for realm **NONE**, which, however should never appear unless you have a broken database or misconfiguration.

If you use the **sort** function in Operations Monitor, use the command to remove the original list after the sorting is complete. Since all entries must be unique, allowing the original list to remain following the sort would introduce duplicate entries. The original list would also exist in an unsorted state.

Run the following command to remove the original list:

```
/var/vsi/ftp/realms# rm list.csv
```

Importing Realms at a Daily Frequency

You can set a specific time at which the new realm patterns are automatically imported each day.

To enable importing realms at a daily frequency, at the command line:

1. Create a folder within the FTP directory:

```
mkdir /var/vsi/ftp/realms
```

2. Open the **etc/iptego/vsp.conf** file and add the following text:

```
[realms]
import-enabled=1
import-task-hour=hour
import-task-minute=minute
```

The *hour* and *minute* variables indicate the hour of the day and the minute of the hour that the feature processes the CSV file. Valid values for the hour field are 0 through 23. Valid values for the minute field are 0 through 59.

The following example schedules an import to take place every day at 03:10 a.m. server time:

```
import-enabled=1
import-task-hour=3
import-task-minute=10
```

3. Save and close the file.
4. Restart the respective process to make above changes active:

```
systemctl restart pld-vsp.service
```

Editing the CSV File

Edit the CSV file externally, then recommit it by using FTP to the **realms** folder. Make sure the CSV file is ordered and with unique entries. On the configured import time, the change will take effect.

There can be multiple CSV files present in Operations Monitor. Ensure that the entries are unique across all the CSV files.

Realms

You configure *Realms Definitions* under the **Realms** section of the **Settings** menu. Each *realm* can have one or more *realm patterns* associated with it.

Realms can be used for limiting the visibility of Operations Monitor's web interface users. They are useful in scenarios such as:

- You have a set of resellers of the SIP service, and you want to give each of them the monitoring abilities of Operations Monitor, but at the same time restrict their view only to the SIP users served by them.
- You have a set of support workers, and you want to give them the fast troubleshooting abilities of Operations Monitor, but in the same time restrict their view to a certain set of users, for privacy reasons.

A *realm* can be defined as a set of *telephone numbers* or as a set of *domains*. The set of rules defining a *realm* are called *realm patterns*. Additionally, a custom header in SIP can contain a realm identifier.

Note

Realms do not need to be disjoint. For example, you can have a single telephone number in multiple realms, and you can have one realm containing the union of other two realms.

If a user has his or her visibility restricted to one *realm*:

- The user only sees the registered subscribers that are part of the *realm*. The *User tracking* feature is restricted as well.
- The user only sees calls in which the caller or the callee are part of the *realm*.
- *Statistics* are adjusted to reflect only the **Realm** section, not the whole platform. For example, the **Active Calls** chart counts only the active calls in which one of the participants is part of the *realm*.

Note

Voice quality statistics are an exception. Realm separation does not apply to voice quality statistics. Users assigned to realms see platform wide voice quality values.

- If the user creates a *trace*, it will only contain the messages that are from or to subscribers of the *realm*.
- *Alerts* are only sent to the user if the cause of the alert is part of his *realm*.

In other words, *realms* are segments of the subscriber base, and if an Operations Monitor user's view is restricted to a *realm*, Operations Monitor will only show information about that segment.

Note

Realm names *cannot be deleted*, only the realm patterns.

Realms are not the only way to limit the view of the web interface users. You can also restrict features by using *user rights*. For more information, see "[User Management](#)".

Realms Table

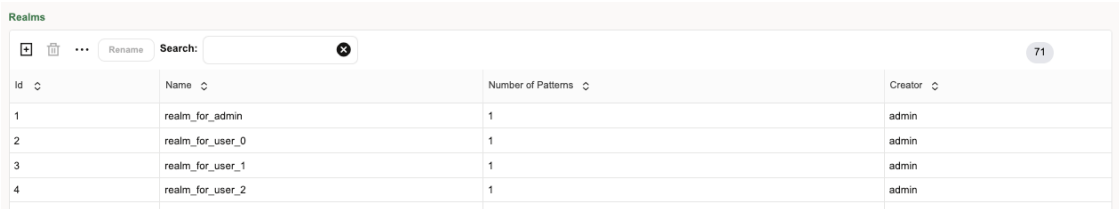
The Realms panel used for adding, editing and deleting *realms*. Realms can also be created from the Realm Patterns Table edit window. Deleting a realm will also delete all its associated patterns.

Note

When deleting a realm, in case there are devices associated with that realm, a warning is displayed showing these devices.

It is the user's responsibility to remove these devices manually. Otherwise, the devices would be still available in the **Platform Devices** settings section without any realm assigned.

Figure 7-45 Realms Definitions



Realms			
71			
Id	Name	Number of Patterns	Creator
1	realm_for_admin	1	admin
2	realm_for_user_0	1	admin
3	realm_for_user_1	1	admin
4	realm_for_user_2	1	admin

Searching for Realm Patterns

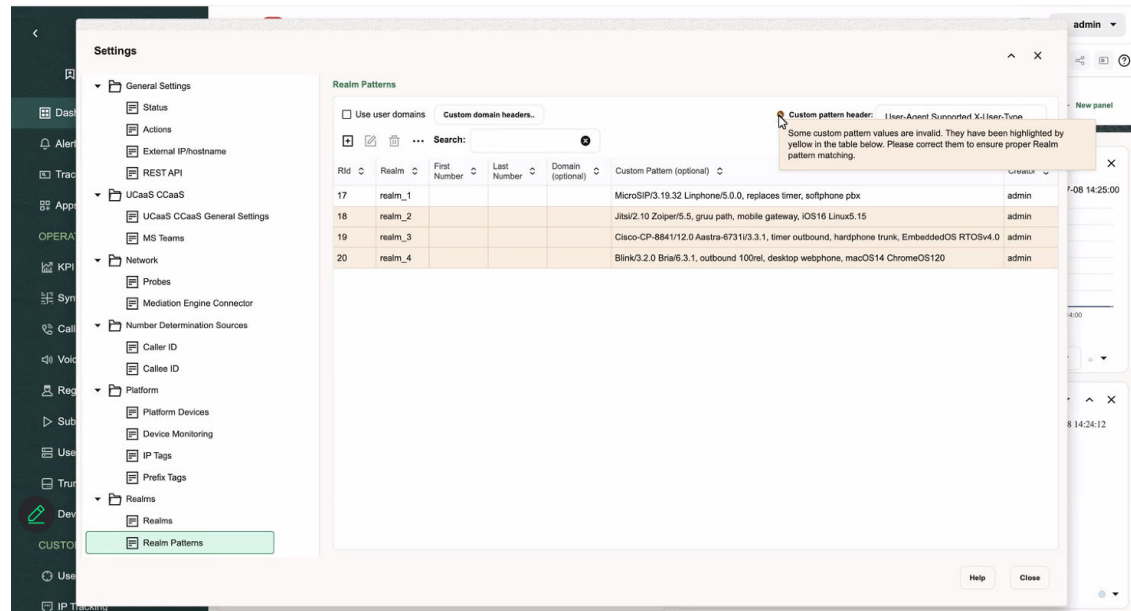
Using the **Search** option, you can search for and filter Realm quickly and efficiently.

The intuitive **Search** option supports keyword searches. This feature allows you to filter Realms based on attributes such as Name, Number of Patterns, and Creator. This ensures that you can locate the exact Realm you need without unnecessary delays. This capability is especially useful for large data sets, allowing you to focus on relevant Realms, and ensures faster access to critical resources.

Realm Patterns

The **Realm Patterns** page shows the panel used for defining *realm patterns*. Selecting a realm pattern and then clicking the toolbar Edit button, or double-clicking an entry opens an editing window.

Figure 7-46 Realm Patterns page



This table describes the fields found in the **Add new realm pattern** table:

Figure 7-47 Add a new realm pattern

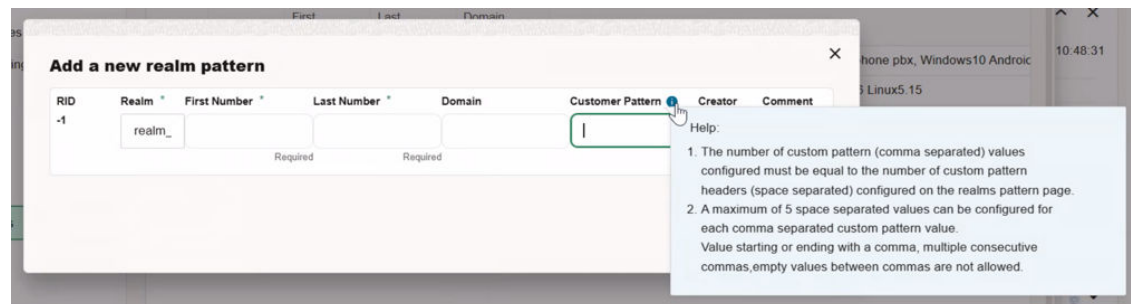


Table 7-11 Add a New Realm Pattern Fields

Field	Description
Rid	The ID of the realm.
Realm	The name of the <i>realm</i> . The edit select menu of the field offers the previous used <i>realms</i> , but also allows entering a new name. By entering a new name and pressing the Create button, a realm with that name is created immediately.
First number	The first phone number from a <i>number range</i> <i>realm</i> . If this is specified, then the <i>Last number</i> must also be specified. The realm will contain all numbers from the range.

Table 7-11 (Cont.) Add a New Realm Pattern Fields

Field	Description
Last number	The last phone number from a <i>number range realm</i> . If this is specified, then the <i>First number</i> must also be specified. The realm will contain all numbers from the range.
Domain	The domain from a <i>domain restricted realm</i>. The realm will contain all the users from the given domain. This can be combined with the <i>First number</i> and <i>Last number</i> options in which case all restrictions apply. If the <i>First number</i> and the <i>Last number</i> are provided, the caller or callee number must be in the range between those values. If Domain (optional) is provided, then the number must be in between the <i>First number</i> and <i>Last number</i>. Additionally, the domain must match the value provided in the Domain field. Therefore, between <i>First number</i>, <i>Last number</i>, and <i>Domain</i>, there exists an AND relationship. The caller or callee information must fulfill all the conditions to be assigned to the realm.
Custom Patterns (Optional)	Add an custom header pattern for matching of Calls/Registrations to this pattern. If a call's invite/SIP registration contains this header pattern then it is counted in the Realm. For Custom Pattern, either the <i>First number</i>, <i>Last number</i>, and <i>Domain</i> OR the Custom Pattern must match. For a Custom Pattern, there exists an OR relationship. • Add multiple comma-separated custom patterns • Each custom pattern can have a maximum of 5 space-separated values. • The comma-separated custom patterns must exactly match the number of custom headers defined in the Custom header for realm definition. • If the custom headers are modified, existing Realms with custom patterns are revalidated. If validation fails, the corresponding rows in the Realm Patterns table are highlighted in Yellow as a warning, and an error message is displayed. For more information, see Realms Header Specification.
Creator	The user who created this realm.
Comment	(Optional) Comment line, only for convenience.

Note

In order for the *domain restricted realms* to work, Operations Monitor needs to be configured to consider the domains in the user identifiers. Set the **Use User Domains** to **true**. For more information, see Use User Domains.

Note

Configuring a large number of realm patterns will affect the performance of the server.

Figure 7-48 Realm Patterns

Realm Patterns							
☐ Use user domains		Custom domain headers..		Custom pattern header: User-Agent P-Asserted-Identity P-Access-Network-Info Supported			
+ ✎ 🗑️ ...		Search:		Import from CSV		Export as CSV	
Rid	Realm	First Number	Last Number	Domain (optional)	Custom Pattern (optional)	Creator	
1	realm_1				zmq* Ekiga* Kphone/3.2 PhoneR-us CiGateway, sip:alpha, 3GPP 5GNNR, outbound	admin	
2	realm_2	595000000170	595000000180			admin	

Figure 7-49 Realm Patterns Definitions

Realm Patterns							
☐ Use user domains		Custom domain headers..		Custom pattern header:			
+ ✎ 🗑️ ...		Search:		Import from CSV		Export as CSV	
Rid	Realm	First Number	Last Number	Domain (optional)	Custom Pattern (optional)	Creator	Comments (optional)
1	realm_for_admin	490000000000	499999999999			admin	
2	realm_for_user_0	490000000000	499999999999			admin	
3	realm_for_user_1	490000000000	499999999999			admin	
4	realm_for_user_2	490000000000	499999999999			admin	

For example, the configuration from the Realms Patterns page defines the realm *reseller A* to contain:

- The phone number range 00491234000 to 00491234999, regardless of the domain name.
- The phone number range 0301234000 to 0301234555, regardless of the domain name.
- All users that have **a.sip.palladion.net** as their domain name.

The *realms* configuration can be exported to and imported from CSV files. This simplifies the *realms* maintenance in case of many *realms patterns*. For example, the configuration in *Realm Pattern Definitions* would be exported to:

```
name,min,max,domain,comments
reseller A,00491234000,00491234999,,
reseller A,0301234000,0301234555,,
reseller B,0301234556,0301234999,,
reseller B,,,b.sip.palladion.net,
reseller A,,,a.sip.palladion.net,
test,00445213000,00445213500,,Test realm with a single number.
```

The realms patterns can also be provisioned automatically by uploading a similar CSV file via FTP.

Searching for Realm Patterns

Using the **Search** option, you can search for and filter Realm Patterns quickly and efficiently.

The intuitive **Search** option supports keyword searches. This feature allows you to filter patterns based on attributes such as First Number, Last Number, Domain etc. This ensures that you can locate the exact Realm Pattern you need without unnecessary delays. This capability is especially useful for large data sets, allowing you to focus on relevant patterns, and ensures faster access to critical resources.

Realms Header Specification

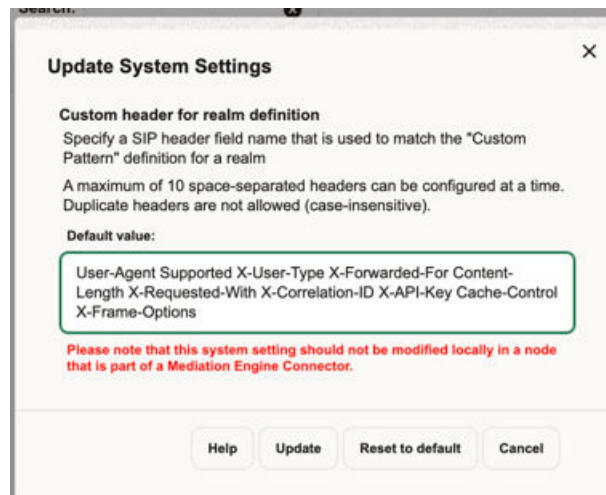
There are two System Settings that modify the way Operations Monitor assigns Realms to Calls/Registrations. By default Operations Monitor checks the **To:** and **From:** header for each SIP invite/SIP Registration message and matches this Call/Registration with all matching Realms ("or").

You can specify additional header fields in the System Setting named **Headers in which to look for realm URIs. Diversion** or **P-Asserted-Identity** could be useful values, depending on the configuration. Operations Monitor generally checks all the occurrences of each of these fields in each SIP Invite/Registration message. Exceptions are possible for header fields whose repetition is forbidden by the SIP standard.

Further customization is possible by:

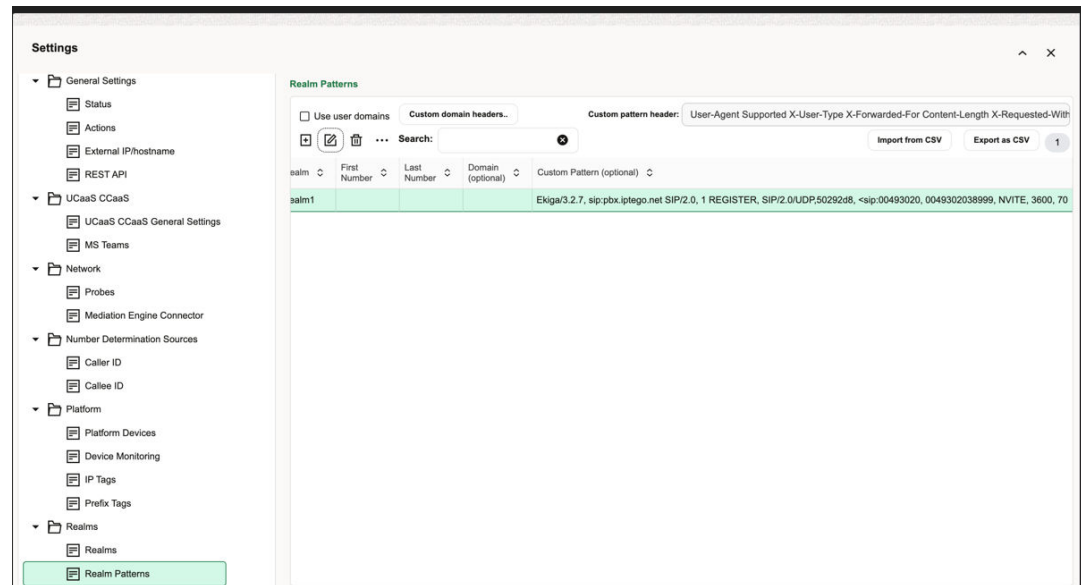
- Matching a custom pattern against an arbitrary header field.
- Use the **Custom header for realm definition** System setting to specify which header to search for.

Figure 7-50 Custom header for realm definition



- Use the **Custom Header Pattern (optional)** column on the **Realms Patterns** page to specify a pattern for each Realm. The pattern matching works similar to the number matching.

Figure 7-51 Custom Header Pattern (optional)



⚠ Caution

Each additional header and custom header matching affect the Operations Monitor's performance.

Custom Headers for the Calls Page

You can define custom header fields in which the field string is searched across all SIP messages, to parse and extract the values and display the headers as a new field in the **Calls** table.

Defining custom headers enables custom monitoring of calls and filtering calls based on your requirements. This feature supports parsing of messages of only SIP protocol. Messages of other protocols like ISUP, ENUM, MEGACO, DIAMETER, MGCP etc are not supported. SIP messages belonging to Calls only are supported, messages related to other functionalities like Registrations, Subscriptions are not supported.

The SIP messages of a call are parsed and searched for the custom header values in the following order. Note that the body of a SIP message is not used to search for custom headers.

Custom headers are displayed in the following pages:

- Dashboard
- Calls
- Devices
- User Tracking
- IP Tracking

Note

By default, the custom header columns are displayed on all Calls panels except the Dashboard. To view on the Dashboard, add the columns manually using the **Set Columns** option.

Creating Custom Headers for Calls

The **Calls Custom Headers** page allows you to configure Custom Headers. It is recommended that you configure Custom Headers during a maintenance window period.

To create custom headers for Calls:

1. Click **admin > Settings** and then expand **Custom Headers**.
2. Click **Calls**.

The **Calls Custom Headers** page displays ten fields that are used to configure the Header names.

Note

The Admin user has access to the permission **Modify Custom Headers**. While creating a new user, this permission is enabled by default. The user can modify it as needed. If this check box is selected, the user is granted access to the **Custom Headers** configuration page in the **Settings** menu.

While creating a new user, if this permission is Disabled, the Custom Headers section is completely hidden from the left-hand navigation menu in **Settings**.

Figure 7-52 Calls Custom Headers

Settings

- Device Monitoring
- IP Tags
- Prefix Tags
- Realms
 - Realms
 - Realm Patterns
- Custom Headers
 - Calls**
- KPI Management
 - KPI Templates
- System Management
 - System Settings
 - Oracle SBC Config Upload
- Privacy Settings
 - Header and Content Privacy
- SFB
 - Skype For Business Filter
- External Devices

Calls Custom Headers

Last Modified at: 2024-11-28 11:12:32 History

Header	Name	Search across all call legs	Search in
1	Request-URI	☒	☒ Requests ☐ Responses ☐ Both
2	Call-ID	☒	☐ Requests ☐ Responses ☒ Both
3	CSeq	☒	☒ Requests ☐ Responses ☐ Both
4	Contact	☒	☒ Requests ☐ Responses ☐ Both
5	Via	☒	☒ Requests ☐ Responses ☐ Both
6		☐	☐ Requests ☐ Responses ☐ Both
7		☐	☐ Requests ☐ Responses ☐ Both
8		☐	☐ Requests ☐ Responses ☐ Both
9		☐	☐ Requests ☐ Responses ☐ Both
10		☐	☐ Requests ☐ Responses ☐ Both

Note

Header names are case sensitive and cannot contain spaces. While adding the Custom Headers, built-in validations check that the custom headers are not one of the following :

- P-Asserted-Identity
- Remote-Party-Id
- Caller
- From
- Callee
- To
- Reason
- Diversion
- Caller User Agent
- Callee User Agent

If you try to add any of the pre-existing ten custom headers, the error message "*Custom header already exists in the calls page*" is displayed, and the **Save** button is disabled.

If you try to add an existing custom header, the error message "*Value already configured in another custom header column*" is displayed.

3. Click the **search_across_all_call_legs** checkbox for the header in all legs of a call. The **search_across_all_call_legs** option remains disabled or unchecked unless the custom header has been configured with a non-empty value. Messages of the calls are parsed based on whether **search_across_all_call_legs** is enabled or disabled
4. Select any of the following options:

'Search in' Option	Description
Requests	The header is searched across all legs in INVITE messages only.
Responses	The header is searched across all legs in the 180, 183, 200OK messages only.
Both	The header is searched across all legs in the INVITE, 180, 183, 200OK messages only

Table 7-12 search_across_all_call_legs

search_across_all_call_legs	Description
search_across_all_call_legs is enabled, and Requests is selected	All INVITE (Re-INVITE messages are not parsed) messages of the call are parsed and if the custom header configured is present, then its values are accumulated
search_across_all_call_legs is enabled, and Responses is selected	180 Ringing, 183 Session Progress, 200OK(of INVITE) messages of the call are parsed and if the custom header is present, the values are accumulated.

Table 7-12 (Cont.) search_across_all_call_legs

search_across_all_call_legs	Description
search_across_all_call_legs is enabled, and Both is selected	INVITE, 180 Ringing, 183 Session Progress and 200 OK of INVITE is parsed and all the values are accumulated.

5. After configuring the custom headers from the **Settings** page, the configured and active headers are shown on the **Calls** panel.
 - The values from different legs are shown as comma separated values (csv) in the Calls table. Not all are shown in a single view. To view all, click on the particular row on the desired header. A pop-up window showing the different custom header values in new lines is displayed. Values can also be copied from here.
 - If the values are for the currently configured custom header, they are displayed in 'Black'
 - If the values are for an older configured Custom Header, the older values are shown as Red, and the newer value for the new header are shown in black. For older values in Red, a title is added to indicate that they are for the older custom header values. You can see this while hovering on the value.

You can apply Simple Filters to the columns - not Advanced Filters. The newly configured rows can also be part of a CSV/Bulk Export, where the columns (unlike other columns) are indicated by the configured custom header name. You can also export or import the custom header names in the Configuration Savepoints.

As the column value now contains comma in itself, to apply a text-based filter for this column, pass the value in double quotes. For example, If the filter to be applied is to search for "callid1, callid2", pass it to the text based filter as Call-Id="callid1, callid2".

6. You can:
 - a. Click **Save** to save all valid custom headers.
 - b. Click **Reset** to reset the custom header names. Doing this, updates the fields in the settings to the last saved values.
 - c. Click **Clear All** which allows you to clear all fields and delete the corresponding columns from the calls table.

Viewing the Custom Header Columns in the Calls Panel

After configuring the custom headers from the **Settings** page, only the configured/active ones are shown on the **Calls** panel.

Note

The columns are visible in the Calls panels depending on the user permission to view the custom header columns.

The custom header columns are visible in the Calls panel of these pages:

- Dashboard
- Operation >> Calls
- Operation >> Devices

- Customers >> User Tracking
- Customers >> IP Tracking

Note

The custom header columns are shown by default in all the Call panels except for the Calls panel on the Dashboard. To view on the Dashboard, add the columns manually using **Set Columns**.

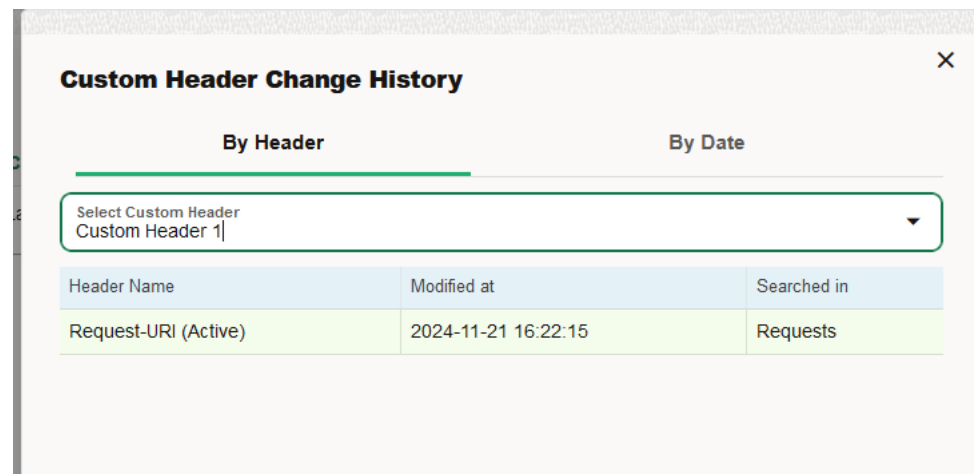
Viewing History of Calls Custom Headers

View the history of the custom headers using the **History** option.

To view the history of configured custom headers:

1. Click **Admin, Settings**.
2. Click **Custom Header**, and **Calls**.
3. In the **Calls Custom Headers** page, click **History**.
4. In the **Custom Header Change History** page, you can view the History of the Custom Headers by Header ID or Date:
 - a. **by Header ID**

Figure 7-53 Viewing the History of Custom Headers by Header ID



- i. Select the custom header from the drop-down list.
The history (if any) of the Header ID is shown. The current active value row is highlighted with a green background and the keyword '**Active**' is added to the Name.

If the Custom Header ID value was deleted, it is indicated by an empty name with the associated time stamp of the change.

- ii. If you see a '(Not Set)' value, it indicates that the 'Search across all legs' option was not checked for that header. Hence, the header is not searched across all legs.

b. By Date:

- i. Select the Date and time from the date-time picker.
The name of all custom headers configured on the specific date and time is displayed.

If a specific header was not configured, the value is shown as null or empty.
- ii. If you see a '(Not Set)' value, it indicates that the 'Search across all legs' option was not checked for that header. Hence, the header is not searched across all legs.

KPI Management

This is the feature documentation for KPI Management

User Management Permissions for KPI

These are the permissions required to manage KPI:

KPI Management

You can find this under:

- admin > Settings > User Management > user name > Edit user >Permission for Settings page.
- admin > Settings > User Management >Add a user >Permission for Settings page.

If the KPI Management permission is enabled for a user, then the user can access the KPI Management page to create, edit and modify the custom templates.

Expand KPI

You can find this under admin > Settings > User Management > user > Edit > Permission for Settings page. The admin user can enable this permission for a user.

- A user with this permission can create or enable the custom user KPIs in the Operations>KPI/Metrics page and in the Operations>KPI/Metrics page>Bulk Add>Device>Device Counters.
- A user without this permission will not be able to create that counter for a device or tag type or any KPI in platform wide list or the Bulk KPI page. An error message is displayed.

Shrink KPI

You can find this under admin>Settings> User Management> user> Edit> Permission for Settings page.

The admin user can enable this permission for a user.

- Users with this permission can delete the custom user KPIs in the Operations> KPI/ Metrics>Select User Custom KPI>Custom>Remove Custom.
- Users without this permission will not be able to:
 - Delete the user custom KPIs in the Operation>KPI/Metrics> Select User Custom KPI>Custom>Remove Custom. An error is displayed.
 - Delete a KPI in the Operation>KPI/Metrics>Bulk KPI>Select device>Select KPI enabled via Expand Permissions>Remove.

View Common KPI from Other Users

You can find this under admin>Settings>User Management>Permission for Settings page. The admin user can enable or disable this permission for a user. By default, this permission is enabled.

Note

When the admin user enables the **View Common KPI from Other Users** permission, the list of common platform-wide KPIs to be deleted are displayed in the new window on clicking Next.

Admin user can enable/disable this permission.

- If View common KPI from other users is true, then the users can see custom KPIs enabled by other users. This deletes all the common user KPIs excluding the KPI which was created first among all the common KPIs in the Platform wide KPI (The KPI with the lowest ID in the database).
- If View common KPI from other users is false, then the users cannot see custom KPIs enabled by other users.

Note

These permissions are available in user role also.

Creating a KPI Custom Template

You can create a custom template for KPIs which allows you to select only the required KPIs for a device/tag type. This way you can avoid creation of unwanted KPIs for device/tags type.

You will need the **KPI Management** permission in order to create a custom template. This setting is available here: admin>settings>User Management>user name>Edit user>Permission for Settings. To create a custom template:

1. Navigate to Username > Settings > KPI Management > KPI Templates.
2. In the KPI Templates section, click **Add**.
3. From the **Choose the Device/Tags** list box, select Platform Device or Tags.
4. In the **Select the Device Type** select the device type.
5. In the **Select the KPI** list, select the KPIs according to your requirement.

Note

You can also select VQ KPIs to be added to the custom template.

6. Save the template. The KPI Templates page now shows the template created. This page lists all custom templates created and show if they have been assigned or not. On clicking the **Yes** box in the **Templated Assigned/Details** column, it displays a list of all devices/tags assigned to that template.

Figure 7-54 KPI Templates Page

Template Name	Template Type	Device Type	Template Assigned Details
pr	Tags	Prefix Tags	No
caps	Tags	Prefix Tags	Yes
PREP1	Tags	Prefix Tags	Yes
Oracle	Tags	Prefix Tags	Yes

This creates the custom template. You can assign this custom template for the specific device or tag type. You can also edit or delete a custom template.

Note

To edit or delete a custom template, there must be no device or tag that is associated with the custom template. As the custom template has information of the KPIs enabled, modifying this when a device/tag is associated, leads to loss of information.

KPI Templates

For any device or tag type listed in the Platform Devices page, you can apply KPIs using templates. The **Assigned Templates** column in the **Platform Devices** page shows the type/name of the template applied.

If the Assigned Templates column shows **No Template**, it means that no template of any type has been applied to the Platform Device.

Figure 7-55 Assigned Templates in the Platform Devices Page

Name	Type	Call Matching	IP Addresses	Visibility	External?	VQ Status	Device Map Status	Assigned Template
Trunk1	TRUNK		1.2.2.33		internal	No VQ	Disabled	Default
Test Device 11	SBC/B2BUA	Using generic ...	2.2.2.23		internal	No VQ	Disabled	No Template
Test Device 1	SBC/B2BUA	Using generic ...	2.2.2.22		internal	No VQ	Disabled	Default
10_A_SBC	SBC/B2BUA	Using generic ...	1.1.1.11		internal	No VQ	Enabled	Default
Dev_test1	SBC/B2BUA	Using generic ...	2.3.2.1		internal	No VQ	Disabled	No Template
dev_stp_520	STP	Using generic ...	10.13.0.40		internal	Only MOScope	Disabled	No Template
dev_stp_519	STP	Using generic ...	10.13.0.39		internal	Only MOScope	Disabled	No Template
dev_stp_518	STP	Using generic ...	10.13.0.38		internal	Only MOScope	Disabled	No Template
dev_stp_517	STP	Using generic ...	10.13.0.37		internal	Only MOScope	Disabled	No Template

Templates can be of the following types:

- **None:** Applying this template deletes all KPIs related to the device or tag. It deletes the VQ KPIs.
- **Custom:**
You can customize the set of KPIs for different devices or tag types and save this list as a custom template. This set of KPIs can be applied to the device or tag type.
- **Default:**
Applying the default set of KPIs provided in the system for the device or tag type. This is a static list of KPIs and cannot be modified.

Before Applying Templates to a Device or Tag

A template has set of KPIs defined.

Default Template

A Default template has set of KPIs defined according to the device or tag types. If a device or tag type is associated with a Default template, then the KPIs defined in the default template are created. This option is read-only and cannot be modified:

- Applying the default template to a device or tag which does not have any KPI, creates the KPIs defined in the default template list.
- When you applying the default template to a device which already has KPIs assigned:
 - The KPIs in the default template are created, if the KPI is not present in existing device or tag.
 - If the existing KPI matches the KPI from the default template, then such KPIs are retained.
 - The KPIs which do not match the KPIs in the default template are deleted for the device/tag.

Note

KPIs created by the Default list template for the device or tag type will remain same as 4.x. As there are no default KPIs created for the IP tag type in 4.x, there is no Default option for IP tag types.

Custom Template

If a device/tag does not have any KPI then applying custom template creates the KPIs present in the custom template list.

- When you apply a custom template for a device/tag which has KPI's associated:
 - The KPIs in the custom template will be created, if KPI is not present for the device/tag.
 - If the custom template KPIs match the existing KPIs for the device/tag then these KPIs are retained.
 - The existing KPIs that do not match the KPIs in the custom template are deleted for that device/tag.

Applying a Default Template for KPIs to a Device or Tag

For any device or tag type listed in the Platform Devices page, you can apply a Default Template, Custom Template, or None.

To apply a default template:

1. Navigate to **Username**, **Settings**, and **Platform Devices**.
2. Select the device/tag or multiple devices/multiple tags for which the default template needs to be applied.
3. Click **Choose Template**, and then **Default**.

Figure 7-56 Applying a default KPI template

Settings

- In the Apply the default type template dialog box, select the **Do you want to delete the non-matching existing KPI?** check box to apply the default template. As a result of this, the existing non-matching KPIs for the selected device are deleted if the KPIs do not match the default list. The KPIs from the default list are added if they are currently present, and the KPIs that are common to the default template and the existing KPIs are retained.

Figure 7-57 Apply the Default type template

Apply the Default type template

Existing Kpi for the selected devices (Test Device 11)

- Call attempts (SIP incoming)
- Call attempts (SIP outgoing)

Note:
Non matching KPI's will be deleted if you will click on apply.

Default KPI list for SBC type Devices

- Active sessions (incoming)
- Active sessions (outgoing)
- Active sessions (traversing)
- Call attempts per second (CAPS) (incoming)
- Call attempts per second (CAPS) (outgoing)
- Call attempts per second (CAPS) (traversing)
- Expired contacts
- Failed registrations
- Refreshed contacts
- Registered contacts
- Registered users
- Response time for this device (msec)
- Subscribed users
- Total number of active calls (including traversing calls)
- Transit time (maximum) for this device (msec)

Do you want to delete the non-matching existing KPI ? ☒

Apply cancel

- Click **Apply**.

The Platform Devices page now lists the template applied under the **Assigned Template** column.

Applying a Custom Template for KPIs to a Device or Tag

To apply a custom template to a device or a tag:

1. Navigate to **Username, Settings, and Platform Devices**.
2. Select the device or multiple devices for which the custom template needs to be applied.
3. Click **Choose Template**, and then **Custom**.

Figure 7-58 Applying a Custom KPI template

Name	Call Matching	IP Addresses	Visibility	External?	VQ Status	Device Map Status	Assigned Template
Trunk1	Default	1.2.2.33		internal	No VQ	Disabled	Default
Test Device 1	Custom	Using generic ...	2.2.2.23	internal	No VQ	Disabled	No Template
Test Device 1	SBC/B2BUA	Using generic ...	2.2.2.22	internal	No VQ	Disabled	Default
10_A_SBC	SBC/B2BUA	Using generic ...	1.1.1.11	internal	No VQ	Enabled	Default
Dev_test1	SBC/B2BUA	Using generic ...	2.3.2.1	internal	No VQ	Disabled	No Template
dev_stp_520	STP	Using generic ...	10.13.0.40	internal	Only MOScope	Disabled	No Template

4. In the **Apply the custom type template** dialog box, select the Custom template name to apply the custom template.

Templates created for a particular Platform device type are only listed for the corresponding associated devices type. For example, for an existing SBC device Dev1, only SBC custom templates are listed and you can select any one among the templates listed.

Figure 7-59 Apply the Custom type template

Apply the Custom type template.

Existing Kpi for the selected devices (Test Device 11)

Call attempts (SIP incoming)

Call attempts (SIP outgoing)

Note:
Non matching KPI's will be deleted if you will change the template.!

Select the KPI template for device

☒ KPI Template 1

Apply cancel

As a result of this, if the existing KPIs of the device match with the KPIs in the custom template then those KPIs are not deleted. The existing KPIs that do not match the KPIs in the custom template are deleted for that device/tag.

5. Click **Apply**.

The Platform Devices page now lists the template applied under the **Assigned Template** column.

Applying the None Template for KPIs to a Device or Tag

To apply the None template to a device or tag:

1. Navigate to **Username, Settings, and Platform Devices**.

2. Select the device or multiple devices for which the None template needs to be applied.
3. Click **Choose Template**, and then **None**.

Figure 7-60 Applying a None KPI template

Name	Call Matching	IP Addresses	Visibility	External?	VQ Status	Device Map Status	Assigned Template
Trunk1	Default	1.2.2.33		internal	No VQ	Disabled	Default
Test Device 1	Custom	2.2.2.23		internal	No VQ	Disabled	No Template
Test Device 1	SBC/IS2BUA	2.2.2.22		internal	No VQ	Disabled	Default
10_A_SBC	SBC/IS2BUA	1.1.1.11		internal	No VQ	Enabled	Default

4. In the **Apply the None type template** dialog box, select the **Do you want to delete the existing KPI ?** check box. After applying None to a device type the template assigned to this device will be cleared. As the deletion of KPIs results in a loss of information, there is a warning that pops-up with a message “All existing KPIs of this group will be deleted. Do you want to continue?” to confirm the deletion of KPIs. The deleted KPI values are lost permanently and cannot be recovered.

Figure 7-61 Apply the None type template

Apply the None type template

Existing Kpi for the selected devices (Test Device 11)

Call attempts (SIP incoming)

Call attempts (SIP outgoing)

Note:
Existing KPI's will be deleted if you will click on apply!

Do you want to delete the existing KPI ? ☒

Apply cancel

5. Click **Apply**.

The Platform Devices page now lists the template applied under the **Assigned Template** column.

Common User KPIs

This feature is only available for admin users.

The Common User KPIs list provides three options:

Table 7-13 Options of the Common User KPIs

Option	Description
Add “View common KPI from other users” permission to all users	Enables the View common KPI from other users permission to all users.
Remove “View common KPI from other users	Disables the View common KPI from other users to all users.

Table 7-13 (Cont.) Options of the Common User KPIs

Option	Description
Delete Common User KPIs	Lists all the common user KPIs present among the platform-wide KPI - not device-specific KPIs. Select the check box next to the KPI to delete these common user KPIs, then click Apply. Note If you select the delete option, it removes all common user KPIs for all users. If any common user KPIs are deleted by the admin for a user without the View common KPI from other users permission, then the user must request the admin for the permission to view the common user KPI.

KPIs for Imported Devices in Configuration Savepoint

On Session Monitor 5.0, after restoring the Configuration Savepoint in a newly installed system, KPIs are preserved for the imported devices. There is no change in the behavior of restoring a configuration savepoint.

KPIs are not created for platform devices imported using the Platform Devices page.

If you have upgraded to 5.0, then the existing KPIs are not affected. If a savepoint is applied on this upgraded system, then KPIs from savepoint are preserved for the imported devices. There is no change in the behavior of restoring a savepoint. You need to apply the templates to the devices in the **Platform Devices** page to assign KPIs for the imported devices. Similarly, no KPIs are created for the list of imported Platform Devices from the Platform Devices page

System Management

Operations Monitor's system is configurable and maintainable through the **System Management** section of the **Settings** link in the upper right corner. The **System Management** section includes the following:

- **System Settings:** Use the System Settings page to configure Operations Monitor system parameters by adjusting the default values to meet your business needs. For example, you can adjust the session-timeout value that defines how long Operations Monitor keeps a call active if no SIP messages are received for the call.
- **Oracle SBC Config Upload:** Use the Oracle SBC Config Upload page to import the device configurations from an Oracle SBC configuration file into Operations Monitor or update existing Oracle SBC configurations.

- **Language Settings:** Use the Language Settings page to configure the default display language for all Operations Monitor users.

List of System Settings

Table 7-14 System Settings

Header 1	Header 2
302 Redirected: From-URI suffix length	How many suffix characters of the user part of the From URI to compare when trying to find a match between a SIP leg that got redirected (received a 300, 301 or 302 response) and the new INVITE. If set to 0 the full user part is compared. • Default value: 0 • Maximum value: 18 • Minimum value: 00
Alerting delay after core restart	Alerting delay after core restart The length of time alerts are suppressed after a core restart, in minutes. • Default value: 15 • Minimum value: 0
Allow No of Notification	Flag to limit the number of NOTIFY to be seen in the ladder diagram. Value '0' depicts none of the Notify messages can be seen in the ladder diagram • Default value: 10 • Maximum value: 20 • Minimum value: 0
Allow No of Publish	Flag to limit the number of NOTIFY to be seen in the ladder diagram. Value '0' depicts none of the Notify messages can be seen in the ladder diagram • Default value: 10 • Maximum value: 20 • Minimum value: 0
Allow No of Refresh subscription	Flag to limit the number of Refresh SUBSCRIBE to be seen in the ladder diagram.(Initial Subscription not included) Value '0' depicts none of the Refresh Subscribe messages can be seen in the ladder diagram • Default value: 10 • Maximum value: 20 • Minimum value: 0
Allow regeneration of registration events for user updates.	If a user is registered in core once, its realm will not be re-checked till the registration expires and gets re-newed. If realms are changed continuously and/or customer needs to have registrations always matched to the current realms configuration, enable this option. Be aware that this has some performance impacts on core registration processing. • Default value: False

Table 7-14 (Cont.) System Settings

Header 1	Header 2
Allow regeneration of subscription events for user updates	If a user is Subscribed in core once, its realm will not be re-checked till the Subscription expires and gets re-newed. If realms are changed continuously and/or customer needs to have subscriptions always matched to the current realms configuration, enable this option. Be aware that this has some performance impacts on core subscription processing. • Default value: False
APID request interval for querying SBCs	Number of seconds interval for retrieving information about autodiscovered SBCs. It's not recommended to alter this value. • Default value: 60 • Maximum value: 31536000 • Minimum value: 4
Append a string at the end of User Tracking searches	When using User Tracking, also look for aliases that have this suffix appended to the number.
Authentication token (shared secret between Mediation Engine Connector and Mediation Engine)	Secret used by the Mediation Engine Connector to sign requests proxied to this Mediation Engine.
Auto-refresh interval for grids	Number of seconds between auto-refresh (if enabled) for grids with this feature • Default value: 5 • Maximum value: 3600 • Minimum value: 1
B2B backlog search for merging 3PCC calls	The number of seconds to search for outgoing call legs in the past when an outgoing leg is received for 3PCC. • Default value: 2 • Maximum value: 5 • Minimum value: 1
B2B incoming backlog search for merging	The number of seconds to search the outgoing call leg in the past when an incoming leg is received. • Default value: 2 • Maximum value: 5 • Minimum value: 1
B2B outgoing backlog search for merging	The number of seconds to search the outgoing call leg in the past when an incoming leg is received. • Default value: 2 • Maximum value: 5 • Minimum value: 1
Bind user sessions to IP addresses	Bind each session to an IP address. • Default value: False
Bulk counters/KPIs maximum limit	The maximum limit of counters being added in bulk. • Default value: 50000 • Maximum value: 500000 • Minimum value: 1

Table 7-14 (Cont.) System Settings

Header 1	Header 2
Cache time interval in minutes for User Agent statistics	When a panel for User Agent statistics is active, its result would be stored in an internal cache and it will be refreshed at the interval defined in this system setting (in minutes). A value of less than 5 minutes disables the cache (not recommended). • Default value: 60 • Minimum value: 0
Call flow max height	The maximum height of the call flow diagram in pixels. • Default value: 10000 • Maximum value: 40000 • Minimum value: 1000
Call flow max width	The maximum width of the call flow diagram in pixels. • Default value: 10000 • Maximum value: 10000 • Minimum value: 1000
Call flow messages	The maximum number of messages displayed in a call flow. • Default value: 500 • Maximum value: 5000 • Minimum value: 1
Call flow parallel loading	When set, the in-browser call flow diagrams will be loaded in several stages, with progressively more information for some messages. This might improve rendering performance. • Default value: True
Call flow timestamp for fragmented messages	Use last fragment's timestamp as the timestamp for the message. • Default value: False
Call flow tree's expanded levels	Expanded levels in the popup for a message. If set to -1, all levels will be expanded. • Default value: 1 • Maximum value: 20 • Minimum value: -1
Call Report Maximum Messages	Maximum number of messages to include in the call report messages section • Default value: 100 • Maximum value: 10000 • Minimum value: 1
Call Report Style	Additional Cascading Style Sheet (CSS) rules can be defined here that will be included when generating a call report PDF.
Call Report Theme Color	Color of the headings and footer on PDF call reports. Can be the name of a color: red, or a hexadecimal representation of the color: #ff0000 Default value: #446498
Call Transfer: correlate using Replaces	Set to true to match calls involved in a call transfer using the Replaces header. Default value: False

Table 7-14 (Cont.) System Settings

Header 1	Header 2
Call Transfer: Seconds for correlating calls using REFER	The number of seconds the Mediation Engine looks back for calls containing a REFER causing the current call. If 0, correlating the referred and referring call is disabled for the Call Transfer information. • Default value: 0 • Maximum value: 1800 • Minimum value: 0
CDR Custom SIP headers length	Size of the buffer for cdr custom sip headers. It denotes the size of a custom sip header value that is to be written in the csv file. For example, if there are multiple values of a particular custom sip header configured, the cumulative size of the string can be big. • Default value: 1000 • Maximum value: 3000 • Minimum value: 1000
CDR Interim Update Interval	This value represents the interval in minutes for which partial CDR data will be created. The allowed range of this interval is from 0 - 10 minutes. If 0 is given then the partial CDR generation feature is turned off. Warning: Turning on this feature has an impact in performance. • Default value: 0 • Maximum value: 10 • Minimum value: 0
Cleanup Actions Syslog logging facility	Which logging facility should be used for the Mediation Engine's cleanup actions. Leave negative if this should be disabled. Allowed values are zero through to seven. • Default value: -1 • Maximum value: 7 • Minimum value: -1
Close Legs on SIP 202 Message	If enabled, legs receiving 202 messages will be marked as finished (closed) as no further messages are expected on the leg. • Default value: False
CPM Transaction time range	The default limit in minutes to cutoff CPM transaction queries. A value of 600 will result in the transactions grid showing transactions in the range of [NOW(), NOW() - 10 Hours]. • Default value: 240 • Minimum value: 1

Table 7-14 (Cont.) System Settings

Header 1	Header 2
Custom header for realm definition	Specify a SIP header field name that is used to match the "Custom Pattern" definition for a realm.
	 Caution This system setting should not be modified locally in a node that is part of a Mediation Engine Connector.
Custom SIP headers in CDR file	A space separated list of custom SIP headers to be included in CDRs
Day on which the week should begin	Day on which the week should begin Defines the day at which the week should begin. A page reload is required for this setting to take effect. Default value: Sunday
Days until inactive account expires	Expire inactive accounts after the given number of days. • Default value: 90 • Minimum value: 1
Device Map Limit	The value decides the maximum number of Platform Devices for which Device Map can be enabled. The permissible values can range from 2 to 50 • Default value: 50 • Maximum value: 50 • Minimum value: 2
Digest delay time	The time between sending out digests of recurring alerts in minutes • Default value: 0 • Maximum value: 30 • Minimum value: 0
Disable logo changes	If enabled, users cannot make logo changes. Default value: False
Disable user changes	If enabled, users cannot make password or logo changes. Default value: False
Dumper raw buffer size	The size of the raw buffer in MB. This buffer is used for creating traces starting in the past. Warning: Increasing this setting might require adjusting memory quotas. Please contact Oracle or your system integrator. • Default value: 1024 • Maximum value: 2147483647 • Minimum value: 0
Enable CDR writer	Enable if you want the Mediation Engine to generate CDR files. Please see the user manual for details about the format used and how to get the files. Make sure you have a valid CDR Extension license. Default value: True

Table 7-14 (Cont.) System Settings

Header 1	Header 2
Enable MEGACO BGF	Enables the processing of BGF messages in MEGACO. Default value: False
Enable sharing saved calls	If enabled, saved calls can be shared globally. If you run a multi-tenancy setup, this feature should be DISABLED. Default value: True
Enabled Device Map	If enabled, Operations Monitor can display a real-time map of the configured platform devices and of the interactions between them. In order to configure the maximum number of devices supported, adjust the 'Device Map Limit' in System Settings.
Enforce stringent password rules	A set of higher security rules for user passwords. Default value: True
Expire passwords periodically	If enabled, non-admin users will be required to change their passwords periodically. This option can be overridden from the Mediation Engine Connector. Default value: True
 Caution Do not be modify this setting locally in a node that is part of a Mediation Engine Connector.	
Export metrics to OCDM	Enable to export selected KPIs via the OCDM file based integration Default value: False
Extend calls by hash inspection	During call legs discovery across multiple sites, a neighboring Mediation Engine can be interrogated multiple times, rather than only once. Default value: True
External authentication enabled	Enable or disable HTTP header authentication driven by the reverse proxy (nginx or Apache) Default value: False
External IP/hostname	External base IP or hostname for deep links (used by alerting emails) Default value:
Find similar aliases in User Tracking by using a suffix of this many characters	If this value is non-zero, the User Tracking page first searches the alias list for similar usernames/ phone numbers and then displays the calls, registration and subscription events for all of them. To usernames/phone numbers are considered similar if the last N number of characters are identical, where N is the value of this setting. Default value: 0 Minimum value: 0
Future maximum search	- Time a search searches in the future (in seconds) • Default value: 10 • Minimum value: 1

Table 7-14 (Cont.) System Settings

Header 1	Header 2
Get updated call states	If enabled, the fronted will query the core process on each request to get the very latest state information. This can increase the delay before the answer is made, but generally makes the information more up to date. Default value: False
Global partitions size	How many hours a database partition should hold. There can be at most 1024 partitions. • Default value: 1 • Maximum value: 24 • Minimum value: 1
Grey out non-preferred numbers	Numbers that haven't been derived from a configured number determination source will be displayed in grey in the calls table. Default value: False
Group new registrations from the same user.	Group new registrations from the same user. Default value: True
Group Non-Call Subscriptions from the same user.	Group Non-Call Subscriptions from the same user and event type. Default value: True •
Guarantee sorting of VSI traces	Due to the distributed nature of the Mediation Engine, it is possible that the packets in the traces buffer are out of order. If this option is enabled, the Mediation Engine will re-sort the packets by their timestamp. Default value: True
Headers in which to look for realm URIs	A space separated list of SIP header fields, ie. "Diversion P-Asserted-Identity". Realm matching will include these fields (in addition to To and From). Default value:
Hide active user sessions	Hide active user session info when limit is reached. Default value: True •
Hide hardware addresses input from devices configuration	If set to true, the hardware addresses field will be hidden from the platform devices wizard Default value: True
Hide Megaco messages before off-hook	This option helps if the MEGACO transactions IDs are reused very quickly. It will hide the messages that are assigned to the leg before the off-hook event Default value: False
High threshold for Jitter	The high threshold for determining the Jitter • Default value: 200 • Maximum value: 500 • Minimum value: 0
High threshold for MOS	The high threshold for determining the MOS • Default value: 3.5 • Maximum value: 5 • Minimum value: 0
High threshold for Packet Loss Rate	The high threshold for determining the Packet Loss Rate • Default value: 50 • Maximum value: 100 • Minimum value: 0

Table 7-14 (Cont.) System Settings

Header 1	Header 2
HTTP address of the Mediation Engine Connector	HTTP address where to reach the Mediation Engine Connector. This is automatically set from the Mediation Engine Connector.
Ignore internal registrations	If disabled, registrations from inside the platform will be recorded. This might make some REGISTER transactions to be incorrectly considered unauthorized because the 401/407 answer is seen more than once. Default value: False.
Ignore internal registrations for User Devices statistics	If disabled, registrations from inside the platform will be recorded. This might make some REGISTER transactions to be incorrectly considered unauthorized because the 401/407 answer is seen more than once. Default value: False.
Ignore mismatch on contact URI (registrations)	Some registrars change the Contact URI in a reply to a REGISTER. This tells the Mediation Engine to ignore mismatching URIs, but might lead to merging multiple registrations into one. Default value: False.
Ignore non RFC 3261 params in SIP URI username	If set to true, the Mediation Engine will remove the params appended to the username before matching the SIP URI username. Default value: False.
Ignore plus prefix number when matching realms	By default the "+" number prefix is ignored in realm matching, when turned on, this option will assign numbers containing + only to the default realm. Default value: False.
Initial search range	The initial search range (in seconds) for calls, registrations etc to search before asking if the search should continue. If 'Paging query range' is bigger, that value will be used. • Default value: 3600 • Maximum value: 2592000 • Minimum value: 1
KPI - RTCP Jitter threshold	Defines a threshold for jitter kpis (in ms) based on RTCP. Any jitter value above this threshold is ignored for the kpi computation. 0 means no threshold. • Default value: 0 • Maximum value: 2000000 • Minimum value: 0
Limit select queries to this many seconds	Stop SELECT queries if they take more than this many seconds. Set to 0 to disable. • Default value: 120 • Maximum value: 3600 • Minimum value: 0
Log user authentication failures	Log information when a user fails to login. Default value: False.
Login Splash Page	A splash page which is shown after login. Removing all content will disable the splash page.

Table 7-14 (Cont.) System Settings

Header 1	Header 2
Loose user searching	If enabled, when searching users by using the live search feature, the last digits of the number act as wildcards to suggest similar numbers from the same range. Default value: False.
Low threshold for Jitter	The low threshold for determining the Jitter • Default value: 20 • Maximum value: 500 • Minimum value: 0
Low threshold for MOS	The low threshold for determining the MOS • Default value: 2.5 • Maximum value: 5 • Minimum value: 0
Low threshold for Packet Loss Rate	The low threshold for determining the Packet Loss Rate • Default value: 5 • Maximum value: 100 • Minimum value: 0
Match registration events by comparing a suffix of the username	The Mediation Engine matches the related registration attempts by the SIP username. If this value is zero, then the whole username is used. If more than zero, the number defines how many digits/characters must match. • Default value: 0 • Maximum value: 50 • Minimum value: 0
Match Subscription events by comparing the username suffix	The Mediation Engine matches the related subscription attempts by the SIP username. If this value is zero, then the whole username is used. If more than zero, the number defines how many digits/characters must match. • Default value: 0 • Maximum value: 50 • Minimum value: 0
Max concurrent sessions	The maximum number of times a user can log in in parallel. • Default value: 5 • Maximum value: 25 • Minimum value: 1
Max concurrent users	The maximum number of users that can be logged in at the same time. • Default value: 20 • Maximum value: 1000 • Minimum value: 1
Maximum concurrent traces	The maximum number of traces that can be running at the same time. • Default value: 3 • Maximum value: 20 • Minimum value: 0

Table 7-14 (Cont.) System Settings

Header 1	Header 2
Maximum frequency for raising alerts	Determines at what point raised alerts that are not read can be raised again. If an alert has been continuously raised for more than this amount of seconds, it is eligible for being raised again. This setting only applies to alerts based on Generic Metrics and Device/Tag Metrics. • Default value: 3600 • Minimum value: 60
Maximum lines of a CDR file	The maximum number of lines that a CDR file can contain. When this limit is reached, the Mediation Engine automatically creates a new CDR file. • Default value: 50000 • Maximum value: 500000 • Minimum value: 1
Maximum lines of a MDR file	The maximum number of lines that a MDR file can contain. When this limit is reached, the Mediation Engine automatically creates a new MDR file. • Default value: 50000 • Maximum value: 500000 • Minimum value: 1
Maximum number of calls exported with bulk export	The maximum number of calls that can be exported with one bulk export. • Default value: 1000 • Maximum value: 10000 (Higher the value, more will be the time taken for export) • Minimum value: 1
Maximum number of items returned by each request to the REST interface	Maximum number of items returned by each request to the REST interface. • Default value: 1000 • Maximum value: 10000 • Minimum value: 1
Maximum number of legs in one call	If a call already has this many calls, the Mediation Engine won't merge new legs in the same call, even if they match according to the merging algorithm. The purpose of setting a maximum is to avoid infinite calls. • Default value: 25 • Maximum value: 5000 • Minimum value: 1
Maximum number of lines exported with CSV export	The maximum number of lines that can be exported with one csv export. • Default value: 1000 • Maximum value: 1000000 • Minimum value: 0
Maximum number of messages per leg	Configure maximum number of messages to be stored per leg. • Default value: 500 • Maximum value: 5000 • Minimum value: 1
Maximum number of number alert definitions per user	Maximum number of number alert definitions that a user can create. • Default value: 20 Minimum value: 1

Table 7-14 (Cont.) System Settings

Header 1	Header 2
Maximum script output size	The maximum output size by script run in bytes that is shown. It's stored in memory. A value of 0 buffer all output. • Default value: 10000 • Minimum value: 0
Maximum simultaneous script runs	The maximum number of script runs that can run simultaneously. • Default value: 3 • Minimum value: 1
Maximum stored script runs	The maximum number of script runs that are stored. If this number is exceeded the oldest script runs are removed as needed to stay under this limit. • Default value: 50 • Minimum value: 0
ME path enabled	ME path enabled Enable or disable the /me path from the URL Default value: False.
Mediation Engine Connector hash on P-Charging-Vector icid-value parameter	Mediation Engine Connector call merging is done by hashing the INVITE message of the corresponding leg. By default, the Mediation Engine hashes the full invite message. If this option is enabled, and the INVITE message contains a P-Charging-Vector header with an icid-value parameter, then the value of that parameter will be used for matching instead of a hash of the entire message. Default value: False.
Mediation Engine Connector hash on P-Charging-Vector icid-value parameter and Source-Dest IP	Mediation Engine Connector call merging is done by hashing the INVITE message of the corresponding leg, where full invite is used. If this option is enabled, and the INVITE message contains a P-Charging-Vector header with an icid-value parameter, then the value of that parameter, source IP and destination IP of the calls leg, will be used to create hash instead of the entire INVITE message. The source and destination IP is additionally used here with icid-value, because there could be many call legs whose P-Charging-Vector icid-value would be same, but actually the calls would be different. This flag and P-Charging-Vector icid-value flag are independent. In case both the flags are enabled, P-Charging-Vector icid-value flag will be honored. Default value: False.
Mediation Engine Connector hash search on all external legs	Mediation Engine Connector call merging is done by hashing the INVITE message of the corresponding leg. By default, a Mediation Engine hashes all the call legs that traverse between a neighboring Mediation Engine. If this option is enabled, additionally all call legs to or from unknown IP addresses are hashed. This will have a negative impact on performance and should not be necessary on a properly configured system. Default value: False.

Table 7-14 (Cont.) System Settings

Header 1	Header 2
Merge globally by Call-ID	If this setting is enabled, Mediation Engine will merge two legs that have the same Call-ID even if they are not incoming/outgoing to the same device Default value: False.
Name of this Mediation Engine, as received from the Mediation Engine Connector	Name of this Mediation Engine, as received from the Mediation Engine Connector.
Newest search cache	Cache expiration time for the newest date in a search query (in seconds) • Default value: 1 • Minimum value: 1
Obfuscate Details in Message-flow Exports	If enabled, Session Monitor obfuscates sensitive call details like IP addresses, MAC addresses, contacts and device names in the downloaded artifacts like message-flow, SVG and PDF. You can also configure headers to be obfuscated in the message header from the Obfuscate Details in Message-flow Exports page. User in any user group or roles can enable this feature. Any User can enable and configure the feature. Default value: False
Oldest search cache	Oldest search cache Cache expiration time for the oldest value in a search query (in seconds) • Default value: 60 • Minimum value: 1
Omit Gray Bars	Omit Gray Bars Omit the gray bars in charts. Default value: True.
Paging query range	Time range a query covers in a single paging request (in seconds) • Default value: 900 • Maximum value: 2592000 • Minimum value: 1
Partitions to display in Recent calls	Number of partitions to display at once in Recent calls • Default value: 3 • Maximum value: 1000 • Minimum value: 1
Partitions to display in User tracking	Number of partitions to display at once in User tracking calls • Default value: 6 • Maximum value: 1000 • Minimum value: 1
Passwords expire duration for non-sensitive enabled users	Number of days after which users without access to sensitive information are required to change their password. • Default value: 180 Minimum value: 1
Passwords expire duration for sensitive enabled users	The number of days after which users with access to sensitive information are required to change their password. • Default value: 90 • Minimum value: 1

Table 7-14 (Cont.) System Settings

Header 1	Header 2
Passwords expire duration for stringend mode	The number of days after which users with access to sensitive information are required to change their password. • Default value: 90 • Minimum value: 1
Recurrent alerts threshold	Days during which a new alert identical to a raised unread one will not be created. • Default value: 1 • Minimum value: 0
Refer: Merging calls requires full Contact match	If call merging on REFER is enabled this option controls whether the full Contact URI must match between the INVITES of the original call and the referred one. If enabled the complete Contact URIs of both INVITES are compared, if disabled only the user name parts are compared. Default value: True
Refer: Seconds for merging calls	The number of seconds the Mediation Engine looks back for calls containing a REFER causing the current call. If 0, merging the referred and referring call is disabled. • Default value: 0 • Maximum value: 1800 • Minimum value: 0
Refer: To-URI suffix length	How many characters of the user part of Refer-To: and To: must match to merge a call. Set to 0 to compare the full user part. • Default value: 0 • Maximum value: 18 • Minimum value: 0
Refresh interval for portlets	The refresh interval in seconds that overrides the default one in each portlet when the user reloads the dashboard. Set to 0 to use each portlet's default interval. • Default value: 0 • Maximum value: 60 • Minimum value: 0
Registrations expired events	If enabled, an "Expired" event will be generated if a registration binding expires (a contact is not refreshed nor deregistered). Default value: True.
Registrations gone events	If enabled, a REGISTER transaction in which not all previous known contacts of the user are seen in the successful answer generates gone events for the missing contacts. Leave disabled if this is expected in your network. Default value: False.
Registrations Match Source	Registrations Match Source Correlation of registration happens based on the Contact URI, destination IP address and VLAN. If enabled, correlation happens based on the Contact URI, source IP address and VLAN. Default value: False.
Rotate CDR files every N seconds	If this option is non-zero, the CDR files are rotated every N seconds, where N is the value of the setting. • Default value: 0 • Minimum value: 0

Table 7-14 (Cont.) System Settings

Header 1	Header 2
Rotate MDR files every N seconds	If this option is non-zero, the MDR files are rotated every N seconds, where N is the value of the setting • Default value: 0 • Minimum value: 0
RUDP quick push	Choose the RUDP decoding mode: when 'quick push' mode is activated, the data chunks will be processed as soon as they are read, rather than waiting for the corresponding ACK. This allows better operation of the Mediation Engine in cases where ACKs are delayed excessively, but it will also prevent the detection of some malfunctions in the protocol (like lost packets). Default value: False.
SCTP quick push	Choose the SCTP decoding mode: when 'quick push' mode is activated, the data chunks will be processed as soon as they are read, rather than waiting for the corresponding SACK. This allows better operation of the Mediation Engine in cases where SACKs are delayed excessively, but it will also prevent the detection of some malfunctions in the protocol (like lost packets). Default value: False.
Search for matching Non-Call subscription segments	When viewing the diagram of a Non-Call Subscription event, Mediation Engine will search for other Non-Call subscription events that are related. This option controls the time span in which it searches, in seconds. If set to 0, the searching of related Non-Call subscription events is disabled. • Default value: 10 • Maximum value: 25 • Minimum value: 0
Search for matching registration segments	When viewing the diagram of a Registration event, Mediation Engine will search for other registration events that are related. This option controls the time span in which it searches, in seconds. If set to 0, the searching of related registration events is disabled. • Default value: 10 • Maximum value: 25 • Minimum value: 0
Seconds for merging 302 calls	The number of seconds the Mediation Engine looks back for related 'redirected by 302' calls. If 0, merging the redirected calls is disabled. • Default value: 0 • Maximum value: 1800 • Minimum value: 0
Seconds for remembering INVITE when merging 302 and REFER calls	The number of seconds the Mediation Engine looks forward for an INVITE if merging calls on 302 and REFER messages. Keep this value low. 0 disables just the forward-looking functionality. • Default value: 2 • Maximum value: 20 • Minimum value: 0

Table 7-14 (Cont.) System Settings

Header 1	Header 2
Secure passwords policy	This option specifies the password algorithm policy. Value 3 indicates a strong hashing algorithm. • Default value: 3 • Maximum value: 3 • Minimum value: 3
Session-timeout for calls	The number of seconds after which the Mediation Engine will consider a call as Timed-Out if no SIP messages are received • Default value: 7200 • Maximum value: 172800 • Minimum value: 0
Show ISUP abnormal termination in details	For certain Q850 codes, add '- abnormal termination' on the details field Default value: False.
Show OCDM widget	Display data gathered from the Oracle Communications Data Model in the User tracking page Default value: False.
SIP packet deduplication	This option sets & enables packet deduplication for SIP on the ME. The value represents the time limit (in ms) for which a packet is considered duplicate. 0 means off. Warning: enabling de-duplication has performance impacts. • Default value: 0 • Maximum value: 10000 • Minimum value: 0
SS7 default flavor	Choose the default standard for the MTP3/ISUP protocols. Supported are ITUT and ANSI. Default value: ITUT.
SS7: Prefer ported number to callee (in IAM)	If IAM contains GAP for Ported number, display this as callee number. The matching algorithm is not affected by this setting. Default value: False.
SS7: Show network-provided number as P-Asserted-Identity	If IAM contains a network-provided Calling Party Number, display it as P-Asserted-Identity. The matching algorithm is not affected by this setting. Default value: False.
Stir/Shaken Response Timeout Interval	The duration(in seconds) to wait for the HTTP Stir/Shaken response once the request is received. • Default value: 3 • Minimum value: 1 • Maximum value: 30
Strict SIP CSeq handling for unauthorized calls	Flag to indicate if the meta data of the UCaaS CCaaS calls to be correlated at Mediation Engine. On Disable meta data of the UCaaS CCaaS calls will not be seen on the Call Info window. (NOTE: This Flag changes will be effective only if UCaaS CCaaS is Enabled in PSA.) Default value: False.
Subscriptions expired events	If enabled, an "Expired" event will be generated if a subscription binding expires. Default value: True.

Table 7-14 (Cont.) System Settings

Header 1	Header 2
Suffix length (H.248, MGCP, Diameter, ENUM correlation)	Define the suffix length for correlation on DIAMETER Public ID, H.248/Megaco, MGCP and ENUM. Set to 0 to only remove leading + from the Request URI/the Public ID. • Default value: 0 • Maximum value: 18 • Minimum value: 0
Support correlation of hairpin call	If set to True, Mediation Engine will detect a hairpin call, if any, by checking whether the ingress and egress device of a correlated call is one and same. For hairpin call, Call state will be updated from terminating(instead of originating) leg of a call. If 'Number Determination Sources'(NDS) is set for Caller and Callee then correlated call will have respective Caller and Callee values as per the NDS configured. Otherwise, Caller and Callee will be updated from originating leg of a call. Note: This setting is applicable only for SIP calls. Default value: False.
Support for BICC Protocol	If set to True BICC protocol messages are decoded and processed further similar to how ISUP messages are handled in the ME. If set to False then BICC protocol messages are simply discarded in ME. Warning: Enabling BICC protocol support has performance impacts. Default value: False.
Support for Non-Call Messages	Flag to indicate if the Non-Call Messages to be processed at Mediation Engine. On Disable Non-Call messages will not be seen on the Subscription Panel. (NOTE: This Flag changes will be effective only if Non-Calls is Enabled in PSA.) Default value: False.
Support Stir/Shaken calls	If enabled, STIR/SHAKEN traffic will be processed, enabling the correlation of SIP and HTTP messages. (NOTE: This Flag changes will be effective only if Stir/Shaken is Enabled in PSA.) Default value: False.
Support UCaaS CCaaS calls	Flag to indicate if the meta data of the UCaaS CCaaS calls to be correlated at Mediation Engine. On Disable meta data of the UCaaS CCaaS calls will not be seen on the Call Info window. (NOTE: This Flag changes will be effective only if UCaaS CCaaS is Enabled in PSA.) Default value: False.
TCP quick push	Choose the TCP decoding mode: when 'quick push' mode is activated, the data chunks will be processed as soon as they are read, rather than waiting for the corresponding ACK. In normal operation, you should not activate this option. If Agents see only one half of TCP traffic (and hence no ACKs are received), enable this option. Default value: False.
TDR enabled	Enable the Transaction Data Record. Default value: False.

Table 7-14 (Cont.) System Settings

Header 1	Header 2
Time difference in probes that will trigger an alert	Time difference in milliseconds between a probe and the ME that will trigger an alert. • Default value: 1500 • Maximum value: 10000000 • Minimum value: 1
Time window for each chunk of records when exporting	Number of seconds defining the interval for sql-querying a chunk of records to be exported. • Default value: 900 • Maximum value: 259200 • Minimum value: 1
Time window for records when exporting	Number of seconds (back from the last record) used for limiting the records to export. The maximum call retention limit supported is 3,628,800 seconds (i.e. 42 days). • Default value: 86400 • Maximum value: 3628800 • Minimum value: 0
Timeout for Mediation Engine querying	Number of seconds to wait for an answer from the Mediation Engine peers. If one of them becomes unavailable, the timeout ensures that the local results are still available. • Default value: 30.0 • Maximum value: 120 • Minimum value: 0
Timeout for Restore Savepoint	The number of seconds after which the Mediation Engine will consider restore configuration savepoint as Timed-Out if no response is received • Default value: 300 • Maximum value: 1500 • Minimum value: 300
Timezone Offset Alignment to Hourly Boundary	When enabled, this setting aligns CSV exports and metric intervals with the customer's local timezone, especially useful for partial-hour offsets like UTC+5:30 or UTC+1:30. Upon toggling, it may take up to 30–90 minutes to realign intervals to local full-hour timestamps (e.g., 1–2 PM, 2–3 PM). Recommendation: Enable only if timezone has partial-hour UTC offsets (like UTC+5:30 or UTC+1:30) and local timestamps are not aligned to whole hours (e.g., 1–2 PM, 2–3 PM). Default value: False.
Trace delay time	The time to wait between starting a new trace from the same alert definition, in minutes • Default value: -1 • Maximum value: 60 • Minimum value: -1

Table 7-14 (Cont.) System Settings

Header 1	Header 2
Transport MAC aware	This setting is used when matching a message to an existing call leg. If this setting is 'true', in case the source IP or destination IP of a new message is not configured as a device, Operations Monitor checks the MAC address before matching this packet to an existing call leg. However, if both source and destination IPs of the new packets can be matched to an existing device, this setting will be ignored and the device MAC address configuration will have precedence when matching the packets to the call leg. Default value: False.
Transport ports aware	Consider ports when comparing packet and device addresses. Default value: False.
Transport VLAN aware	Consider ports when comparing packet and device addresses. Default value: False.
Use the hash of preferred number config to link it to Caller/Callee.	If enabled the hash of a Preferred Number config will be used to link it to numbers in calls. If you delete a config, and then re-create it with the same parameters, the link between the Caller or Callee and the Device+HeaderType will be re-established in the UI. If this option is disabled the Database ID of the config will be used to link. In this case if the Preferred Number source config is modified at all the relation will be lost for all historical call data. Default value: True.
Use user domains	Set to true to match users based on the SIP URI (domain name), in addition to the user name (number). Changing this value restarts the core process. Default value: False
 Caution Please note that this system setting should not be modified locally in a node that is part of a Mediation Engine Connector.	
User Actions File logging	Whether or not the Mediation Engine's user action should be logged into the dedicated file logging facility. Default value: True.
User Actions Syslog logging facility	Which logging facility should be used for the Mediation Engine's user action. Set to -1 if this should be disabled. Allowed values are zero through to seven. • Default value: -1 • Maximum value: 7 • Minimum value: -1

Table 7-14 (Cont.) System Settings

Header 1	Header 2
User default locale	Assign newly created users this locale Default value: en-us
	 Caution Please note that this system setting should not be modified locally in a node that is part of a Mediation Engine Connector
User devices chart history limit	Fetches only calls not older than specified number of seconds • Default value: 1800 • Minimum value: 0
User Roles	Assign users roles containing predefined permissions. Default value: False.
User tracking calls paging query range for	Time range a query covers in a single paging request (in seconds) for user tracking calls. Should typically be larger than the normal paging query range. • Default value: 3600 • Maximum value: 2592000 • Minimum value: 1
Validate Packet Inspector filters in real time	Enables validation of Packet Inspector filters as they are being entered. Default value: True.
Voice Quality Chart scale in minutes/minute	If true, the Voice Quality Chart scale will be minutes/minute instead of minutes/15 minutes. Default value: false.
Web Session Timeout	Default value for Web Session Timeout is 30 minutes .When Web Session Timeout is set to "0" session timeout functionality is disabled .The maximum Web Session timeout value allowed in the system 30 minutes. • Default value: 30 • Maximum value: 30 • Minimum value: 0

System Settings

System settings allows you to configure Operations Monitor's internal parameters and several advanced settings.

Note

Some of these settings may affect the performance and stability of Operations Monitor. Please consult with Oracle or your system integrator if you are unsure about a configuration.

The **Only Custom** toggle switch is located on the right-side corner of the page. When you click this toggle switch you can view only the custom system settings are displayed.

System Settings shown here is an example of possible system settings. A short description about every system option is displayed when you hover with the mouse over the name of the option.

Figure 7-62 System Settings

Name	Value
Allow No of Publish	10
Allow No of Refresh subscription	10
Allow regeneration of registration events for user updates.	false
Allow regeneration of subscription events for user updates	false
APID request interval for querying SBCs	60
Append a string at the end of User Tracking searches	
Authentication token (shared secret between Mediation Engine Connector and Mediation Engine)	e995b749e33c988383b71806e7bf7876
Auto-refresh interval for grids	5
B2B backlog search for merging 3PCC calls	2
B2B incoming backlog search for merging	2
B2B outgoing backlog search for merging	15
Bind user sessions to IP addresses	false
Bulk counters/KPIs maximum limit	50000
Cache time interval in minutes for User Agent statistics	60
Call flow max height	10000
Call flow max width	10000
Call flow message	500

This table describes the system options:

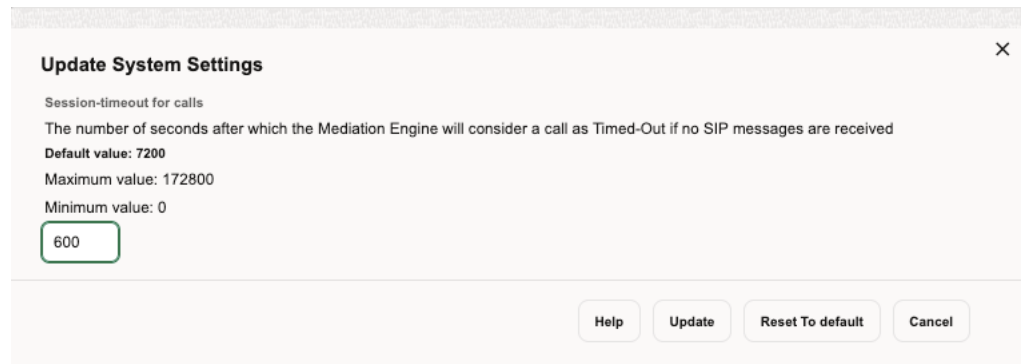
Table 7-15 System Options

Option	Description
Name	The name of the system option.
Status	Can be <i>user defined</i> if the option was changed by the administrator, or <i>default</i> if the option has the factory default value.
Type	The type of the system option. There are three types defined: - string - number - boolean
Value	The current value of the setting.

To change the value for a setting, double-click the table row. For example when you double-click the Session-timeout for calls setting, the **Update System Settings** window is shown. The

Update System Settings window contains a short description of the system option, the default value, a maximum value in case of a number type option, and a value box or a check box in case of a Boolean type option. The **Update** button is for changing the system option to the new given value, and **Reset to default** resets the current value to the default one.

Figure 7-63 Update System Settings



For a list of all system settings, see [List of System Settings](#).

B2B Backlog Search for Merging 3PCC Call

When merging calls across B2B/SBC, the Operations Monitor searches for the matching call in the recent outgoing calls on that device. This parameter sets the default number of seconds in the past to search when an outgoing leg is received. The range is from 1 to 5; the default is 2.

Note

If the call merging algorithm for 3PCC calls uses the `time_diff` function, then the values defined by it take precedence over this system setting.

B2B Incoming Backlog Search for Merging

When doing call merging across B2B/SBC or Proxy device types, Operations Monitor is searching for the matching call in the recent calls going to or from that device. This options sets the default number of seconds to search the incoming call leg in the past when an outgoing leg is received.

Note

If the call merging algorithm uses the `time_diff` function, then the values defined by it take precedence over this system setting.

Because the outgoing leg is normally seen by Operations Monitor after the incoming leg, we recommend setting a small value for this option.

B2B Outgoing Backlog Search for Merging

When doing call merging across B2B/SBC or Proxy device types, Operations Monitor is searching for the matching call in the recent calls going to or from that device. This options sets the default number of seconds to search the outgoing call leg in the past when an incoming leg is received.

Note

If the call merging algorithm uses the `time_diff` function, then the values defined by it take precedence over this system setting.

Call Flow Messages

The maximum number of messages displayed in a **Message Flow** window. This number should be limited as a large amount of messages can significantly slow down the web browser. When the number is exceeded, a warning icon is displayed. By default, it is set to 100. The maximum value is 5000 messages.

Call Flow Maximum Height/Width

The maximum number of pixels (height or width) for rendered *Message Flow*. Limit the number of pixels if the diagrams take too long to render.

Call Flow Parallel Loading

If enabled, the *Message Flow* will render progressively, instead of all at once.

Calls Partition Size

As of release 2.10.0 the calls table in Operations Monitor is partitioned into several partitions. Operations Monitor only writes to one partition at a time. When this partition reaches its size limit, a new partition is created and subsequent calls are written to this partition. This setting gives the partition size limit in number of calls.

Call Report Maximum Number of Messages

The maximum number of messages to include in a *Message Flow* that is part of a call report (PDF).

Enabled Device Map

Operations Monitor can display a real-time map of the traffic going through the configured platform devices with respect to **Call Attempts** and **Active Calls** KPIs. Set it to **True** and from **Platform devices** settings, enable the devices to be displayed in the device map. Adjust the **Device Map Limit** setting as required.

Future Maximum Search

Sets a range of time in which new incoming calls can be included in a search you have initiated. Since new incoming calls can occur after a search has been initiated, this setting

allows a range of time in which these incoming calls will be included in search results. The default setting is 10 seconds.

High Threshold for MOS

The upper threshold for good voice quality MOS value. Estimated MOS values higher than this threshold will be displayed in green in the Calls table. Lower values will be displayed in orange or red.

Group New Registrations from the Same User

If enabled, new registrations from the same user will be grouped together. However, the grouping is done per requested chunk, sometimes leading to duplicates still being displayed in the grid if the grid needs to do multiple requests to fill up a page. This is mostly notable when navigating back and forth through recent registration events, sometimes displaying different results for the same page.

Ignore Internal Registrations

A REGISTER SIP message exchanged between two devices from the platform is considered an internal registration. If disabled, registrations from inside the platform will be recorded. Otherwise, only the registrations between the end points and the first device from the platform are recorded. The default value is *disabled*. The value of this option must be the same as the [Registrations Gone Events](#) both enabled or both disabled.

Low Threshold for MOS

The lower threshold for good voice quality MOS value. Estimated MOS values lower than this threshold are displayed in red in the Calls table. Higher values are displayed in orange or green.

Match Registration Events by Comparing a Suffix of the Username

Operations Monitor matches the related registration attempts by the SIP username. If this value is 0, then the whole username is used. If non-zero, only that many of the last digits/characters are compared.

Set this to a non-zero if the Registration device is changing the SIP username/phone number when forwarding the message.

See also "[Search for Matching Registration Segments](#)".

Matching a Message to a Device

When a new message arrives, Operations Monitor tries to match it to a source device and to a destination device. The match is made based on the IP address, but there are some additional checks:

- If the message has VLAN tag N: in order for the message to be matched to a device, the device must have either VLAN=N or no VLAN configured.
- If source has specific MAC address(es) configured: in order for the message to be matched, the source MAC address of the message must match one of the MAC addresses configured for the device.

- If destination has specific MAC address(es) configured: in order for the message to be matched, the destination MAC address of the message must match one of the MAC addresses configured for the device.

Matching a Message to an Existing Call Leg

When a new message arrives, Operations Monitor tries to match it to an existing call leg. In order for it to match, the following conditions have to be fulfilled:

- In case both source IP and destination IP of the new message are configured as a device, the match to the existing leg is successful only if BOTH source and destination devices matched by the new message match the ones of the existing leg. For more information, see "[Matching a Message to a Device](#)".
- In case the source IP or destination IP of a new message is not configured as a device, the following settings are also checked:

- Transport VLAN aware

If this setting is 'true', Operations Monitor checks that the VLAN tag is the same (or that there is no VLAN tag) before matching this packet to an existing call leg. If this setting is 'false', the VLAN tag is ignored.

Note

If the device is defined with **VLAN=0** or **VLAN=off**, then the check only matches packets with no VLAN. See "[Device Identification](#)" for more information on VLAN tag matching in device definitions.

- Transport MAC aware

If this setting is true, Operations Monitor checks that both source and destination MAC addresses are the same before matching this packet to an existing call leg. If one of the endpoints was already matched via device lookups, the MAC address check for that endpoint is skipped. If this setting is 'false', the MAC address is ignored.

Maximum Concurrent Sessions

The maximum number of parallel sessions a user can be logged into. If the limit is reached, the user cannot start additional sessions. In case the user has the permission to always log in, the user will still be able to log in, but for every new session that exceeds the limit the oldest of the user's existing sessions will be destroyed. For a description of permissions, see "[User Management](#)".

Maximum Stored Script Runs

The maximum number of stored app runs. Before an app is executed, scheduled or run manually, we check to make sure we are not violating this limit. The oldest stored app runs are removed as needed. This prevents frequently running or large result producing apps from depleting resources.

Maximum Script Output Size

The maximum size a script output can show. It is defined in bytes and limits the size that can be shown during a script run.

Maximum Simultaneous Script Runs

The maximum number of scripts that can be running simultaneously.

Newest Search Cache

Checks how often the newest date in the search cache is refreshed. The default setting is 1 second.

Note

Changing this system setting can result in a loss of incoming calls.

Oldest Search Cache

Checks how often the oldest date in the search cache is refreshed. The default setting is 60 seconds.

Recurrent Alerts Threshold

Operations Monitor compares the time difference between a new alert and any previous unread alert that is identical (same definition and message) to avoid the creation of similar alerts within that period. You can specify the number of days for that period.

Registrations Gone Events

If enabled, when a REGISTER transaction occurs and not all previous known contacts of the user are seen in the successful answer, generates '**Gone**' *registration events* for the missing contacts. In other words, if the subscriber registers a new SIP contact without explicitly de-registering the old one, a registration 'Gone' event is generated for the old contact. By default, this option is *disabled*.

Note

In some networks in which the REGISTER messages are routed by intermediate devices that change the **Contact** header, this option can cause false **Gone** events. In this case, Oracle recommends you disable this option.

Search for Matching Registration Segments

When viewing the diagram of a *Registration* event, Operations Monitor searches for other related registration events. This option controls the time span during which Operations Monitor searches. If set to 0, the searching of related registration events is disabled.

This is useful for getting the *flow* of the registration request inside the platform. If you have devices that forward registration requests or that register themselves on behalf of the customer (as some SBC devices do), set this option to a non zero value. Also, make sure to disable the **Ignore Internal Registrations** option.

Session-Timeout For Calls

Session-timeout defines the number of seconds that Operations Monitor keeps a call active if no SIP messages are received for it. When the session timer expires, Operations Monitor marks the call with the state *Timed out*.

If the calls are not periodically refreshed in the monitored SIP network at SIP level, you might consider increasing this value. The default value is 2 hours (7200 seconds).

Timeout for Mediation Engine Querying

This setting gives a timeout for requests made by this Mediation Engine to its peer Mediation Engines. Ignore, if you use this Mediation Engine in standalone mode.

Timeout for Restore Savepoint

The number of seconds after which, if no response is received, the Mediation Engine will consider the restore configuration savepoint as timed out.

Note

Use this setting when restoring large save points that require extra time for processing.

User Devices Ignore Internal Registrations

Similar as Ignore Internal Registrations, but for the *User Devices* statistics. There are cases when it is desirable to take the internal registration into account but not to count them for the User Devices statistics. An example of this is when all the internal registrations use the same User-Agent string. If the **Ignore Internal Registrations** option is enabled, this option is ignored.

Users Loose Searching

If enabled, when searching users by using the live search feature, the last digits of the number act as wildcards to suggest similar numbers from the same range. By default it is *disabled*.

Use User Domains

Note

Changing this system setting requires a core restart, which causes a temporary drop in all metrics.

If *enabled*, Operations Monitor uses the domain part of the SIP URI to differentiate the subscribers, in addition to the user name part/phone number. If the option is enabled, Operations Monitor also displays the domain part of the AOR of the subscribers in the web interface. See the graphics for comparative examples. By default, this option is *disabled*.

Figure 7-64 Calls Panel with Use Users Domains Disabled

Recent Calls											
Details ... 🔍 Type to filter eg- callee=575,caller=115											
☐	Caller	Callee	Start timestamp	Caller IP address	End timestamp	Call time	Segments	Code	State	Request-URI	Call-ID
☐	556023025226	666023025228	2024/12/20 09:04:59	10.0.0.7	2024/12/20 09:07:30	2'30"	4	200	Finished	sip:666023025228@10.0.0.27.sip:66602302522...	19564a@10.0.0.7,19564a@...
☐	111023025225	222023025227	2024/12/20 09:04:59	10.0.0.6	2024/12/20 09:07:30	2'30"	4	200	Finished	sip:222023025227@10.0.0.26.sip:22202302522...	195649@10.0.0.6,195649@...
☐	333023025224	444023025226	2024/12/20 09:04:59	10.0.0.5	2024/12/20 09:07:30	2'30"	4	200	Finished	sip:444023025226@10.0.0.25.sip:44402302522...	195648@10.0.0.5,195648@...
☐	556023025223	666023025225	2024/12/20 09:04:59	10.0.0.4	2024/12/20 09:07:30	2'30"	4	200	Finished	sip:666023025225@10.0.0.24.sip:66602302522...	195647@10.0.0.4,195647@...
☐	111023025222	222023025224	2024/12/20 09:04:59	10.0.0.3	2024/12/20 09:07:29	2'30"	4	200	Finished	sip:222023025224@10.0.0.23.sip:22202302522...	195646@10.0.0.3,195646@...
☐	333023025221	444023025223	2024/12/20 09:04:59	10.0.0.2	2024/12/20 09:07:29	2'30"	4	200	Finished	sip:444023025223@10.0.0.22.sip:44402302522...	195645@10.0.0.2,195645@...
☐	556023025220	666023025222	2024/12/20 09:04:59	10.0.0.1	2024/12/20 09:05:19	487	4	487	Cancelled	sip:666023025222@10.0.0.21.sip:66602302522...	195644@10.0.0.1,195644@...
☐	111023025219	222023025221	2024/12/20 09:04:59	10.0.0.10	2024/12/20 09:07:29	2'30"	4	200	Finished	sip:222023025221@10.0.0.20.sip:22202302522...	195643@10.0.0.10,195643@...
☐	333023025218	444023025220	2024/12/20 09:04:59	10.0.0.9	2024/12/20 09:07:29	2'30"	4	200	Finished	sip:444023025220@10.0.0.19.sip:44402302522...	195642@10.0.0.9,195642@...
☐	556023025217	666023025219	2024/12/20 09:04:59	10.0.0.8	2024/12/20 09:07:29	2'30"	4	200	Finished	sip:666023025219@10.0.0.18.sip:66602302521...	195641@10.0.0.8,195641@...
☐	111023025216	222023025218	2024/12/20 09:04:59	10.0.0.7	2024/12/20 09:07:29	2'30"	4	200	Finished	sip:222023025218@10.0.0.17.sip:22202302521...	195640@10.0.0.7,195640@...
☐	333023025215	444023025217	2024/12/20 09:04:59	10.0.0.6	2024/12/20 09:07:29	2'30"	4	200	Finished	sip:444023025217@10.0.0.16.sip:44402302521...	195639@10.0.0.6,195639@1...
☐	556023025214	666023025216	2024/12/20 09:04:59	10.0.0.5	2024/12/20 09:07:29	2'30"	4	200	Finished	sip:666023025216@10.0.0.15.sip:66602302521...	195638@10.0.0.5,195638@...
☐	111023025213	222023025215	2024/12/20 09:04:59	10.0.0.4	2024/12/20 09:07:29	2'30"	4	200	Finished	sip:222023025215@10.0.0.14.sip:22202302521...	195637@10.0.0.4,195637@...
☐	333023025212	444023025214	2024/12/20 09:04:59	10.0.0.3	2024/12/20 09:07:29	2'30"	4	200	Finished	sip:444023025214@10.0.0.13.sip:44402302521...	195636@10.0.0.3,195636@...
☐	556023025211	666023025213	2024/12/20 09:04:59	10.0.0.2	2024/12/20 09:07:29	2'30"	4	200	Finished	sip:666023025213@10.0.0.12.sip:66602302521...	195635@10.0.0.2,195635@...
☐	111023025210	222023025212	2024/12/20 09:04:59	10.0.0.1	2024/12/20 09:05:19	487	4	487	Cancelled	sip:222023025212@10.0.0.11.sip:22202302521...	195634@10.0.0.1,195634@...
☐	333023025209	444023025211	2024/12/20 09:04:59	10.0.0.10	2024/12/20 09:07:29	2'30"	4	200	Finished	sip:444023025211@10.0.0.10.sip:44402302521...	195633@10.0.0.10,195633@...
☐	556023025208	666023025210	2024/12/20 09:04:59	10.0.0.9	2024/12/20 09:07:29	2'30"	4	200	Finished	sip:666023025210@10.0.0.9.sip:666023025210...	195632@10.0.0.9,195632@...

Figure 7-65 Calls Panel with Use Users Domains Enabled

Recent Calls											
Details ... 🔍 Type to filter eg- callee=575,caller=115											
☐	Caller	Callee	Start timestamp	Caller IP address	End timestamp	Call time	Segments	Code	State	Request-URI	Call-ID
☐	556023025226	666023025228	2024/12/20 09:04:59	10.0.0.7	2024/12/20 09:07:30	2'30"	4	200	Finished	sip:666023025228@10.0.0.27.sip:66602302522...	19564a@10.0.0.7,19564a@...
☐	111023025225	222023025227	2024/12/20 09:04:59	10.0.0.6	2024/12/20 09:07:30	2'30"	4	200	Finished	sip:222023025227@10.0.0.26.sip:22202302522...	195649@10.0.0.6,195649@...
☐	333023025224	444023025226	2024/12/20 09:04:59	10.0.0.5	2024/12/20 09:07:30	2'30"	4	200	Finished	sip:444023025226@10.0.0.25.sip:44402302522...	195648@10.0.0.5,195648@...
☐	556023025223	666023025225	2024/12/20 09:04:59	10.0.0.4	2024/12/20 09:07:30	2'30"	4	200	Finished	sip:666023025225@10.0.0.24.sip:66602302522...	195647@10.0.0.4,195647@...
☐	111023025222	222023025224	2024/12/20 09:04:59	10.0.0.3	2024/12/20 09:07:29	2'30"	4	200	Finished	sip:222023025224@10.0.0.23.sip:22202302522...	195646@10.0.0.3,195646@...
☐	333023025221	444023025223	2024/12/20 09:04:59	10.0.0.2	2024/12/20 09:07:29	2'30"	4	200	Finished	sip:444023025223@10.0.0.22.sip:44402302522...	195645@10.0.0.2,195645@...
☐	556023025220	666023025222	2024/12/20 09:04:59	10.0.0.1	2024/12/20 09:05:19	487	4	487	Cancelled	sip:666023025222@10.0.0.21.sip:66602302522...	195644@10.0.0.1,195644@...
☐	111023025219	222023025221	2024/12/20 09:04:59	10.0.0.10	2024/12/20 09:07:29	2'30"	4	200	Finished	sip:222023025221@10.0.0.20.sip:22202302522...	195643@10.0.0.10,195643@...
☐	333023025218	444023025220	2024/12/20 09:04:59	10.0.0.9	2024/12/20 09:07:29	2'30"	4	200	Finished	sip:444023025220@10.0.0.19.sip:44402302522...	195642@10.0.0.9,195642@...
☐	556023025217	666023025219	2024/12/20 09:04:59	10.0.0.8	2024/12/20 09:07:29	2'30"	4	200	Finished	sip:666023025219@10.0.0.18.sip:66602302521...	195641@10.0.0.8,195641@...
☐	111023025216	222023025218	2024/12/20 09:04:59	10.0.0.7	2024/12/20 09:07:29	2'30"	4	200	Finished	sip:222023025218@10.0.0.17.sip:22202302521...	195640@10.0.0.7,195640@...
☐	333023025215	444023025217	2024/12/20 09:04:59	10.0.0.6	2024/12/20 09:07:29	2'30"	4	200	Finished	sip:444023025217@10.0.0.16.sip:44402302521...	195639@10.0.0.6,195639@1...
☐	556023025214	666023025216	2024/12/20 09:04:59	10.0.0.5	2024/12/20 09:07:29	2'30"	4	200	Finished	sip:666023025216@10.0.0.15.sip:66602302521...	195638@10.0.0.5,195638@...
☐	111023025213	222023025215	2024/12/20 09:04:59	10.0.0.4	2024/12/20 09:07:29	2'30"	4	200	Finished	sip:222023025215@10.0.0.14.sip:22202302521...	195637@10.0.0.4,195637@...
☐	333023025212	444023025214	2024/12/20 09:04:59	10.0.0.3	2024/12/20 09:07:29	2'30"	4	200	Finished	sip:444023025214@10.0.0.13.sip:44402302521...	195636@10.0.0.3,195636@...
☐	556023025211	666023025213	2024/12/20 09:04:59	10.0.0.2	2024/12/20 09:07:29	2'30"	4	200	Finished	sip:666023025213@10.0.0.12.sip:66602302521...	195635@10.0.0.2,195635@...
☐	111023025210	222023025212	2024/12/20 09:04:59	10.0.0.1	2024/12/20 09:05:19	487	4	487	Cancelled	sip:222023025212@10.0.0.11.sip:22202302521...	195634@10.0.0.1,195634@...
☐	333023025209	444023025211	2024/12/20 09:04:59	10.0.0.10	2024/12/20 09:07:29	2'30"	4	200	Finished	sip:444023025211@10.0.0.10.sip:44402302521...	195633@10.0.0.10,195633@...
☐	556023025208	666023025210	2024/12/20 09:04:59	10.0.0.9	2024/12/20 09:07:29	2'30"	4	200	Finished	sip:666023025210@10.0.0.9.sip:666023025210...	195632@10.0.0.9,195632@...

Note

Realms definitions delimited by domain names only work if this setting is enabled.

Voice Quality Chart Scale in Minutes/Minute

Determines the scale of the **Voice Quality** chart. If true, the scale will be minutes/minute instead of minutes/15 minutes. Default is false (minutes/15 minutes).

Web Session Timeout

This value allows the user to dynamically change the Web Session Timeout. The default value is 30 minutes. When the Web Session Timeout is set to "0", Session Timeout functionality is disabled. The maximum Web Session Timeout value allowed by the system is 30 minutes.

Oracle SBC Config Upload

You can create new SIP trunks and devices based on an SBC configuration with the **Oracle SBC Config** function. The **Oracle SBC Config** function can also update existing SBC configurations. Every data point (for example, a **trunk**) that is added from an SBC configuration is marked in the configuration. This allows that all trunks created via an SBC configuration can be identified and later removed.

This graphic shows the **Oracle SBC Config Upload** page.

Figure 7-66 Oracle SBC Config Upload Page

SBC Configuration Import Wizard

The following entries have been found in the SBC configuration provided. Please select a bulk action or set an action per entry.

Bulk Actions

SBC Interfaces:

Session Peers:

Session Peer Types:

Entries in SBC Configuration

Device Name	SBC Interface	IP	Action	Device Type	Status
M00:0		1.10.177.31	Create		
M10:0		1.20.177.31	Create		
Avaya	1.10.177.31	1.30.33.9	Create	Trunk	

The SBC Configuration upload section contains the following check boxes:

- **Add device groups as single device**

If this check box is selected before an upload, the session agents in the configuration file that are part of a session agent group are added to Operations Monitor as a single device with multiple IPs.

- **Resolve hostnames**

By default, devices that do not have a numeric IP address specified in the configuration file, are skipped. If the **Resolve hostnames** check box is selected before an upload, Operations Monitor will try to resolve the hostnames for those devices.

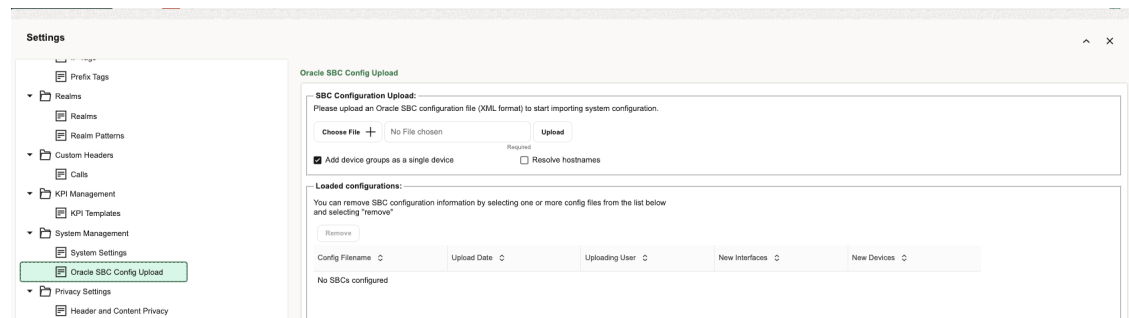
Note

This will increase the processing time for the change.

Import Window

The import window shows all the changes that could be committed based on the given SBC configuration.

Figure 7-67 SBC Configuration Import Wizard Page



The SBC Configuration Import Wizard dialog box contains the following:

- **Bulk Actions** section

Bulk actions set the per data point action to be applied. It does not automatically execute the action but sets the action for the given data points accordingly.

The Bulk Actions section contains the following fields:

- SBC Interfaces
- Session Peers
- Session Peer Types

- **Entries in SBC Configuration** table

This table lists all the entries that were found in the configuration.

Existing entries are marked with the **Create** check box disabled so that duplicates cannot be created. Valid options are **Create** and **Ignore**. All entries are identified by their IP or IP pair (in case of trunks) address.

The user can double-click a device to rename it.

- **Execute/Reset** buttons

The **Execute** and **Reset** buttons at the bottom of the page are used to execute all actions on the page or reset to the default values.

Language Settings

In the Session Monitor Release 6.1, only English language is supported as the language in the user interface.

Privacy Settings

Access these settings by clicking **Admin**, and then **Settings**, and then **Privacy Settings**, and then **Header and Content Privacy**.

SIP Header Anonymization

The **Operations Monitor Settings** supports masking or anonymizing sensitive information in selected SIP headers before storing them in the backend database. The Mediation Engine anonymizes headers by replacing the header value with a single hyphen.

The following SIP headers can be anonymized:

- Subject (selected by default)
- Call-Info
- Cellular-Network-Info
- Contact
- Geolocation
- Geolocation-Routing
- In-Reply-To
- Organization
- P-Access-Network-Info
- P-Preferred-Identity
- P-Private-Network-Indication
- Record-Route
- Reply-To
- Server
- Warning

The Subject header as well as the CPIM content or message body are always anonymized when **Chat/Custom SIP headers Anonymization** is selected.

Example

In this example, the Subject and Call-Info check boxes in the Custom SIP Headers section are selected.

Before anonymization

```
INVITE sip:alice100@open-ims.test;transport=udp SIP/2.0
Via: SIP/2.0/UDP 192.168.80.2:5060;rport;branch=z9hG4bK-6593-1-0
Path: <sip:192.168.80.150:5060;p-acme-serving>
From: <sip:bob100@open-ims.test>;tag=1
To: <sip:alice100@open-ims.test>
Call-ID: 1-6593@192.168.80.2
CSeq: 1 INVITE
Subject: How are you?
Contact: <sip:bob100@192.168.80.2:5060>
P-Asserted-Identity: <sip:bob100@open-ims.test>
Accept-Contact: *;+g.oma.sip-im
Max-Forwards: 70
```

```
Call-Info:<http://www.example.com/alice/photo.jpg>;purpose=icon
Allow-Events: kpml
```

Content-Type: message/cpim

Content-Length: 385

From: <sip:anonymous@anonymous.invalid>

To: <sip:anonymous@anonymous.invalid>

DateTime: 2018-04-11T17:23:12.708+02:00

NS: imdn <urn:ietf:params:imdn>

imdn.Message-ID: opdNmM3aAvk7KcFQZDHyrD0j00KH0SBk

Subject: How are you?

imdn.Disposition-Notification: positive-delivery, display

Content-Type: text/plain; charset=utf-8

Content-Length: 21

Hello, where are you?

After anonymization

INVITE sip:alice100@open-ims.test;transport=udp SIP/2.0

Via: SIP/2.0/UDP 192.168.80.2:5060;rport;branch=z9hG4bK-6593-1-0

Path: <sip:192.168.80.150:5060;p-acme-serving>

From: <sip:bob100@open-ims.test>;tag=1

To: <sip:alice100@open-ims.test>

Call-ID: 1-6593@192.168.80.2

CSeq: 1 INVITE

Subject: -

Contact: <sip:bob100@192.168.80.2:5060>

P-Asserted-Identity: <sip:bob100@open-ims.test>

Accept-Contact: *;+g.oma.sip-im

Max-Forwards: 70

Call-Info: -

Allow-Events: kpml

Content-Type: message/cpim

Content-Length: 354

From: <sip:anonymous@anonymous.invalid>

To: <sip:anonymous@anonymous.invalid>

DateTime: 2018-04-11T17:23:12.708+02:00

NS: imdn <urn:ietf:params:imdn>

imdn.Message-ID: opdNmM3aAvk7KcFQZDHyrD0j00KH0SBk

Subject: -

imdn.Disposition-Notification: positive-delivery, display

Content-Type: text/plain; charset=utf-8

Content-Length: 1

-

The Content-Length header is recalculated after anonymization with the appropriate value.

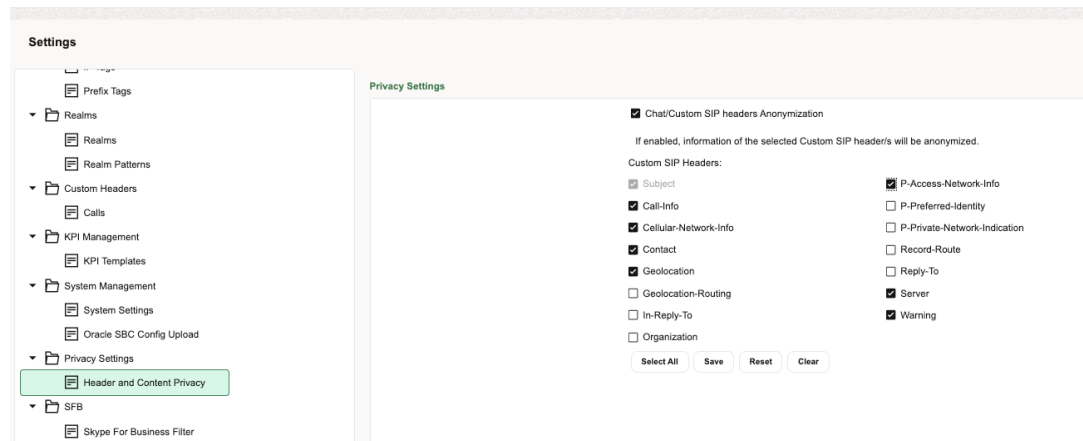
Anonymizing SIP Headers

This page enables or disables the Mediation Engine's anonymization feature.

1. Log in to the Mediation Engine.

2. Navigate to **Admin**, and then **Settings**, and then **Privacy Settings**, and then **Header and Content Privacy**.

Figure 7-68 Header and Content Privacy



3. Check the **Chat/Custom SIP headers Anonymization** checkbox.
4. (Optional) Select any additional SIP headers to be anonymized.
5. Click **Save** and **Close**.

SFB

The **SFB** section of the **Settings** window contains configuration options for Skype For Business.

Skype For Business Filter

The Skype For Business (SFB) Filter allows you to configure which types of Skype-based communications are displayed in the Operations Monitor interface. This setting is only shown when the SFB extension is enabled during installation.

Audio calls are displayed by default. Additional call types that can be displayed are:

- Video
- IM
- Conference
- Desktop Sharing
- File Transfer

To select which call types to display, select the checkboxes and then click on **Save**.

External Devices

You can configure communication with external devices in the **External Devices** section, which includes the following sub-sections:

- [RADIUS Authentication](#)
- [SNMP Options](#)

- [SFTP Server](#)
- [Voice Quality Collector](#)

RADIUS Authentication

Note

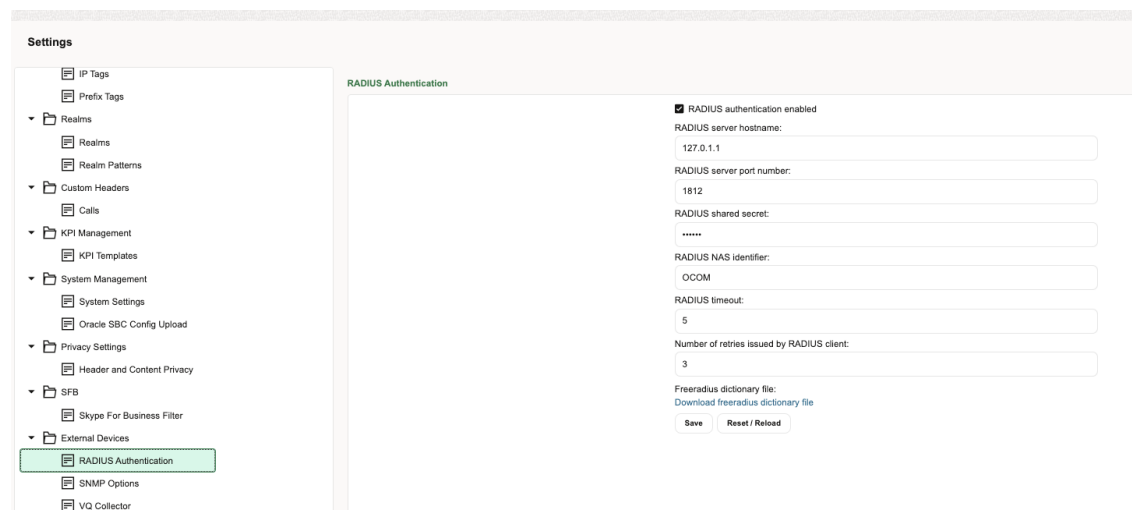
User Roles cannot work together with RADIUS Authentication.

RADIUS authentication allows you to configure whether or not Operations Monitor will perform RADIUS authentication against a RADIUS authentication server each time you log in.

To configure RADIUS authentication over TLS (RadSec), refer to the section [Configuring RADIUS Authentication over TLS \(RADSEC\)](#) in the Session Monitor Release 6.1 Installation Guide.

This illustration shows Radius Authentication Settings:

Figure 7-69 Radius Authentication Settings



To enable RADIUS authentication on an Operations Monitor installation, click the **RADIUS authentication enabled** check box. When enabled:

- The **RADIUS server hostname** and **RADIUS server port number** fields control the address of the RADIUS server against which Operations Monitor performs authentication.
- The **RADIUS shared secret** field must contain the secret that is shared by Operations Monitor and the RADIUS server used for authentication.
- The **RADIUS NAS identifier** is a string identifier and is used by the RADIUS server to determine whether or not the request is coming from Operations Monitor.
- The **RADIUS timeout** is number of seconds to wait response from RADIUS server.
- The **Number of retries issued by RADIUS client** is the number of attempts to connect to server, expressed as positive integer value. Number of retries multiplied by timeout value should not exceed 30 (seconds), otherwise both fields (timeout and number of retries) will be marked as invalid.

For more information about RADIUS authentication in Operations Monitor, see [Requirements for RADIUS Authentication](#).

SNMP Options

The **SNMP Options** subsection allows you to configure:

- Whether Operations Monitor sends SNMP traps.
- Whether Operations Monitor can be queried using SNMP.

Regarding the queries Operations Monitor can answer, they are in turn split in two:

- All the counters of Operations Monitor are exported as gauges.
- All operating parameters of the system of Operations Monitor.

SNMP Traps

To enable SNMP traps, click the **SNMP traps enabled** check box as shown in the graphic. When enabled, SNMP traps can be sent on several *Alerts*. You must configure the SNMP community name, IP address, and port where the SNMP traps will be sent.

When you select SNMPv3, traps/alerts are generated with authentication or security level as authPriv by default. That is, Operations Monitor supports only authPriv in SNMPv3 traps.

To test the settings, a test trap can be sent by clicking **Send test trap**. To send SNMP traps to more than one target, you enter more than one SNMP trap target IP address.

If you specify more than one community string, Operations Monitor will use the first community string and the first IP address, and so on. You cannot specify more than one port.

Figure 7-70 SNMP Traps Settings

The screenshot shows the 'Settings' page with a sidebar on the left containing a tree view of settings categories. The 'SNMP Options' option is highlighted. The main content area is titled 'SNMP Options' and contains the following configuration fields:

- SNMP version:** A dropdown menu set to 'v3'.
- SNMP traps enabled:** An unchecked checkbox.
- SNMP trap target username:** A text input field containing 'oracle'.
- Engine ID for traps (10-64 hex digits):** A text input field with a 'Generate New Engine ID' button next to it.
- SNMP trap target address(es):** A text input field.
- SNMP trap target UDP port number:** A text input field containing '162'.
- SNMP daemon enabled:** An unchecked checkbox.
- SNMP daemon username:** A text input field containing 'oracle'.
- SNMP daemon UDP port number to bind to:** A text input field containing '161'.
- MIB file for values exported by the Session Monitor via SNMP:** A section with a 'Download MIB file' link and three buttons: 'Save', 'Reset', and 'Send Test Trap'.

SNMP traps are interpreted using the *MIB* file, which is downloaded from the **SNMP Options configuration** page.

The traps include descriptive text which interprets the trap as well as the subsystem that caused the trap to be generated. Included in this description are the current value assigned to the system (value of the counter, IP address, actual user or device name), and the severity of the trap.

Some instances that generate traps are:

- Counters exceeding thresholds.
- IP addresses or user names meeting certain conditions.
- Failing network devices.

SNMP Daemon

To enable SNMP Daemon, click the **SNMP daemon enabled** check box. With the SNMP daemon enabled, you can query Operations Monitor using SNMP. For SNMP Daemon to work properly, you must also specify the community name and UDP port, which listens for SNMP requests coming in. Operations Monitor supports SNMP Version 2 over UDP.

When SNMP commands such as `snmpwalk`, `snmpget` are used with SNMPv3 version to query Exported Counters, then the authentication or security level supported is only `noAuthNoPriv`.

Figure 7-71 SNMP Options

The screenshot shows the 'Settings' page with a sidebar menu on the left containing items like IP Tags, Prefix Tags, Realms, Custom Headers, KPI Management, System Management, Privacy Settings, SFB, External Devices, RADIUS Authentication, **SNMP Options** (highlighted), and VQ Collector. The main content area is titled 'SNMP Options' and contains the following fields:

- SNMP version: v3 (dropdown)
- ☐ SNMP traps enabled
- SNMP trap target username: oracle
- Engine ID for traps (10-64 hex digits): [empty field] [Generate New Engine ID](#)
- SNMP trap target address(es): [empty field]
- SNMP trap target UDP port number: 162
- ☒ SNMP daemon enabled
- SNMP daemon username: oracle
- SNMP daemon UDP port number to bind to: 161
- MIB file for values exported by the Session Monitor via SNMP: [Download MIB file](#)
- Buttons: Save, Reset, Send Test Trap

Exported Counters

The counters are available in the MIB tree under the OID: **.1.3.6.1.4.1.29631.2.2.0.256**. Enter the following command to list all counter information using Net-SNMP's `snmpwalk`:

```
snmpwalk -Os -c public 10.1.0.78:162 -v 2c \
.1.3.6.1.4.1.29631.2.2.0.256
```

```
snmpwalk -v3 -On -u oracle -l noAuthNoPriv 10.75.220.182
1.3.6.1.4.1.29631.2.2.0.256
```

The next node is the counter ID. Under it, the counter object has the following fields as listed in [Table 7-16](#):

Table 7-16 Counter Object Fields

Field	Description
.0.0	The counter ID.
.1.0	The name of the counter.
.2.0	The device or IP/Prefix tag name (if it is a device or IP/Prefix tag counter).
.3.0 .4.0 .5.0	The counter parameters.
.6.0	The current second value.
.7.0 .8.0 .9.0	The last minute average/min/max.
.10.0 .11.0 .12.0	The last 5 minutes avg/min/max.
.13.0 .14.0 .15.0	The last hour avg/min/max.

For example, here is how to get the active calls counter. Note, that the ID of the counter (422 as used in this example), will vary from one box to another:

```
snmpwalk -Os -c public 10.1.0.78:162 -v 2c \
    .1.3.6.1.4.1.29631.2.2.0.256.442

snmpwalk -v3 -On -u oracle -l noAuthNoPriv 10.75.220.182
1.3.6.1.4.1.29631.2.2.0.256.442
```

```
enterprises.29631.2.2.0.256.442.1.0 = STRING: "Active calls"
enterprises.29631.2.2.0.256.442.3.0 = INTEGER: 0
enterprises.29631.2.2.0.256.442.4.0 = INTEGER: 0
enterprises.29631.2.2.0.256.442.5.0 = INTEGER: 0
enterprises.29631.2.2.0.256.442.6.0 = Counter64: 136
enterprises.29631.2.2.0.256.442.7.0 = Counter64: 13751
enterprises.29631.2.2.0.256.442.8.0 = Counter64: 133
enterprises.29631.2.2.0.256.442.9.0 = Counter64: 141
enterprises.29631.2.2.0.256.442.10.0 = Counter64: 10319
enterprises.29631.2.2.0.256.442.11.0 = Counter64: 66
enterprises.29631.2.2.0.256.442.12.0 = Counter64: 141
enterprises.29631.2.2.0.256.442.13.0 = Counter64: 10068
enterprises.29631.2.2.0.256.442.14.0 = Counter64: 63
enterprises.29631.2.2.0.256.442.15.0 = Counter64: 141
```

Note

When using `snmpwalk` the following should be considered:

- Because of large values, the Counter64 type is used, but this is not available in SNMPv1. You must use SNMPv2 or later.
- Even with Counter64 type in use, the counters act like gauges in SNMP talk. For example, over time the value of the counter is presented, and not the sum.
- The averages are computed per-second. For example, for the last 5 minutes, all the values measured every second are added and then divided by 300. Since we cannot transport floats over SNMP, the $\text{avg} * 100$ is returned. In *cacti* <<http://www.cacti.net/>>, you would divide back with 100. In this example, the last 5-minute average, or .10.0, means: On average, there was 103.19 active calls in the last 5 minutes (measured every second).

We recommend this when creating the graphs. The min and max values might also be informative.

System Monitoring

Operations Monitor runs Net-SNMP which provides a large set of monitoring objects for the Operations Monitor system itself. For example, you can get the UC Davis <http://www.net-snmp.org/docs/mibs/ucdavis.html> values with:

```
snmpwalk -Os -c test1 10.1.0.72:161 -v 2c .1.3.6.1.4.1.2021
```

```
snmpwalk -v3 -On -u oracle -l noAuthNoPriv 10.75.220.182 1.3.6.1.4.1.2021
```

As these are standard Unix MIBs, most SNMP managers are able to interpret them.

SFTP Server

You can create CDRs, which are based on the traffic displayed and the platform topology configured. For more information, see "[Public CDR Generation](#)".

The CDRs generated CDRs, can be retrieved and deleted using SFTP.

Enabling Access using SFTP

Follow the steps given in this section to enable access using SFTP:

1. Log in to the OCSM server as root user.
2. Create a new user using the command:

```
useradd <username>
```

3. Set the password using the command:

```
passwd <username>
```

4. Set the r-x permission to folder /opt/oracle/ocsm/var/vsi/ftp using the command:

```
setfacl -R -m u:<username>:r-x /opt/oracle/ocsm/var/vsi/ftp
```

5. Run this command to verify the permissions and access to this directory /opt/oracle/ocsm/var/vsi/ftp.

```
getfacl /opt/oracle/ocsm/var/vsi/ftp
```

6. Open the /etc/ssh/sshd_config file and add these lines at the end of the file (provide username created above in the specified locations):

```
Match User <username>
ForceCommand internal-sftp -R -d /opt/oracle/ocsm/var/vsi/ftp
PasswordAuthentication yes
PermitTunnel no
AllowAgentForwarding no
AllowTcpForwarding no
X11Forwarding no
```

Note

You can create multiple users for SFTP access by following the same steps, they can be added the in /etc/ssh/sshd_config file separated by comma as below:

```
Match User <username_1>, <username_2>, <username_3>
ForceCommand internal-sftp -R -d /opt/oracle/ocsm/var/vsi/ftp
PasswordAuthentication yes
PermitTunnel no
AllowAgentForwarding no
AllowTcpForwarding no
X11Forwarding no
```

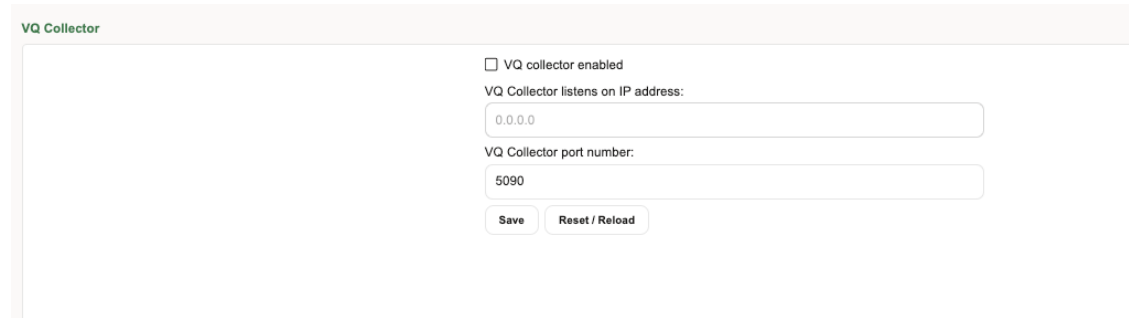
7. Restart the sshd service: `systemctl restart sshd`
8. You can now log in from another Linux machine using SFTP command or use software such as FileZilla to access the /opt/oracle/ocsm/var/vsi/ftp folder and its contents.

Voice Quality Collector

Operations Monitor can gather the voice quality information sent by IP phones in SIP PUBLISH messages and display it on the **Voice Quality** page.

As defined in RFC 6035, SIP User Agents may send voice quality reports derived from RTCP Extended Reports (RTCP-XR) and Operations Monitor acts as the collector of SIP vq-rtcpxr events using the PUBLISH method.

The vq-rtcpxr event collector is configurable as shown:

Figure 7-72 Configure VQ Collector

To configure the voice quality collector:

1. Select the **VQ collector enabled** check box to enable the collection of voice quality metric reports.
2. In the **VQ Collector IP address** field, enter the IP address that is used by the vq-rtcpvr event collector to listen for PUBLISH messages.
3. In the **VQ Collector port number** field, enter the port number.
4. Click **Save**.

Note

The same collector must be configured at the IP phone in order to let it send the voice quality metric reports to Operations Monitor.

Configuration Savepoints

Operations Monitor allows you to create configuration snapshots. Savepoints include most of the configuration values:

- Settings dialog sections:
 - Platform
 - System Management
 - External Devices
 - Number Determination Sources
 - Realms
- Alert Definitions
- Operations Monitor user accounts
- Counters currently configured on pages:
 - KPIs/Metrics
 - Devices

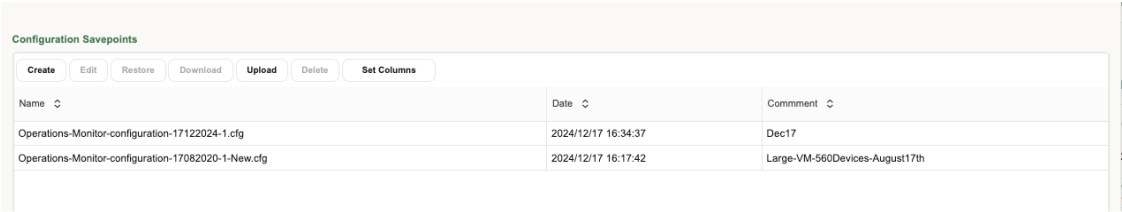
The management functionality for configuration savepoints is only available to the administration user. Savepoints can be created and used to restore the above mentioned settings. They can be downloaded as a file and uploaded again.

Note

Savepoints are only valid for the exact Operations Monitor version for which they were taken. A savepoint might work in other Operation Monitor versions as well, however, when restoring a savepoint it is recommended to use a Operations Monitor version which is either the same or nearest to the original version. The reason being that sometimes changes between various Operations Monitor version may cause the savepoint to not get fully restored.

For example, if a savepoint was created for safety reason and then a system reinstall is required, the recommended approach would be reinstalling the same Operations Monitor version of which you have taken the savepoint, or the one nearest version to it.

Figure 7-73 Configuration Savepoints



Configuration Savepoints		
Create Edit Restore Download Upload Delete Set Columns		
Name	Date	Comment
Operations-Monitor-configuration-17122024-1.cfg	2024/12/17 16:34:37	Dec17
Operations-Monitor-configuration-17082020-1-New.cfg	2024/12/17 16:17:42	Large-VM-560Devices-August17th

The **Configuration Savepoints** section lists all savepoints with name and creation date. The table lists the actions, which are provided by the buttons in the table's toolbar:

Table 7-17 Configuration Savepoint Fields

Field	Description
Create Savepoint	Creates a new savepoint from the current Operations Monitor configuration.
Restore Savepoint	Restores the Operations Monitor configuration contained in the selected savepoint. Note, that on restoring a savepoint, Operations Monitor needs to restart some internal services, which can result in a downtime in monitoring. Restoring a savepoint in an Operations Monitor deployment will result in downtime. The duration of downtime depends on the size and the configuration of the deployment.
Download Savepoint	Downloads the selected savepoint as a file.
Upload Savepoint	Uploads an Operations Monitor savepoint contained in a file.
Delete Savepoint	Removes the selected savepoint from the list and the system.

Note

When using Mediation Engine with a Mediation Engine Connector, it is not possible to restore the configuration savepoint.

Note

Do not manually alter savepoint files unless you know what you are doing, as this may lead to severe inconsistencies in the Operations Monitor setup.

User Management

This section of the configuration allows to administer the access control over the web interface. The Operations Monitor web resources can be accessed concurrently from multiple network locations. This is done using a traditional user access mechanism.

Figure 7-74 The User Management Panel

Username	Email	Realm	Role
admin	ocsmadmin@oracle.com	ALL	
user_0	user_0@oracle.com	realm_for_user_0	Role2
user_1		realm_for_user_1	
user_2		realm_for_user_2	
user_3		realm_for_user_3	
user_4		realm_for_user_4	
user_5		realm_for_user_5	
user_6		realm_for_user_6	
user_7		realm_for_user_7	
user_8		realm_for_user_8	
user_9		realm_for_user_9	
user_10		realm_for_user_10	
user_11		realm_for_user_11	
user_12		realm_for_user_12	
user_13		realm_for_user_13	
user_14		realm_for_user_14	
user_15		realm_for_user_15	
user_16		realm_for_user_16	
user_17		realm_for_user_17	
user_18		realm_for_user_18	

A *user* is a data set whose most important elements are: a log-in name, a password, a set of access rights, the set of relations to other users, and the realm the user has access to; other less significant elements are name, email address, logo image.

The access to the web interface is fragmented into individual, non-overlapping domains. In order to access such a domain, a user needs to have the permission (or *right*) to do so. These rights, that control which parts of the web interface a user can see, are granted by the parent user that created it. Of course, the user *admin* has unrestricted access.

The **User Management** panel:

The left most three of them allow a user to manage his sub-users: Add a new, edit an already added one, or remove a no longer needed user. To modify or delete a sub-user, its parent-user needs to select a row out of the table and press the corresponding button. Both the **Add a new user** and the **Edit user** buttons invoke a wizard (in a new window) asking for the needed detail in order to set-up a new or change an existing user. The **Add rights...** and the **Remove rights...** buttons make it possible to add selected rights to selected or all users created by the current user, respectively to remove selected rights from selected or all users created by the current user. The rights to add or remove can be selected in a wizard, that is in accordance with the last two pages of the wizard. The **Login as selected user** button allows a parent user to login as a sub-user without having to enter a password. The **Set Column** button allows you to hide/unhide columns from display in the table. The **Common User KPIs** is related to KPI management. For more information, see KPI Management. The **Edit own profile** button to the right of the page allows the current user to edit one's own profile information. The **Search** option allows you to search for or filter users existing in the system. The right-side corner displays the total number of users.

Setting Field Visibility (Calls Panel) for a User

The **Calls Field Permission** setting in the **Permission for Modules** dialog box allows the Admin/User to control the visibility of fields in the **Calls** panel, and fields to be exported to a CSV file or bulk export.

To set the fields visibility:

1. Click **Admin > Settings > User Management > User Management**.
2. In the **Add a User** or **Edit User > Permissions for Modules** dialog box, check the **Calls Field Permission** and click the edit button next to it.

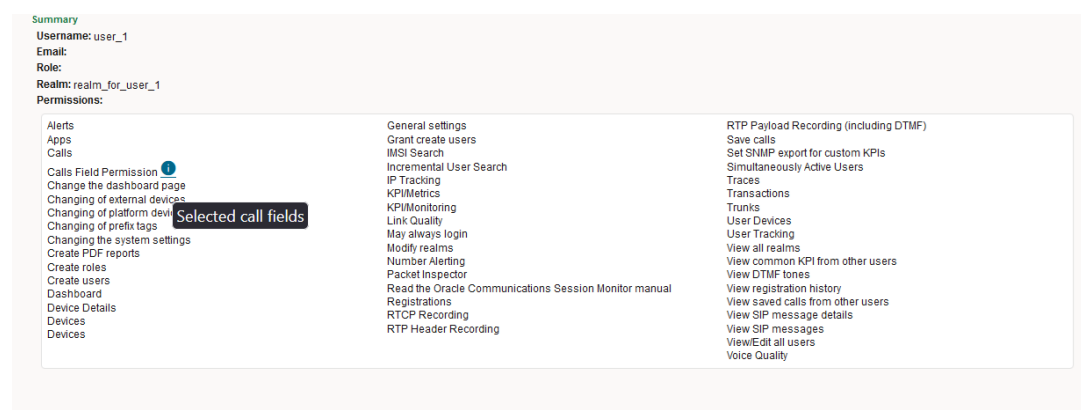
Note

For custom headers, only such fields will be visible in the modules, if they are added in the **Settings> Custom Headers> Calls**.

3. Choose the fields that the user should have visibility to.
4. Click **Apply**.
5. Click the info icon next to **Calls Field Permission**.

The selected fields are shown in the **Summary** page.

Figure 7-75 Summary page



Note

While creating a new role or modifying an existing role, the Admin can specify permissions to be assigned to that role. On assigning the role to a user, the permissions given to the role are pre-selected and assigned to the user. These permissions can be modified later also. These will get updated once the role's permissions are modified.

6. The visibility rules will be effective on the next login. User can view and access those selected fields in Calls panel.

Note

Although the user has visibility permissions, some fields are not added in the CSV export files. You can view such fields from a warning message that is displayed if you select any field that is not going to be added in the export files.

The User Administrator Role

User Administrator is a role in the Mediation Engine. A user with the User Administrator role can perform only user administrations tasks.

A user created with this role cannot perform any other tasks.

A user with the User Administrator role cannot add or modify own entitlements. The scope of this role is restricted to only Settings > User Management.

Only the admin user can create or delete a user that is assigned the User Administrator role. The admin user can create only one user with this role. Once a user with the User Administrator role is created, all user management entitlements such as create, modify, and delete are disabled for other users created by this user. However, the admin user and the users created by the admin user can still perform user management tasks.

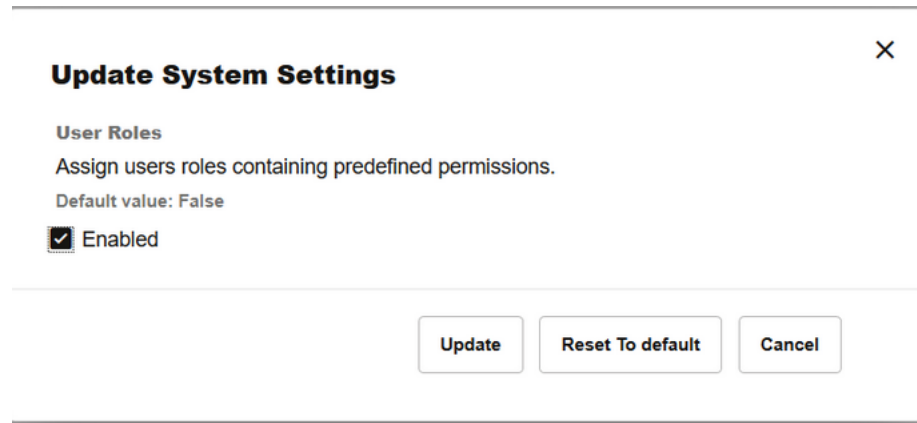
When the admin user deletes the user with User Administrator role, then the admin user falls back to create, modify, or delete any users.

Enable User Roles

Update the system setting to enable a user to assign user roles with pre-defined permissions to a newly created user.

To update the system settings:

1. Log in to the Mediation Engine.
2. Navigate to **Settings, System Management, System Settings, and User Roles**.
3. Select **Enabled**.

Figure 7-76 Update System Setting

4. Click **Update**.

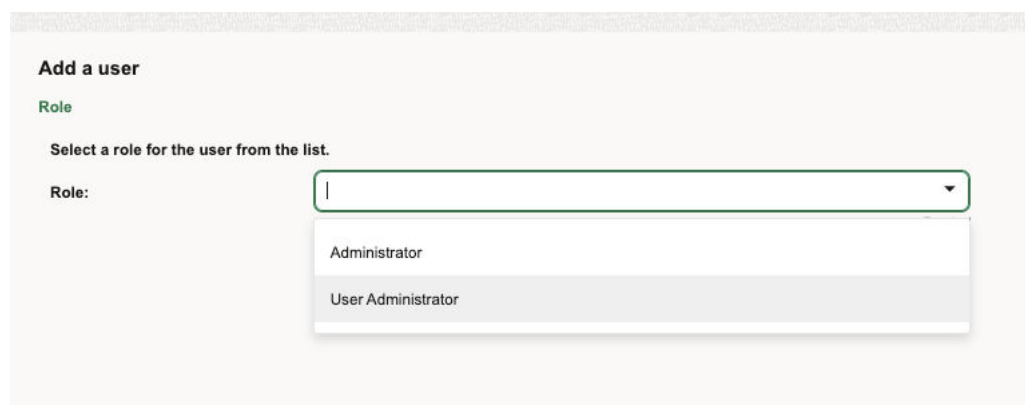
This enables a user to assign roles with pre-defined permissions.

Add the User Administrator User

As the admin user, you can create a user with User Administrator role. A user with this role can perform only user administration functions. This role cannot perform any other tasks using the Mediation Engine GUI.

To add the user with the User Administrator Role:

1. On the Mediation Engine, click **admin**, **Settings**, and **User Management**.
2. In the **User Management** screen, click **Add a new User**.
3. In the **User Information** screen, add information about the new user such as username, Email address, password and so on.
4. Click **Next**.
5. In the **Roles** screen, select the **User Administrator** role.

Figure 7-77 User Administrator Role

6. In the **Summary** screen, review the information of the new user, and click **Finish**.

The **User Management** screen now displays the new user with the User Administrator role.

Tasks List of the User Administrator User

The scope of the User Administrator user is limited to user management tasks. This user cannot perform any other function using the GUI.

User Administrator Tasks

Table 7-18 User Administration Task List

Task	Yes/No
Create a User Administrator	No
Add or remove rights of the User Administrator user	No
Edit an existing user created by the admin user or User Administrator before the upgrade	Yes
Delete the admin user	No
Delete a non-admin user	Yes
Add permissions given to a user	Yes
Edit admin user privileges	No
Enable an option to force users to change their passwords regularly	Yes
Set a period(days) after which users with or without sensitive data are forced to change their password	Yes
Enable users to create a new role	Yes
Create, edit, delete a user associated with a realm	Yes
Allow users to edit privileges assigned to Custom or Administrator roles	Yes
In Mediation Engine, logged in as a User Administrator user, add or remove own rights	No
In Mediation Engine, logged in as a User Administrator user, edit password settings	Yes
In Mediation Engine, logged in as a User Administrator user, create a new user role	Yes
Change Administrator role to User Administrator	No
Add a New User	Yes
- User Information - Selecting a Role - User Permissions - Add User Realm - See the Overview Information - Requirements for RADIUS Authentication	
Role Management:	Yes
- Adding a Role - Editing a Role - Deleting a Role - Adding Rights to a Role - Removing Rights from a Role	
External Authentication Authorization	Yes
Password Settings	Yes
Enabling or Disabling User Accounts	

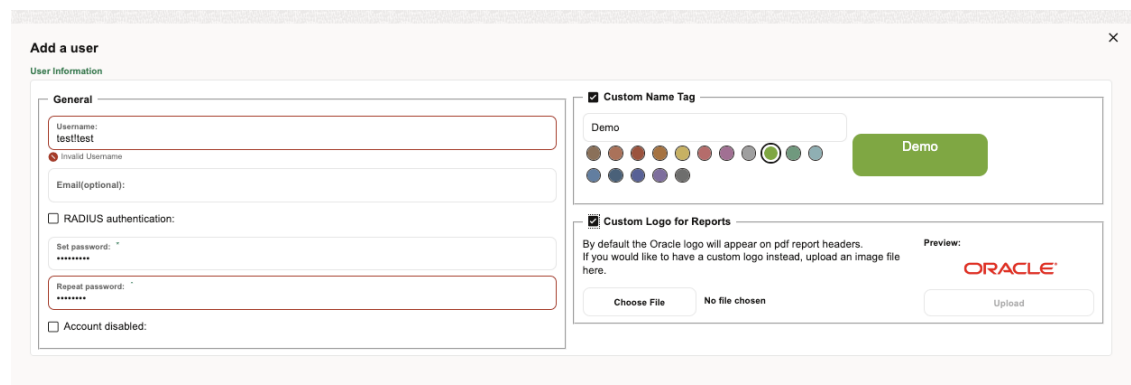
Add a New User

We'll next walk through the steps needed to add a new user. The same steps need to be performed for editing a user, with the difference that a field for the name of the new user is present when adding. When editing one's own profile, only the first step of this process is necessary.

User Information

The first step, named *User Information*, requires providing the log-in name (the username), an optional email address, and a password (asked two times to prevent accidental mistyping) as seen in the graphic. Instead of entering a password, it is also possible to opt for *RADIUS* authentication, if RADIUS authentication has been set up for this Operations Monitor instance. To learn more about Operations Monitor's RADIUS authentication feature, see "[Requirements for RADIUS Authentication](#)".

Figure 7-78 Adding a new user



A logo image is located in the upper left corner of the user interface. By default, this is the Oracle logo, but it can be customized for each individual user; this is useful when the web interface is accessed by multiple clients of the same provider, sharing the same Operations Monitor setup. The **Custom Logo for Reports** section provides an upload field where the user can insert the picture to use as a logo.

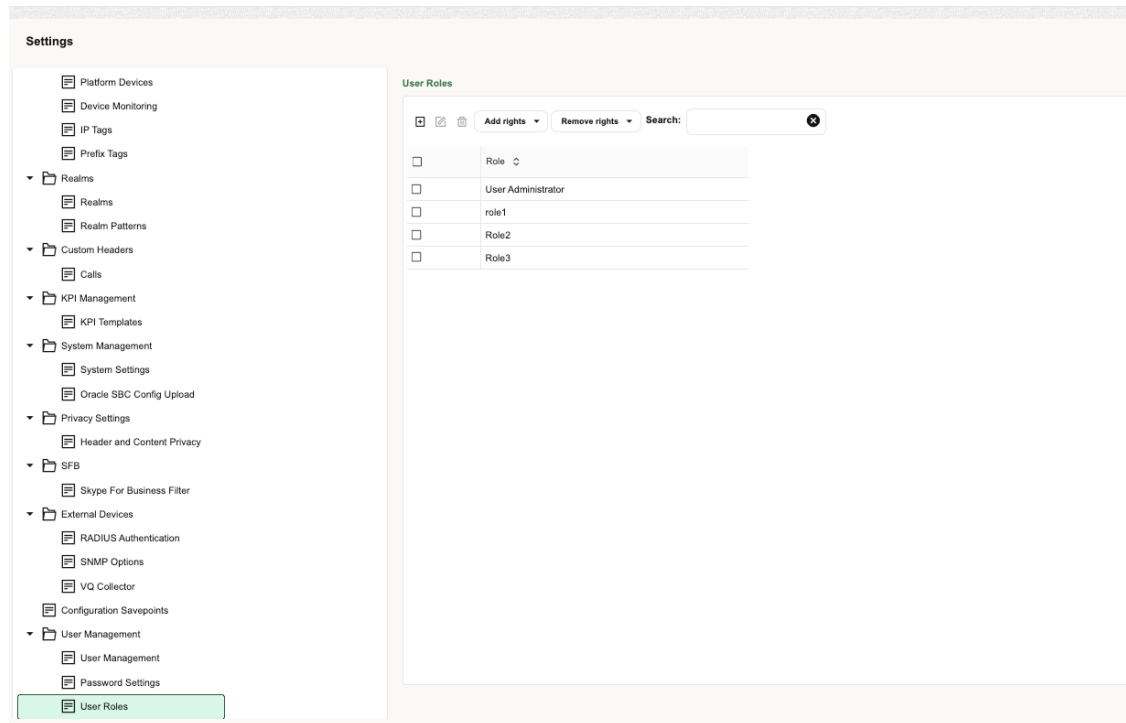
Note

The following logo formats are supported: TIF, TIFF, EPS, PDF, JPG, JPEG, GIF, and PNG.

After specifying the path, click **Upload** to upload the file.

Selecting a Role

After choosing a username and password, the user is given the option of selecting a role providing roles have been defined in addition to the custom role. If no roles are available, the dialogue will continue directly to the realms selection if they exist, otherwise onto the individual permissions selection.

Figure 7-79 Setting a Role for the New User**Note**

If you are creating a user to perform user management tasks only, select the User Administrator role.

User Permissions

In case *User Roles* is enabled, a role is set for the user that gives the user a predefined set of permissions that are tied to the role. For more information on role management, see the Role Management section.

In case *User Roles* is disabled, the permissions need to be set individually for each module, and for each setting.

The **Permissions for Modules** page, is where the parent user can control what the new user will be able to access. The set of permissions are grouped in four, reflecting the grouping of functionality on the actual web interface:

Figure 7-80 Setting Permissions for Modules for a New User

Add a user

Permissions for Modules
Check the boxes of the modules the user will be permitted to use

General	Operations	Customer Experience	Control Plane Monitor
☒ Dashboard	☒ KPI/Monitoring	☒ User Tracking	☒ IMSI Search
☒ Traces	☒ Calls	☒ IP Tracking	☒ Transactions
☒ Alerts	☒ Calls Field Permission	☒ Link Quality	☒ KPI/Metrics
☒ Packet Inspector	☒ Voice Quality	☒ Simultaneously Active Users	☒ Devices
☐ Apps	☒ Registrations	☐ SFB Filter	
☐ Read Only Dashboard	☐ Subscriptions		
	☐ Non Call (User Devices, Devices, IP Tracking)		
	☒ User Devices		
	☒ Trunks		
	☒ Devices		
	☒ Device Details		
	☒ Number Alerting		

- General
- Operations
- Customer Experience
- Control Plane Monitor

Each check box in these groups corresponds to a menu item in the main menu of Operations Monitor. If it is checked, the new user will have the corresponding menu item in his main menu.

The **Permissions for Settings** page can control the settings the created user will be allowed to modify. The access right to some advanced functionality of Operations Monitor can also be controlled here.

Figure 7-81 Permissions for Settings

Add a user

Permissions for Settings
Check the boxes of the settings the user will be permitted to modify

Settings	User Interface
☒ General settings	☒ View SIP messages
☒ Changing of platform devices	☒ View SIP message details
☒ Changing of prefix tags	☐ View Media Info
☒ Create users	☒ Create PDF reports
☒ Grant create users	☒ View registration history
☒ View/Edit all users	☐ View Subscriptions in User Tracking
☒ Create roles	☒ Incremental User Search
☒ Changing of external devices	☒ Read the Oracle Communications Session Monitor manual
☒ Changing the system settings	☒ Change the dashboard page
☒ Modify realms	☒ May always login
☒ Set SNMP export for custom KPIs	☒ Save calls
☐ UCaaS CCaaS Calls Settings	☒ View saved calls from other users
	☒ View all realms
	☒ View DTMF tones
	☐ KPI Management
	☐ Expand KPI
	☐ Shrink KPI
	☒ View common KPI from other users

The check boxes in the **Settings** group to the left of the section roughly correspond to sections in the **Settings** page.

The table describes the user setting options.

Table 7-19 User Settings Options

Field	Description
General Settings	If checked, the user allows access to the General Settings section. The General Settings section of the Operations Monitor Settings dialog box allows the user to view the status of the Operations Monitor server, configure date and time, update the Operations Monitor software or license, view properties of the currently installed license and execute some system-wide actions.
Changing of platform settings	If checked, the created user is allowed to access the Platform Settings section in the Operations Monitor settings dialog.
Changing of prefix tags	If checked, the user is allowed to change the number prefix tags in the Platform Settings. However, the user will still be able to view them even without this permission.
Create users	If checked, the created user is allowed to create and manage new users himself using the User Management section of the Operations Monitor settings dialog.
Grant create users	If checked, the created user can grant the 'Create users' permission described above.
View/Edit all users	If checked, the user is able to see and modify users created by other users.
Create roles	If checked, the user is able to view and modify the roles management section in the user management folder. For more information, see Role Management .
Changing of external devices	If checked, the created user is allowed to access the External Devices section in the Operations Monitor settings dialog.
Changing the system settings	If checked, the created user is allowed to access the Settings section in the Operations Monitor settings dialog.
Modify realms	If checked, the created user is able to view and modify the realms management section of the settings. If the user is assigned a realm, on a previous screen, he will only be able to modify realms that intersect or are contained within the user's own realm.
Set SNMP Export for custom KPIs	If checked, user can export the selected metric/KPI via SNMP.

This table describes the user interface setting options.

Table 7-20 User Interface Settings Options

Field	Description
View SIP messages	If checked, the created user can see only the SIP message headers in the messages tab of the Call Details window and in the Registration Details window. For more information, see Calls and Registrations .
View SIP message details	If checked, the created user can view SIP message bodies in the messages tab of the Call Details window and in the Registration Details window. For more information, see Calls and Registrations . Message bodies cannot be captured in packet capture downloads unless they are set as viewable to the user.
View Media Info	
Create PDF reports	If checked, the new user can create PDF call reports on the Calls page. For more information, see Calls .
View registration history	If checked, the new user is allowed to see the registration history of a platform user in the User Tracking page. For more information, User Tracking .
View Subscriptions in User Tracking	
Incremental User Search	If checked, the new user is allowed to use the incremental user search on the User Tracking page. For more information, User Tracking .
Read the Session Monitor manual	If checked, the new user is allowed to see the online version of the Operations Monitor User's Guide.
Change the dashboard page	If checked, the new user is allowed to add and remove items from the Dashboard page.
May always log in	If checked, the new user is always allowed to log in, even if the concurrent session limit for one user or the global concurrent session limit is surpassed. In case the global concurrent session limit is surpassed, another user will be logged out in order to allow this user to log in.
Save calls	If checked, the new user is allowed to save calls for further debugging.
View saved calls from other users	If checked, the new user is allowed to view the saved calls created by other users.
View all realms	If checked, the new user is allowed to view all the realms not only the ones created by itself.
RTP Header Recording	If checked, the new user is allowed to record the header part of RTP packet in a call.
RTP Payload Recording (including DTMF)	If checked, the new user is allowed to record the entire RTP packets of a call. This includes audio, video, and image data, voice quality data, and DTMF tones.
RTCP Recording	If checked, the new user is allowed to record RTCP voice quality data.

Table 7-20 (Cont.) User Interface Settings Options

Field	Description
View DTMF Tones	If checked, the new user is allowed to view DTMF tones in the call flow diagram and to see the presence of DTMF tones in a call in the calls grid.
KPI Management	If enabled for a user, then the user can access the KPI Management page to create, edit and modify the custom templates.
Expand KPI	A user with this permission can create or enable the custom user KPIs. A user without this permission will not be able to create that counter for a device or tag type or any KPI in platform wide list or the Bulk KPI page. An error message is displayed.
Shrink KPI	Users with this permission can delete the custom user KPIs.
UCaaS CCaaS Calls Settings	This user permission defines whether the user can view and modify the UCaaS CCaaS Settings or not.

User Realm

The second step sets the realms that the future user will be able to access.

A user assigned to a realm can only see devices that are also assigned to that realm. Users assigned to the realm **ALL** are unrestricted and can see all devices, regardless of the realm the device is assigned to. For more information about the realm concept in Operations Monitor, see [Realms](#)

On the **KPI/Metrics** page, users also only see the devices listed in their assigned realm. For more information, see [KPI/Metrics](#)

A user can access either one or **ALL** the realms.

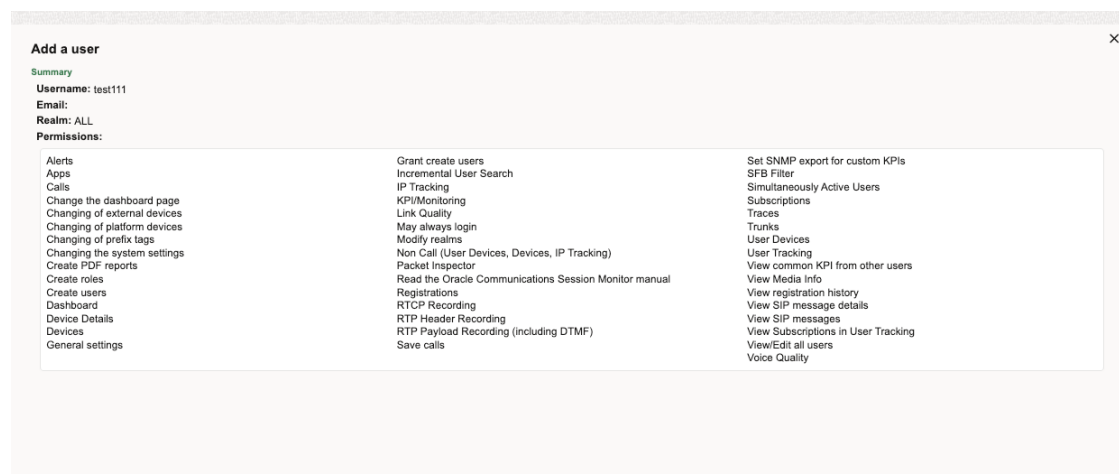
Figure 7-82 Setting Realm for a New User

The screenshot shows a web interface for adding a user. The title is "Add a user" with a close button (X) in the top right. Below the title, the section "Realms" is highlighted. The instruction "Select a realm for the user from the list" is followed by a label "Realm:" and a dropdown menu. The dropdown menu is open, showing a list of realms: "ALL", "realm_for_admin", "realm_for_user_0", "realm_for_user_1", "realm_for_user_2", "realm_for_user_3", "realm_for_user_4", "realm_for_user_5", "realm_for_user_6", "realm_for_user_7", and "realm_for_user_8".

Overview Information

The summary screen gives a brief overview of the new user. Included is the username, email address (if entered), role, realm and permissions bitmask.

Figure 7-83 Summary of the New User



Requirements for RADIUS Authentication

When a user logs in, Operations Monitor supports RADIUS authentication if it has been enabled in the **RADIUS Authentication** section of the Settings dialog box. RADIUS authentication is performed if it has been enabled for the user.

For RADIUS authentication to work, the RADIUS server has to respond to the Operations Monitor access request sent with the set of required user attributes. Operations Monitor sends its access request with a configurable **NAS_Identifier** attribute, which can be used to identify requests from Operations Monitor on the server side, and with the encrypted password as the **Password** attribute. Upon successful authentication, Operations Monitor expects the following user attributes:

Table 7-21 RADIUS Authentication User Attributes

Attribute	Description
PLD-User-First-Name	Not applicable.
PLD-User-Last-Name	Not applicable.
PLD-User-Email	(Optional) The e-mail address of the user.
PLD-User-Realm	The integer realm ID of the user's realm.
PLD-User-Creator	The user ID of the parent user for the user.
PLD-User-Permissions	A bitmask describing the permissions of the user.
PLD-User-Logo	(Optional) A field containing the logo image for the user.
PLD-User-Options	A JSON-encoded object describing per user options.

The numeric IDs for these user attributes are defined in a RADIUS dictionary file, which is delivered together with Operations Monitor.

Note

The **PLD-User-First-Name** and **PLD-User-Last-Name** fields in the radius definition are not used.

The **PLD-User-Permissions** attribute deserves special explanation. It contains a bitmask describing the permissions that a user has. Each of the permissions introduced above has a position in the bitmask. To generate a specific permissions bitmask you can use the wizard for adding users (choose **RADIUS authentication** on the first page of the wizard, then select the appropriate permissions, and the permissions bitmask will be displayed on the last page of the wizard).

Role Management

Note

User Roles cannot work together with RADIUS Authentication.

In this folder of the Operations Monitor settings, the user roles are administered to define default sets of permissions for users. It is not required to assign a role to a user, however it is recommended as it simplifies the user creation process.

For instance an administrator role would generally contain all permissions, a power user may contain most screens and a subset of system permissions, and a basic user a subset of screens. During the user creation process if a role other 'custom' is selected, then later on the individual permission check boxes will be skipped.

Note

Regarding role management, the terms *permissions* and *rights* are used interchangeably.

Figure 7-84 Roles

	Role
☐	Administrator
☐	User Administrator
☐	R1
☐	R2

Note

By default, the roles feature is disabled. In order to make use of the roles, the **User Roles** system setting must be enabled. For more information, see [Enable User Roles](#).

Adding a Role

Adding a role is performed after selecting the **Add a new role** button. As shown in the images below, this is equivalent to the permissions screens of adding a new user, however after setting the permissions there is a prompt for the role name, the role name is mandatory.

Figure 7-85 Setting Permissions for Modules for a New Role

Create a new user role

Permissions for Modules
Check the boxes of the modules the user will be permitted to use

General ☒ Dashboard ☒ Traces ☒ Alerts ☒ Packet Inspector ☒ Apps ☐ Read Only Dashboard	Operations ☒ KPI/Monitoring ☒ Calls ☐ Calls Field Permission ☒ Voice Quality ☒ Registrations ☒ Subscriptions ☒ Non Call (User Devices, Devices, IP Tracking) ☒ User Devices ☒ Trunks ☒ Devices ☒ Device Details ☐ Number Alerting	Customer Experience ☒ User Tracking ☒ IP Tracking ☒ Link Quality ☒ Simultaneously Active Users ☒ SFB Filter	Control Plane Monitor ☒ IMSI Search ☒ Transactions ☒ KPI/Metrics ☒ Devices

Previous Next Finish Cancel

Figure 7-86 Setting Permissions for Settings for a New Role

Create a new user role

Permissions for Settings

Check the boxes of the settings the user will be permitted to modify

Settings	User Interface
☒ General settings	☒ View SIP messages
☒ Changing of platform devices	☒ View SIP message details
☒ Changing of prefix tags	☒ View Media Info
☒ Create users	☒ Create PDF reports
☒ Grant create users	☒ View registration history
☒ View/Edit all users	☒ View Subscriptions in User Tracking
☒ Create roles	☒ Incremental User Search
☒ Changing of external devices	☒ Read the Oracle Communications Session Monitor manual
☒ Changing the system settings	☒ Change the dashboard page
☒ Modify realms	☒ May always login
☒ Set SNMP export for custom KPIs	☒ Save calls
☐ UCaaS CCaaS Calls Settings	☐ View saved calls from other users
	☐ View all realms
	☒ RTP Header Recording
	☒ RTP Payload Recording (including DTMF)
	☒ RTCP Recording
	☐ View DTMF tones

Previous Next Finish Cancel

Figure 7-87 Setting the Name of the Role

Create a new user role

Role Name

Please enter a name for the role

Role

Required

Editing a Role

After selecting only one role, it may be edited by selecting the **Edit** option in the **role management** panel. When multiple roles are selected this option is not available.

Deleting a Role

Deleting a role may also only be performed after selecting a single role. There is a confirmation prompt that must be confirmed before the role is deleted.

Adding Rights to a Role

One can either add rights to a selected role or generally to all roles. In the **User Roles** dialog box, select the role which needs to be modified and click **Add Rights**. Select one of the two options:

- to selected roles
- to all roles

The following procedure is equivalent to the normal role dialog, only without the option to change the role name. The selected check boxes designate the rights that will be added to the selected role(s) or all roles.

Removing Rights from a Role

Likewise, one can remove rights from individual roles or generally across all roles. In the User Roles dialog box, select the role for which rights need to be removed, and click Remove Rights. Select one of the two options:

- from selected roles
- from all roles

Removing rights is the mirror process to adding rights, with the selected check boxes will be removed from the selected role(s) or all roles.

Searching for a User Role

Using the search option, you can search for and filter User Roles.

The Search functionality helps administrators locate specific roles by applying search keywords as role name. It makes it easier to manage large systems with numerous users. The search tool enhances productivity by reducing the time spent manually sorting through roles.

External Authentication Authorization

The Mediation Engine Connector supports authenticating users using an external authentication provider, such as LDAP, RADIUS. This authentication must be configured on the reverse proxy (NGINX or Apache), which acts as a gateway for the Mediation Engine. Authorization for the user must be done using Mediation Engine permissions, as described in the section, "[Add a New User](#)".

External authentication is controlled by the system setting, **External authentication enabled**. When enabled, the *X-Forwarded-User* HTTP header set by the reverse proxy must contain the authenticated user's login name.

Password Settings

In this folder of the Operations Monitor settings, you can define the password settings that are followed by users.

To modify the password settings:

1. From the Settings screen, click **Password Settings**.
2. To enforce users to change their password regularly, set the time period by doing the following:
 - a. Select **Force users to change their password regularly**.
 - b. Enter the number of days in the **Period in days to force password change for users with access to sensitive data** field. The default setting is 90 days
 - c. Enter the number of days in the **Period in days to force password change for users without access to sensitive data** field. The default setting is 180 days.

- d. Click **Save** to save the changes or click **Cancel**.

Note

The entries in these fields are applied when the user changes the password next time.

3. Enforce stringent password rules by doing the following:

- a. Select **Enforce stringent password rules** to increase the level of security required in user passwords.

Note

A stringent password:

- Should not begin with a digit
- Must contain at least one uppercase letter
- Must contain at least one lower case letter
- Must contain at least one digit
- Must contain a special character such as @, #, \$, -, _
- Must be different from the previous password

The account locking is enabled.

- b. By default, the account gets locked after three unsuccessful attempts for 15 minutes. To change the default account locking time, open the **/opt/oracle/ocsm/etc/iptego/vsp.local.conf** file. Add a line in the vsp.local.conf file. For example:

```
[usermanagement]
unlock_admin_timeout = 600
```

The value for the unlock_admin_timeout key indicates the time in seconds after which accounts get unlocked.

- c. Click **Save**.

Enabling or Disabling User Accounts

To enable or disable the user accounts:

1. Login to Operations Monitor as admin.
2. From **Settings**, click **User Management**.
3. Select the user you want enable or disable the account and click **Edit**.
4. Do one of the following:
 - To enable the suspended user account:
 - a. Deselect the **Account disabled** check box and click **Next**.

The Permission for Modules screen appears.

- b. Assign the required permissions for modules by selecting the check box and click **Next**.
The permissions for Settings screen appears.
 - c. Assign the required permissions for settings by selecting the check box and click **Next**.
The Summary screen appears.
 - d. Verify the summary and click **Finish**.
The user account is enabled.
- To suspend an user account:
 - a. Select the **Account disabled** check box and click **Next**.
The Permission for Modules screen appears.
 - b. Click **Next**.
The permissions for Settings screen appears.
 - c. Click **Next**.
The Summary screen appears.
 - d. Verify the summary and click **Finish**.
The user account is disabled.

View Logged in Users in the Mediation Console

As a privileged Linux user with *root* access, you can run the `palladion-print-logged-users` CLI command from the Mediation Engine console to view the users who are currently logged in.

To view the logged in users:

1. Log in with root access to the Mediation Engine console.
2. Run the command: `palladion-print-logged-users`.

The list of users who are currently logged in is displayed on the console.

Log Out Users in the Mediation Engine Console

As a privileged Linux user with *root* access, use the `palladian-logout-user` CLI command to log out a specific user or users using the Mediation Engine console.

To log out a user in the Mediation Engine Console:

1. Log in with root access to the Mediation Engine console.
2. Use the following command to log off a user or multiple users:
 - Syntax:
`palladian-logout-user <user name>`

`palladian-logout-user <user name>`

A list containing the user names along with the number of users logged out is displayed on the console.

8

Call Merging Algorithms

Oracle Communications Operations Monitor has the ability to find the *call legs* of the same call. This is an essential feature for troubleshooting and for providing deep device visibility and accurate statistics. While in the case of some SIP devices (like Proxies and B2BUAs that keep the **Call-ID** header) finding the matching call legs is easy, many other devices change most of the fields from the incoming leg for purposes like topology hiding, decoupling, and interoperability. This makes the call merging problem hard and impossible to solve in all cases with a single algorithm.

Operations Monitor gives the network operator the power to adjust the call merging algorithm by providing a comprehensive list of *tests* and a flexible way to combine them in **call merging** algorithms. This section describes the available tests and how to write the algorithms. The resulting scripts can be entered in the **Platform Devices** section for *SBC/B2BUA* devices by choosing the **Use custom algorithm** option.

The call merge algorithms always return a single Boolean value: **true** if the *call legs* are part of the same *call*, and **false** otherwise. They provide ordered tests, tests with parameters, and nested decisions trees. To keep the real-time nature of Operations Monitor, the tests are implemented natively in the Operations Monitor core, and the algorithms are compiled to an internal representation which can be executed with maximum performance.

This chapter also contains links to KM notes that describe how to enable various types of call merging and call correlation. For more information, see "[Merging and Correlating Calls](#)".

Note

When call correlation is based on the correlation algorithm of a device, an incoming leg can be correlated with multiple outgoing legs. An outgoing leg, however, can be correlated to only one incoming leg.

For global call correlation based on the SIP Call ID, the restriction for outgoing legs does not apply. Call ID based correlation can be enabled with the **Merge globally by Call ID** setting in **System Settings** under **System Management** on the Settings page. For more information on this setting, see [List of System Settings](#).

Merging and Correlating Calls

This section contains links to KM notes that describe how to enable various types of call merging and call correlation. For more information, see the KM note located at: <https://support.oracle.com/epmos/faces/DocumentDisplay?id=1638050.1>

For information on call merging and call correlation using the Replaces parameter, see the KM note at: <https://support.oracle.com/epmos/faces/DocumentDisplay?id=2012218.1>

Syntax

Syntax wise, they are formed from a single LISP expression. Apart from the tests, there is only the special function `cond`, and two terminals:

- `#t` for true.
- `#f` for false.

The LISP `cond` function accepts an arbitrary number of arguments. Each argument is a list of two elements: a **condition** and a **result**.

```
(cond
  (condition1 result1)
  (condition2 result2)
  ...
  (conditionN resultN)
)
```

The conditions are evaluated in order, and for the first being **true**, the result is returned:

if condition1 is **true** return result1, **else if** condition2 is **true** return result2, **else if** ...; **else if** conditionN is **true** return resultN.

If none of the conditions is **true**, then **false** is returned for the whole expression, as a convenience.

Usually in *call merging algorithms*, the conditions are tests and the results are terminals:

```
(cond
  (test1 #t)
  (test2 #t)
  (test3 #f)
  (test4 #t)
)
```

But the result does not have to be a terminal. For example, this is a possible **AND** statement:

```
(cond
  (test1 test2)
)
```

The result part can also be another `cond` expression for providing nested tests:

```
(cond
  (test1 (cond
            (test2 #t)
            (test3 #t)
          ))
  (test4 #t)
)
```

The above example translates in the following pseudo-code:

```
if test1:
  if test2:
```

```
        return True
    elif test3:
        return True
    else:
        return False
elif test4:
    return True
else:
    return False
```

The tests can accept an arbitrary number of parameters which have to be provided right after the test name, for example:

```
(cond
  (test1 param1 param2)
)
```

translates to:

```
if test1(param1, param2):
    return True
else:
    return False
```

The parameters can be strings, integers, or list of strings:

```
(test "string" 12 ("list" "of" "parameters"))
```

Line comments can be inserted by using the semicolon symbol:

```
; this is a comment
```

Tests Reference

This section lists the tests available for custom call merging algorithms.

`call_id ([suffix])`

Returns #t if the **Call-ID** headers of the two *call legs* are equal.

Parameters:

suffix - If this parameter is provided and it is non-zero, then only the last suffix characters are compared from the two **Call-ID** headers, and if they are equal, it returns #t.

Example:

```
(call_id 12)
```

returns #t if the last 12 characters from the **Call-ID** headers are equal.

hf_equals (*header*)

Returns #t if the values of the header whose name is given as a parameters are equal in the two call legs. The header name is case-insensitive.

For example, the following snippet returns #t, if the INVITE messages from both call legs contain a header named **Session-ID** and their values are equal:

```
(hf_equals "Session-ID")
```

hf_any_equals (*headers*)

Like hf_equals, but compares any header value in headers list with any header value from the second call; for a more complete example what this means see also uri_user.

hf_any_equals_all (*headers*)

This function is like hf_any_equals, but differs in the way that it treats the case where a header field contains a list of values, either separated by commas or in several header field rows with the same field name. In that case hf_any_equals will use only the first header field row with a given field name and use the entire row as one value, whereas hf_any_equals_all will try to match each individual element of the list.

hf_equals_prefix (*length*, *header*)

Limits the comparison performed by hf_equals to length characters from the beginning of the header value.

hf_param_equals (*header*, *param*)

Works like hf_equals but compares only the value of the named param.

hf_uri_param_equals (*header*, *param*)

Returns #t if the values of the named URI parameter of the specified header are equal in the two call legs. The header name is case-insensitive.

Example 8-1 Example

```
(hf_uri_param_equals "From" "x-to")
```

```
From: <sip:7788864164@10.0.0.8:5060;x-to=0702>;tag=00511620-9759-194F-  
A7CD-0DC114A3AA77-9534047
```

Here x-to is a URI parameter so we have to use the hf_uri_param_equals algorithm in order to correlate the two call legs.

sdp_media_ip_port ()

Returns #t if the SDP bodies from the initial INVITE messages of the two call legs contain the same media IP address and UDP port number in the first media description.

This is usually a good indicator, if the *B2BUA* device does *not* relay media.

sdp_session_id ()

Returns #t if the *SDP* bodies from the initial INVITE messages of the two call legs contain the same non-zero session ID.

time_diff (interval1, interval2)

Returns #t if the time difference between the two legs is smaller than the accepted intervals.

Parameters:

- **interval1** - The maximum time difference between the initial INVITE message of incoming call leg and the initial INVITE of the outgoing call leg.
- **interval2** - The maximum time difference between the initial INVITE message of outgoing call leg and the initial INVITE of the incoming call leg.

For example, the following code returns #t if the outgoing leg comes after the incoming leg with more than 15 seconds, **or** if the incoming leg comes after the outgoing leg with more than 2 seconds:

```
(time_diff 15000 2000)
```

Note

The maximum value that you can use for the **time_diff** function is the same as the Operations Monitor system settings. Where,

- The maximum value for **B2B incoming backlog search for merging** is 5 seconds.
- The maximum value for **B2B outgoing backlog search for merging** is 1800 seconds.

If you do not include the **time_diff** function in your algorithm, your Operations Monitor **B2B incoming backlog search for merging** and **B2B outgoing backlog search for merging** system settings are used.

Note

The **time_diff** function is treated differently than the others within the call correlation algorithm. It is considered for each correlation regardless of its position inside the algorithm.

uri_user (suffix, list_of_headers)

Returns #t if the user part of any of the *URIs* is specified in the *list_of_headers* matches.

Parameters:

- **suffix** - If non-zero, only the last *suffix* characters from each URI is compared with the rest. URI length must be at least this size.

- **list_of_headers** - A list containing the headers from which to extract the URI usernames to compare. A set of shortcuts are defined:
 - **ruri** - Request-URI.
 - **from** - From header URI.
 - **to** - To header URI.
 - **diversion** - Diversion header URI.
 - **pai** - P-Asserted-Identity URI.
 - **ppid** - P-Preferred-Identity URI.
 - **rpidd** - Remote-Party-ID URI.

The URIs are compared in all possible permutations. For example, this snippet:

```
(uri_user 6 ("from" "pai"))
```

compares:

- The **From** user from leg 1, with the **From** user from leg 2.
- The **From** user from leg 1, with the **P-Asserted-Identity** user from leg 2.
- The **P-Asserted-Identity** user from leg 1, with the **From** user from leg 2.
- The **P-Asserted-Identity** user from leg 1, with the **P-Asserted-Identity** user from leg 2.

Similarly, the following snippet makes at most 9 comparisons:

```
(uri_user 6 ("to" "ruri" "diversion"))
```

In addition to the specified shortcut header names, URIs can be also specified by the name of the header containing them.

For example, the following expression returns #t if the last 7 characters from the username of the first **Contact** header from both calls are equal:

```
(uri_user 7 ("Contact"))
```

The header name is case-insensitive.

uri_user_max(suffix, list_of_headers)

The same as uri_user function, but it tries to match the call if a string is shorter than the *suffix*. For example, phone numbers **5551234** and **1234** will match, even if the suffix is **6**.

uri_user_all(suffix, list_of_headers)

This function behaves in the same way as uri_user , except that if one of the relevant headers of one the call legs contains more than one URI, then all of these URIs are used for comparison, whereas uri_user would only use the first. Therefore if in the example:

```
(uri_user 6 ("from" "pai"))
```

one leg contains one **P-Asserted-Identity** and the other three, then up to 8 comparisons will be performed.

uri_user_all_max (suffix, list_of_headers)

As uri_user_max , but treats lists in header fields in the same way as uri_user_all.

cxpn_uri (suffix, list_of_headers)

Matches an in- with an out-going call comparing all possible header permutations like uri_user. It also supports ISUP *cdpn* and *cgpn* and allows for cross matching of SIP and ISUP calls.

Parameters:

- **suffix** - If non-zero, only the last *suffix* characters from each URI is compared with the rest. URI length must be at least this size.
- **list_of_headers** - In addition to the values supported by uri_user, cxpn_uri also supports:
 - **cdpn** - Matching on the callee.
 - **cgpn** - Matching on the caller.

cxpn_uri_max (suffix, list_of_headers)

The same as cxpn_uri function, but it tries to match the call if a string is shorter than the *suffix*. For example, phone numbers **5551234** and **1234** will match, even if suffix is **6**.

cxpn_uri_all (suffix, list_of_headers)

Variants of cxpn_uri that use all URIs if a header of the SIP leg contains several, just as uri_user_all.

cxpn_uri_all_max (suffix, list_of_headers)

Same as cxpn_uri_max, but treats lists in header fields in the same way as uri_user_all.

cdpn (suffix)

Like uri_user, but matches only on the callee.

cgpn (suffix)

Like uri_user, but matches only on the caller.

Test Usage Limitations

Depending on the kind of device that is used for matching, different sets of test functions are available:

- **B2BUA**
Supports SIP matching which comprises these tests: *call_id*, *uri_user*, *time_diff*, the *hf_equals* family of tests and *sdp_session_id* as well as *sdp_media_ip_port*.
- **STP**

Supports ISUP call matching with `cdpn`, `cgpn` and `time_diff` as tests.

- **SGW**

Supports all the tests available for the other two device types and the `cxpn_uri` test.

Examples

The following examples describe how to create an algorithm using the test references.

Match by the Caller and the Callee

The following algorithm matches two call legs if:

- The last 6 characters of caller are equal, as found in either the **From** header or in the *P-Asserted-Identity*,
- **And** the last 6 characters of the callee are equal, as found in either the **To** header or in the *Request-URI*.

```
(cond
  ((uri_user 6 ("from" "pai"))
   (uri_user 6 ("to" "ruri")))
)
```

The following example modifies the one above to return **true**, if either the caller or the callee matches:

```
(cond
  ((uri_user 6 ("from" "pai")) #t)
  ((uri_user 6 ("to" "ruri")) #t)
)
```

Match by Generic Algorithm

The following algorithm is an example of a *generic* algorithm, which should give good results for a wide range of SIP devices.

```
(cond
  ((call_id 0) #t)
  ((sdp_media_ip_port) #t)

  ; custom header
  ((hf_equals "session-id") #t)

  ((time_diff 15000 2000) #f)

  ; Matching by from and to
  ((uri_user 6 ("from" "pai" "rpid" "ppid"))
   (cond
     ((uri_user 6 ("to" "ruri" "diversion")) #t)
     (#t #f)
   )
  )

  ; nothing matched, return false
  (#t #f)
```


)

The above algorithm:

- Checks first the **Call-ID**. If the two call legs have the same **Call-ID** header, then it returns **true**.
- Checks the **SDP** bodies. If the two call legs have the same media IP and port number, or if the session ID are equal, then it returns **true**.
- Checks if the custom **Session-ID** header is present in both call legs, and if their values are equal, then it returns **true**.
- Checks if the start time stamps of the two call legs are too far one from each other, and if so, returns **false**.
- Checks if both the caller and the callee match, by comparing the URIs from several headers. If a match is found for both of them, it returns **true**.

If none of the above is **true**, it returns **false**.

9

Implementing Apps

Apps provide an easy way to extend Oracle Communications Operations Monitor with analytical capabilities that are not present in the user interface. Apps can query information from Operations Monitor, process this information, and store results in an output table.

Structure of an App

A valid Operations Monitor extension app consists of a Python 3.9 module and of an app specification file, that declares the parameters of the app and the schema of the app's result table. The Python module file and the app specification file must be packed into a ZIP archive, containing no other files and no directories. Such a ZIP archive can be uploaded to Operations Monitor as described in [Apps](#).

Further requirements for the app module and the app specification file apply. The app module must contain a **run** function with the following signature:

run (facade, params)

Parameters:

- **facade**
An instance of **libpalladion.scripting.Facade** which provides access to the Apps API.
- **params**
A dict instance which represents the parameters supplied to the app.

This function is called by Operations Monitor when the app is executed from the web interface or via remote procedure calls.

The app specification file must be an XML file which complies with the Operations Monitor app-specification DTD cited below:

```
<!DOCTYPE script [  
<!ELEMENT script (param-spec?,result-schema?)>  
<!ATTLIST script xmlns CDATA #FIXED "http://iptego.de/palladion/script-spec">  
<!ATTLIST script name CDATA #REQUIRED>  
<!ATTLIST script description CDATA #IMPLIED>  
<!ATTLIST script result-type (custom|calls) #REQUIRED>  
  
<!ELEMENT param-spec (param+)>  
  
<!ELEMENT param EMPTY>  
<!ATTLIST param name CDATA #REQUIRED>  
<!ATTLIST param label CDATA #REQUIRED>  
<!ATTLIST param type (string|datetime|numeric) #REQUIRED>  
<!ATTLIST param required CDATA #IMPLIED>  
<!ATTLIST param default CDATA #IMPLIED>  
  
<!ELEMENT result-schema (column+,primary-key?,unique-key*)>  
  
<!ELEMENT column EMPTY>  
<!ATTLIST column name CDATA #REQUIRED>  
<!ATTLIST column type CDATA #REQUIRED>
```

```

<!ATTLIST column null (true|false) #IMPLIED>
<!ATTLIST column auto-increment (true|false) #IMPLIED>
<!ATTLIST column default CDATA #IMPLIED>

<!ELEMENT primary-key EMPTY>
<!ATTLIST primary-key columns NMTOKENS #REQUIRED>

<!ELEMENT unique-key EMPTY>
<!ATTLIST unique-key name CDATA #REQUIRED>
<!ATTLIST unique-key columns NMTOKENS #REQUIRED>
]>

```

The top-level **script** element is used to configure some important properties of an app. Its **name** attribute specifies a name for the app which is displayed in the **Available Apps** table. The **description** attribute can contain a longer description for the app. Most importantly, the **result-type** attribute specifies what kind of result table the app will have. It can be either **custom**, in which case you must specify the result table in the **result-schema** element, or **calls**, in which case the result table is fixed as a calls table.

The **param-spec** element is a container for parameter specifications declared by the **param** element. Parameter specifications are used by the web interface to generate the right kind of parameter entry dialog when an app is started. The **name** attribute of the **param** element specifies the name of the parameter, that is passed to the app. The **label** attribute specifies a label that is displayed in the parameter entry dialog. The **type** attribute specifies how the parameter entry is rendered in the parameter entry dialog. The **required** attribute decides whether the parameter must be entered or can be left blank. The **default** attribute specifies a default value, that is filled into the parameter entry.

The **result-schema** element is used to specify a schema for the result table of the app. This is required when the **result-type** attribute of the main **script** element is set to **custom**. The contents of the **result-schema** element are translated into an SQL CREATE TABLE statement. You can specify columns in the result table, as well as a primary key and multiple unique keys. The **column** element specifies a column. The **name** attribute gives the name of the column. The **type** attribute specifies the type of the column. It can contain any of the data type specifications valid in MySQL. For more information, see the *Create Table Syntax* in the *MySQL 5.0 Reference Manual*:

<http://dev.mysql.com/doc/refman/5.0/en/create-table.html>

The **null** attribute decides whether the column is nullable or not. The **auto-increment** attribute specifies whether the column can be filled via auto increment on insert. The **default** attribute gives a default value for the column. The **primary-key** element declares a primary key for the result table. Its **columns** attribute is a list of columns that make up the primary key. The **unique-key** element declares a unique key in the result table. Its **name** attribute gives the name for the unique key. Its **columns** attribute is a list of columns that make up the unique key.

Apps API

class libpalladion.scripting.Call (facade)

This class represents a call in Operations Monitor. For general information on how Operations Monitor handles calls, see "[Calls](#)".

[Table 9-1](#) describes the fields for the Call class.

Table 9-1 Call Class Fields

Field	Type	Description
id	String	Indicates the ID of the call.
nlegs	Integer	Indicates the number of legs in the call consists of.
state_msg	String	Indicates the call state. The available call states are: • Unauthorized • Proceeding • Ringing • Established • Finished • Timed out • Error • Failed • Closed by CleanBye • Not found • Moved • Off-line • Busy • Canceled
state_details	String	Indicates an additional description of the call state.
setup_start_ts	String, Integer	Indicates a timestamp specifying when the call was initiated.
setup_time	Integer	Indicates the time in milliseconds taken for the call to reach the Established state. Note: Only available if state_msg equals Established .
call_time	Integer	Indicates the duration of the call in milliseconds for which the call was in the Established state. Note: Only available if state_msg equals Finished .
code	Integer	Indicates the final response code of the INVITE transaction associated with the call.
src_user	String	Indicates the user creating the call. This is usually taken from the From header field of the first <i>call leg</i> .
src_ua	String	Indicates the user agent for the caller.
src_codecs	String	Indicates the comma separated list of codecs proposed in the SDP body by the UAC in the INVITE message. Example: On each re-INVITE from inside the dialog, this field is updated to the last proposed list of codecs. This is useful for detecting T.38 calls.

Table 9-1 (Cont.) Call Class Fields

Field	Type	Description
src_initial_codecs	String	Indicates the comma separated list of codecs proposed in the SDP body by the UAC in the first INVITE message. Note: This field is not updated at <i>re-INVITES</i> .
src_ip	String	Indicates the IP address of the caller.
dst_user	String	Indicates the user to which the call is addressed. This is usually taken from the To header field of the first call leg.
dst_ua	String	Indicates the user agent string for the callee.
dst_codecs	String	Indicates the comma separated list of codecs proposed in the SDP body by the UAS. On each <i>re-INVITE</i> from inside the dialog, this field is updated to the last proposed list of codecs.
dst_initial_codecs	String	Indicates a comma separated list of codecs proposed in the SDP body by the UAS, usually in the first INVITE message. This field is not updated at <i>re-INVITES</i> .
dst_ip	String	Indicates the IP address of the callee if the call was successful.
term_devs	String	Indicates a comma separated list of device IDs for devices that this call has an inbound leg to.
init_devs	String	Indicates a comma separated list of device IDs for devices that this call has an outbound leg from.
ingress_devs	String	Indicates a comma separated list of ingress devices for this call.
egress_devs	String	Indicates a comma separated list of egress devices for this call.
traversing_devs	String	Indicates a comma separated list of traversed devices for this call.
gateway_devs	String	Indicates a comma separated list of gateway devices for this call.
MOSlqe_avg	Float	Indicates the average MOSlqe value for all the relevant streams in the call.
MOSlqe_min	Float	Indicates the minimum MOSlqe value of all the stream chunks associated with the call.
end_ts	Integer	Indicates the timestamp of the message that closes the main leg of the call (usually the first BYE message).

Table 9-1 (Cont.) Call Class Fields

Field	Type	Description
reason_hdr	String	Indicates the content of the Reason field from the BYE, CANCEL, SIP request, or from a failure SIP reply.
pai	String	Indicates the content of the P-Asserted-ID header from the initial INVITE SIP request.
rpidd	String	The content of the Remote-Party-ID or P-Preferred-Identity header from the initial INVITE SIP request.
megaco_mg_ip	String	Indicates the IP address of the MEGACO Gateway.
megaco_mgc_ip	String	Indicates the IP address of the MEGACO Gateway Controller.
megaco_termination_id	String	Indicates a MEGACO TerminationID defined for a PSTN line, a channel in a Trunk, or RTP stream. Format is a string. For example, line/1 or rtp/1 for RTP streams.
megaco_cmds	String	Indicates the commands placed by the MEGACO Gateway Controller to the MEGACO Gateway in a transaction. For example, Commands exist to add, modify, and subtract Terminations from the Context.
megaco_txids	String	Indicates a MEGACO Transaction is identified by a Transaction ID.
mgcp_mg_ip	String	Indicates the IP address of the MGCP Gateway.
mgcp_mgc_ip	String	Indicates the IP address of the MGCP Media Gateway Controller.
mgcp_capabilities	String	Defines the capabilities of the endpoints.
mgcp_connection_ids	String	Indicates the connection identifier that is encoded as a hexadecimal string, at most 32 characters in length.
mgcp_call_ids	String	Indicates the hexadecimal strings of maximum of 32 characters that identify uniquely a call.
opc	String	Originating Point Codes (OPC) contains the address of the originator for the ISUP call. This is always taken from the first ISUP leg seen by Operations Monitor.
dpc	String	Destination Point Codes (DPC) contains the address of the destination for the ISUP call. This is always taken from the first ISUP leg seen by Operations Monitor.

Table 9-1 (Cont.) Call Class Fields

Field	Type	Description
q850_code	Integer	Q.850 cause code for the ISUP call.
q850_state_msg	String	Q.850 State for the ISUP call.
q850_state_details	String	Q.850 Details for the ISUP call.
merged_into_call_id	Integer	If the call has been merged into another call, then this is the id of that call.
rtcp_streams	Integer	Indicates the number of RTCP streams belonging to the call.
rtcp_delay_max	Integer	Indicates the maximum round-trip delay time reported by RTCP.
rtcp_delay_avg	Integer	Indicates the average round-trip delay time reported by RTCP.
src_user_pref_tag	Integer	Indicates the number of the caller determined by the configurable number determination mechanism, if available.
dst_user_pref_tag	Integer	Indicates the number of the callee determined by the configurable number determination mechanism, if available.
setup_delay	Integer	Indicates the number of the callee determined by the configurable number determination mechanism, if available.
setup_delay	Integer	This field represents the time elapsed between the initial 'INVITE' message and the first valid network response, like '180 Ringing', '183 Session in progress', '480 Temporarily Unavailable', etc. It fulfills Session Request Delay for RFC6076. If the call contains ISUP, Setup Delay is computed on the first SIP leg. This field has a precision of milliseconds. By default, this column is hidden.
setup_delay_type	Integer	Shows the type of Setup Delay computed. Available options are: • Successful Session Request Delay • Failed Session Request Delay By default, this column is hidden.
diversion	String	Diversion URI of first Diversion header in call.

Table 9-1 (Cont.) Call Class Fields

Field	Type	Description
diversion_type	String	Diversion type of first Diversion header in call. Possible values are: • deflection (CD) • do-not-disturb (DND) • follow-me • no-answer (CFNA) • time-of-day (CFTOD) • unavailable (CFUNV) • unconditional (CFUNC) • unknown: for unknown and all cases that could not be matched to any of the above • user-busy (CFB) • out-of-service
transfer	Integer	True, if this call has been transferred using the call transfer capabilities in SIP.
dtmf	Integer	Displays Yes if there is DTMF information available for this call. Unless the user has the correct rights this field will not be available.
media_types	String	Indicates the media types that were negotiated in the call. Multiple media types are separated by a comma (for example: audio, video).
getLegs ()		Query legs that belong to this call. Note that this method works only for calls that are in the permanent history (that is, finished for more than 15-20 seconds). Return type: QueryIterator over Leg instances.
getMessages (filter=[])		Query all SIP messages, that belong to this call. Note that this method works only for calls that are in the permanent history (that is, finished for more than 15-20 seconds). Return type: QueryIterator over Message instances.
getOneWayAudio (filter=[], keys={}, orderBy=[])		Query all voice quality information, that belong to this call. Return type: Integer Values: • 0: No audio. • 1: There is a media leg with audio only in one direction. • 2: All media legs with two way audio.

Table 9-1 (Cont.) Call Class Fields

Field	Type	Description
<code>getRawMessages (filter=[])</code>		Query all raw signaling messages, that belong to this call. Note that this method works only for calls that are in the permanent history (that is, finished for more than 15-20 seconds). Parameters filter - A filter specification to be applied to the queried RawMessage instances. Return type: QueryIterator over RawMessage instances.
<code>getVoiceQuality (filter=[], keys={}, orderBy=[])</code>		Query all voice quality information, that belong to this call. Parameters filter - A filter specification to be applied to the queried VoiceQuality instances. keys - Keys that the queried VoiceQuality instances must match. orderBy - Ordering specification. Return type: QueryIterator over VoiceQuality instances.
<code>getVoiceQualityChunks (filter=[], keys={}, orderBy=[])</code>		Query all voice quality information, that belong to this call. Parameters filter - A filter specification to be applied to the queried Chunk instances. keys - Keys that the queried Chunk instances must match. orderBy - Ordering specification. Return type: QueryIterator over Chunk instances.

`class libpalladion.scripting.Leg (facade)`

The Leg class represents a leg found by Operations Monitor. A leg is the portion of a call that happens between two given devices. [Table 9-2](#) describes the fields for the Leg class.

Table 9-2 Leg Class Fields

Field	Type	Description
<code>id</code>	Integer	Corresponds to the Call.id attribute of the associated call.
<code>state</code>	Integer	Indicates a numeric representation of the call state.

Table 9-2 (Cont.) Leg Class Fields

Field	Type	Description
state_msg	String	Indicates a string describing the call state. Following options are available: • Unauthorized • Proceeding • Finished • Timed out • Error • Failed • Closed by CleanBye • Not found • Moved • Off-line • Busy • Canceled
state_details	String	Indicates an additional description of the call state.
setup_start_ts	Integer	Indicates the timestamp of the first message (in seconds) in this leg.
setup_time	Integer	The time in milliseconds that the leg took to reach the Established state. Note: Only available, if state_msg equals Established .
call_time	Integer	Indicates the time in milliseconds that the leg was in the Established state. Note: Only available, if state_msg equals Finished .
code	Integer	Indicates the final response code in this leg.
src_user	String	Indicates the identifier of the caller.
src_uri	String	Indicates the URI of the caller.
src_ip	String	Indicates the IP address of the caller.
src_mac	String	Indicates the hardware address of the caller.
src_port	Integer	Indicates the port the caller is listening on.
src_ua	String	Indicates the user agent string of the caller.
dst_user	String	Indicates the identifier of the callee.
dst_uri	String	Indicates the URI of the callee.
dst_ip	String	Indicates the IP address of the callee.
dst_mac	String	Indicates the hardware address of the callee.
dst_port	Integer	Indicates the port the callee is listening on.

Table 9-2 (Cont.) Leg Class Fields

Field	Type	Description
dst_ua	String	Indicates the user agent string of the callee.
ruri	String	Indicates the request URI.
callid	String	Indicates the value of the Call-ID header.
from_tag	String	Indicates the value of tag parameter of the From header.
to_tag	String	Indicates the value of tag parameter of the To header.
transfer	List of Integer	Indicates the list of integer IDs of the calls that relate to this leg because of a call transfer
getMessages (<i>filter=[]</i>)	-	Query all SIP messages, that belong to this leg. Parameters filter - A filter specification to be applied to the queried Message instances. Return type: QueryIterator over Message instances.
getRawMessages (<i>filter=[]</i>)	-	Query all raw signaling messages, that belong to this leg. Parameters filter - A filter specification to be applied to the queried Message instances. Return type: QueryIterator over RawMessage instances.

class S6Transaction (facade)

The S6Transaction class represents a S6 transaction.

[Table 9-3](#) describes the fields for the Counter class.

Table 9-3 S6Transaction Class Fields

Field	Type	Description
sessionid	Integer	Indicates an unique identifier for the S6 transaction.
timestamp_msecs	Integer	Indicates a timestamp specifying the time since when the session is running.
imsi	String	Indicates a string used to identify the user of the S6 transaction.
command_code	Integer	The command code of the S6 transaction. For example for the command UPDATE_LOCATION the code would be 316. All the possible codes are defined in 3GPPTS 29.272 at the interface commands for S6a/S6d and S13.
msisdn	CHAR (16)	Identifies the subscription to a mobile network.

Table 9-3 (Cont.) S6Transaction Class Fields

Field	Type	Description
result_code	Integer	The numerical value of the Result-Code of the Diameter S6 transaction. For example 2001 for DIAMETER_SUCCESS.
result	TINYINT	The high-level result of the overall Diameter S6 transaction. For example 0 for Successful, 1 for Failed, or 2 for Timed out.
error_diagnostic	Integer	Shows information about possible errors that can appear in S6 transaction configuration.
origin_realms	String	Contains the realm of the originator of the Diameter messages of this transaction.
destination_realms	String	Contains the realm the messages of a Diameter transaction should be routed to.
visited_plmn_id	String	The decoded visited PLMN ID found in the transaction with the 3 digit Mobile Country Code (MCC) and 2 or 3 digit Mobile Network Code (MNC) as defined in TS 123000 at section 12.1.
rat_type	Integer	A numeric code used to identify radio access technology that is serving the UE. Defined in TS 29212 at section 5.3.31.
initiator_devices	SET	Comma-separated list of numerical device IDs of the initiator devices for the transaction, that is, of devices from where the transaction is started.
terminator_devices	SET	Comma-separated list of numerical device IDs of the terminator devices for the transaction, that is, of devices from where the transaction is ended.
traversed_devices	SET	Comma-separated list of numerical device IDs of the terminator devices for the transaction.

`class libpalladion.scripting.RegistrationEvent (facade)`

This class represents registration events found by Operations Monitor. For a general description of registration events in Operations Monitor, see "[Registrations](#)".

[Table 9-4](#) describes the fields for the Registration Event class.

Table 9-4 Registration Event Class Fields

Field	Type	Description
id	Integer	Indicates an unique ID for this registration event.
ts	Integer	Indicates the timestamp of the registration event.
realms	Integer	Indicates the realms bit mask for this registration event.
type	Integer	Indicates the type of the registration event.
type_msg	String	Displays an additional message associated with the type of registration event.
user	String	Indicates the identifier of the user that is associated with this registration event.
ip	String	Indicates the source IP address of this registration event.
dest_ip	String	Indicates the destination IP address of this registration event.
contacts	String	Indicates the content of the contact header of the REGISTER request.

Table 9-4 (Cont.) Registration Event Class Fields

Field	Type	Description
code	Integer	Indicates the response code for this registration event.
dev_id	Integer	Indicates the unique identifier of the device that handled the registration event.
getMessages (<i>filter=[]</i>)		Query all SIP messages, that belong to this registration event. Parameters filter - A filter specification to be applied to the queried Message instances. Return type: QueryIterator over Message instances.
getRawMessages (<i>filter=[]</i>)	-	Query all raw SIP messages, that belong to this registration event. Parameters filter - A filter specification to be applied to the queried RawMessage instances. Return type: QueryIterator over RawMessage instances.

class libpalladion.scripting.Message(facade)

This class encapsulates a single SIP message. [Table 9-5](#) describes the fields for the Message class.

Table 9-5 Message Class Fields

Field	Type	Description
ts	Integer	The timestamp, when the message was received by Operations Monitor.
request	Boolean	True if the message is a request, False otherwise.
proto	String	Protocol used.
src_ip	String	Source IP address.
src_mac	String	Source MAC address.
dst_ip	String	Destination IP address.
dst_mac	String	Destination MAC address.
method	String	The request method of this message. Only present, if this is a request message.
ruri	String	The request URI of this message. Only present, if this is a request message.
code	Integer	The response code of this message. Only present, if this is a response message.
reason	String	The response reason of this message. Only present, if this is a response message.
headers	List	A list of (fieldname, field body) tuples, representing the headers of this message.
body	String	Indicates the message body.
getBody ()	-	Returns the body of the message. Return type: str.

Table 9-5 (Cont.) Message Class Fields

Field	Type	Description
getHeaders ()	-	Returns a list of (fieldname, field body) tuples for all defined header fields. Field name and field body are both instances of <i>str</i> . Return type: list of tuples.
getHeadersByName (<i>name</i>)	-	Returns a list of header field bodies for header fields where the field name equals the given <i>name</i> . A field body is an instance of <i>str</i> . Parameters name - Name to match header fields against. Return type: list of <i>str</i> .
isRequest ()	-	Returns, whether this message is a request. Return type: bool.

`class libpalladion.scripting.RawMessage(facade)`

This class encapsulates a raw signaling message. [Table 9-6](#) describes the fields for the Raw Message class.

Table 9-6 Raw Message Class Fields

Field	Type	Description
ts	Integer	The timestamp, when the message was received by Operations Monitor.
h	DICT	A dictionary representing the PCAP header.
frame	String	The raw data.

`class libpalladion.scripting.VoiceQuality(facade)`

This class represents voice quality measurements for a call found by Operations Monitor, or reported by one of the User Agents from the call. A call can have more Voice Quality instances associated, one for each RTP stream.

It cannot be invoked directly. It is used for the return objects of the method **getVoiceQuality** for **Call** objects.

Note

Following are the requirements for Voice Quality App to support the data from an SBC probe:

- The SBC must be running on an Enterprise version, ECZ7.3.0m1p1 and above.
- Ensure the platform is 4600/6300.
- Ensure that the setting on the SBC, **interim-qos-update** is enabled. If this setting is not available, upgrade the SBC to the latest version.

For all other platforms and releases, the Voice Quality app does not display the data received from SBC probes.

For more information on how Operations Monitor gathers voice quality data, see "[Voice Quality](#)".

[Table 9-7](#) describes the fields for the Voice Quality class.

Table 9-7 Voice Quality Class Fields

Field	Type	Description
start_ts	Integer	The timestamp of the first measured RTP packet.
probe	String	IP address of the probe that received the data.
vlan	String	VLAN of the probe.
direction	String	The direction of the RTP stream that was measured. One of 'src2dst' or 'dst2src'.
dst_ip	String	The destination IP of the call.
dst_port: INTEGER	Integer	The destination port of the call.
src_ip: STRING	String	The source ip of the call.
src_port: INTEGER	Integer	The source port of the call.
start_ts	Integer	The timestamp of the call.
packets_received	Integer	The number of RTP packets received.
packets_lost_rate	Integer	Packet loss rate for the RTP stream.
forward	Boolean	True if forward.
source	String	Source Device Name.
moscqe_avg	Float	MOS average for voice quality.
jitter_total	Float	Sum of the jitter value for each packet, in milliseconds.
jitter_max	Float	Average jitter value for the RTP packets from the call.
latency	Integer	Latency as reported by the client's User Agent, when available.
r_factor	Float	R-factor value for voice quality.
rtcp	OBJECT	If present, this optional object contains the following fields: - start_ts: DATETIME The timestamp of the first measured RTP packet. - end_ts: DATETIME The timestamp of the last measured RTP packet. - jitter_max: FLOAT Maximum jitter value for a single packet, in milliseconds. - jitter_avg: FLOAT Average jitter value for the RTP packets from the call. - packets_lost: INTEGER Packets lost for the RTP stream. - source: STRING Source Device Name.

class libpalladion.scripting.Chunk(facade)

This class represents a single chunk of voice quality data.

It cannot be invoked directly. It is used for the return objects of the method **getVoiceQualityChunks** for **Call** objects.

For more information on how Operations Monitor gathers voice quality data, see "[Voice Quality](#)".

[Table 9-8](#) describes the fields for the Chunk class.

Table 9-8 Chunk Class Fields

Field	Type	Description
start_ts	Integer	The timestamp of the first measured RTP packet.
end_ts	Integer	The timestamp of the last measured RTP packet.
received	Integer	The number of RTP packets received.
expected	Integer	The number of RTP packets expected.
codec	String	The codec used for this chunk.
pkt_delay_variation_us	Double	Variation on packet delay.
no_mosqcq_reason	String	If there is no MOS data, its cause.

class libpalladion.scripting.Device(facade)

This class represents a platform device configured in Operations Monitor. For a general introduction on platform devices in Operations Monitor, see "[Platform Devices](#)".

[Table 9-9](#) describes the fields for the Device class.

Table 9-9 Device Class Fields

Field	Type	Description
id	Integer	The unique numeric ID of the device.
type	String	The type of the device. One of 'SBC', 'PROXY', 'L2LB', 'GW', or 'TRUNK'.
name	String	The user visible name of the device.
description	String	A description for the device.
match_type	String	If the device is of type 'SBC', this value indicates how call matching is performed.
suffix	Integer	Some call matching types require a suffix parameter.
match_script	String	This attribute contains a script that specifies the call matching algorithm.
ipranges	String	The IP address ranges which are occupied by this device.
hw_addrs	String	The hardware addresses of this device.
up_since	Integer	A timestamp specifying the time since when the device is known to be running.

Table 9-9 (Cont.) Device Class Fields

Field	Type	Description
dtg	String	If the device is of type TRUNK and device identification via DTG/OTG URI parameters was configured, this attribute contains the value of the DTG request URI parameter to look for.
otg	String	If the device is of type TRUNK and device identification via DTG/OTG URI parameters was configured, this attribute contains the value of the OTG From URI parameter to look for.
getCreatedCalls (<i>filter</i> =[], <i>keys</i> =[], <i>orderBy</i> =[])	-	Query calls that are created by this device, that is, calls that have an outbound leg from this device and no inbound leg to this device. See <code>Facade.query()</code> for the meaning of the parameters. Parameters filter - A filter specification to be applied to the queried Call instances. keys - Keys that the queried Call instances must match. orderBy - An ordering specification. Return type: QueryIterator over Call instances.
getRegistrationEvents (<i>filter</i> =[], <i>keys</i> =[], <i>orderBy</i> =[])	-	Query registration events that are handled by this device. See <code>Facade.query()</code> for the meaning of the parameters. Parameters filter - A filter specification to be applied to the queried RegistrationEvent instances. keys - Keys that the queried RegistrationEvent instances must match. orderBy - An ordering specification. Return type: QueryIterator over RegistrationEvent instances.

Table 9-9 (Cont.) Device Class Fields

Field	Type	Description
getRelayedCalls (<i>filter</i> =[], <i>keys</i> ={}, <i>orderBy</i> =[])	-	Query calls that are relayed by this device, that is calls that have an inbound leg to this device and an outbound leg from this device. See Facade.query() for the meaning of the parameters. Parameters filter - A filter specification to be applied to the queried Call instances. keys - Keys that the queried Call instances must match. orderBy - An ordering specification. Return type: QueryIterator over Call instances.
getTerminatedCalls (<i>filter</i> =[], <i>keys</i> ={}, <i>orderBy</i> =[])	-	Query calls that are terminated by this device, that is, calls that have an inbound leg to this device and no outbound leg from this device. See Facade.query() for the meaning of the parameters. Parameters filter - A filter specification to be applied to the queried Call instances. keys - Keys that the queried Call instances must match. orderBy - An ordering specification. Return type: QueryIterator over Call instances.
hasIP	Boolean	- This method checks whether a given IP address (ip) belongs to any of the IP ranges in self.ipranges, and matches a given VLAN (vlan). - If dvlan is None, the match is accepted → return True - If dvlan is not None, it checks if dvlan == vlan → return the result True or False
hasMac	Boolean	- This method checks whether a given MAC address (mac) is present in the list of hardware addresses stored in self.hw_addrs - If it finds a match between the provided mac and any of the addresses in the list, it returns True. - If there is no match after checking all addresses, the method returns False.

`class libpalladion.scripting.Counter(facade)`

A Counter is an object in Operations Monitor that takes periodic measurements of a numeric property of the monitored platform. For a general introduction on counters, see "[KPI/Metrics](#)".

[Table 9-10](#) describes the fields for the Counter class.

Table 9-10 Counter Class Fields

Field	Type	Description
id	Integer	A unique identifier for the counter.
name	String	The name of the counter.
maintype	Integer	The main type of the counter.
subtype	Integer	The sub type of the counter.
device	String	The device this counter belongs to. May be None.
p1	String	The first parameter for the counter.
p2	String	The second parameter for the counter.
p3	String	The third parameter for the counter.
sec	Integer	The last second measurement.
m_avg	Float	The last minute average of measurements.
h_avg	Float	The last hour average of measurements.
getHourValues (<i>span, offset=0</i>)	-	Query hour average values from the counter history. The returned query iterator yields a dict instance for each hour in the supplied time span. The yielded dict instances contain the keys <i>avg</i>, <i>min</i>, <i>max</i> and <i>sum</i>, with the obvious meanings. The time span is given by the parameters <i>span</i> and <i>offset</i>, where <i>offset</i> specifies the end point of the time span relative to the current time. Parameters span - The length of the queried time span in seconds. offset - The offset of the queried time span from the current time, specified in seconds. Return type: QueryIterator over dict instances.
getMinuteValues (<i>span, offset=0</i>)	-	Query minute average values from the counter history. The returned query iterator yields a dict instance for each minute in the supplied time span. The yielded dict instances contain the keys <i>avg</i>, <i>min</i>, <i>max</i>, and <i>sum</i>, with the obvious meanings. The time span is given by the parameters <i>span</i> and <i>offset</i>, where <i>offset</i> specifies the end point of the time span relative to the current time. Parameters span - The length of the queried time span in seconds. offset - The offset of the queried time span from the current time, specified in seconds. Return type: QueryIterator over dict instances.

`class libpalladion.scripting.Alert(facade)`

This class represents alerts raised by Operations Monitor. [Table 9-11](#) describes the fields for the Alert class.

Table 9-11 Alert Class Fields

Field	Type	Description
ts	Integer	The time when this alert was raised.
type	String	The type of the alert raised.
subtype	String	The sub type of the alert raised.
new: BOOLEAN	Boolean	Whether this alert is new or read.
message	String	The message issued when raising the alert.
details	String	Some details about the raised alert.
prio	Integer	The priority of the alert.

`class libpalladion.scripting.RegisteredUser(facade)`

This class represents a registered user. [Table 9-12](#) describes the fields for the Registered User class.

Table 9-12 Registered User Class Fields

Field	Type	Description
identifier	String	Username of the registered user.

`class libpalladion.scripting.QueryIterator(facade, query_handle, cls=None)`

Instances of this class can be used to iterate over query result sets. You cannot instantiate a QueryIterator directly, but various query methods in this API return QueryIterator instances.

Instances conform to the Python iterator protocol and can be used in 'for item in iterable:' constructs. You can also use the next() method directly to retrieve one result at a time. QueryIterator instances also provide a close() method, which frees resources tied by the query. Once close() has been called, iteration stops. close() is called automatically when all references to a QueryIterator instance are gone.

[Table 9-13](#) describes the fields for the Query Iterator class.

Table 9-13 Query Iterator Class Fields

Field	Type	Description
close()	-	Free the resources tied up by the query.
next()	-	Return the next item in the query result set. Return type: Depends on the type of query.

Using the Apps API Examples

The following app searches the Operations Monitor database for calls which have a given Call-ID header and have been set up between two given points in time:

```
from libpalladion.scripting.Model import Call, Leg

def run(facade, args):

    # Get input parameters
    start_ts = args.get("start_ts")
    end_ts = args.get("end_ts")
    callid = args.get("callid")

    callid = callid.strip()

    for call in facade.getCalls(
        filter=[Call.setup_start_ts >= start_ts, Call.setup_start_ts <= end_ts]
    ):
        # search for the specific callid in all the call legs
        # the callid of each call leg might be different
        for leg in call.getLegs():
            if leg.callid == callid:
                facade.addResult(
                    {"id": call.id},
                    on_duplicate_key='ignore'
                )
```

This app has to be packaged with an app specification file, which should specify the type of the result table (*calls* in this case), and the names and types of the parameters *callid*, *start_ts*, and *end_ts*. The following specification file achieves this:

```
<?xml version="1.0" encoding="utf-8"?>
<script xmlns="http://iptego.de/palladion/script-spec"
    name="Call-Id Search"
    description="This script will find all the calls with a given Call-ID value"
    result-type="calls">
    <param-spec>
        <param name="start_ts" label="Started after" type="datetime" required="yes"/>
        <param name="end_ts" label="Started before" type="datetime" required="yes"/>
        <param name="callid" label="Call-ID" type="string" required="yes"/>
    </param-spec>
</script>
```

Note, that the parameters specified as *datetime* are passed as the standard Python datetime type. If the *result-type* of an app is specified as *calls*, it has a result table with one integer column, ID. When displaying the results table of such an app in the user interface, a join with the *calls* table is performed. In the example above, the call to *facade.addResult* has to be surrounded by *try ... except* because there can be multiple **libpalladion.scripting.Leg** objects, with the same ID attribute. This is because a call can have multiple legs. Adding the same ID twice to the *calls* result table results in a duplicate key error.

In the next example we look at an app that requires a custom result table. We will see how this custom result table can be specified in the app specification file. The app calculates a statistics of which user agents use which codecs how often. Again the source data for the app is restricted to calls that were set up between two given points in time.

```

from libpalladion.scripting.Model import Call

def run(facade, args):
    start_ts = args.get("start_ts")
    end_ts = args.get("end_ts")

    stats = {}
    filter = [Call.setup_start_ts > start_ts, Call.setup_start_ts <= end_ts]
    for call in facade.getCalls(filter=filter):
        ua = call.src_ua
        if ua is not None:
            codecs = call.src_codecs
            if (ua, codecs) not in stats:
                stats[(ua, codecs)] = 0
            stats[(ua, codecs)] += 1

    for ((ua, codecs), count) in stats.items():
        facade.addResult({'ua': ua, 'codecs': codecs, 'count': count})

```

The **facade.addResult** call on the last line makes the assumption that the result table has the columns **ua**, **codecs**, and **count**. So this schema has to be specified in the script specification file.

```

<?xml version="1.0" encoding="utf-8"?>
<script xmlns="http://iptego.de/palladion/script-spec"
    name="Statistics of which user agent uses which codecs"
    description="This app calculates a statistic of which user agents use which codecs"
    result-type="custom">
    <param-spec>
        <param name="start_ts" label="Start time" type="datetime" required="yes"/>
        <param name="end_ts" label="End time" type="datetime" required="yes"/>
    </param-spec>
    <result-schema>
        <column name="ua" type="VARCHAR(255)" null="false"/>
        <column name="codecs" type="VARCHAR(255)" null="false"/>
        <column name="count" type="INT(11)" null="false" default="1"/>
        <primary-key columns="ua codecs"/>
    </result-schema>
</script>

```

⚠ Caution

When creating your own applications, or using third-party applications, test your scripts in a test environment to ensure they are safe before uploading them to your production environment. Applications approved by Oracle are safe to use in your environments. However, non-approved applications could cause security and performance issues. Oracle is not responsible for any loss, costs, or damages incurred from using your own applications, or third-party applications.

Remote App Procedure Calls

Remote app procedure calls provide programmatic access to the app functionality of Operations Monitor. It is possible to invoke apps installed on Operations Monitor and get their results via a simple HTTP GET interface. For more information, see [Apps](#) and [Implementing Apps](#) section of this manual.

Apps are possibly long running processes. Therefore invoking an app and retrieving the results of an app run have been split into two separate steps.

Invoking an App

Invoking an app is done by an HTTP GET request to the URL `/scripts/run/ app_name` on the Operations Monitor host, where `app_name` is to be replaced by the identifier of an app. Note, that you can lookup the identifier of an app in the **Id** column of that app's entry in the Available Apps table. The parameters of the app have to be encoded as URL parameters into the GET request URL.

If invoking the app succeeds, an app run is created, and the GET request returns the numeric run ID for the app run in the response body. This run ID can later be used to retrieve the results of the app run.

There are two possible failure cases when invoking an app. First, the given app name could be invalid. In this case Operations Monitor responds with an HTTP '404 Not found' error code. Secondly, the parameters given in the request could be invalid when a required parameter is missing or a given parameter cannot be parsed. In this case Operations Monitor responds with an 'HTTP 400 Bad request' error code.

A note regarding parameter encoding is required here: Datetime values have to be encoded in a special way to make Operations Monitor recognize them. Operations Monitor expects datetime values to be in the format `YYYY-mm-dd HH:MM:SS`, where the 4-digit string `YYYY` gives the year, `mm` gives the month, `dd` gives the day, `HH` gives the hour, `MM` gives the minute, and `SS` gives the second.

Retrieving the Results of an App Run

Retrieving the results of an app run is done by an HTTP GET request to the URL `/scripts/get/run_id` on the Operations Monitor host, where `run_id` is a numeric run ID. Run IDs are returned when invoking an app. They can also be looked up in the **Id** column of the **App runs** table. For more information, see [Apps](#).

There are three possible outcomes of this request. First, if the run ID given is invalid an HTTP '404 Not found' error code is returned. Secondly, if the run ID is valid but the app run is not yet finished, an HTTP '202 Accepted' status code is returned. In this case the body of the response contains the string **202 Accepted**. The third case is when the run ID is valid and the app run is finished already. In this case an HTTP '200 OK' status code is returned, and the body of the response contains the app run result table in CSV format.

REST API

This chapter describes how to work with the Oracle Communications Operations Monitor REST API.

A simple REST API facilitates access to much of the information generated by Operations Monitor.

REST is a way of implementing Remote Procedure Call (RPC) systems on top of HTTP. REST APIs are stateless, since they don't use mechanisms of application state keeping that are traditionally employed together with HTTP, such as cookies or sessions. Everything necessary for keeping the application state must be encoded into the HTTP requests. REST APIs are structured around addressable resources, that means all information, that is provided or manipulated by the API, is addressable with HTTP URLs. Conceptually, resources are like the files and directories of a file system, organized into a tree of parents and children.

From the generally used HTTP methods GET, POST, PUT, and DELETE, Operations Monitor's REST API only uses the GET method, as the interface is intended to only query information from Operations Monitor.

Note

The remote application needs to authenticate itself with the administrator password over the standard HTTP Basic mechanism.

Note

REST API searches are not guaranteed to be real-time without advanced hardware sizing. Continuous REST API searches or queries to Oracle Communications Operations Monitor may impact its performance, potentially causing UI slowness, slower REST API response times.

Example call:

```
$ curl -L -u admin:<passwd> https://10.1.0.81/r/users/00493077715680/calls/recent
```

```
{
  "data": [
    {
      "state_msg": "Finished",
      "code": 200,
      "dst_codecs": "PCMU, PCMA, iLBC, telephone-event",
      "src_codecs": "PCMU, PCMA, telephone-event, iLBC",
      "pid": 1250018007,
      "url": "\/r\/users\/00493077715680\/calls\/1250018007:16739",
      [...]
    }
  ]
}
```


Note

Oracle recommends to replace the self-signed certificate delivered with the software with a certificate signed by a certificate authority. If you are using self-signed certificate, it is possible that the connection fails as the certificate could not be verified. You have to either install the certificate of the signing CA or provide a method to use the tool directly.

For curl, you could pass the certificate as follows:

```
curl --cacert <file with the certificate> -L -u admin:<passwd>  
https://10.1.0.81/r/users/00493077715680/calls/recent
```

Interface Description

The resources accessible via the REST interface are encoded in JSON. You can access the following resources on each Operations Monitor system (with variables denoted in angle brackets):

/r/calls

A structure containing information about the available calls. It contains the fields listed in [Table 10-1](#):

Table 10-1 */r/calls* Fields

Field	Description
end_call_id	The call ID of the last call.
end_ts	A timestamp giving the second in which the last call was started.
name	Is always calls .
start_call_id	The call ID of the first call (not the same ID used in conjunction with a partition ID).
start_ts	A timestamp giving the second in which the first call was started.
total	The number of calls in the partition.

Note

In the Operations Monitor version before 3.1 this method returned a list of structures with partitioning information. Starting with version 3.1, partitions are no longer used.

/r/calls/recent

The list of recent calls similar to the one that is displayed in the recent calls table in the web interface. This resource is a list resource and has the common format of list resources and allows filtering and paging. For more information, see "[The Format of List Resources](#)".

The list items are structures consisting of the fields listed in [Table 10-2](#):

Table 10-2 */lr/calls/recent* Fields

Field	Description
call_time	The time the call was in state ESTABLISHED.
code	The code of the last response for the first INVITE message.
dst_codecs	The codecs proposed by the callee.
dst_initial_codecs	The codecs initially proposed by the callee.
dst_ip	The IP address of the called user that connected first. This may be an empty string.
dst_ua	The user agent of the callee.
dst_user	The identifier of the callee.
egress_devs	The egress device(s).
id	Together with pid makes up the unique identifier of a call.
in_devs	The in device(s).
ingress_devs	The ingress device(s).
init_devs	The initiator device.
MOSlqe_avg	The average MOS estimation for this call.
MOSlqe_min	The minimum MOS estimation for this call.
nlegs	The number of legs in the call.
out_devs	The out device(s).
pid	Together with id makes up the unique identifier of a call.
realms	A bitmask of the realms this call belongs to.
setup_start_ts	The time the first INVITE message was issued.
setup_time	The time before the call reached the state ESTABLISHED.
src_codecs	The audio codecs proposed by the caller.
src_initial_codecs	The audio codecs initially proposed by the caller.
src_ip	The IP address of the device initiating the call. This includes the IP address string.
src_ua	The user agent of the caller.
src_user	The caller identifier.
state_details	Details about the current state of the call.
state_msg	The current state of the call.
term_devs	The terminator device.
url	The url of the full call rest resource.

/lr/calls/<start_ts>/<end_ts>

A list of calls started between *<start_ts>* and *<end_ts>*. This list is structured exactly like the list of recent calls, but the calls are from a definable timespan. The timestamps have to be written in ISO 8601 format and then be url encoded.

The following query gets the calls started between, 22 Mar 2010 16:30 and 22 Mar 2010 17:00:

```
$ curl -L -user admin:<passwd> https://10.1.0.81/r/calls/2010-03-22+16:30:00/2010-03-22+17:00:00
```

A list of calls might be filtered by following parameters:

- MOSlqe_avg
- MOSlqe_min
- init_devs
- term_devs
- traversing_devs
- ingress_devs
- egress_devs
- gateway_devs

For Example:

```
$ curl -L -user admin:<passwd> https://10.1.0.89/r/calls/2014-01-01+00:00:00/2014-02-01+00:00:00?term_devs__eq=52
```

/r/calls/<start_ts>/<end_ts>/<pid>:<id>

The call with the given *<pid>* and *<id>*. The returned resource is a structure with the fields listed in [Table 10-3](#):

Table 10-3 */r/calls/<start_ts>/<end_ts>/<pid>:<id>* Fields

Field	Description
call_id	An identifier that makes up a unique identifier of a call. Can be used instead of <i><pid></i> and <i><id></i> .
call_time	The time the call was in state ESTABLISHED.
code	The code of the last response for the first INVITE message.
dst_user	The identifier of the callee.
id	Together with pid makes up the unique identifier of a call.
legs	A list of legs belonging to this call.
messages_url	The url of the messages resource for this call.
nlegs	The number of legs in the call.
pid	Together with id makes up the unique identifier of a call.
realms	A bitmask of the realms this call belongs to.
setup_start_ts	The time the first INVITE message was issued.
setup_time	The time before the call reached state ESTABLISHED.
src_user	The caller identifier.
state_details	Details about the current state of the call.
state_msg	The current state of the call.
vq_url	The url of the voice quality resource for this call.

Note

<call_id> can be used to identify a call instead of the <pid>:<id> combination.

/r/calls/<start_ts>/<end_ts>/<pid>:<id>/messages

A representation of the SIP messages of a given call. This resource is a list resource and has the common format of list resources and allows paging but not filtering. For more information, see "[The Format of List Resources](#)".

The list items are structures with the fields listed in [Table 10-4](#):

Table 10-4 */r/calls/<start_ts>/<end_ts>/<pid>:<id>/messages* Fields

Field	Description
code	If the message is a response message - the response code.
data	The whole message as a string.
dst_ip	The destination IP address.
dst_mac	The destination hardware address.
dst_port	The destination port.
method	If the message is a request message - the request method. For example, INVITE or ACK.
msgid	The unique ID of this message.
proto	UDP or TCP.
reason	If the message is a response message - the response reason.
ruri	If the message is a request message - the request uri of this message.
src_ip	The source IP address.
src_mac	The source hardware address.
src_port	The source port.
ts	The time this message was received by Operations Monitor.

/r/calls/<start_ts>/<end_ts>/<pid>:<id>/vq

Voice quality information for each RTP stream that belongs to the given call. This resource is a list resource and has the common format of list resources. It does not allow for filtering or paging. For more information, see "[The Format of List Resources](#)".

The list items are structures with the fields listed in [Table 10-5](#):

Table 10-5 */r/calls/<start_ts>/<end_ts>/<pid>:<id>/vq* Fields

Field	Description
avg_jitter	Average jitter value for the packets from the RTP stream.
burst_cnt	The number of sequences of lost RTP packets (gaps).
cid	Corresponds to the ID of the call the voice quality information belongs to.
decoder	The codec used by the RTP stream.

Table 10-5 (Cont.) /r/calls/<start_ts>/<end_ts>/<pid>:<id>/vq Fields

Field	Description
dir	The direction of the RTP stream either 'src2dst' or 'dst2src'.
expected	Expected number of packets in the RTP stream.
first_ts	The timestamp of the first measured RTP packet.
leeff	Effective Equipment Impairment Factor.
last_ts	The timestamp of the last measured RTP packet.
lid	No meaningful value.
max_burst	The maximum number of RTP packets lost in sequence (in a single gap).
max_jitter	The maximum jitter value for the packets from the RTP stream.
MOS	MOS estimation for voice quality.
pid	The pid of the call this voice quality information belongs to.
pl_rate	Packet loss rate for the RTP stream.
R	R-value score for voice quality.
received	Received number of packets in the RTP stream.
source	The source that generated the voice quality information. For example, Operations Monitor.
total_jitter	Total jitter value for the packets from the RTP stream.
ts	The timestamp.

/r/registrations

The list of recent registration events. This resource is a list resource and has the common format of list resources and allows for filtering and paging of the list items. For more information, see "[The Format of List Resources](#)".

The list items are structures with the fields listed in [Table 10-6](#):

Table 10-6 /r/registrations Fields

Field	Description
code	The response code of the last response to the REGISTER request.
contacts	The content of the contact header of the REGISTER request.
dest_ip	The destination IP address of the registration event.
dev_id	The numeric ID of the platform device that handled the registration event.
device	The name of the device that handled the registration event.
id	The unique ID of the registration event.
ip	The source IP address of the registration event.
realms	A bitmask of the realms this event belongs to.
ts	The time stamp of the registration event.
type	The type of registration event.

Table 10-6 (Cont.) /r/registrations Fields

Field	Description
type_msg	Human readable form of the type of registration event. One of New, Failed, Unauthorized, Expired, or Gone.
url	The url of the full registration event resource.
user	The identifier of the registered user.

/r/registrations/<id>

The registration event with the given *<id>*. This resource is a structure with the fields listed in [Table 10-7](#):

Table 10-7 */r/registrations/<id>* Fields

Field	Description
code	The response code of the last response to the REGISTER request.
contacts	The content of the contact header of the REGISTER request.
dest_ip	The destination IP address of the registration event.
dev_id	The numeric ID of the platform device that handled the registration event.
device	The name of the device that handled the registration event.
id	The unique ID of the registration event.
ip	The source IP address of the registration event.
messages_url	The url of the messages resource for this registration event.
realms	A bitmask of the realms this event belongs to.
type	The type of registration event.
type_msg	Human readable form of the type of registration event. One of New, Failed, Unauthorized, Expired, or Gone.
user	The identifier of the registered user.

/r/registrations/<id>/messages

The SIP messages belonging to a given registration event. This resource is a list resource and has the common format of list resources and allows paging but not filtering. The list items are exactly like the list items of the */r/calls/<pid>:<id>/messages* resource. For more information, see "[The Format of List Resources](#)".

/r/devices

The list of configured platform devices. This resource is a list resource and has the common format of list resources. For more information, see "[The Format of List Resources](#)".

The list items are structures with the fields listed in [Table 10-8](#):

Table 10-8 */r/devices* Fields

Field	Description
id	The device ID.
inbound	The number of inbound calls to this device.
name	The device name.
outbound	The number of outbound calls from this device.
url	The resource url for this device.
users	The number of registered users at this device.

/r/devices/<devId>

A representation of the given platform device. This resource is a structure with the fields listed in [Table 10-9](#):

Table 10-9 */r/devices/<devId>* Fields

Field	Description
created_calls_url	The url to the created_calls resource for this device.
id	The device ID.
inbound	The number of inbound calls to this device.
name	The device name.
outbound	The number of outbound calls from this device.
registrations_url	The url to the registrations resource for this device.
relayed_calls_url	The url to the relayed_calls resource for this device.
terminated_calls_url	The url to the terminated_calls resource for this device.
users	The number of registered users at this device.

/r/devices/<devId>/created_calls

A list of calls created by the given platform device. The format of this resource is exactly like the format of the **/calls** resource.

/r/devices/<devId>/relayed_calls

A list of calls which are relayed by the given platform device. The format of this resource is exactly like the format of the **/calls** resource.

/r/devices/<devId>/terminated_calls

A list of calls which are terminated by the given platform device. The format of this resource is exactly like the format of the **/calls** resource.

/r/devices/<devId>/registrations

A list of registration events handled by the given platform device. The format of this resource is exactly like the format of the **/registrations** resource.

/r/users/<userid>

Information belonging to a user registered on the monitored platform, similar to the information displayed on the user tracking page. This resource is a structure with the fields listed in [Table 10-10](#):

Table 10-10 */r/users/<userid>* Fields

Field	Description
calls_url	The url to the calls resource for this user.
current_registrations	A list containing current registrations of the user.
registrations_url	The url to the registrations resource for this user.
user	The user ID.

The **current_registrations** field is a list whose list items are structures with the fields listed in [Table 10-11](#):

Table 10-11 *current_registrations* Fields

Field	Description
dev_id	The numeric ID of the platform device that handled the current registrations event.
expires	The negotiated expiry time of the registration.
expires_in	The time remaining until registration expiry.
first_seen_ts	First time the user registered.
last_refreshed_ts	The last time the user refreshed the registration.
last_seen_ts	The last time the user registered.
last_suggested_expires	The value of the expires header of the REGISTER request.
link_quality	An indication of the quality of the network link between platform and user.
srcip	The source IP address of the current registrations event.
uri	The uniform resource identifier (URI) for the current registrations resource.
usrdev	The name of the device that handled the current registrations event.

/r/users/<userid>/calls

Calls belonging to the given platform user. The format of this resource is exactly like the format of the ***/r/calls*** resource.

/r/users/<userid>/registrations

Registration events belonging to the given platform user. The format of this resource is exactly like the format of the ***/r/registrations*** resource.

/r/counters

The list of counters for the admin user and the **ALL** realm. This resource is a list resource and has the common format of list resources. For more information, see "[The Format of List Resources](#)".

The list items are structures with the fields listed in [Table 10-12](#):

Table 10-12 */r/counters* Fields

Field	Description
datatype	The datatype of the counter.
h_avg	The average of measurements over one hour.
h_max	The maximum of measurements over one hour.
h_max	The maximum of measurements over one hour.
h_sum	The sum of measurements over one hour.
id	The numeric counter ID.
m_avg	The average of measurements over one minute.
m_max	The maximum of measurements over one minute.
m_min	The minimum of measurements over one minute.
m_sum	The sum of measurements over one minute.
maintype	The numeric counter main type.
name	The counter name.
p1	Counter parameter one.
p2	Counter parameter two.
p3	Counter parameter three.
subtype	The numeric counter sub type.
url	The url to the full counter resource.
value	The current second measurement.

/r/counters/<id>

A representation of the given counter. This resource is a structure with the fields listed in [Table 10-13](#):

Table 10-13 */r/counters/<id>* Fields

Field	Description
autoreset	If the counter is reset every second.
datatype	The counter datatype.
days	For average counters, the number of days to average over.
hours_url	The url to the hours resource for this counter.
id	The numeric counter ID.
maintype	The numeric counter main type.
minutes_url	The url to the minutes resource for this counter.
name	The name of the counter.
owner	The owner of the counter: either "system" or "user".
p1	Counter parameter one.
p2	Counter parameter two.
p3	Counter parameter three.

Table 10-13 (Cont.) /r/counters/<id> Fields

Field	Description
realm	The realm that this counter belongs to.
seconds_url	The url to the seconds resource for this counter.
src_cnt	For average counters, the source counter for the average.
subtype	The numeric counter sub type.
user_id	The user ID of the user who owns the counter.
value	The current second measurement.
weekdays	For average counters, whether the average is calculated for each weekday separately.

/r/counters/<id>/seconds

The list of recent second measurements for the given counter. This resource is a list resource and has the common format of list resources and allows paging. The list items are integer values. The list contains up to 3600 values, one value for each of the last 3600 seconds, in chronological order from oldest to youngest. For more information, see "[The Format of List Resources](#)".

/r/counters/<id>/minutes

The list of minute values for the given counter. This resource is a list resource and has the common format of list resource and allows paging. The list items are float values. The list contains all the minute averages of the counter measurements stored in the database of Operations Monitor in chronological order from oldest to youngest. For more information, see "[The Format of List Resources](#)".

/r/counters/<id>/hours

The list of hour values for the given counter. This resource is a list resource and has the common format of list resources and allows paging. The list items are float values. The list contains all the hour averages of the counter measurements stored in the Operations Monitor database in chronological order from oldest to youngest. For more information, see "[The Format of List Resources](#)".

The Format of List Resources

List resources like the **/r/calls/recent** resource are structures with the fields listed in [Table 10-14](#):

Table 10-14 List Resources Fields

Field	Description
data	The actual list. The format of the list item depends on the resource.
limit	The number of returned items.
start	The index of the first returned item.
total	The total number of items that exist.

All list resources allow paging. Paging is enabled by default and can be controlled by giving the **start** and **limit** GET parameters when requesting the resource. The **start** parameter gives the index of the first item to be returned, the **limit** parameter gives the number of items to be returned.

Note, that *limit* cannot exceed the value given in the **vsp.rest.max_limit** system setting and is adjusted if it does exceed this value. For the counter seconds, minutes and hours resource you can also give *start_ts* instead of *start*, meaning that the request will only return items with an associated timestamp that is greater or equal than the given timestamp.

Some list resources also allow filtering. Filtering is controlled by additional GET request parameters. A filter controlling parameter must have the form `<fieldname>_<verb>`, where `<fieldname>` is the name of a field of the list items of the resource and `<verb>` determines the logic of the filter. The known verbs and their meaning are listed in [Table 10-15](#):

Table 10-15 List Resources Verbs

Verb	Description
contains	This filter applies if the set valued field contains the set given. The parameter must be given as a list separated by '+'.
deq	This filter applies if the date contained in the field and the given date are equal. The date must be given as "mm/dd/yyyy", where mm is the month, dd the day of the month and yyyy the year.
dgeq	This filter applies if the date contained in the field is younger or equal to the given date. The date must be given as "mm/dd/yyyy", where mm is the month, dd the day of the month and yyyy the year.
dgt	This filter applies if the date contained in the field is younger than the date given in the parameter. The date must be given as "mm/dd/yyyy", where mm is the month, dd the day of the month and yyyy the year.
dleq	This filter applies if the date contained in the field is older or equal to the given date. The date must be given as "mm/dd/yyyy", where mm is the month, dd the day of the month and yyyy the year.
dlt	This filter applies if the date contained in the field is older. The date must be given as "mm/dd/yyyy", where mm is the month, dd the day of the month and yyyy the year.
dteq	This filter applies if the date and time contained in the field is equal to the date and time given. The date and time must be given as "yyyy/mm/dd HH:MM:SS", where yyyy is the year, mm the month, dd the day of the month, HH the hour, MM the minute and SS the second.
dtgeq	This filter applies if the date and time contained in the field is younger or equal to the date and time given. The date and time must be given as "yyyy/mm/dd HH:MM:SS", where yyyy is the year, mm the month, dd the day of the month, HH the hour, MM the minute and SS the second.

Table 10-15 (Cont.) List Resources Verbs

Verb	Description
dtgt	This filter applies if the date and time contained in the field is younger than the date and time given in the parameter. The date and time must be given as "yyyy/mm/dd HH:MM:SS", where yyyy is the year, mm the month, dd the day of the month, HH the hour, MM the minute and SS the second.
dtleq	This filter applies if the date and time contained in the field is older or equal to the date and time given. The date and time must be given as "yyyy/mm/dd HH:MM:SS", where yyyy is the year, mm the month, dd the day of the month, HH the hour, MM the minute and SS the second.
dtlt	This filter applies if the date and time contained in the field is older than the given date and time. The date and time must be given as "yyyy/mm/dd HH:MM:SS", where yyyy is the year, mm the month, dd the day of the month, HH the hour, MM the minute and SS the second.
eq	This filter applies if the numeric value contained in the field is equal to the number given.
geq	This filter applies if the numeric value contained in the field is greater than or equal to the number given.
gt	This filter applies if the numeric value contained in the field is greater than the numeric value given in the parameter.
leq	This filter applies if the numeric value contained in the field is smaller than or equal to the number given.
lt	This filter applies if the numeric value contained in the field is smaller than the number given.
oneof	This filter applies if the value contained in the field is equal to one of the values given. The values must be given as a list separated by '+'. The values must be given as a list separated by '+'.
substr	This filter applies if the value of the parameter is contained in the field.

In case the GET request parameters cannot be parsed, an HTTP 400 Bad Request status code is returned.

11

New REST API

With the new REST API almost all Oracle Communications Operations Monitor features are now easily accessible through HTTPS REST calls. Nearly every feature you already use through the web interface of Operations Monitor can now be automated and used with your HTTPS capable toolchain of choice.

Plus with the new API Key, authentication is now more simple and secure than before. Authentication is now as simple as passing your personal API Key along with your request.

Note

REST API searches are not guaranteed to be real-time without advanced hardware sizing. Continuous REST API searches or queries to Oracle Communications Operations Monitor may impact its performance, potentially causing UI slowness, slower REST API response times, etc.

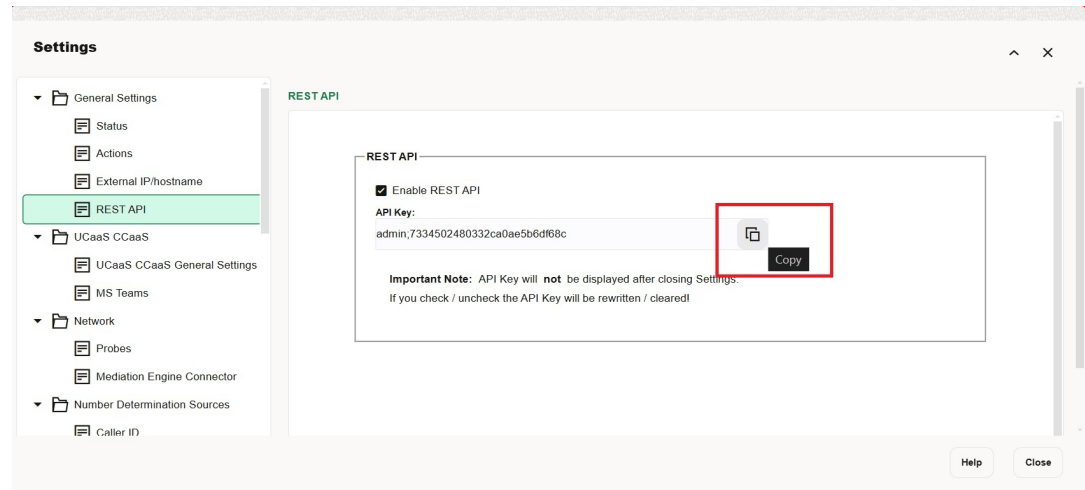
API Key

The new API Key is used to authenticate the user when using the new REST API. The API Key is connected to your user account — so when using the REST API with the API Key you have the same access rights as with your user account. Before using the new REST API you first have to enable and generate your personal API Key. The API Key is comprised of the username and a hexcode delimited by a semicolon.

For security reasons the API Key is disabled by default.

To enable your API Key:

1. From the **Settings** menu, select **General Settings**, and then select **REST API**.
2. Select the **Enable REST API** option, which generates a new API Key.

Figure 11-1 API Key

Use the **Copy** button located next to each key/value pair in the REST API General Settings section. When you click **Copy**, the corresponding key/value pair is copied to the clipboard.

If the **Enable REST API** option is deselected, the API Key will automatically be deleted, which disables the REST API. For more information how to use the API Key and the new REST API, see "[Getting Started](#)".

Note

It is strongly recommended that you store your API Key in a safe and secret place. For example, your script's configuration files.

Note

After closing the **Settings** dialog box the API Key will no longer be displayed. The API Key is displayed only once when it is first created.

The graphic shows the General Settings REST API page.

Getting Started

To get started with using the new REST API please make sure you have your API Key enabled as described in "[API Key](#)".

To test if everything is setup correctly please open a terminal window and have your API Key ready. We are going to use the curl command to call the REST API. Please note that this is an example. What we are doing is essentially just placing a HTTPS request with a custom header **-X-API-Key** (the custom header contains the API Key). (We use the **-k** option to make sure that we don't run into any certificate complications when using the API).

Example call:

```
curl -k -X POST -H "X-API-Key: musterman;samplehexcode" https://mypalladion.com/me/saveApplianceConfiguration
```

Please replace **musterman;samplehexcode** with your personal API Key. If the API Key is correct and all parameters are provided as per reference, then the HTTP response will be 200 OK with the JSON response containing a **success** field that will have the value **true**.

Usecase Backup

With the new REST API it is now possible to create and download savepoints of configurations automatically. To achieve this we are going to use the **saveApplianceConfiguration** and **downloadApplianceConfiguration** methods.

First we will call the **saveApplianceConfiguration** method, which will create a new savepoint on the server and return the name of the savepoint upon success.

In the second step we will then call the **downloadApplianceConfiguration** method with the filename we just received as a parameter to download the configuration file to our local computer.

The two scripts below automate the task of downloading a configuration savepoint using the two API functions we just discussed. In both scripts it is assumed that the IP address of the instance we want to backup is ME_IP and our API Key is **API_KEY**.

Python 3.9:

```
import requests

API_KEY = 'username;somehexcode'
URL = 'https://' + ME_IP + '/me/'
HEADERS = {'X-Api-Key': API_KEY}

resp = requests.get(URL+'saveApplianceConfiguration', headers=HEADERS)
remote_cfg = None

if resp.status_code == 200:
    data = resp.json()
    remote_cfg = data['name']
else:
    print('Unexpected status code: ' + str(resp.status_code))
    exit()

resp = requests.get(URL+'downloadApplianceConfiguration',
                    headers=HEADERS,
                    params={"name": remote_cfg})

if resp.status_code == 200:
    with open(remote_cfg, 'w') as f:
        f.write(resp.text)
else:
    print('Unexpected status code: ' + str(resp.status_code))
```

Even less code is required when Bash scripting is used. The Bash scripting example uses the **curl** command to call the REST API.

```
#!/usr/bin/env bash

API_KEY="X-Api-Key: username;somehexcode"
URL="https://ME_IP/me/"
SAVE_URL="${URL}saveApplianceConfiguration"
DOWNLOAD_URL="${URL}downloadApplianceConfiguration"

remote_cfg=$(curl -k -s -X GET -H"${API_KEY}" $SAVE_URL | grep -Po 'Palladion\-
```

```
configuration.*\cfg')  
  
curl -k -s -H "${API_KEY}" -d"name=${remote_cfg}" -o ${remote_cfg} $DOWNLOAD_URL
```

Usecase High Availability

High availability can be achieved by setting up two Mediation Engines — one master and one slave — with a load balancer in front of the two.

In a high-availability setup, it is important to keep the configuration of the master and slave instances synchronized. With the new REST API, you can utilize a simple bash script to download the configuration from the master (as seen in the previous example) and upload and restore it on the slave.

For uploading a configuration file to an instance, use the **uploadApplianceConfiguration** API call, and for restoring the configuration after it has been uploaded, use the **restoreApplianceConfiguration** API call.

The following example shows how you can use bash script to automate your setup:

```
#!/usr/bin/env bash  
  
API_KEY="X-Api-Key: my_api_key "  
URL="https://my_ip/me/"  
UPLOAD_URL="${URL}uploadApplianceConfiguration"  
RESTORE_URL="${URL}restoreApplianceConfiguration"  
local_cfg="Palladion-configuration-10042014-1.cfg"  
  
curl -k -s -X POST -H"${API_KEY}" -F configuration=@"${local_cfg}" ${UPLOAD_URL}  
curl -k -s -X POST -H"${API_KEY}" -d"configuration=${local_cfg}" ${RESTORE_URL}
```

Note

When using Mediation Engine with a Mediation Engine Connector, it is not possible to restore the configuration savepoint.

Examples

List the last 20 calls:

```
curl -k -X POST -H "X-API-Key: API_Key" -d "limit=20" "https://IP:Port/me/getPagedCalls"
```

where,

- *API_Key*, is your personal key code. For more information on how to generate this key, see ["API Key"](#).
- *IP*, is the IP address of Oracle Communications Session Monitor Mediation Engine.
- *Port*, is the port number of the SSL web interface of Mediation Engine. The *:Port* section can be omitted if the default HTTPS port (443) is used.

Get the next 20 calls (after executing the previous example):

```
curl -k -X POST -H "X-API-Key: API_Key" -d "limit=20&older_than=next_value"
"https://IP:Port/me/getPagedCalls"
```

Where *next_value* is the returned content of the **next_value** field from the previous example.

List all failed calls starting from last week, from a specific caller:

```
curl -k -X POST
-H "X-API-Key:API_Key"
-d 'filters=[{"field":"src_user","data":{"type":"string","value":"src_user"}},
{"field":"setup_start_ts","data":{"type":"datetime","comparison":"gt",
"value":"start_date"}},
{"field":"state_msg","data":{"type":"list","value":["Failed"]}]'
"https://IP:Port/me/getPagedCalls"
```

Where,

- *src_user*, is the ID of the user whose failed calls your retrieving.
- *start_date*, specifies the starting date to retrieve failed calls. The format is YYYY-MM-DD hh:mm:ss, for example 2015-04-13 00:00:00.

Reference

This section lists the most common API calls. However if you want to access a feature of Operations Monitor through the new REST API that is not listed here, see ["Reverse Engineering of API Calls"](#).

Note

All parameter names and options (given in round brackets, separated by vertical lines) are case sensitive.

Note

All parameters are mandatory with all REST API calls unless marked as **optional**. This is not enforced by the server. For many parameters fall back values are defined. You are strongly advised not to rely on these fall back values as any software updates could break your code in the case that fall back values have been changed.

Fundamental Concepts

Please note that there are some basic principles to the new REST API that you should know in order to have a better understanding of the API:

- All REST API calls are made using HTTPS. Any requests using plain HTTP will result in a HTTP/1.1 301 Moved Permanently.
- All parameters of calls are transmitted as HTTP header fields.

- Responses are JSON Objects.
- If the API call succeeded the response will be a **200 Ok** HTTP message and the **success** field of the response will have the value **true**.
- If a call doesn't succeed, the response will be a **200 Ok** HTTP message too. The **success** field of the response however will be **false** and there will be a field **errorMsg** containing a brief description of what went wrong.

Note

In some cases instead of a **200 Ok** HTTP message, a **404** type message will be returned. In this rare event instead of a JSON object a HTML string, containing an error page, will be returned. So please be sure to also check for **404**, and **301** HTTP responses (see above) when checking for errors!

- Often calls have a method for limiting the result set. This is done just as in the database world where you can specify from which element you want to start and how many elements you want to have returned at most.
- The filtering concept that is used in **getPagedCalls** is also available for any other data that is being presented as a sortable grid with optional filters in Operations Monitor. For more information on how to design filters and reverse engineer the API for any other data accessible through Operations Monitor, see "[Examples](#)" and "[Reverse Engineering of API Calls](#)".

In order to get a better understanding of all these concepts please feel free to play around with the little snippets presented in the "[Examples](#)" section.

Configuration Savepoints

Note

For security reasons, REST APIs are not stored in configuration savepoint.

[Table 11-1](#) describes the **/me/saveApplianceConfiguration** savepoint object.

Table 11-1 **/me/saveApplianceConfiguration**

Description	Method	Parameters	Returns
Creates a savepoint on the server and returns the name of the savepoint.	POST	None.	<i>name</i> Name of the save point.

[Table 11-2](#) describes the **/me/uploadApplianceConfiguration** savepoint configuration.

Table 11-2 /me/uploadApplianceConfiguration

Description	Method	Parameters	Returns
Uploads a savepoint to the Server and returns the name of the savepoint.	POST	<i>configuration</i> Local file name. <i>name</i> "configuration".	<i>name</i> Name of the save point on the server.

[Table 11-3](#) describes the **/me/downloadApplianceConfiguration** savepoint object.

Table 11-3 /me/downloadApplianceConfiguration

Description	Method	Parameters	Returns
Downloads a previously saved or uploaded configuration savepoint.	POST	<i>name</i> Name of the savepoint to be downloaded.	The requested file. File name is included in the content-disposition Response Header field.

[Table 11-4](#) describes the **/me/restoreApplianceConfiguration** savepoint object.

Table 11-4 /me/restoreApplianceConfiguration

Description	Method	Parameters	Returns
Restores a previously saved to uploaded savepoint.	POST	<i>configuration</i> Name of the savepoint to be restored.	<i>warnings</i> Warnings that occurred during the restore process, separated by newline characters.

[Table 11-5](#) describes the **/me/deleteApplianceConfiguration** savepoint object.

Table 11-5 /me/deleteApplianceConfiguration

Description	Method	Parameters	Returns
Deletes a savepoint.	POST	<i>name</i> Name of the savepoint to be deleted.	None.

[Table 11-6](#) describes the **/me/listApplianceConfigurations** savepoint object.

Table 11-6 /me/listApplianceConfigurations

Description	Method	Parameters	Returns
Gets list of save points.	POST	<i>start</i> Starting offset for the results to be returned. <i>limit</i> Limits the number of results to be returned. <i>sort</i> Column by which to sort the results ("date" "name"). <i>dir</i> Whether to sort results ascending or descending ("ASC" "DESC").	<i>configurations</i> Array with informations about the individual savepoints. <i>totalCount</i> Number of savepoints in total (not the number of returned savepoints).

Calls

[Table 11-7](#) describes the **/me/getPagedCalls** call object.

Table 11-7 /me/getPagedCalls

Description	Method	Parameters	Returns
Gets a list of calls around a given point in time or around a given call.	POST	<i>filters</i> See the filter design template and the tables below to design your own filters for the result set. If you do not want to filter the result set, please pass an empty list instead (<code>[]</code>). <i>older_than</i> Pass an ID of an element of the result set here to retrieve elements older than the given element. <i>older_than_ts</i> Same as the above, only here you pass the timestamp of an object, not its ID. <i>newer_than, newer_than_ts</i> Same as the above, just into the opposite direction. <i>limit</i> Limits the amount of results to be returned.	<i>calls</i> Array with calls objects. See the below table for details. <i>first_page</i> Whether or not the returned result set is the first page of results available (true false). <i>last_page</i> Whether or not the returned result set is the last page of results available (true false). <i>next_value</i> When you want to retrieve the next page of results using the same parameters, use <i>next_value</i> for the <i>older_than</i> field in the request header.

Filter Design Template

```
{ "field": "<field>", "data": { "type": "<type>", "comparison": "<comparison>",
"value": "<value>" } }
```

Where:

- `<field>` is the name of the field that the filter applies to.
- `<type>` is the type of the filter. Depending on the type of the field there are different filters available. See [Table 11-10](#) for details.
- `<comparison>` is the comparator to be used for filtering. See [Table 11-10](#) for details.
- `<value>` is the value to compare against in the filter. See [Table 11-10](#) for details.

Creating a Filter for a Specific Column

To create a filter for a specific column:

1. Locate the `<field>` value for the desired column (see the **Field (<field>)** column in [Table 11-8](#)).
2. Locate the type of the column (see the **Type** column in [Table 11-8](#)).
3. Refer to [Table 11-10](#) to see which filters are available and how to use them.
4. Refer to "[Examples](#)" and "[Reverse Engineering of API Calls](#)" for in depth examples on how to use **getPagedCalls** and how to watch network traffic to get a better understanding of the API.

[Table 11-8](#) lists the columns and fields in the calls objects that can be filtered.

Note

[Table 11-9](#) lists fields, which are also part of the calls objects that cannot be filtered.

Table 11-8 Fields and Types (in alphabetical order)

Field (<field>)	Type	Column in the Calls Table
call_time	Numeric	Call time
code	Numeric	Code
dpc	String	DPC
dst_codecs	String	Callee Codecs
dst_initial_codecs	String	Callee Initial Codecs
dst_ip	IP address	Callee IP address. For the data field of the filter, set type to ipaddr and value to the IP address string (e.g. 192.168.1.123 or 10.0.0.0/8).
dst_ua	String	Callee User Agent
dst_user	String	Callee
dst_user_pref_tag	Boolean	Preferred Callee Number? For the data field of the filter: • To filter to True, set type to string and comparison to notnull. • To filter to False, set type to string and comparison to null.
dtmf	Boolean	DTMF
egress_devs	List	Egress device(s)
end_ts	Datetime	End timestamp

Table 11-8 (Cont.) Fields and Types (in alphabetical order)

Field (<field>)	Type	Column in the Calls Table
gateway_devs	List	Gateway Devices
in_devs	List	In devices
ingress_devs	List	Ingress device(s)
init_devs	List	Initiator device
megaco_cmds	String	MEGACO Commands
megaco_context_id	String	MEGACO Context ID
megaco_mg_ip	String	MEGACO Gateway
megaco_mgc_ip	String	MEGACO Gateway Controller
megaco_termination_id	String	MEGACO Termination ID
megaco_txids	String	MEGACO Transaction IDs
mgcp_call_ids	String	MGCP Call IDs
mgcp_capabilities	String	MGCP Capabilities
mgcp_connection_ids	String	MGCP Connection IDs
mgcp_mg_ip	String	MGCP Gateway IP
MOSlqe_avg	Numeric	Avg. MOS
MOSlqe_min	Numeric	Min. MOS
nlegs	Numeric	Segments
opc	String	OPC
out_devs	List	Out devices
pai	String	P-Asserted-ID
prefix_group	List	Prefix Group
q850_code	Numeric	Q.850 Code
q850_state_details	String	Q.850 Details
q850_state_msg	String	Q.850 State
realms_recordings	Boolean	Media For the data field of the filter, set type to custom:streams_availability and value to false , or true depending on which you want to filter for.
reason_hdr		Reason
rpipid	String	Remote-Party-ID
rtcp_delay_avg	Numeric	Avg RTCP delay
rtcp_delay_max	Numeric	Max RTCP delay
rtcp_streams	Numeric	RTCP streams
setup_delay	Numeric	Setup Delay
setup_delay_type	List	Setup Delay Type With this column you have two options which you can filter for. You may filter for either one, or both options: - To filter for Successful Session Request Delay include 1 (as a String) in the list you pass for <value>. - To filter for Failed Session Request Delay include the String 2 in the list you pass for <value>.

Table 11-8 (Cont.) Fields and Types (in alphabetical order)

Field (<field>)	Type	Column in the Calls Table
setup_start_ts	Datetime	Start timestamp
setup_time	Numeric	Setup time
src_codecs	String	Caller Codecs
src_initial_codecs	String	Caller Initial Codecs
src_ip	IP address	Caller IP address. For the data field of the filter, set type to ipaddr and value to the IP address string (e.g. 192.168.1.123 or 10.0.0.0/8).
src_ua	String	Caller User Agent
src_user	String	Caller
src_user_pref_tag	Boolean	Preferred Caller Number? For the data field of the filter: - To filter to True, set type to string and comparison to notnull. - To filter to False, set type to string and comparison to null.
state_details	String	State details
state_msg	List	State Options are as follows: - Blocked - Busy - Canceled - Error - Established - Failed - Finished - Not Found - Off-line - On hold - Proceeding - Redirected - Reset - Ringing - Setup - Terminate - Timed out - Unauthorized - Unequipped You may filter for one or more of the above options. Just include the desired value(s) from the above list as Strings in the array you pass for <value>.
term_devs	List	Terminator device

[Table 11-9](#) lists fields that are not in the above table (cannot be filtered) but are part of the calls objects:

Table 11-9 Call Object Fields that Cannot be Filtered

Field	Description
pid	Process ID.
id	ID of the call. A call is uniquely identified through its pid and id .
id32	Internal only.
strictly_increasing	ID which can be used for sorting call events chronologically.
state	Numeric representation of state.
state_cls	Color of state. - Green - Calls in Established State - Black - Calls in Finished State - Red - Timed-Out or Failed - Orange - Cancelled/Offline Calls
end_ts	Timestamp of when the call was finished.
mos_cls	Color of the mos column.
overload	Whether during the processing of the call a system overload occurred.
number_prefix	Contains a comma separated list for all the number prefixes, that the respective call is matching.

[Table 11-10](#) lists all available filter types. Please note that the table has been grouped by column data type (see above table) to show which filter options are available for the corresponding field type.

Table 11-10 Filter Types (grouped by column data types)

Type (<type>)	Comparators (<comparison>)	Description
String exactstring string	None. None.	Matches exact string. Match string.
DateTime date datetime datetime_utc	lt gt eq neq leq geq (lt gt eq neq leq geq) (lt gt eq neq leq geq)	less than (before given date) (<). greater than (after given date) (>). equal (on the given date) (=). not equal (not on the given date) (!=). less or equal (on or before the given date) (<=). greater or equal (on or after the given date) (>=). Equals only compares dates. Equals only compares dates. Use this version if <value> is a UTC timestamp.
Numeric numeric	(lt gt eq neq leq geq)	Does the job of any first grader only slightly faster.
List in_list list not_in_list	None. None. None.	Matches one value of the array given in <value>. Matches at least one element of the array given in <value>. Does not match a value of the array given in <value>.

[Table 11-11](#) describes the `/me/getCallDetails` call object.

Table 11-11 */me/getCallDetails*

Description	Method	Parameters	Returns
After you called <i>getPagedCalls</i> to retrieve a list of calls you can use <i>getCallDetails</i> to obtain further information about a specific call.	POST	<i>id</i> ID of call as returned in the id field of a call. <i>pid</i> As returned in the pid field of a call. <i>saved_id</i> (Optional) Instead of passing the previous two IDs you can just pass this ID in case you saved this call. <i>no_legs</i> (true false).	An array with essentially the same fields as <i>getPagedCalls</i> but also a few additional fields: <i>legs</i> - Array with the legs of the call. <i>megaco_id</i> - Megaco ID. <i>merged_into_call_id</i> <i>total_legs</i> - Total amount of legs. Internal only fields: <i>mgcp_id</i> <i>mgcp_mgc_ip</i> <i>mgcp_txids</i> <i>mgcp_verbs</i> <i>traversing_devs</i>

[Table 11-12](#) describes the */me/getCallMsgs* call object.

Table 11-12 */me/getCallMsgs*

Description	Method	Parameters	Returns
Returns the SIP messages associated with a given call.	POST	<i>id</i> ID of call as returned in the id field of a call. <i>pid</i> As returned in the pid field of a call. <i>saved_id</i> (Optional) Instead of passing the previous two IDs you can just pass this ID in case you saved this call.	<i>proto</i> Protocol. <i>src_ip</i> Source IP. <i>src_mac</i> Source Mac. <i>opc</i> Source PC. <i>dst_ip</i> Destination IP. <i>dst_mac</i> Destination MAC. <i>dpc</i> Destination PC. <i>ts</i> Date and Time. <i>method</i> Message. <i>ruri</i> Details

[Table 11-13](#) describes the */me/getCallsTime* call object.

Table 11-13 */me/getCallsTime*

Description	Method	Parameters	Returns
Returns the current time stamp (for use in for example <i>getPagedCalls</i> as value for the <i>older_than_ts</i> parameter) and the time stamp of the latest call.	POST	None.	<i>ts_first</i> Timestamp of the first call in the database. <i>ts_now</i> Current timestamp - can be used as a value for <i>older_than_ts</i> . For example in <i>getPagedCalls</i> .

[Table 11-14](#) describes the */me/getAvailablePcaps* call object.

Table 11-14 */me/getAvailablePcaps*

Description	Method	Parameters	Returns
Get the available pcaps and the streams available in the respective pcap.	POST	<i>id</i> ID of call as returned in the id field of a call. <i>pid</i> As returned in the pid field of a call. <i>saved_id</i> (Optional) Instead of passing the previous two IDs you can just pass this ID in case you saved this call	<i>available</i> An object which contains all available recorded streams for the specified user grouped by stream type.

[Table 11-15](#) describes the */me/callPcap* call object.

Table 11-15 /me/callPcap

Description	Method	Parameters	Returns
Download a pcap file for a specific call.	POST	<i>id</i> ID of call as returned in the id field of a call. <i>pid</i> As returned in the pid field of a call. <i>saved_id</i> (Optional) Instead of passing the previous two IDs you can just pass this ID in case you saved this call. <i>filename</i> If this is not empty it is going to be the filename of the pcap file that is retrieved from the server. <i>streams</i> Array which includes which stream types you would like to retrieve. Include the string "EN10MB" in the array to include signaling messages, and for every stream for which you want to retrieve the RTP payload include a string of the format: "<Media type>#<src_ip>:<src_port>#<dst_ip>:<dst_port>#<media_content_type>" Example: "MEDIA#62.220.31.225:19848#62.220.31.239:27998#rtp_full" If the above fields are not familiar please make sure to experiment with <i>getAvailablePcaps</i> and play around with the RTP recording feature and the save PCAP feature in the regular Operations Monitor web interface.	The requested pcap file.

Registrations

[Table 11-16](#) describes the **/me/getRegsPaged** registrations object.

Table 11-16 /me/getRegsPaged

Description	Method	Parameters	Returns
Retrieves a list of registrations around a point in time or around another registration.	POST	<i>filters</i> See the Filter Design Template section to design your own filters. <i>older_than</i> Pass an ID of an element of the result set here to retrieve elements older than the given element. <i>older_than_ts</i> Same as the above, only here you pass the timestamp of an object- not its ID. <i>newer_than, newer_than_ts</i> Same as the above, just into the opposite direction.	<i>data</i> Array containing all registrations of the current result set. Fields contained in data: <i>dev_id</i> – Registrar. <i>code</i> – Code. <i>contacts</i> – Contacts. <i>ip</i> – Source IP address. <i>ts</i> – Timestamp. <i>type_msg</i> – Event. <i>user</i> – User. <i>dest_ip</i> – Destination IP address. <i>first_page</i> Whether or not the returned result set is the first page of results available (true false). <i>last_page</i> Whether or not the returned result set is the last page of results available (true false). <i>next_value</i> When you want to retrieve the next page of results using the same parameters, use <i>next_value</i> for the <i>older_than</i> field in the request header.

[Table 11-17](#) describes the **/me/getRegsTime** registrations object.

Table 11-17 /me/getRegsTime

Description	Method	Parameters	Returns
Returns the current time stamp (for use in for example <i>getPagedRegs</i> as value for the <i>older_than_ts</i> parameter) and the timestamp of the latest registration.	POST	None.	<i>ts_first</i> Timestamp of the first registration result set using the passed filters. <i>ts_now</i> Current timestamp- can be used as a value for <i>older_than_ts</i> for example in <i>getPagedCalls</i>.

[Table 11-18](#) describes the **/me/getRegEvent** registrations object.

Table 11-18 */me/getRegEvent*

Description	Method	Parameters	Returns
Gets details about a registration event.	POST	<i>id</i> ID of the event for which you want to retrieve the SIP messages.	<i>reg</i> Array containing the SIP messages for the specified event.

[Table 11-19](#) describes the */me/getRegEvMsgs* registrations object.

Table 11-19 */me/getRegEvMsgs*

Description	Method	Parameters	Returns
Gets the SIP messages for a specified event.	POST	<i>id</i> ID of the event for which you want to retrieve the SIP messages. <i>start</i> Starting offset for the results to be returned. <i>limit</i> Limits the amount of results to be returned.	<i>totalCount</i> Total count of the result set - not the amount of elements returned. <i>data</i> Array with the requested SIP messages.

Fields and Types for getRegsPaged

Table 11-20 */me/getRegsPaged*

Field (<field>)	Type	Column in the Calls Table
user	strings	User
contacts	strings	Contacts
ip	strings	Source IP address
dest_ip	strings	Destination IP addresss
ts	datetime	Timestamp
dev_id	list	Registrars
type_msg	list	Event • New • Failed • Unauthorized • Expired • Gone
code	numeric	Code

KPI

[Table 11-21](#) describes the */me/getCounterValues* KPI object.

Table 11-21 */me/getCounterValues*

Description	Method	Parameters	Returns
Returns counters marked as favorites and their recent values.	POST	None.	<i>counters</i> An array containing the requested counters.

[Table 11-22](#) describes the */me/addOrModifyCounter* KPI object.

Table 11-22 */me/addOrModifyCounter*

Description	Method	Parameters	Returns
Add or modify a counter.	POST	<i>action</i> Whether to edit or add a counter ("add" "edit"). <i>snmp_export</i> (Optional) Set this to "on" to enable snmp export, or do not use this parameter to disable snmp export. <i>maintype</i> Numeric representation of the counter. Use <i>getCounterTypes</i> to find out the main types of counters. <i>subtype</i> Numeric representation of the counter. Use <i>getCounterTypes</i> to find out the subtypes of counters. If you want to create an average counter include the three properties below: <i>weekdays</i> (Optional) Set weekdays to 1 if you want the average to be taken only over weekdays otherwise set it to 0. <i>days</i> (Optional) The average will be taken over the amount of days specified here. <i>name</i> (Optional) The name for the average counter.	<i>id</i> ID of the added or changed counter.

[Table 11-23](#) describes the */me/deleteCounter* KPI object.

Table 11-23 */me/deleteCounter*

Description	Method	Parameters	Returns
Removes a counter.	POST	<i>id</i> ID of the counter to be removed.	None.

[Table 11-24](#) describes the */me/toggleSNMPExport* KPI object.

Table 11-24 */me/toggleSNMPExport*

Description	Method	Parameters	Returns
Enables or disables the SNMP export of a counter.	POST	<i>ids</i> List of counter IDs. <i>action</i> (<i>'enable'</i> <i>'disable'</i>).	None.

[Table 11-25](#) describes the */me/getCounterRealm* KPI object.

Table 11-25 */me/getCounterRealm*

Description	Method	Parameters	Returns
Get a counter's realm.	POST	<i>id</i> ID of the counter.	<i>realm</i> Realm of the given counter.

[Table 11-26](#) describes the */me/getCounterConfig* KPI object.

Table 11-26 */me/getCounterConfig*

Description	Method	Parameters	Returns
Retrieves the configuration of a user counter. You can modify the returned configuration and pass it to <i>addOrModifyCounter</i> to update/create a counter with the modified configuration.	POST	<i>id</i> ID of the user counter to be retrieved.	<i>data</i> An object with the configuration fields of the desired counter: <i>id</i> – ID of the counter (numeric). <i>name</i> – Name of the counter. <i>service_id</i> – Internal only. <i>maintype</i> – Numeric main type of the counter. <i>subtype</i> – Numeric sub type of the counter. <i>snmp_export</i> – Boolean if snmp export is enabled. <i>src_cnt</i> – For average counters, the source counter for the average. <i>weekdays</i> – For average counters, whether the average is calculated for each weekday separately. <i>days</i> – For average counters, whether the average is calculated for each weekday separately. <i>param1</i> – First counter parameter. <i>param2</i> – Second counter parameter. <i>param3</i> – Third counter parameter.

[Table 11-27](#) describes the */me/getSimpleCounters* KPI object.

Table 11-27 */me/getSimpleCounters*

Description	Method	Parameters	Returns
Gets counters which are no average counters.	POST	<i>device_id</i> Device ID of the counter. <i>tag_id</i> Tag ID of the counter.	<i>counters</i> Object containing the following fields: <i>id</i> – ID of the counter (numeric). <i>name</i> – Name of the counter. <i>subtype</i> – Numeric sub type of the counter. <i>owner</i> – Owner of the counter. <i>params</i> – List with the first, second and third parameter of the filter

[Table 11-28](#) describes the */me/getCounters* KPI object.

Table 11-28 /me/getCounters

Description	Method	Parameters	Returns
Gets all types of counters- even if they are average counters.	POST	<i>device_id</i> Device ID of the counter. <i>tag_id</i> Tag ID of the counter.	<i>counters</i> Object containing the following fields: • <i>id</i> – ID of the counter (numeric). • <i>maintype</i> – Main type of counter. • <i>name</i> – Name of the counter. • <i>subtype</i> – Numeric sub type of the counter. • <i>owner</i> – Owner of the counter. • <i>params</i> – List with the first, second and third parameter of the filter.

[Table 11-29](#) describes the **/me/counters** KPI object.

Table 11-29 /me/counters

Description	Method	Parameters	Returns
Get all visible counter IDs.	POST	<i>alias</i> (true false) Whether or not to include the user's aliases in the search for counters.	<i>counters</i> List with IDs of visible counters.

[Table 11-30](#) describes the **/me/getCounterTotal** KPI object.

Table 11-30 /me/getCounterTotal

Description	Method	Parameters	Returns
Gets the current and maximum allowed amount of counters.	POST	None.	<i>total</i> Total count of current counters. <i>max_counters</i> Maximum possible amount of counters. <i>counters_lock</i> Whether there is currently an operation on the counters active.

[Table 11-31](#) describes the **/me/getCounterTypes** KPI object.

Table 11-31 */me/getCounterTypes*

Description	Method	Parameters	Returns
Gets the counter types with names and parameters.	POST	All parameters are optional: • <i>device_id</i> Device ID of counter. • <i>device_list</i> List of devices. • <i>iptag_list</i> List of IP tags. • <i>iptag_id</i> IP tag ID. • <i>tag_id</i> Tag ID. • <i>only_active</i> (true false) Whether to return only active counters. • <i>remove_create_new</i> Description.	List with counters, fitting the given parameters.

[Table 11-32](#) describes the */me/MonitorGraph* KPI object.

Table 11-32 */me/MonitorGraph*

Description	Method	Parameters	Returns
Draws and returns a counter graph.	POST	All parameters are optional: • <i>period</i> int - period in seconds. • <i>utcdatetime</i> date in format '2012-10-31T20:16:52Z'. • <i>format</i> Call returns a SVG image, if parameter is "svg"- else returns a PNG image (or JSON- see <i>raw_data</i>). • <i>raw_data</i> (true false) If True, return json, no image. • <i>selected</i> A list of IDs to determine which metrics to render. • <i>tzoffset</i> Offset for the time zone.	<i>data</i> JSON object with the raw data in case <i>raw_data</i> was set to true. Else the requested image file.

Reverse Engineering of API Calls

As stated earlier, the above documentation only covers the most important features of the new REST API. With the new API Key however you have the same access to the features of Operations Monitor as with the regular web interface. So in the following section we will be

using the Google Chrome browser's development tools to reverse engineer how to use API calls that are not documented here. You can also follow this guide using the Mozilla Firefox browser in conjunction with the Firebug extension. It is a fairly straightforward process though - so if you're impatient go ahead and use the web interface of Operations Monitor and watch the network activity while you're at it to figure out how to use parts of the API not covered here. For an in-depth guide how to achieve this goal please continue reading.

Note

When watching the network activity of Operations Monitor you will often see URLs that have a weird suffix.

For example:

```
getSystemSettings/?_dc=1398269727192
```

The suffix is pretty much a timestamp appended by our frontend framework. This is done to avoid any possible caching of HTTP requests by altering the URL with the timestamp. This is done to ensure that any results are always directly from the server and not any outdated, cached results.

This scenario is very unlikely however and is merely a workaround to bad network configuration. You can go ahead and ignore this parameter when analyzing backend calls and leave the parameter out when using backend calls from a custom script.

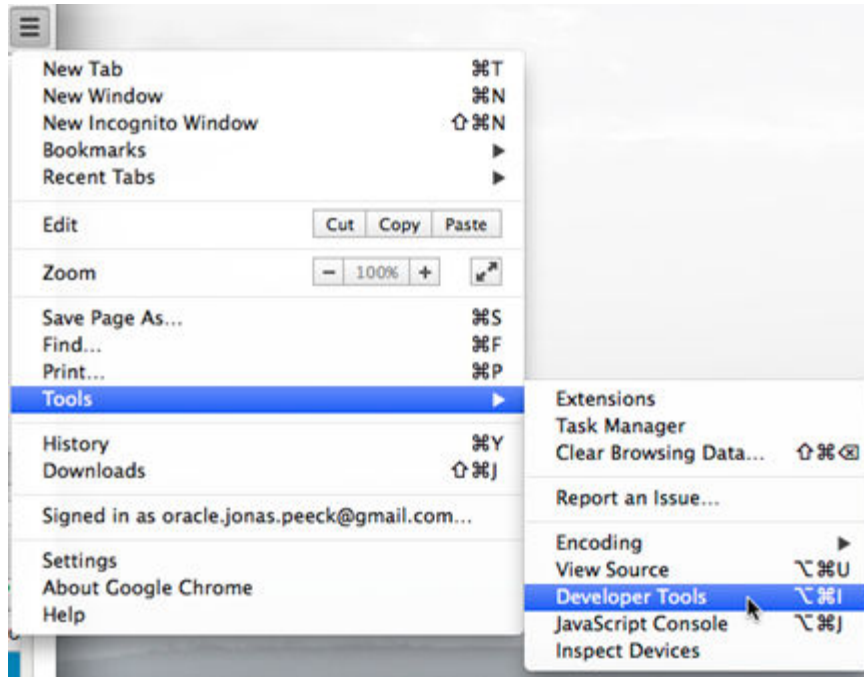
As you might recall Operations Monitor has a feature for saving calls (you might have noticed that in many Calls related API calls you can pass a **saved_id** for identifying a call instead of the **id** and the **pid**). If we were to use that functionality through a script an interesting use case might be to save certain calls in the course of an operation, in order to have a human user review these later.

So let's find out, how to save calls using the new REST API. In order to walk you through the process you need to have a good understanding of how the new REST API works. If you think you might need a refresher on that please head over to the **API Key** and the **Getting Started** sections and have a quick look at our use cases **Usecase Backup** and **Usecase High Availability**.

To get started, please retrieve your API Key, and have your tools ready for action.

Next go to the **Calls** section in the web interface of Operations Monitor.

Go ahead and open the developer tools so that we know what's going on in the background. Click the Customize and control Google Chrome icon to access **Developer Tools** as shown in [Figure 11-2](#):

Figure 11-2 Accessing the Google Chrome Developer Tools

Please make sure that you have the **Network** tab open and that recording is enabled, so that we can observe the network activities that are happening in the background while using the web interface of Operations Monitor.

In the **Recent calls** section of the web interface of Operations Monitor, double click on any call to open up the call details dialog.

On the bottom of the now open dialog you will find a set of buttons, including a **Save** button, place your mouse cursor above that button and use it by firmly pressing your left mouse button.

Now it's time to name the to be saved call. Please use the name **TestSavedCall123456789** or a name that will be easily recognizable as your custom name.

Next, if you click **Save**, you should see a **saveCall** https call popup in the network monitoring section of the developer tools as shown in [Figure 11-3](#). You may go ahead and stop the recording of network activity at this point as we have all the info we need to find out how to use this call in the future.

Figure 11-3 saveCall https Call Popup

The screenshot displays the Oracle Operations Monitor interface. On the left, a list of requests is shown, with 'saveCall /me' selected. The main panel on the right shows the details for this request, including the Remote Address, Request URL, Request Method, Status Code, and Request Headers. The status code is 200 OK. The request headers include Accept, Accept-Encoding, Accept-Language, Cache-Control, Connection, Content-Length, Content-Type, Cookie, Host, Origin, Pragma, Referer, and User-Agent.

Name	Path	Headers	Preview	Response	Cookies	Timing
☐	pulse?_dc=1403111491073 /me					
☒	saveCall /me	Remote Address: 10.165.75.127:443 Request URL: https://10.165.75.127/me/saveCall Request Method: POST Status Code: 200 OK				
☐	log /me					
☐	MonitorGraph?aggregate=false&selected=270&wid... /me					
☐	MonitorGraph?aggregate=false&selected=272&wid... /me					
☐	MonitorGraph?aggregate=false&selected=270&wid... /me					
☐	MonitorGraph?aggregate=false&selected=272&wid... /me					

15 requests | 71.7 KB transferred

Scroll down to the section **Form Data** as shown in [Figure 11-4](#).

Figure 11-4 The Form Data Section of the saveCall Request

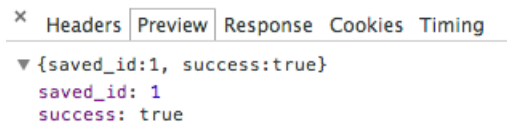
The screenshot shows the 'Form Data' section of the saveCall request. It lists the pid, id, and name of the saved call. The response headers are also visible, including Connection, Date, and Server.

Headers	Preview	Response	Cookies	Timing
Pragma: no-cache Referer: https://10.165.75.127/me/ User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_3) AppleWebKit X-Requested-With: XMLHttpRequest				
Form Data pid: 1401969361 id: 2 name: TestSavedCall123456789				
Response Headers Connection: keep-alive Date: Wed, 18 Jun 2014 17:11:34 GMT Server: Apache/2.4.6 (Ubuntu)				

Here we can easily read out the parameters for the **saveCall** request:

- *pid*
The Process ID of the call we opened and saved.
- *id*
The ID of the call we saved.
- *name*
The name for the saved call as previously entered.

If you now switch to **Preview** tab of the request we can discover the returns of this call as shown in [Figure 11-5](#):

Figure 11-5 Preview Tab

- *saved_id*

The **saved_id** of the call we just saved. In the future we may use this to identify this call instead of using the **id** and **pid** parameter.

- *success*

This field is always part of the return if no error occurred.

And with that you now know how to save calls using the new REST API. You can use the same approach for any other functionality in the web interface of Operations Monitor that you would like to automate.

All you have to do is to play around with the web interface a bit and see how requests behave differently based on changes you perform.

12

Client-Side Add-Ons

Apps provide an easy way to customize and extend Oracle Communications Operations Monitor with capabilities that are not currently present in the user interface using Javascript and CSS.

You can enable or disable add-ons at login time using the **Disable add-ons** check box from the login form. The check box label shows the number of enabled extensions that will be loaded (unless the check box is selected), and the tooltip shows the name and the description of each add-on.

Note

Any pre-5.0 customized add-on may not work after upgrading to Session Monitor Release 6.1. Please consult with Oracle representatives for further support.

Structure of an Add-On

A valid Operations Monitor add-on consists of a **manifest.json** file and a set of files that will be exposed to the client. The **manifest.json** file must be a valid JSON file and include the fields found in [Table 12-1](#):

Table 12-1 manifest.json File Required Fields

Field	Description
api_version	The current supported API version is "0.1.0".
Description	Describes the functions of the add-on.
name	Name of the extension. This name will be used as the extension files path in the server

Example:

```
{  "api_version":
    "0.1.0",  "description": "Display Blue
    style",  "name":
    "p1_ojet"
}
```

Creating Customized Add-ons

Starting with the Session Monitor 5.0 release, the working functionality of the custom add-ons has changed.

Here is a sample demonstration of an add-on where you can add a simple text on the header of Operations Monitor GUI.

1. As an example, create a simple add-on on the header of the Operations Monitor.

2. Open the file **header.js**. You can find the file under in the path for the JavaScript code: `/opt/oracle/ocsm/usr/share/acme/public/web/js/viewModels/child`. This is the Javascript file.

```
self.headerAddonFlag = ko.observable(false);
self.sampleAddonFunction = function(){
    if (self.psaArrayFromController.includes('sampleaddon')) {
        self.headerAddonFlag(true);
        console.log ("Simple custom addon on OCOM 5.0")
    }
    else{
        self.headerAddonFlag(false);
    }
}
self.sampleAddonFunction();
```

3. Add the above function and call it. Check if the **sampleaddon** is enabled. If it is enabled then make a flag true and text is visible on the header.
4. For the HTML, code file is `header.html`: `/opt/oracle/ocsm/usr/share/acme/public/web/js/view/child`.

```
<oj-bind-if test="[[headerAddonFlag()]]">
  <div>
    <h3>
      <div style="background-color:powderblue;">
        <oj-bind-text style="color: blueviolet;"
value="Sample      custom addon">
      </oj-bind-text>
    </div>
  </h3>
</div>
</oj-bind-if>
```

Note

Write the above OJET code exactly where you want to have the text of addon. In this case, we are adding in the Header.

5. Create a file called `manifest.json` and its content is as follows:

```
{
  "api_version": "0.1.0",
  "description": "Demonstration of an addon",
  "name": "sampleaddon"
}
```

Note

Ensure that the name of the add-on is the same as the name written in the code - `sampleaddon`.

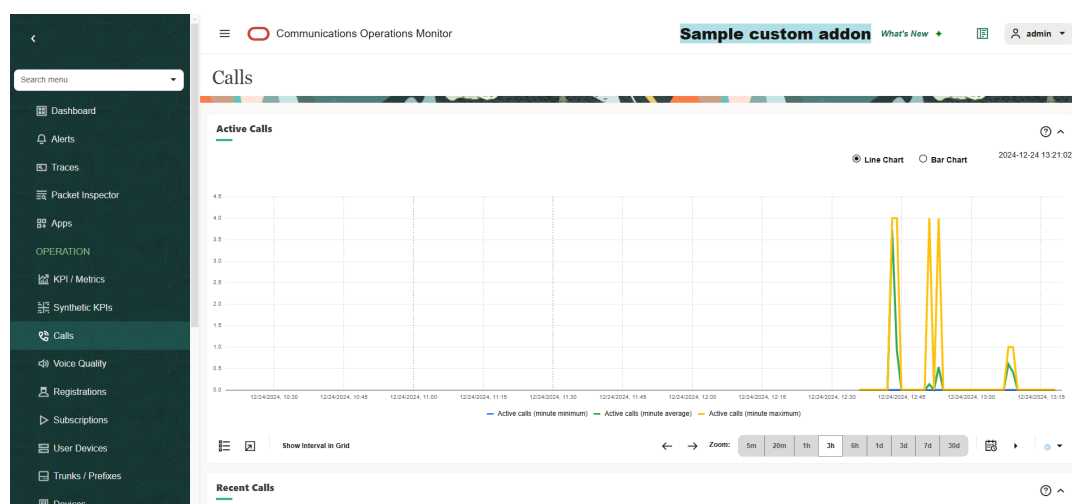
6. Create a folder and compress the contents of the folder into .zip file. This .zip file contains the manifest.json file,
7. Upload the .zip package in the PSA-Add-on and then enable it. If you disable it, it should not be visible.

Note

The files will change if we are working on different regions of Operations Monitor.

Here's a screen grab of the custom add-on.

Figure 12-1 Sample add-on



Packaging

The add-on files must be packed in ZIP format and its filename must use the **.zip** extension. The resulting ZIP file can contain a root folder. The name of that folder is not meaningful. Such a ZIP archive can be uploaded to the Platform Setup Application using the provided form in the Add-ons page.

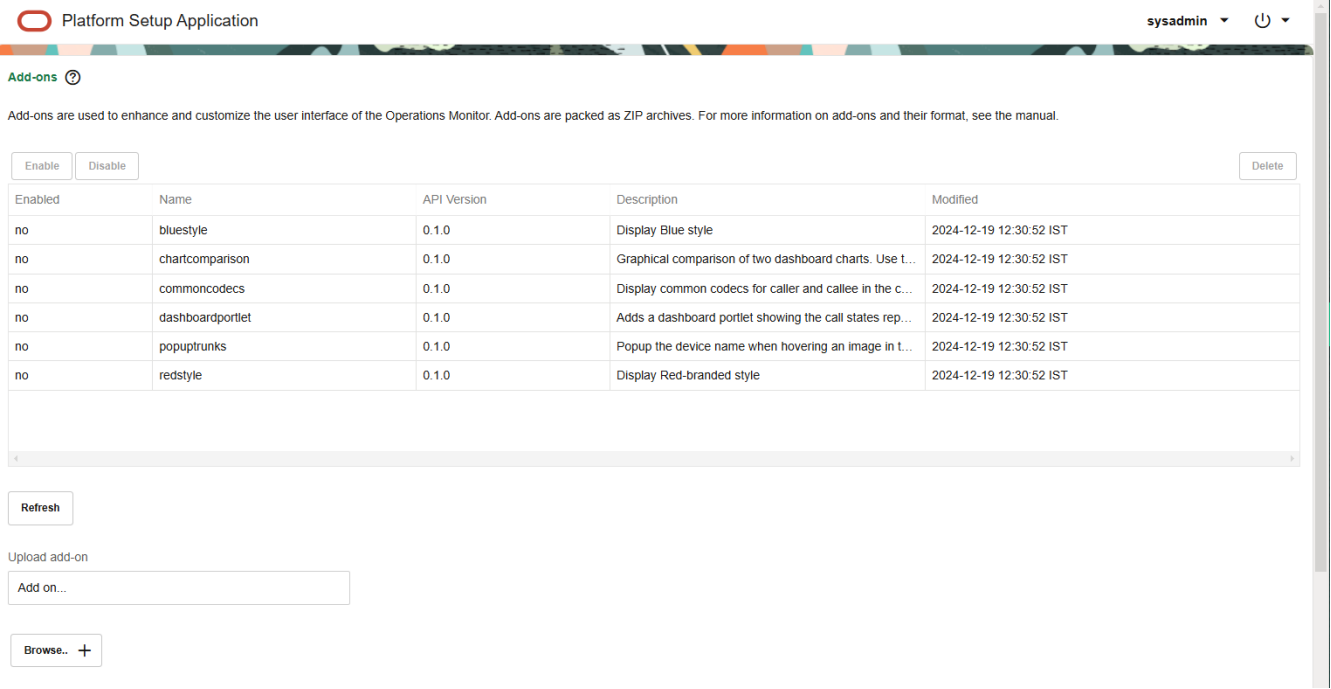
Here is a sample directory structure for the ZIP archive:

```
In file manifest.json:
{
  "api_version": "0.1.0",
  "description": "Demonstration of an add-on",
  "name": "sampleaddon"
}
```

Management

In the Add-ons page of the Platform Setup Application, a grid is provided where the system administrators can enable, disable, and sort the extensions load order. Each extension operation in this page will be applied for all ME active instances immediately on the next page reload. [Figure 12-2](#) shows the Add-ons page.

Figure 12-2 Add-ons Page



Code Examples

Javascript file:

```
self.headerAddonFlag = ko.observable(false);
self.sampleAddonFunction = function(){
    if (self.psaArrayFromController.includes('sampleaddon')) {
        self.headerAddonFlag(true);
        console.log ("Simple custom addon on OCOM 5.0")
    }
    else{
        self.headerAddonFlag(false);
    }
}
self.sampleAddonFunction();
```

HTML File

```
<oj-bind-if test="[[headerAddonFlag()]]">
    <div>
        <h3>
            <div style="background-color:powderblue;">
                <oj-bind-text style="color: blueviolet;"
value="Sample
</oj-bind-text>
                custom addon">
            </div>
        </h3>
```

```
</div>  
</oj-bind-if>
```

13

Diameter Transaction Records (TDRs)

Oracle Communications Operations Monitor creates Diameter Transaction Records (TDR files) in CSV format. The files are placed in the **tdr/** directory under the FTP/FTPS root. The TDR files have the following format:

```
tdr-unix_timestamp-sequence.csv
```

where:

- *unix_timestamp* is the Unix timestamp when the file was created.
- *sequence* is a number monotonically increasing.

The files are rotated when they reach their maximum size (10000 records). When a CSV file is finished, another empty file having the following format is created:

```
tdr-unix_timestamp-sequence.csv.FIN
```

Several times per day, old TDR files are compressed to files having the following format, while the corresponding uncompressed files are deleted:

```
tdr-unix_timestamp-sequence.csv.gz
```

The recommended way of gathering the TDR files is to connect via FTP/FTPS, copy and delete all the files ending in **csv.gz**. Alternatively, to get the TDR data in near real time, the MDR files that have a corresponding **.FIN** file can be copied and deleted.

Operations Monitor automatically limits the size of the **tdr/** directory to 5 GB, by deleting the oldest files.

[Table 13-1](#) lists the fields present in the generated CSV files:

Table 13-1 TDR CSV Fields

Field	Description
application-id	The IANA assigned Application Identifier of the Diameter transaction. The possible values as defined in RFC 5516 are outlined below: • 0: Diameter Common Messages • 1: Nasreq • 2: Diameter mobile ip • 3: Diameter Base Accounting • 0xffffffff: Diameter Relay • 16777216: 3GPP Cx application • 16777251: 3GPP S6a/S6d application • 16777252: 3GPP S13/S13' application • 16777272: 3GPP S6b application • 16777310: 3GPP S6m application

Table 13-1 (Cont.) TDR CSV Fields

Field	Description
command	A human readable string describing the Diameter command-code. Can be one of the following: • Authentication-Information • Cancel-Location • Delete-Subscriber-Data • Insert-Subscriber-Data • Location-Info • ME-Identity-Check • Multimedia-Auth • Notify • Purge-UE • Push-Profile • Registration-Termination • Reset • Server-Assignment • Update-Location • User-Authorization
command-code	The Diameter command code of the transaction. For example for the command UPDATE_LOCATION the code would be 316. All the possible codes are defined in 3GPPTS 29.272 at the interface commands for S6a/S6d and S13.
destination-realm	Contains the realm the messages of a Diameter transaction should be routed to.
dst-dev-id	Identifier of the destination Diameter device.
dst-ip	Destination IP address of the Diameter transaction.
duration	The duration of the transaction in seconds (with a precision of microseconds), from the time the request is received to the time the transaction completes.
IMEI	IMEI value of the user.
internal-id	Unique internal identifier used by Operations Monitor to identify Diameter transactions.
msisdn	The msisdn number of the Diameter transaction identifying the subscription to a mobile network.
network-access-mode	Describes the networks that the user is registered to. Values range from 0 to 2.
network-access-mode-text	Describes the networks that the user is registered to. Possible values can be one of the following: • PACKET_AND_CIRCUIT • Reserved • ONLY_PACKET
origin-realm	Contains the realm of the originator of the Diameter messages of this transaction.
rat-type	A numeric code used to identify radio access technology that is serving the UE. Defined in TS 29212 at section 5.3.31.
realm-ids	Diameter transaction realm ID - not currently exported.
result	Human readable string of the result code.

Table 13-1 (Cont.) TDR CSV Fields

Field	Description
result-code	The numerical value of the Result-Code of the diameter transaction. For example 2001 for DIAMETER_SUCCESS. For all possible values refer to the standards.
session-id	A string with the Session-ID AVP of the Diameter transaction.
src-dev-id	Identifier of the source Diameter device.
src-ip	Source IP address of the Diameter transaction.
start_ts	Time value for the transaction request.
stop_ts	Time value for the transaction response.
timestamp	Unix timestamp of the start of the transaction.
user-name	IMSI used to identify the user of the Diameter transaction.
visited-plmn-id	The decoded visited PLMN ID found in the transaction with the 3 digit Mobile Country Code (MCC) and 2 or 3 digit Mobile Network Code (MNC) as defined in TS 123000 at section 12.1.

Public CDR Generation

Note

CDR file generation can be enabled and disabled using the system setting **Enable CDR Writer**.

Oracle Communications Operations Monitor creates call detail record (CDR) files in CSV format. The files are placed in the **cdr/** directory from the FTP/FTPS root. The CDR files have the following format:

`palladion-unix_timestamp-sequence.csv`

where:

- `unix_timestamp` is the Unix timestamp when the file was created.
- `sequence` is a number monotonically increasing.

The CDR files are rotated whenever one of the following three conditions is met:

- The file reaches the maximum number of records. The maximum size is configurable in Operations Monitor with the system setting, **Maximum lines of a CDR file**. The default is 5000 records.
- The maximum time is reached. The maximum time is configurable in Operations Monitor with the system setting, **Rotate CDR files every N seconds**. The default value is 0 for no time limit.
- There is no new record for 150 seconds.

When a **CSV** file is finished, an empty **CSV** file with the following format is created:

`palladion-unix_timestamp-sequence.csv.FIN`

Several times per day, old CDR files are compressed to files having the following format, while the corresponding uncompressed files are deleted:

`palladion-unix_timestamp-sequence.csv.gz`

The recommended way of gathering the CDR files is to connect via FTP/FTPS, copy and delete all the files ending in **csv.gz**. Alternatively, to get the CDR data in near real time, the CDR files that have a corresponding **FIN** file can be copied and deleted.

Operations Monitor automatically limits the size of the **cdr/** directory to 1 GB, by deleting the oldest files.

One record (CDR) for each call seen is created. If the call is visible in different segments, all of them are taken into account for computing the call details, but only a single record will be written. The call details are always the same as presented in Operations Monitor's web interface.

Operations Monitor also allows the creation of periodic CDRs for a call while a call is still active. This functionality can be enabled and disabled by using the system setting **CDR Interim Update Interval**.

By default the value should be 0. A value of 0 means no periodic CDR. The legal values for the system setting are between 1 and 10. This value represents the number of minutes at which a periodic CDR entry will be added to the CDR file.

Note

Activating the periodic CDR functionality will have an adverse effect on performance.

[Table 14-1](#) lists the fields present in the generated CSV files:

Table 14-1 CDR CSV Fields

Field	Description
acct_status_type	Used for the periodic CDR. Can be one of the following: - start. This is the first CDR for an established call. - update. This is a periodic CDR update for an already established call. - stop. This is either the last CDR that closes an already established call or it is not a periodic CDR or it is a canceled/failed call. To determine which of the above it is read the sequence_number CDR field and also the state_msg.
avg_jitter	Average jitter value for the packets from the RTP stream.
avg_mos	The average of MOS estimation values according to the E-model, computed by Operations Monitor either from the RTP stream or from the end point messages, depending on availability.
avg_packet_loss	The packet-loss statistic indicates whether the host has dropped packets.
avg_rtcp_delay	Average RTCP delay in milliseconds: - If there is RTCP-XR with a delay value, this value is used. If there are multiple streams with RTCP-XR delay values, the average of those values is used. - If there is no RTCP-XR delay value, the RTCP delay is calculated using pairs of RTCP Sender Reports (see RFC 3550)
call_time	The duration in milliseconds of the call. The time is measured from the final successful message until the first BYE message.
callee_ip	The IP address of the called user that connected first. This field may be empty if the call was not successful.

Table 14-1 (Cont.) CDR CSV Fields

Field	Description
caller_ip	The IP address of the device initiating the call.
callid	The Call-ID header value from the initial INVITE.
cdpn_noa	NOA (Nature of address indicator) of the called party from the IAM message.
cgpn_noa	NOA (Nature of address indicator) of the calling party from the IAM message.
cic	Circuit Identification Code from the IAM message.
dpc	Destination Point Codes from the IAM message.
diversion_params	This field contains a ";" (semicolon) separated list of the parameters of the first Diversion header we see in the call.
diversion_uri	This field contains the uri of the first Diversion header we see in the call.
dst_codecs	The codecs, in order, offered by the callee. In case the codecs are changed during the call by using re-INVITES, this field will contain the last offer of the callee.
dst_ip	Destination IP address of the first INVITE message.
dst_mac	Destination hardware address of the first INVITE message.
dst_port	Transport layer port of the first INVITE message.
dst_ua	User agent string of the callee.
dst_uri	Session Initiation Protocol (SIP) URI of the callee as present in the In header field.
dst_user	The user to which the call is addressed. This is usually taken from the To header field of the first <i>call leg</i> , or as defined by the Number Determination algorithm.
dst_user_pref_tag	If the called user string is defined as the result of the Number Determination algorithm, this field is set to the numerical ID of the matching Number Determination rule.
dtg	The value of the dtg URI parameter from the Request-URI of the initial INVITE.
egress_devs	Comma-separated list of numerical device IDs of the egress devices for the call, that is, through which the call leaves the platform.
end_ts	UNIX timestamp of BYE message.
fraud_action	Shows the fraud action taken by the SBC for the fraudulent calls.
from_tag	The value of the tag parameter from the From header of the initial INVITE.
id	Unique identifier of the call within the Operations Monitor core instance.

Table 14-1 (Cont.) CDR CSV Fields

Field	Description
ingress_devs	Comma-separated list of numerical device IDs of the ingress devices for the call, that is, through which the call enters the platform.
init_devs	Comma-separated list of numerical device IDs of the initiator devices for the call, that is, of devices that initiated a call segment without incoming segments.
max_jitter	The maximum jitter value for the packets from the RTP stream.
max_packet_loss	The maximum packet loss for the packets from the RTP stream.
max_rtcp_delay	Maximum RTCP delay in milliseconds. This is the maximum value of RTCP delay values seen across all streams for this call.
mec_ids	Comma-separated list of hexadecimal strings that can be used to correlate CDRs found on multiple Mediation Engines.
media_leg_locations	Comma-separated list of storage locations for Media Leg details. Voice quality records are kept in separate CSV files with Media Detail Records. For more information, see "Voice Quality Records (MDRs)". If an MDR is related to this call, its media_leg_location field will match one of the CDR media_leg_locations. Note: There may be locations without MDRs if no RTP stream was seen by Operations Monitor.
media_types	Indicates the media types that were negotiated in the call. Multiple media types are separated by a comma (for example: audio, video).
megaco_gateway	String with the IP address of the H.248/Megaco Media Gateway.
mgcp_gateway	String with the IP address of the MGCP Media Gateway.
MOS	The minimum MOS estimation according to the E-model, computed by Operations Monitor either from the RTP stream or from the end point messages, depending on availability.
opc	Originating Point Codes from the IAM message.
otg	The value of the otg URI parameter from the From header of the initial INVITE.
pai	The uri of the P-Asserted-Identity of the initial INVITE.
pid	Identifier of the Operations Monitor core instance that created the record.
privacy	The value of the Privacy header of the initial INVITE.

Table 14-1 (Cont.) CDR CSV Fields

Field	Description
q850_cause	This header contains the Q.850 cause code learned from native Q.850/ISUP signaling and NOT SIP.
realm_ids	Comma-separated list of numerical IDs of the realms the call belongs to.
ruri	The Request-URI from the initial INVITE.
sequence_number	A sequence number for each periodic CDR update entry. Is unique in the context of each call. For non-Periodic CDR it should always have the value of 1 .
setup_delay	The duration for the call setup in milliseconds. The time is measured from the first INVITE messages until the last bit of the first provisional response is received.
setup_delay_type	The setup delay type used for the setup delay. Can be one of the following: • Successful Session Request Delay • Failed Session Request Delay
setup_start_ts	UNIX timestamp of the initial INVITE message.
setup_time	The duration in milliseconds of the call setup. The time is measured from the first INVITE message until the final successful answer.
sip_code	The SIP response code of the last received message from the INVITE transaction. For Failed calls, this represents the SIP error code.
sip_reason_cause	The code value of the SIP Reason header.
sip_reason_protocol	If there is a Reason header then this field shall contain the protocol of that header. Can be one of the following: • SIP • Q.850
sip_reason_text	The text explanation contained in the SIP Reason header. If the protocol is Q.850 then this field will be empty.
src_codecs	The codecs, in order, offered by the caller. In case the codecs are changed during the call by using re-INVITES, this field will contain the last offer of the caller.
src_ip	Source IP address of the first INVITE message.
src_mac	Source hardware address of the first INVITE message.
src_port	Transport layer port of the first INVITE message.
src_ua	User Agent string of the caller.
src_uri	SIP URI of the caller as present in the From header field.
src_user	The user making the call. This is usually taken from the From header field of the first <i>call leg</i> or as defined by the Number Determination algorithm.

Table 14-1 (Cont.) CDR CSV Fields

Field	Description
src_user_pref_tag	If the calling user string is defined as the result of the Number Determination algorithm, this field is set to the numerical ID of the matching Number Determination rule.
state_details	Operations Monitor can add details about the call state. Example: BYE seen but no 200 OK.
state_msg	Call state. It can be one of the following: - Established. The call was successfully established. - Redirected. The call was not established but was redirected. - Finished. The call was successfully established and closed. - Timed out. The call was successfully established but the BYE message was never received, so it expired. - Error. The call was not recognized properly. - Unauthorized. - Canceled. - Failed. The call failed to get established, or there was some other reason for not being successful. - Not found. 404 User not found, 604. - Off-line. 480. - Busy. 486, 600. - Terminated. 487 If a call is ISUP based, state message might differ. - For information on Failed calls, refer to the Failed row in Table 4-3
term_devs	Comma-separated list of numerical device IDs of the terminator devices for the call, that is, of devices that terminated a call segment without outgoing segments.
to_tag	The value of the tag parameter from the To header of the initial INVITE.
trav_devs	Comma-separated list of numerical device IDs of traversed devices for the call, that is, of devices that have both incoming and outgoing segments.
uid	Unique identifier for the call, generated from the <i>Call-ID</i> , <i>to_tag</i> , and <i>from_tag</i> . Can be used for merging the CDRs generated by different Operations Monitor instances.
ucaas_ccaas_org	Shows as "TEAMS_DR" if the call is identified as having originated from MS Teams and terminating at PSTN (MS Teams to PSTN call)
ucaas_ccaas_term	Shows as "TEAMS_DR" if the call is identified as having originated from PSTN and terminating at MS Teams (PSTN to MS Teams call)

Note

The fields **ts**, **setup_time**, and **call_time** are time related.

- Because the hardware clock of the Operations Monitor server has limited precision over time, we recommend configuring NTP servers.
- The timestamp precision may be affected by the delays introduced by tapping devices. The timestamp of the message is always saved the moment it reaches Operations Monitor's network interface.
- The fields **setup_time** and **call_time** are computed by subtracting the timestamps of the messages INVITE, 200 OK, and BYE with a precision of milliseconds.

The field **sip_code** in the final CDR of periodic CDRs of a canceled call may be 200 (from the response to CANCEL) instead of 487 because writing the CDR is triggered after the end of the CANCEL transaction.

Customizing CDR Generation

You can customize CDR generation by adding more columns to CSV files based on the values from SIP request header fields. This customization can be enabled and disabled using the system setting **Custom SIP headers in CDR file**. For more information on system settings, see [List of System Settings](#). The system setting **Custom SIP headers in CDR file** has a space-separated list of custom SIP header field names. For each custom SIP header field name in the list, a corresponding column of the same name, prefixed with *Custom-* is added to the CDR CSV fields listed in [Table 14-1](#).

For example, when the system setting is set to *X-Foo Bar*, the two additional columns corresponding to the custom SIP header field names *X-Foo* and *Bar* are added in the CDR CSV file called *Custom-X-Foo* and *Custom-Bar*. The position of these columns is not guaranteed, so the software which processes these CSV files must take header names in the first line of the CSV file into account.

The value of the column *Custom-X-Foo* for a given call is a comma-separated list of all the values occurring in the *X-Foo* header field of all the SIP requests (in all segments) for the call. Each value occurs only once in the list. Note that a custom SIP header field can have multiple values per message (separated by commas or in multiple header field lines) and the custom SIP header field names are case sensitive.

Note

Creating CDRs by enabling the **Custom SIP headers in CDR file** setting will have an adverse effect on the performance of Session Monitor.

When you enable CDR Interim Update Interval, the list of values of the configured custom SIP header fields for a call are cleared whenever an interim CDR is written. The lists of values in the final CDR of a call do not contain all the values from all the SIP requests belonging to that call. The final CDR has the values that are seen in requests since the last interim CDR.

Voice Quality Records (MDRs)

Oracle Communications Operations Monitor creates media detail records (MDR) files in CSV format. The files are placed in the **mdr/** directory under the FTP/FTPS root. The MDR files have the following format:

```
mdr-unix_timestamp-sequence.csv
```

where:

- *unix_timestamp* is the Unix timestamp when the file was created.
- *sequence* is a number monotonically increasing.

The MDR files are rotated whenever one of the following three conditions is met:

- The file reaches the maximum number of records. The maximum size is configurable in Operations Monitor with the system setting, **Maximum lines of a MDR file**. The default is 5000 records.
- The maximum time is reached. The maximum time is configurable in Operations Monitor with the system setting, **Rotate CDR files every N seconds**. The default value is 0 for no time limit.
- There is no new record for 150 seconds.

When a **CSV** file is finished, an empty **CSV** file with the following format is created:

```
mdr-unix_timestamp-sequence.csv.FIN
```

Several times per day, old MDR files are compressed to files having the following format, while the corresponding un-compressed files are deleted:

```
mdr-unix_timestamp-sequence.csv.gz
```

The recommended way of gathering the MDR files is to connect via FTP/FTPS, copy and delete all the files ending in **csv.gz**. Alternatively, to get the MDR data in near real time, the MDR files that have a corresponding **FIN** file can be copied and deleted.

Operations Monitor automatically limits the size of the **mdr/** directory to 5 GB, by deleting the oldest files.

There are two types of data sources: Operations Monitor probe machines, which see and analyze the RTP stream and the VQ collector of Operations Monitor, which receives SIP PUBLISH messages with Voice Quality reports. Operations Monitor writes one MDR per RTP stream per data source. That means for one RTP stream there may be multiple MDRs. For example, if the stream was seen by two Operations Monitor probes or if it was seen by a probe and a VQ report was received. However, the streams which were interrupted for more than two seconds appear as separate rows.

To correlate a RTP stream record (MDR) with a call (CDR), you may use Media Leg information. A media leg is defined by a UDP address pair found by an SDP offer/answer exchange. Depending on the call scenarios there may be multiple media legs per call (for example, from multiple segments or after a re-negotiation) or multiple calls per media leg (for

example, if the same SDP appears in different calls). Usually each media leg will contain two RTP streams, one per direction. In an MDR the media leg the stream belongs to can be identified using the **media_leg_location** field. In a CDR the **media_leg_locations** field lists the media legs correlated with the call. To find the CDR(s) related to an MDR, use the MDR **media_leg_location** and look for the CDRs where this string is one of the **media_leg_locations**. To find the MDRs related to a call, use all entries in the **media_leg_locations** field of the CDR and look for the corresponding **media_leg_location** in an MDR. Note that there may be media legs which do not have any MDRs, for example, because no RTP was seen by Operations Monitor.

[Table 15-1](#) lists the fields present in the generated CSV files.

Table 15-1 MDR CSV Fields

Field	Description
avgPDV	Average packet delay variation in milliseconds.
discarded	Number of packets received, but dropped by the jitter buffer.
dst_ip	Destination IP address of the RTP stream.
dst_port	Destination UDP port of the RTP stream.
end_ts	UNIX timestamp when the last RTP packet was seen (floating point number). For a VQ report from a SIP PUBLISH message, this is the timestamp when the report was received (start_ts and end_ts will have the same value).
expected	Number of RTP packets expected.
lost	Number of lost RTP packets.
maxPDV	Maximum of the packet delay variation values of all 10 second intervals.
media_leg_id	Unique identifier of the media leg (unique if combined with pid). Note, there may be multiple records per media leg, one per RTP stream.
media_leg_location	Internal identifier which can be used to find the media leg inside the Operations Monitor system.
mediatype	The stream media type. Following are the available media types: • Audio • Video • Image • Text • Message • Application
minMOSlqe	Minimum MOSlqe value of all 10 sec intervals of the stream. Available only for the Operations Monitor source.
MOSlqe	MOS Listening Quality score for the whole stream, based on the E-Model, if available.
npayloads	A list of standard numeric RTP/AVP audio and video payload types in the stream (as per RFC3551).
packet_loss_rate	Percentage of lost packets (100 * lost/expected).
payloads	Codecs used by the stream: format names like PCMA, G729, telephone-event.
pid	Identifier of the Operations Monitor process instance that created the record.

Table 15-1 (Cont.) MDR CSV Fields

Field	Description
source	The source of the measurement: ID of the Operations Monitor probe machine where the RTP stream was seen or "RTCPXR" if the Operations Monitor VQ collector received a SIP PUBLISH message with a Voice Quality report.
src_ip	Source IP address of the RTP stream.
src_port	Source UDP port of the RTP stream.
ssrc	RTP SSRC identifier.
start_ts	UNIX timestamp when the first RTP packet was seen (floating point number). For a VQ report from a SIP PUBLISH message, this is the timestamp when the report was received (start_ts and end_ts will have the same value).
vlan	VLAN tag of the RTP stream.

Troubleshooting

This chapter describes how to fix common Oracle Communications Operations Monitor problems.

First Aid

In case you have a problem, please follow this checklist:

- Re-read the corresponding passages in the manual. Some features have special requirements, so make sure to check out these as well. For example, previous configurations, which may be covered in a different context.
- Try to find your problem in the list of suggestions in "[Suggestions for Specific Error Cases](#)".
- If you can't find a solution for your problem, you should create a system diagnostic report from Platform Setup Application and notifying your Operations Monitor support contact.

Suggestions for Specific Error Cases

This section lists problems you might encounter and provides information on how to fix them.

All calls are in the Proceeding state

Please check that both directions of the traffic are correctly mirrored to Operations Monitor. You can verify if both directions are correctly seen by using the diagram from the **Call Details** window.

A sudden drop shows in all charts

This usually means that the Operations Monitor core process was restarted. This can have two causes:

- A configuration change that requires the core to restart. We are continuously trying to reduce the number of configuration changes that require the core to restart. There are a few, however, that still require restarting, for example the **Use Usr Domains** system option.
The option's changes that require a core restart are generally marked with a warning.
- Due to a system error, the core was restarted in order to return to the functional state as soon as possible.

'Sorry, an error occurred while processing your request'

This is the default error message shown by Operations Monitor when an unexpected exception occurs. It can be due to unexpected user input or due to a software regression. In these cases, creating an error report and sending it to Oracle or your system integrator will help us to fix the problem as soon as possible.

Domain realms do not work

Even though you have configured domain based realms, they do not work unless you enable the Use User Domains system option. For more information, see "[Use User Domains](#)".

After updating, some of the users don't see the new pages

After an update of Operations Monitor that adds functionality, you need to explicitly add the user rights to see and use new pages. To make this process as easy as possible, you have the option to add rights at once to multiple users in the **User Management** section.

No voice quality is displayed

Please make sure that the RTP traffic is mirrored to Operations Monitor, and the RTP module is enabled by the license you currently use.

All registration contacts are marked as Gone soon after the registration refresh

This is usually caused by the fact that the network has a SIP device (for example, SBC) that forwards the registration attempts and also alters the contact requested by the user. In this case, the issue can be solved by changing the values of the **Registrations Gone Events** and the **Ignore Internal Registrations** system options. For more information, see "[Registrations Gone Events](#)" and "[Ignore Internal Registrations](#)".

Created traces are empty

In the **Traces** page, please check that the requested trace period is covered by the raw buffer content.

Health Check Daemon

This chapter provides the information about Session Monitor Health Check Daemon for viewing memory usage of the services.

Introduction

Oracle Communications Operations Monitor consists of several interdependent parts realized as system services. To avoid a situation in which one of the parts consumes so much memory that it would impair the functioning of the whole system, it includes a mechanism to restart services with high memory usage. For some installations, the default limit on memory use of the system may not be suitable, or the mechanism may not choose to restart those services which are actually responsible for the high memory usage. Health Check Daemon, cghealth is designed on systemd and cgroups which controls the memory consumption of the services on Operations Monitor.

The cghealth sets the hard limit for each service for the total memory consumption. cghealth attempts a restart of specific services if the service memory consumption reaches near to the set limit and creates a system log whenever cghealth daemon restarts a service. The hard limit is set by the configuration setting 'limit' in section 'memory'. It is a limit for the total memory consumption of all Session Monitor services (called PLD slice), not for individual processes.

Note

To effectively change the configuration, the task should only be performed by system administrators who understand how cghealth works.

Note

cghealth restarts services only when the total memory usage is above the high water mark (setting 'hiwm' in section 'memory'), which is by default defined as a percentage of the hard limit.

Editing cghealth Daemon Configuration File

You can edit cghealth daemon using command line interface. To edit cghealth daemon:

To edit cghealth daemon:

1. Login to a system that has Operations Monitor installed as admin (root user).
2. Open Command Line Interface.

Note

The current default values are stored in file, **/opt/oracle/ocsm/etc/iptego/cghealth.conf**. Read this file first to know the current limits, but do not change the values there. Instead, you can set the values by creating a new file, **/opt/oracle/ocsm/etc/iptego/cghealth.conf.local**. When you are adding new values in **cghealth.conf.local**, you should also add the proper [section] for it, by copying it from the default file, **cghealth.conf**.

3. Run the following command to edit specific values:

```
vi /opt/oracle/ocsm/etc/iptego/cghealth.conf.local
```

As a result of the command input, you can set the memory consumption of the services. For example,

```
[memory_high]
pld-vsi = 40%
```

4. To restart the service, run the following command:

```
systemctl restart pld-cghealth.service
```

Setting Hard Limit for Services

cghealth sets a limit on the total memory consumption including swap of the PLD slice. If the measures specified fails, kernel enforces the limit by killing processes. The limit is configured in the **cghealth.conf** file. The local changes should be made via **cghealth.conf.local** file.

```
[memory]
limit = 60%
```

The percentage is in relation to the total physical memory of the machine. You can specify an absolute value, for example, `limit = 17179869184` or, equivalently, a value with measurement, for example, `limit = 16G`.

Note

- Customizing cghealth services is optional.
- MySQL is not part of **pld.slice** file. This limit should be chosen low enough to leave sufficient space for it.

Restarting Services

cghealth restarts a service when the total memory consumption is near to the set limit.

For example, following is a service memory consumption.

```
[memory]
hiwm = 90%
```

The percentage is in relation to the hard limit. Absolute values are also possible.

If the total memory consumption of all services in the `pld.slice` exceeds the high water mark, `cghealth` will, via `systemd`, restart all services in that slice whose memory consumption is high.

Here is an example of the individual limit for the `vsi` service

```
[memory_high]
pld-vsi = 30%
```

This defines that the memory consumption of `pld-vsi.service` is considered high if it is above 30% of the configured total limit. Again, absolute values can also be used.

For services which do not have an explicit value set, a default value is used. `cghealth` creates a system log whenever the services are restarted. Following is an example of such a log entry from `/var/log/messages`:

```
Jun 12 15:21:21 ocsd journal: OCSM memory usage: 20,498,919,424 bytes
Jun 12 15:21:21 ocsd journal: * 7,272,095,744 pld-vsi.service
...
Jun 12 15:21:21 ocsd journal: 5,971,968 pld-enum-probe.service
Jun 12 15:21:21 ocsd journal: Restarting marked services.
```

Here is a calculation example:

For this example, we will assume that the entire system memory size is 36 GB.

From file, `/opt/oracle/ocsm/etc/iptego/cghealth.conf`, you can view the existing limits:

```
limit = 60% (from all memory, this means 60% x 36 = 21.6 GB)
hiwm = 90% (from limit, this means 90% x 21.6) = 19.44 GB
pld-vsi = 30% = (from limit, this means 30% x 21.6) = 6.48 GB
```

This means, that as soon as memory usage for all Session Monitor services together is over 19.44 GB, `cghealth` will start looking at individual services to see which one is above its individual limit, in which case those services will be restarted.

For example `pld-vsi`, because the limit is 30%, the service will be restarted if its current memory usage is over 6.48 GB.

Nightly Check for Individual Service Memory Usage

During the night (at 03:27 am) there is an additional check for individual used memory. At this time, `cghealth` checks each individual service and looks at the memory it used throughout the day. If the memory used by the individual service is above the value in the 'memory_high' section for that service (or the "default" value in the 'memory_high' section), that service is restarted. Note that the nightly check is independent of the memory used by the full PLD slice. This means that during the nightly check it will not matter what the full PLD slice memory consumption is, because only the individual service memory usage is checked.

For Example:

Assuming that the 'memory_high' section in the `/opt/oracle/ocsm/etc/iptego/cghealth.conf` file (or `/opt/oracle/ocsm/etc/iptego/cghealth.local.conf` file) looks as follows:

```
[memory_high]
default = 10%
pld-vsi = 40%
pld-meco = 30%
```

During the night, `cghealth` checks each individual service and looks at the memory it used throughout the day. If `pld-vsi` memory usage goes above 40% of the limit (the limit defined in the 'memory' section), it is restarted. If `pld-meco` goes above 30% of the limit, it is restarted.

For all other service from the PLD slice (for example pld-apid), the memory usage is compared to 10% of the limit (because that is the default value).

Multiple-VSP - Overview

Enabling Multi-VSP feature improves user experience for Mediation Engine UI concurrent users and overall reliability of applications.

With this feature enabled on the Mediation Engine, the NGINX or the Apache httpd web server acts as a load balancer and the REST API HTTP request load is distributed across multiple servers (VSPs) based on the API requests. For example, all KPI requests can be handled by one instance of VSP and all requests from the Calls page by another VSP instance.

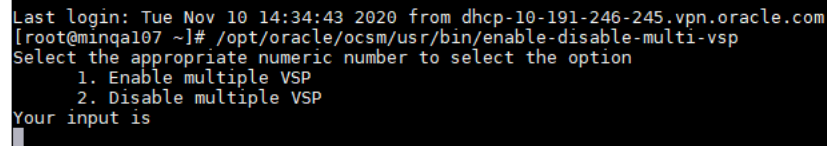
Enabling or Disabling Multiple-VSP

1. Run this script during a low traffic load or during a maintenance window.

```
# /opt/oracle/ocsm/usr/bin/enable-disable-multi-vsp
```

2. Type **1** to enable multi-VSP. Enabling VSP starts 4 additional VSP services, pld-vsp1, pld-vsp2, pld-vsp3, pld-vsp4

Figure 18-1 Enabling or Disabling Multiple VSP



```
Last login: Tue Nov 10 14:34:43 2020 from dhcp-10-191-246-245.vpn.oracle.com
[root@mqal07 ~]# ./opt/oracle/ocsm/usr/bin/enable-disable-multi-vsp
Select the appropriate numeric number to select the option
    1. Enable multiple VSP
    2. Disable multiple VSP
Your input is
█
```

3. Type **2** to disable multi-VSP.
4. Restart all services after enabling or disabling:

```
# pld-systemctl restart
```

MGCP Correlation

This chapter provides the information about configuring the Media Gateway Configuration Protocol (MGCP) correlation.

Introduction

Operations Monitor can now capture MGCP transactions before CRCX or after DLCX events that request and notify on-hook and off-hook events, caller IDs, and dual tone multi frequency (DTMF) collections. An MGCP protocol leg transaction can now be correlated with SIP when the SIP RTP IP address does not match the MGCP RTP IP address by using a provisioned table that maps MGCP endpoint IDs to phone numbers. Transactions on special MGCP endpoints with the **disp** prefix (used by MGCP-controlled business phones) can now be correlated with SIP.

For more information on these MGCP correlation and how they can be configured, see "[Configuring the MGCP Correlation](#)".

Configuring the MGCP Correlation

This section describes how to configure the MGCP correlation.

- [Understanding MGCP NCS Signalling](#)
- [Mapping Endpoint IDs to Phone Numbers](#)
- [Working with MGCP Endpoints With a disp Prefix](#)
- [Endpoint Utilities Reference](#)

Understanding MGCP NCS Signalling

Network-based Call Signalling (NCS) is a variant of the Media Gateway Control Protocol (MGCP) that is defined by the **PacketCable** standards for MGCP-controlled terminal adapter access gateways. These gateways process on-hook and off-hook events, caller IDs, and DTMF collections. Operations Monitor captures the MGCP protocol leg whether it starts with an on-hook or an off-hook event in a MGCP NTFY transaction and whether the CRCX transaction is before or after the NTFY transaction.

No configuration is required.

Mapping Endpoint IDs to Phone Numbers

When the Session Initiation Protocol (SIP) Real-time Transport Protocol (RTP) IP address does not match the MGCP RTP IP address, correlation based on the session description protocol (SDP) cannot be achieved.

Correlation is achieved by creating a provisioned table that maps the MGCP endpoint identifiers (endpoint ID) with the subscribers phone numbers and making the table available during processing.

Note

Only one phone number can be assigned to one MGCP endpoint ID.

Creating an MGCP Endpoints Table

To create an MGCP endpoints table:

1. Create an **endpoints.tab** text file that contains a table with two columns. Where each row defines the mapping for one MGCP endpoint ID and the row consists of the phone number and the MGCP endpoint ID separated by spaces or a tab, and where:
 - The phone number must contain digits or A, B, C, D (lower or upper case).
 - The MGCP endpoint ID is case-insensitive.

For example:

```
0305551234    aaln/1@gw1.domain.com
0305551235    aaln/2@gw1.domain.com
03315556666   aaln/1@gw2.domain.com
```

2. Save the **endpoints.tab** file to the *OCOM_home/var/vsi/ftp/mgcp* directory.
Where *OCOM_home* is the directory in which Operations Monitor is installed.
3. Open the *OCOM_home/etc/lptego/mgcp_probe.local.conf* file and add the following lines:

```
[endpoint_table]
enabled = 1
file = OCOM_home/var/vsi/ftp/mgcp/endpoints.tab
```

Note

The default path for the **endpoints.tab** file is *OCOM_home/var/vsi/ftp/mgcp*.

4. Save the file.
5. Open a command terminal and run the following command, which loads the **endpoints.tab** file dynamically without restarting the module:

```
OCOM_home/usr/share/pld/mgcp_probe/load_endpoint_table.py
```

Updating the MGCP Endpoints Table

To update an MGCP endpoints table:

1. Open the *OCOM_home/var/vsi/ftp/mgcp/endpoints.tab* file, make your changes, and save the file.
2. Open a command terminal and run the following command, which loads the **endpoints.tab** file dynamically without restarting the module:

```
OCOM_home/usr/share/pld/mgcp_probe/load_endpoint_table.py
```

Working with MGCP Endpoints With a disp Prefix

Some MGCP-controlled business phones use the following MGCP endpoint IDs:

- An MGCP endpoint ID that controls analog lines named **aaln/1@host**. This MGCP endpoint ID controls RQNT and NTFY transactions for signals and events and CRCX, MDCX, DLCX transactions that manage the RTP connection.
- An MGCP endpoint ID named **disp/aaln/1@host**. This MGCP endpoint ID controls the XML package that is used for transactions that send **xml/xml** events to and from the phone in NTFY and RQNT messages respectively.

There are no off-hook events and no CRCX transactions on **disp** endpoints. The **disp** endpoint ID is a prefixed variant of the normal (**non-disp**) endpoint.

If you require correlation of the NTFY and RQNT transactions that are related to a call, you can add a configuration option that ignores the given prefix and captures and correlates all **disp** transactions between off-hook or CRCX and on-hook or DLCX on **non-disp** endpoints. The **disp** endpoints are processed as if they were **non-disp** endpoints and are included in the correlation.

Additionally, the **disp** endpoints can send an event to the call agent when the user dialed a number. In this case, a NTFY with an **xml** event that contains a parameter string, such as **post?invk?DIAL?num=0305551234** is sent instead of the usual **NTFY with an off-hook** event. Operations Monitor can use this **xml** event as an indication that an MGCP call has started (in addition to **off-hook** events and CRCX).

Configuring disp Endpoints

To configure **disp** endpoints:

1. Open the `OCOM_home/etc/liptego/mgcp_probe.local.conf` file and add one or more of the following:
 - To configure a **disp** endpoint as part of a **non-disp** endpoint, add:


```
[mgcp]
ignore_endpoint_prefix = disp/
```
 - To configure the **xml/xml** (`post?invk?DIAL?num=0305551234`) event as an indication that an MGCP call has started, add:


```
[mgcp]
xml_dial = post?invk?DIAL?num=
```
2. Save the file.

Endpoint Utilities Reference

The **load_endpoint_table.py** utility reads the MGCP endpoints mapping table when the SIP RTP IP address does not match the MGCP RTP IP address.

Location

`OCOM_home/usr/share/pld/mgcp_probe/load_endpoint_table.py`

Syntax

```
load_endpoint_table.py [-h] [-p PORT] [-f FILE | -c]
```

Parameters

- **-h**
Displays the syntax and parameters for this utility.
- **-p PORT**
The mgcp_probe XMLRPC port name (default=10005).
- **-f FILE**
The input file name and path (default=/var/vsi/ftp/mgcp/endpoints.tab).
- **-c**
Clears the endpoint table by removing all existing table entries that are currently running. The **endpoints.tab** file is not changed.

Storage Expansion Support for Mediation Engine

The Storage Expansion tool allows administrators to increase the storage allocated to Session Monitor without requiring a full reinstallation.

This capability is achieved using a command-line script that supports both single-disk and dual-disk system configurations, enabling a flexible expansion of MySQL database and Block Storage independently or together, according to the available space.

Key Capabilities

- Expand storage for MySQL database, Block Storage, or both.
- Support for single-disk and dual-disk system setups.
- Ensure zero downtime during expansion without requiring system reinstallation.
- Validate inputs robustly and confirm with users to reduce misconfiguration risks.
- Provide comprehensive information and Help command options.
- Exclude support for reducing (shrinking) storage allocations.

Important Notes

- Storage expansion is supported on Mediation Engine and Mediation Engine + Probe nodes only.
- Only dual-disk system setups support separate expansion of MySQL and Block storage.
- **It is recommended to run the script during off-peak traffic hours.**

Expanding Storage

Follow the instructions given in this section to expand the storage for Session Monitor.

For Single Disk systems, this script allows you to input only one disk size, which is automatically allocated across both MySQL and Block Storage. Independent allocation for either MySQL or Block Storage is not supported on Single Disk systems, as both reside on the same partition.

For Dual Disk systems, the script provides the flexibility to input disk sizes independently for either the MySQL partition, or the Block Storage partition, or for both partitions, allowing a more granular control over storage allocation.

To Expand OCSM Storage:

1. Log in to the Session Monitor server's CLI as the root user or root privileged user.
2. Verify the space available. Before expanding the storage, review the available space by executing the following command:

```
/usr/bin/df -kh /var/lib/mysql /opt/oracle/ocsm/var/vsi
```

If your local files are taking up space, move or delete the local files to free up space, or adjust your expansion plan based on the available size.

3. Prepare the environment: Before running any commands to expand, initialize the environment:

```
source /opt/oracle/ocsm/ocsm_env.sh
```

4. Review the current configuration: Run the storage expansion tool with the --info (or -i) option to view information about the current disk configuration, including the maximum expandable capacity for each disk, without making any changes:

```
ocsm-resize-storage --info
```

Note

All sizes shown by the script are approximate and may vary by a few Gigabytes. If you encounter an error during the expansion process, adjust the values accordingly.

Figure 20-1 : Example output of the --info option on a Dual Disk system

```
[root@r54p17x9ocsm010123140018 ~]# ocsm-resize-storage -i

===== OCSM Storage Resizer =====

+-----+
|  !! This tool changes the disk usage. Use with caution!  |
+-----+

[ Disk Information ]

Disk1 Partition           : /var/lib/mysql
Disk1 Filesystem          : /dev/mapper/data_vg-var_lib_mysql
Current Disk1 Allocation  : ~1.0 TB
Max Expandable Disk1 Size : ~4.0 TB

Disk2 Partition           : /opt/oracle/ocsm/var/vsi
Disk2 Filesystem          : /dev/mapper/data_vg-opt_oracle_ocsm_var_vsi
Current Disk2 Allocation  : ~7.0 TB
Max Expandable Disk2 Size : ~20.64 TB

Number of disks in the system: Dual Disk
```

5. Execute storage expansion script:

Input Restrictions:

Note

- The input size must be the **new total size** (not just the size being added). E.g. if your current disk is 500GB and you added 250GB, your input should be 750GB
- The size should be provided as a non-decimal integer, immediately followed by the unit, with no spaces (e.g., 100G).
- Supported units are: M or m (megabytes), G or g (gigabytes), and T or t (terabytes).
- It is not necessary for the units for disk1 and disk2 to be the same; different units can be used for each disk. (e.g. --disk1 500G --disk2 2T)
- Decimal values are not supported for input sizes. Instead of entering values like **200.5G** or **2.1T**, use the equivalent whole number in a smaller unit (For example. enter **2148G** instead of **2.1T**).

- a. **For Single Disk system**, execute the following command to expand storage:

```
ocsm-resize-storage --disk1 <NEW_TOTAL_SIZE>
```

or

```
ocsm-resize-storage -d1 <NEW_TOTAL_SIZE>
```

Example: If your current disk is 500 GB and you added 250 GB, run the command:

```
ocsm-resize-storage --disk1 750G
```

- b. **For dual-disk systems**, execute the appropriate command from the list below to expand storage:

- To Expand both MySQL (disk1) and Block Storage (disk2):

```
ocsm-resize-storage --disk1 <NEW_MYSQL_SIZE> --disk2  
<NEW_BLOCK_SIZE>
```

(or)

```
ocsm-resize-storage -d1 <NEW_MYSQL_SIZE> -d2 <NEW_BLOCK_SIZE>
```

- To Expand only MySQL storage:

```
ocsm-resize-storage --disk1 <NEW_MYSQL_SIZE> (or) ocsm-resize-  
storage -d1 <NEW_MYSQL_SIZE>
```

- To Expand only Block Storage:

```
ocsm-resize-storage --disk2 <NEW_BLOCK_SIZE> (or) ocsm-resize-  
storage -d2 <NEW_BLOCK_SIZE>
```

Examples;

```
ocsm-resize-storage --disk1 500G --disk2 2T
ocsm-resize-storage --disk1 500G
ocsm-resize-storage --disk2 2T
```

6. Review the displayed allocation summary: If all validations pass, the script displays a summary comparing current and target storage allocations before proceeding. Review the allocation before proceeding.

Figure 20-2 Sample Output

```
[root@r54p17x9ocsm010123140018 ~]# ocsm-resize-storage --disk1 3T --disk2 14T

===== OCSM Storage Resizer =====

+-----+
| !! This tool changes the disk usage. Use with caution! |
+-----+

Please review the allocation info below before proceeding:

+-----+-----+
| Current Storage Allocation: | Target Storage Allocation: |
+-----+-----+
| MySQL Database Size = 919.8 GB | MySQL Database Size = 2.7 TB |
| Block Storage Size = 6.62 TB | Block Storage Size = 13.27 TB |
+-----+-----+
| Disk1 Allocation = ~1.0 TB | Disk1 Allocation = ~3.0 TB |
| Disk2 Allocation = ~7.0 TB | Disk2 Allocation = ~14.0 TB |
+-----+-----+

Note: Disk1/Disk2 space isn't fully utilized by MySQL and Block Storage; a portion is reserved for miscellaneous activities.

Do you want to proceed with storage expansion ('yes' or 'no') : <USER_INPUT>
```

Note

Not all of the specified disk size is allocated to MySQL and Block storage; OCSM reserves a portion for system use, so the displayed sizes may be less than the total disk size entered.

7. Type 'yes' to start the storage expansion. This process may take a few seconds to a few minutes, depending on the storage size.
8. After it is completed, the storage is successfully expanded.

Options for Storage Expansion Command

Options for Storage Expansion Command:

Table 20-1 Options for Storage Expansion Command:

Option	Meaning
-d1 D1, --disk1 D1	In single-disk systems, --disk1 refers to the total size allocated for the entire disk. Since both MySQL database storage and block storage share the same single disk, the size you specify for --disk1 will be automatically divided between these two types of storage according to Session Monitor internal allocation logic. In dual-disk systems, --disk1 refers specifically to the size allocated for MySQL database storage.
-d2 D2, --disk2 D2	In dual-disk systems, --disk2 refers specifically to the storage allocated for Block Storage on the second disk. In single-disk systems, --disk2 option is not supported.
-i, --info	Allows users to view detailed information about current disk configurations without making any changes. Displays whether the system is using a Single Disk or Dual Disk setup and provides a comprehensive breakdown of current storage allocations and capacity. The information includes details about each disk's partitions, underlying filesystem paths (typically through LVM or device mapper), and the maximum expandable capacity of each disk.
-h, --help	Gives an informative summary of how to use the storage expansion command.

Storage Soft Limits

In both single-disk and dual-disk systems, there are soft limits for storage expansion, which are based on lab-tested performance benchmarks.

For Dual-Disk Systems:

- For MySQL database storage in a dual-disk system, the recommended limit for storage expansion is 4TB.
- For Block Storage in a dual-disk system, the recommended limit for storage expansion is 46TB.

For Single-Disk Systems:

- In single-disk systems, the recommended storage limit for storage expansion is 50TB.

This recommendation is based on extensive lab-tested performance benchmarks that have shown optimal performance up to this size. These are considered as a soft limit, meaning the system may still function beyond this size, but performance has not been validated for systems exceeding this threshold.

When you attempt to expand storage beyond these soft limits, the OCSM Storage Expansion tool will provide a warning message, informing you that the expansion may result in unvalidated performance and will only proceed with the expansion if the user explicitly agrees.

21

Key Performance Indicator Reference

This chapter provides the details of the key performance indicators (KPIs) related to Oracle Communications Operations Monitor.

KPIs

The KPI Metrics is a standards of measurement by which efficiency, performance, progress, or quality of the platform are assessed.

The following KPI categories are described:

- [Platform-Wide and Prefix Tag KPIs](#)
- [Device, Trunk and IP Tag KPIs](#)

Platform-Wide and Prefix Tag KPIs

[Table 21-1](#) describes the Operations Monitor platform-wide and prefix tag KPIs, where:

- The platform-wide KPIs provide data about the overall signaling of the network, such as the total number of calls across all devices.
- The prefix tag KPIs provide data about traffic that is specific to the selected prefix number.

Table 21-1 Platform Wide and Prefix Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
Default	Active calls	Platform, Prefix tag	-	Number of established concurrent calls. Counts end-to-end calls (an end-to-end call can comprise of several correlated call legs).
Default	Registered users	Platform, Prefix tag	-	Number of registered users with at least one active binding/contact. Counts only once if a user is registered with multiple contacts or on multiple servers.
Default	Registered contacts	Platform, Prefix tag	-	Number of registered contacts. Each active binding/contact is counted if a user is registered with multiple contacts or on multiple servers.

Table 21-1 (Cont.) Platform Wide and Prefix Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
Default	Call attempts since startup	Platform, Prefix tag	-	Number of call attempts counted since the core process started. Counts end-to-end calls (an end-to-end call can comprise of several correlated call legs).
Default	Call attempts for each second (CAPS)	Platform, Prefix tag	-	Number of call attempts for each second. Counts end-to-end calls (an end-to-end call can comprise of several correlated call legs).
Default	Calls established	Platform, Prefix tag	-	Number of established calls for each second. Counts end-to-end calls (an end-to-end call can comprise of several correlated call legs).
Default	Closed calls for each second	Platform, Prefix tag	-	Number of calls that finished for each second. Counts end-to-end calls (an end-to-end call can comprise of several correlated call legs).
Default	Register attempts for each second	Platform, Prefix tag	-	Number of completed SIP REGISTER transactions for each second

Table 21-1 (Cont.) Platform Wide and Prefix Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
IETF KPIs and metrics	Ineffective registration attempts	Platform, Prefix tag	-	Ineffective registration attempts are utilized to detect failures or impairments causing an inability for a registrar to receive a UA REGISTER request. A failed registration attempt is a final failure response to the initial REGISTER request. It indicates a failure received from the destination registrar, interim proxies, or due to a timeout of the REGISTER request at the originating UA. A failure response is described as a 4XX (excluding 401, 402, and 407 non-failure challenge response codes), 5XX, or possible 6XX message. IRA may be used to detect problems in downstream signaling functions, which may be impairing the REGISTER message from reaching the intended registrar; or, it may indicate a registrar has become overloaded and is unable to respond to the request. Calculated as a percentage of failed and timed-out REGISTER transactions out of all REGISTER transactions.
IETF KPIs and metrics	Ineffective registration attempts by code	Platform, Prefix tag	Lower bound for the code Upper bound for the code	Percentage of SIP REGISTER transactions that failed with a response code in the given range out of all REGISTER transactions.

Table 21-1 (Cont.) Platform Wide and Prefix Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
IETF KPIs and metrics	Session establishment ratio (SER)	Platform, Prefix tag	-	This metric is used to detect the ability of a terminating UA or downstream proxy to successfully establish sessions per new session INVITE requests. SER is defined as the ratio between the number of new session INVITE requests resulting in a 200 OK response to the total number of attempted INVITE requests less INVITE requests resulting in a 3XX response. This metric is similar to Answer Seizure Ratio (ASR) in telephony applications of SIP.

Table 21-1 (Cont.) Platform Wide and Prefix Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
IETF KPIs and metrics	Session Establishment Effectiveness Ratio (SEER)	Platform, Prefix tag	-	SEER is defined as follows: $\text{SEER} = \frac{\text{Number of INVITE requests resulting in a 200 OK, 480, 486, 600, or 603 response}}{\text{Total number of attempted INVITE requests} - \text{Number of INVITE requests resulting in a 3XX response}}$ The response codes 480, 486, 600, and 603 were chosen as they indicate the effect of an individual user of the UA. It is possible that an individual user could cause a negative effect on the UA. For example, they may have incorrectly configured the UA causing a response code not directly related to a SSP, but this cannot be easily determined from an intermediary B2BUA somewhere in between the originating and terminating UA. With this in consideration, response codes such as 401, 407, and 420 (not an exhaustive list) are not included in the numerator of the metric. • If defined for a device, it counts the incoming calls to that device. • If defined for a trunk, it counts the calls for the initial INVITE that comes from the platform to the trunk (egress). This metric is similar to Network Effectiveness Ratio (NER). KPI value is a percentage that takes

Table 21-1 (Cont.) Platform Wide and Prefix Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
				only INVITEs on ingress legs into account.
IETF KPIs and metrics	Session defects ratio	Platform, Prefix tag	-	Session defects provide a subset of SIP failure responses, which consistently indicate a failure in dialog processing. Defects are necessary to provide input to calculations such as Defects for each Million (DPM) or other similar metrics. These failure responses are in response to initial session setup requests, such as a new INVITE. The following failure responses provide a guideline for defective criterion: • 500 Server Internal Error • 503 Service Unavailable • 504 Server Timeout KPI value is a percentage that takes only INVITEs on ingress legs into account.

Table 21-1 (Cont.) Platform Wide and Prefix Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
IETF KPIs and metrics	Ineffective session attempts ratio	Platform, Prefix tag	-	Ineffective session attempts occur when a proxy or agent internally releases a setup request with a failed or overloaded condition. This metric is similar to Ineffective Machine Attempts (IMA) in telephony applications of SIP. The following failure responses provide a guideline for this criterion: • 408 Request Timeout • 500 Server Internal Error • 503 Service Unavailable • 504 Server Timeout KPI value is a percentage that takes only INVITES on ingress legs into account.

Table 21-1 (Cont.) Platform Wide and Prefix Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
IETF KPIs and metrics	Session disconnect failure ratio	Platform, Prefix tag	-	Session disconnect failures occur when an active session is terminated due to a failure condition that can be identified by a REASON header in a BYE message. This occurs, for example, when a user agent (UA) is controlling an IP or TDM (Time Division Multiplexing) media gateway, and the media gateway notifies the UA of a failure condition causing the loss of media related to an established session. The REASON value is utilized to determine whether the disconnect was a failure. This metric is similar to Cutoff Calls (CC) in telephony applications of SIP. KPI value is a percentage that takes only INVITES on ingress legs into account.
IETF KPIs and metrics	Successful session completion ratio	Platform, Prefix tag	-	This metric is defined as the ratio between successfully completed sessions and the total number of session attempts. A successfully completed session is when it begins with a setup request and ends with a session completion message. This metric is similar to Call Completion Ratio (CCR) in telephony applications of SIP. KPI value is a percentage that takes only INVITES on ingress legs into account.

Table 21-1 (Cont.) Platform Wide and Prefix Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
IETF KPIs and metrics	Failed session completion ratio	Platform, Prefix tag	-	Session completion fails when an INVITE is sent from the originating UA, but there is no indication the INVITE reached the target UA. This can also occur if the target UA does not respond to the INVITE or the response never reaches the target UA associated with the session. KPI value is a percentage that takes only INVITES on ingress legs into account.
IETF KPIs and metrics	Session success ratio	Platform, Prefix tag	-	Session success ratio is defined as the percentage of successfully completed sessions compared to sessions that fail due to ISA or SDF. This metric is also known as Call Success Ratio (CSR) in telephony applications of SIP. KPI value is a percentage that takes only INVITES on ingress legs into account.

Table 21-1 (Cont.) Platform Wide and Prefix Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
IETF KPIs and metrics	Combined maximum successful session request delay	Platform, Prefix tag	-	This metric combines the ISUP Post Dial Delay (PDD) and SIP Session Request Delay (SRD) into a single metric. SSRD is defined as the time interval from the first bit of the initial INVITE message containing the information sent by the originating user agent to the intended mediation or destination agent until the last bit of the first provisional response is received indicating an audible or visual status of the initial session setup request.
IETF KPIs and metrics	Combined maximum failed session request delay	Platform, Prefix tag	-	This metric combines the ISUP Post Dial Delay (PDD) and SIP Session Request Delay (SRD) into a single metric. Failed Session Request Delay (FSRD) is the time interval from the first bit of the initial INVITE message containing the information sent by the originating agent or user to the intended mediation or destination agent until the last bit of the first provisional response or a failure indication response. A failure response is described as a 4XX (excluding 401, 402, and 407 non-failure challenge response codes), 5XX, or possible 6XX message.

Table 21-1 (Cont.) Platform Wide and Prefix Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
IETF KPIs and metrics	Combined maximum session request delay	Platform, Prefix tag	-	This metric combines the ISUP Post Dial Delay (PDD) and SIP Session Request Delay (SRD) into a single metric. Session Request Delay (SRD) is utilized to detect failures or impairments causing a delay in responding to a UA session request. SRD is measured for both successful and failed session setup requests as this metric relates to the user experience. It is recommended that the SSRD and the FSRD are used instead of SRD as the time greatly varies between the two. SRD is similar to Post-Selection Delay from telephony applications.
IETF KPIs and metrics	Session disconnect delay	Platform, Prefix tag	-	Session Disconnect Delay (SDD) is the time interval between the first bit of the sent session completion message, such as a BYE, and the last bit of the subsequently received 2XX response.

Table 21-1 (Cont.) Platform Wide and Prefix Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
IETF KPIs and metrics	Session duration time	Platform, Prefix tag	-	Session Duration Time (SDT) is utilized to detect technical issues causing short session durations. For example, poor audio quality. SDT is defined as an average of duration of the interval between receipt of the first bit of a 200 OK response to an INVITE plus the receipt of the last bit of an associated BYE message. Retransmissions of the 200 OK and ACK messages due to network impairments do not reset the metric timers.
IETF KPIs and metrics	Average successful session request delay	Platform, Prefix tag	-	Average of all per-leg SSRD values for a second. SSRD is defined as the time interval from the first bit of the initial INVITE message containing the information sent by the originating user agent to the intended mediation or destination agent until the last bit of the first provisional response is received, indicating an audible or visual status of the initial session setup request. Calculated based on the timings of the state-defining leg of a call.

Table 21-1 (Cont.) Platform Wide and Prefix Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
IETF KPIs and metrics	Average failed session request delay	Platform, Prefix tag	-	Average of all per-leg FSRD values for a second. Failed Session Request Delay (FSRD) is the time interval from the first bit of the initial INVITE message containing the information sent by the originating agent or user to the intended mediation or destination agent until the last bit of the first provisional response or a failure indication response. Calculated based on the timings of the state-defining leg of a call.
IETF KPIs and metrics	Maximum successful session request delay	Platform, Prefix tag	-	Maximum of all per-leg SSRD values for a second. SSRD is defined as the time interval from the first bit of the initial INVITE message containing the information sent by the originating user agent to the intended mediation or destination agent until the last bit of the first provisional response is received, indicating an audible or visual status of the initial session setup request. Calculated based on the timings of the state-defining leg of a call.

Table 21-1 (Cont.) Platform Wide and Prefix Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
IETF KPIs and metrics	Maximum failed session request delay	Platform, Prefix tag	-	Maximum of all per-leg FSRD values for a second. Failed Session Request Delay (FSRD) is the time interval from the first bit of the initial INVITE message containing the information sent by the originating agent or user to the intended mediation or destination agent until the last bit of the first provisional response or a failure indication response. Calculated based on the timings of the state-defining leg of a call.
Advanced metrics	Number of ISUP Q.850 cause codes	Platform, Prefix tag	Minimum Q.850 cause code Maximum Q.850 cause code	Number of ISUP call segments that finished or failed with a cause code in the given range.
Advanced metrics/ Network/ TCP	Total number of active TCP streams	Platform	-	Total number of TCP streams being tracked.
Advanced metrics/ Network/ TCP	Number of TCP streams created	Platform	-	Number of new TCP streams for each second.
Advanced metrics/ Network/ TCP	Number of TCP streams timed out	Platform	-	Number of TCP streams for each second that timed out.
Advanced metrics/ Network/ TCP	Number of TCP ACK messages	Platform	-	Number of TCP SYN messages.
Advanced metrics/ Network/ TCP	Number of TCP SYN messages	Platform	-	Number of TCP ACK messages.
Advanced metrics/ Network/ TCP	Number of TCP RST messages	Platform	-	Number of TCP RST messages for each second.
Advanced metrics/ Network/ TCP	Number of TCP FIN Messages	Platform	-	Number of TCP FIN messages for second.
Advanced metrics/ Network/ SCTP	Number of SCTP DATA chunks	Platform	-	-
Advanced metrics/ Network/ SCTP	Number of SCTP INIT chunks	Platform	-	-
Advanced metrics/ Network/ SCTP	Number of SCTP INIT ACK chunks	Platform	-	-

Table 21-1 (Cont.) Platform Wide and Prefix Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
Advanced metrics/ Network/ SCTP	Number of SCTP SACK chunks	Platform	-	-
Advanced metrics/ Network/ SCTP	Number of SCTP HEARTBEAT chunks	Platform	-	-
Advanced metrics/ Network/ SCTP	Number of SCTP HEARTBEAT ACK chunks	Platform	-	-
Advanced metrics/ Network/ SCTP	Number of SCTP ABORT chunks	Platform	-	-
Advanced metrics/ Network/ SCTP	Number of SCTP SHUTDOWN chunks	Platform	-	-
Advanced metrics/ Network/ SCTP	Number of SCTP SHUTDOWN ACK chunks	Platform	-	-
Advanced metrics/ Network/ SCTP	Number of SCTP ERROR chunks	Platform	-	-
Advanced metrics/ Network/ SCTP	Number of SCTP COOKIE ECHO Chunks	Platform	-	-
Advanced metrics/ Network/ SCTP	Number of SCTP ECNE chunks	Platform	-	-
Advanced metrics/ Network/ SCTP	Number of SCTP CWR chunks	Platform	-	-
Advanced metrics/ Network/ SCTP	Number of SCTP SHUTDOWN COMPLETE chunks	Platform	-	-
Advanced metrics/ Network/ SCTP	Number of active SCTP associations	Platform	-	-
Advanced metrics/ Network/ SCTP	Number of SCTP associations created	Platform	-	Total number of SCTP associations being tracked.
Advanced metrics/ Network/ SCTP	Number of SCTP associations created	Platform	-	Number of new SCTP associations for each second.
Advanced metrics/ Network/ SCTP	Number of SCTP packets	Platform	-	Number of SCTP packets for each second.
Advanced metrics/ Network	Number of IPv4 packets	Platform	-	Number of IPv4 packets for each second.
Advanced metrics/ Network	Number of IPv6 packets	Platform	-	Number of IPv6 packets for each second.
Advanced metrics/SIP Traffic	SIP requests	Platform	-	Number of SIP requests for each second.

Table 21-1 (Cont.) Platform Wide and Prefix Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
Advanced metrics/SIP Traffic	SIP replies	Platform	-	Number of SIP replies for each second.
Advanced metrics/SIP Traffic	Number of SIP requests with a given method name: REGISTER requests	Platform	-	Number of SIP REGISTER request messages for each second.
Number of SIP REGISTER request messages for each second	Number of SIP requests with a given method name	Platform	-	Number of SIP requests with the given method name for each second.
Advanced metrics/SIP traffic	Number of SIP responses with a given response code	Platform	Minimum answer code Maximum answer code	Number of SIP answer messages for each second with a response code in the given range.
Advanced metrics/SIP traffic	Number of SIP messages over a given transport protocol	Platform	Transport protocol (UDP, TCP, SCTP)	Number of SIP messages for each second over the given transport protocol.
Advanced metrics/SIP traffic	Number of fragmented UDP SIP messages	Platform	-	Number of SIP messages for each second that were received in multiple UDP fragments.
Advanced metrics/Megaco/ H.248	Number of Megaco legs created	Platform	-	Number of new Megaco legs for each second.
Advanced metrics/Megaco/ H.248	Number of active Megaco legs	Platform	-	Total number of Megaco legs.
Advanced metrics/Megaco/ H.248	Number of Megaco legs that finished	Platform	-	Number of Megaco legs that finished for each second.
Advanced metrics/Megaco/ H.248	Number of Megaco legs that finished after a completed SDP negotiation	Platform	-	Number of Megaco legs that finished for each second with a previous complete SDP negotiation.
Advanced metrics/Megaco/ H.248	Percentage of finished Megaco connections with a complete SDP negotiation	Platform	-	Percentage of finished Megaco legs with a complete SDP negotiation (out of all finished Megaco legs).
Advanced metrics/MGCP	Number of MGCCP legs created	Platform	-	Number of new MGCP legs for each second.
Advanced metrics/MGCP	Number of active MGCP legs	Platform	-	Total number of MGCP connections being active.
Advanced metrics/MGCP	Number of MGCP legs that finished	Platform	-	Number of MGCP legs that finished for each second.

Table 21-1 (Cont.) Platform Wide and Prefix Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
Advanced metrics/ MGCP	Number of MGCP legs that finished after a complete SDP negotiation	Platform	-	Number of MGCP legs that finished for each second where a complete SDP negotiation happened before.
Advanced metrics/ MGCP	Percentage of finished MGCP connections with a complete SDP negotiation	Platform	-	Percentage of finished MGCP connections with a complete SDP negotiation (out of all finished MGCP connections).
Advanced metrics/SIP transactions	Number of completed transactions	Platform	-	Number of completed SIP transactions for each second.
Advanced metrics/SIP transactions	Number of completed transactions with a given method name	Platform	Transaction Method	Number of completed SIP transactions for each second with a given method name.
Advanced metrics/SIP transactions	Number of completed transactions with a given method name and response code	Platform	Transaction method Minimum answer code Maximum answer code	Number of completed SIP transactions for each second with a given method name and a response code in the given range.
Advanced metrics/SIP transactions	Number of completed transactions with a given response code	Platform	Minimum answer code Maximum answer code	Number of completed SIP transactions for each second with a response code in the given range.
Advanced metrics/SIP transactions	Number of timeout transactions	Platform	-	Number of SIP transactions for each second that timed out, for example, did not see a final response in time.
Advanced metrics/SIP transactions	Number of completed transactions with the number of request retransmissions bigger than a given value	Platform	Method to monitor Minimum number of retransmissions	Number of SIP transactions with a given method name for each second where the number of retransmissions was at least the configured count.

Table 21-1 (Cont.) Platform Wide and Prefix Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
Advanced metrics/SIP transactions	Number of INVITE transactions completed with a code > 299 with the number of retransmissions of the final response bigger than a given value	Platform	Minimum number of retransmissions	Number of SIP INVITE transactions for each second that failed (response code > 299) where the final response was retransmitted at least the number of configured times.
Advanced metrics/SIP transactions	Number of timeout transactions with a certain method	Platform	Method to Monitor	Number of SIP transactions for each second with a given method name that timed out, for example, did not see a final response.
Advanced metrics/SIP transactions	Maximum response time	Platform	-	Displays the maximum response time, platform wide, in any given second. All non-INVITE transactions are taken into account.
Advanced metrics/Calls	Number of calls ended because of a session timeout	Platform, Prefix tag	-	Number of end-to-end calls (an end-to-end call can comprise of several correlated call legs) for each second that stopped being monitored because they were longer than the threshold (System setting, Session-timeout for calls).
Advanced metrics/Calls	Number of currently active calls	Platform, Prefix tag	Relevant Call State	Number of concurrent calls that are in the given call state.
Advanced metrics/Calls	Number of calls with a given call length	Platform, Prefix tag	Call length (milliseconds)>= Call length (milliseconds)<	Number of calls for each second that finished after being established for a time in the given range.
Advanced metrics/Calls	Number of calls with a given ringing time	Platform, Prefix tag	Ringing time (milliseconds)>= Ringing time (milliseconds)<	Number of calls for each second that were established after ringing for a time in the given range.

Table 21-1 (Cont.) Platform Wide and Prefix Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
Advanced metrics/ Calls	Number of calls with Q.850 cause codes	Platform, Prefix tag	Minimum Q.850 cause code Maximum Q.850 cause code	Number of SIP or ISUP calls for each second where one of the segments finished or failed and received a Q.850 reason (SIP) or cause value (ISUP) in the given range.
Advanced metrics/ Calls	Number of SIP calls with Q.850 cause codes in headers	Platform, Prefix tag	Minimum Q.850 cause code Maximum Q.850 cause code	Number of calls for each second where a SIP segment finished or failed and a Reason header contained a Q.850 cause value in the given range.
Advanced metrics/ Calls	Number of ISUP calls with Q.850 cause codes	Platform, Prefix tag	Minimum Q.850 cause code Maximum Q.850 cause code	Number of calls for each second where an ISUP segment finished or failed with a cause value in the given range.
Advanced metrics/ Calls	SDP declared RTP Transcoding	Platform, Prefix tag	Transcoding type Predicate type	Number of times for each second when an RTP transcoding event was detected within a SIP call. RTP transcoding is detected by comparing the negotiated SDP between the SIP segments of the call.
Advanced metrics/ Calls	Active calls with a RTP Transcoding	Platform, Prefix tag	Transcoding type Predicate type	Number of active SIP calls for each second in which RTP transcoding was detected. RTP transcoding is detected by comparing the negotiated SDP between the SIP segments of the call.
Advanced metrics/ Calls	Number of calls closed by the callee	Platform, Prefix tag	-	Number of calls for each second where the called party ended the call.
Advanced metrics/ Calls	Number of active calls belonging to this probe	Platform, Prefix tag	-	This is a KPI created on behalf of an Mediation Engine Connector. It counts only those active calls where the ingress leg is not touching a neighbor device.

Table 21-1 (Cont.) Platform Wide and Prefix Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
Advanced metrics/ Calls	Number of calls closed with a reason header in the BYE message	Platform, Prefix tag	-	Number of calls for each second that were ended with a BYE message containing a reason header indicating Session Disconnect Failure (SDF). To count as SDF the reason header must contain a Q.850 cause value other than 16, 17, 18, 19, 21, or 31.
Advanced metrics/ Calls	Number of calls failed due to a timeout during a session setup	Platform, Prefix tag	-	Number of calls for each second that timed out during session setup.
Advanced metrics/ Calls	Number of calls timed out while waiting for the response to the BYE message	Platform, Prefix tag	-	Number of calls for each second where the response to BYE was not received in time.
Advanced metrics/ Calls	Number of calls failed due to a non-200 OK response to the INVITE	Platform, Prefix tag	-	Number of calls for each second that failed due to a non-200 OK response to the INVITE.
Advanced metrics/ Calls	Number of established ingress legs	Platform, Prefix tag	-	Number of ingress legs for each second that were established.
Advanced metrics/ Calls	Number of redirected ingress legs	Platform, Prefix tag	-	Number of ingress legs for each second where the INVITE was answered with a response in the 300 range.
Advanced metrics/ Calls	Number of failed ingress legs	Platform, Prefix tag	-	Number of ingress legs for each second where the INVITE was answered with a response greater than or equal to 400.
Advanced metrics/ Calls	Number of ingress legs timed out during the setup	Platform, Prefix tag	-	Number of ingress legs for each second that timed out during session setup.

Table 21-1 (Cont.) Platform Wide and Prefix Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
Advanced metrics/ Calls	Number of ingress legs with a session time out	Platform, Prefix tag	-	Number of ingress legs for each second that stopped being tracked because they were established for longer than the threshold (System setting, Session-timeout for calls).
Advanced metrics/ Calls	Number of successfully closed ingress legs	Platform, Prefix tag	-	Number of ingress legs for each second that were closed successfully.
Advanced metrics/ Calls	Number of ingress legs closed with SDF	Platform, Prefix tag	-	Number of ingress legs for each second that were ended with a BYE message containing a reason header indicating Session Disconnect Failure (SDF). To count as SDF the reason header must contain a Q.850 cause value other than 16, 17, 18, 19, 21, or 31.
Advanced metrics/ Calls	Number of ingress legs with timeout after the BYE was sent	Platform, Prefix tag	-	Number of ingress legs for each second with a timeout after the BYE was sent.
Advanced metrics/ Calls	Number of ingress legs failed with a certain response code	Platform, Prefix tag	Lower bound for the code Upper bound for the code	Number of ingress legs for each second where the INVITE was answered with a response code in the given range.
Advanced metrics/ Calls	Number of ingress legs with Q.850 cause code	Platform, Prefix tag	Minimum Q.850 cause code Maximum Q.850 cause code	Number of ingress SIP or ISUP legs that finished or failed for each second and received a Q.850 reason (SIP) or cause value (ISUP) in the given range.
Advanced metrics/ Calls	Number of SIP ingress legs with the Q.850 cause code in the headers	Platform, Prefix tag	Minimum Q.850 cause code Maximum Q.850 cause code	Number of ingress SIP legs that finished or failed for each second and received a reason header with a Q.850 cause value in the given range.

Table 21-1 (Cont.) Platform Wide and Prefix Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
Advanced metrics/ Calls	Number of ISUP ingress legs with a Q.850 cause code	Platform, Prefix tag	Minimum Q.850 cause code Maximum Q.850 cause code	Number of ingress ISUP legs that finished or failed for each second and received a Q.850 cause value in the given range.
Advanced metrics/ Calls	Number of session establishments	Platform, Prefix tag	-	Indicates the number of session establishments. A session is established when one of the following events occurs in a call: • A 180 response is received • A 183 response is received • A successful final response (2xx) is received Counted once for each end-to end call.
Advanced metrics/ Registrations	Expired contacts in the last second	Platform, Prefix tag	-	Number of registered contacts that expired for each second. Counts for each binding for each server.
Advanced metrics/ Registrations	New contacts in the last second	Platform, Prefix tag	-	Number of new contacts for each second (first-time REGISTER). Counts for each binding for each server.
Advanced metrics/ Registrations	Contacts refreshed in the last second	Platform, Prefix tag	-	Number of contacts refreshed for each second (refreshing REGISTER). Counts for each binding for each server.
Advanced metrics/ Registrations	Failed registrations in the last second	Platform, Prefix tag	-	Number of failed REGISTER attempts for each second. Counts REGISTER transactions that failed with response codes ≥ 300 , except 302, 401, or 407.

Table 21-1 (Cont.) Platform Wide and Prefix Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
Advanced metrics/ Registrations	Unauthorized registrations in the last second	Platform, Prefix tag	-	Number of failed REGISTER attempts for each second where a 401/407 response was not followed by another attempt.
Advanced metrics/ Registrations	Registered contacts gone in the last second	Platform, Prefix tag	-	Number of contacts that were gone for each second. A contact is gone if it is explicitly unregistered (expires=0). Additionally contacts that are not listed in a REGISTER response anymore are treated as gone if System setting Registrations gone events is enabled.
Advanced metrics/ RTCP	Number of RTCP packets (all types)	Platform	-	Number of RTCP packets for each second.
Advanced metrics/ RTCP	Number of RTCP-XR packets	Platform	-	Number of RTCP Extended Report (XR) packets for each second.
Advanced metrics/ RTCP	Minimum jitter values reported in the RTCP of finished streams	Platform	-	Lowest jitter value (in milliseconds) from RTCP Receiver Reports of all streams that ended in a given second.
Advanced metrics/ RTCP	Maximum jitter values reported in the RTCP of finished streams	Platform	-	Highest jitter value (in milliseconds) from RTCP Receiver Reports of all streams that ended in a given second.
Advanced metrics/ RTCP	Average jitter values reported in the RTCP of finished streams	Platform	-	Average of the jitter values (in milliseconds) from RTCP Receiver Reports of all streams that ended in a given second.
Advanced metrics/ RTCP	Minimum delay values reported in the RTCP of finished streams	Platform	-	Lowest delay value (in milliseconds) of all streams that ended in a given second. The delay for each stream is calculated or taken from RTCP-XR (preferring the latter).

Table 21-1 (Cont.) Platform Wide and Prefix Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
Advanced metrics/ RTCP	Maximum delay values reported in the RTCP of finished streams	Platform	-	Highest delay value (in milliseconds) of all streams that ended in a given second. The delay for each stream is calculated or taken from RTCP-XR (preferring the latter).
Advanced metrics/ RTCP	Average delay values reported in the RTCP of finished streams	Platform	-	Average of the delay values (in milliseconds) of all streams that ended in a given second. The delay for each stream is calculated or taken from RTCP-XR (preferring the latter).
Advanced metrics/ RTCP	Minimum MOScq values reported in the RTCP-XR of finished streams	Platform	-	Lowest MOSCQ value from RTCP-XR VoIP Metrics Report Blocks of all streams that ended in a given second. Only streams which reported MOS are taken into account.
Advanced metrics/ RTCP	Maximum MOScq values reported in the RTCP-XR of finished streams	Platform	-	Highest MOSCQ value from RTCP-XR VoIP Metrics Report Blocks of all streams that ended in a given second. Only streams which reported MOS are taken into account.
Advanced metrics/ RTCP	Average MOScq values reported in the RTCP-XR of finished streams	Platform	-	Average of all MOSCQ values from RTCP-XR VoIP Metrics Report Blocks of all streams that ended in a given second. Only streams which reported MOS are taken into account.
Advanced metrics/ RTCP Usage	Streams with RTCP	Platform	-	Counter is increased for each RTP stream that ended and where at least one RTCP packet was seen (incl. RTCP-XR).
Advanced metrics/ RTCP Usage	Streams with RTCP-XR	Platform	-	Counter is increased for each RTP stream that ended and where at least one RTCP-XR packet was seen.

Table 21-1 (Cont.) Platform Wide and Prefix Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
Advanced metrics/ RTCP Usage	Streams with RTCP- XR Block Type 1 (Loss RLE Report Block)	Platform	-	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
Advanced metrics/ RTCP Usage	Streams with RTCP- XR Block Type 2 (Duplicate RLE Report Block)	Platform	-	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
Advanced metrics/ RTCP Usage	Streams with RTCP- XR Block Type 3 (Packet Receipt Times Report Block)	Platform	-	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
Advanced metrics/ RTCP Usage	Streams with RTCP- XR Block Type 4 (Receiver Reference Times Report Block)	Platform	-	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
Advanced metrics/ RTCP Usage	Streams with RTCP- XR Block Type 5 (DLRR Report Block)	Platform	-	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
Advanced metrics/ RTCP Usage	Streams with RTCP- XR Block Type 6 (Statistics Summary Report Block)	Platform	-	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
Advanced metrics/ RTCP Usage	Streams with RTCP- XR Block Type 7 (Statistics Summary Report Block)	Platform	-	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
Advanced metrics/ RTCP Usage	Streams with RTCP- XR Block Type 8 (BT's Extended Network Quality Report Block)	Platform	-	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.

Table 21-1 (Cont.) Platform Wide and Prefix Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
Advanced metrics/ RTCP Usage	Streams with RTCP- XR Block Type 9 (Texas Instrument Extended VoIP Quality Report Block)	Platform	-	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
Advanced metrics/ RTCP Usage	Streams with RTCP- XR Block Type 10 (Port-repair Loss RLE Report Block)	Platform	-	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
Advanced metrics/ RTCP Usage	Streams with RTCP- XR Block Type 11 (Multicast Acquisition Report Block)	Platform	-	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
Advanced metrics/ RTCP Usage	Streams with RTCP- XR Block Type 12 (IDMS Report Block)	Platform	-	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
Advanced metrics/ RTCP Usage	Streams with RTCP- XR Block Type 13 (ECN Summary Report Block)	Platform	-	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
Advanced metrics/ RTCP Usage	Streams with RTCP- XR Block Type 14 (Measurement Information Report Block)	Platform	-	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
Advanced metrics/ RTCP Usage	Streams with RTCP- XR Block Type 15 (Packet Delay Variation Metrics Block)	Platform	-	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
Advanced metrics/ RTCP Usage	Streams with RTCP- XR Block Type 16 (Delay Metrics Block)	Platform	-	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.

Table 21-1 (Cont.) Platform Wide and Prefix Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
Advanced metrics/ RTCP Usage	Streams with RTCP- XR Block Type 17 (Burst/Gap Loss Summary Statistics Block)	Platform	-	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
Advanced metrics/ RTCP Usage	Streams with RTCP- XR Block Type 18 (Burst/Gap Discard Summary Statistics Block)	Platform	-	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
Advanced metrics/ RTCP Usage	Streams with RTCP- XR Block Type 19 (Frame Impairment Summary Statistics Block)	Platform	-	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
Advanced metrics/ RTCP Usage	Streams with RTCP- XR Block Type 20 (Burst/Gap Loss Metrics Block)	Platform	-	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
Advanced metrics/ RTCP Usage	Streams with RTCP- XR Block Type 21 (Burst/Gap Discard Metrics Block)	Platform	-	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
Advanced metrics/ RTCP Usage	Streams with RTCP- XR Block Type 22 (MPEG2 Transport Stream PSI-Independent Decodability Statistics Metrics Block)	Platform	-	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
Advanced metrics/ RTCP Usage	Streams with RTCP- XR Block Type 23 (De-jitter Buffer Metrics Block)	Platform	-	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
Advanced metrics/ RTCP Usage	Streams with RTCP- XR Block Type 24 (Discard Count Metrics Block)	Platform	-	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.

Table 21-1 (Cont.) Platform Wide and Prefix Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
Advanced metrics/ RTCP Usage	Streams with RTCP- XR Block Type in range 25-254	Platform	-	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
Advanced metrics/ RTCP Usage	Streams with RTCP- XR Block Type 255	Platform	-	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
Default	UCaaS Call attempts per second	Platform	-	Number of UCaaS CCaaS call attempts for each second
Default	Teams DR Call attempts per second	Platform	-	Number of Teams DR call attempts for each second
Default	Teams Caller to PSTN DR Callee CAPS	Platform	-	Number of Teams DR call attempts for each second made from Teams Caller to PSTN Callee
Default	PSTN Caller to Teams DR Callee CAPS	Platform	-	Number of Teams DR call attempts for each second made from PSTN Caller to Teams Callee
Default	UCaaS Active Calls	Platform	-	Number of established UCaaS CCaaS concurrent calls
Default	TEAMS DR Active Calls	Platform	-	Number of established Teams DR concurrent calls
Default	Teams Caller to PSTN DR Callee Active Calls	Platform	-	Number of established Teams DR concurrent calls made from Teams Caller to PSTN Callee
Default	PSTN Caller to Teams DR Callee Active Calls	Platform	-	Number of established Teams DR concurrent calls made from PSTN Caller to Teams Callee

Note

The Prefix KPI - **Ineffective NONCALL Subscription attempts** is not applicable for Subscriptions scenarios and will not be incremented.

Device, Trunk and IP Tag KPIs

[Table 21-2](#) describes the Operations Monitor device trunk and IP tag KPIs, where:

- The device, and trunk KPIs provide data about the devices.
- The IP tag KPIs provide data about the IP addresses that match specific IP tags.

Table 21-2 Device, Trunk and IP Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
Default	Active sessions (incoming)	Device, IP tag	-	Number of established call legs to the device.
Default	Active sessions (outgoing)	Device, IP tag	-	Number of established call legs from the device.
Default	Active sessions (traversing)	Device	-	Number of established calls that traverse the device (where there is both an incoming and an outgoing leg).
Default	Call attempts for each second (CAPS) (incoming)	Device, IP tag	-	Number of call attempts for each second to the device. Counts for each incoming leg.
Default	Call attempts for each second (CAPS) (outgoing)	Device, IP tag	-	Number of call attempts for each second out of the device. Counts for each outgoing leg.
Default	Call attempts for each second (traversing)	Device	-	Number of call attempts for each second traversing the device (where there is both an incoming and an outgoing leg)
Default	Registered Users	Device, IP tag	-	Number of users registered to the device. Users with multiple bindings/contacts are counted only once.
Default	Registered Contacts	Device, IP tag	-	Number of contacts registered to the device
Default	Response time for this device	Device, IP tag	-	Maximum response time in milliseconds. Based on all completed transactions where the device is the server.
Default	Transit time (maximum) for this device	Device	-	Maximum time difference in milliseconds between an incoming and an outgoing leg of the same call traversing a device.
IETF metrics	Combined Maximum successful session request delay	Device, IP tag	-	This metric combines the ISUP Post Dial Delay (PDD) and SIP Session Request Delay (SRD) into a single metric. Sessions are only accounted for if they originated at this specific device. SSRD is defined as the time interval from the first bit of the initial INVITE message containing the information sent by the originating user agent to the intended mediation or destination agent until the last bit of the first provisional response is received indicating an audible or visual status of the initial session setup request.

Table 21-2 (Cont.) Device, Trunk and IP Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
IETF metrics	Combined maximum failed session request delay	Device, IP tag	-	This metric combines the ISUP Post Dial Delay (PDD) and SIP Session Request Delay (SRD) into a single metric. Sessions are only accounted for if they originated at this specific device. Failed Session Request Delay (FSRD) is the time interval from the first bit of the initial INVITE message containing the information sent by the originating agent or user to the intended mediation or destination agent until the last bit of the first provisional response or a failure indication response. A failure response is described as a 4XX (excluding 401, 402, and 407 non-failure challenge response codes), 5XX, or possible 6XX message.
IETF metrics	Combined maximum session request delay	Device, IP tag	-	This metric combines the ISUP Post Dial Delay (PDD) and SIP Session Request Delay (SRD) into a single metric. Sessions are only accounted for if they originated at this specific device. Session Request Delay (SRD) is utilized to detect failures or impairments causing delay in responding to a UA session request. SRD is measured for both successful and failed session setup requests as this metric relates to the user experience. It is recommended that the SSRD and the FSRD are used instead of SRD as the time greatly varies between the two. SRD is similar to Post-Selection Delay from telephony applications.
IETF metrics	Incoming session establishment ratio	Device, IP tag	-	SER is defined as follows: $\text{SER} = \frac{\text{Number of new session INVITE requests resulting in a 200 OK response}}{\text{Total number of attempted INVITE requests} - \text{Number of INVITE requests resulting in a 3XX response}}$ If defined for a device, it counts the incoming calls to that device. If defined for a trunk, it counts the calls for which the initial INVITE goes to that trunk (egress). This metric is similar to Answer Seizure Ratio (ASR) in telephony applications of SIP.
IETF metrics	Outgoing session establishment ratio	Device, IP tag	-	SER is defined as follows: $\text{SER} = \frac{\text{Number of new session INVITE requests resulting in a 200 OK response}}{\text{Total number of attempted INVITE requests} - \text{Number of INVITE requests resulting in a 3XX response}}$ If defined for a device, it counts the outgoing calls to that device. If defined for a trunk, it counts the calls for which the initial INVITE goes to that trunk (ingress). This metric is similar to Answer Seizure Ratio (ASR) in telephony applications of SIP.

Table 21-2 (Cont.) Device, Trunk and IP Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
IETF metrics	Incoming session establishment effectiveness ratio	Device, IP tag	-	This metric is complimentary to SER, but is intended to exclude the potential effects of an individual user of the target UA from the metric. SEER is defined as follows: $\text{SEER} = (\text{Number of INVITE requests resulting in a 200 OK, 480, 486, 600, or 603 response}) / (\text{Total number of attempted INVITE requests} - \text{Number of INVITE requests resulting in a 3XX response}).$ The response codes 480, 486, 600, and 603 were chosen as they indicate the effect of an individual user of the UA. It is possible that an individual user could cause a negative effect on the UA. For example, they may have incorrectly configured the UA causing a response code not directly related to a SSP, but this cannot be easily determined from an intermediary B2BUA somewhere in between the originating and terminating UA. With this in consideration, response codes such as 401, 407, and 420 (not an exhaustive list) were not included in the numerator of the metric. If defined for a device, it counts the incoming calls to that device. If defined for a trunk, it counts the calls for which the initial INVITE comes from the platform to that trunk (egress). This metric is similar to Network Effectiveness Ratio (NER).

Table 21-2 (Cont.) Device, Trunk and IP Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
IETF metrics	Outgoing session establishment effectiveness ratio	Device, IP tag	-	This metric is complimentary to Session establishment ratio (SER), but is intended to exclude the potential effects of an individual user of the target UA from the metric. SEER = (Number of INVITE requests resulting in a 200 OK, 480, 486, 600, or 603 response)/(Total number of attempted INVITE requests - Number of INVITE requests resulting in a 3XX response). The response codes 480, 486, 600, and 603 were chosen as they accurately indicate the effect of an individual user of the UA. It is possible that an individual user could cause a negative effect on the UA. For example, they may have incorrectly configured the UA resulting a response code that is not related to a SSP. This cannot be easily determined from an intermediary B2BUA somewhere in between the originating and terminating UA. With this in consideration, response codes such as 401, 407, and 420 (not an exhaustive list) were not included in the numerator of the metric. If defined for a device, this metric counts the outgoing calls to that device. If defined for a trunk, this metric counts the calls for which the initial INVITE comes from the platform to that trunk (ingress). This metric is similar to Network Effectiveness Ratio (NER).
IETF metrics	Incoming ineffective registration attempts	Device, IP tag	-	Ineffective registration attempts are utilized to detect failures or impairments causing an inability for a registrar to receive a UA REGISTER request. A failed registration attempt is a final failure response to the initial REGISTER request. It indicates a failure received from the destination registrar, interim proxies, or due to a timeout of the REGISTER request at the originating UA. A failure response is described as a 4XX (excluding 401, 402, and 407 non-failure challenge response codes), 5XX, or possible 6XX message. IRA may be used to detect problems in downstream signaling functions, which may be impairing the REGISTER message from reaching the intended registrar; or, it may indicate a registrar has become overloaded and is unable to respond to the request.

Table 21-2 (Cont.) Device, Trunk and IP Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
IETF metrics	Outgoing ineffective registration attempts	Device, IP tag	-	Ineffective registration attempts are utilized to detect failures or impairments causing an inability for a registrar to receive a UA REGISTER request. A failed registration attempt is a final failure response to the initial REGISTER request. It indicates a failure received from the destination registrar, interim proxies, or due to a time-out of the REGISTER request at the originating UA. A failure response is described as a 4XX (excluding 401, 402, and 407 non-failure challenge response codes), 5XX, or possible 6XX message. IRA may be used to detect problems in downstream signaling functions, which may be impairing the REGISTER message from reaching the intended registrar; or, it may indicate a registrar has become overloaded and is unable to respond to the request.
IETF metrics	Incoming session success ratio	Device, IP tag	-	Session Success Ratio (SSR) is defined as the percentage of successfully completed sessions compared to sessions, which fail due to ISA or SDF. This metric is also known as Call Success Ratio (CSR) in telephony applications of SIP.
IETF metrics	Outgoing session success ratio	Device, IP tag	-	Session Success Ratio (SSR) is defined as the percentage of successfully completed sessions compared to sessions, which fail due to ISA or SDF. This metric is also known as Call Success Ratio (CSR) in telephony applications of SIP.
IETF metrics	Session disconnect delay	Device, IP tag	-	Session Disconnect Delay (SDD) is the time interval between the first bit of the sent session completion message, such as a BYE, and the last bit of the subsequently received 2XX response.
IETF metrics	Incoming session duration time	Device, IP tag	-	Session Duration Time (SDT) is utilized to detect technical issues causing short session durations. For example, poor audio quality. SDT is defined as an average of duration of the interval between receipt of the first bit of a 200 OK response to an INVITE plus receipt of the last bit of an associated BYE message. Retransmissions of the 200 OK and ACK messages due to network impairments do not reset the metric timers.
IETF metrics	Outgoing session duration time	Device, IP tag	-	Session Duration Time (SDT) is utilized to detect technical issues causing short session durations. For example, poor audio quality. SDT is defined as an average of duration of the interval between receipt of the first bit of a 200 OK response to an INVITE plus receipt of the last bit of an associated BYE message. Retransmissions of the 200 OK and ACK messages due to network impairments do not reset the metric timers.

Table 21-2 (Cont.) Device, Trunk and IP Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
IETF metrics	Average successful session request delay	Device, IP tag	-	Successful Session Request Delay (SSRD) is defined as the time interval from the first bit of the initial INVITE message containing the necessary information is sent by the originating user agent to the intended mediation or destination agent until the last bit of the first provisional response is received indicating an audible or visual status of the initial session setup request. Sessions are only accounted for if they originated at this specific device.
IETF metrics	Average successful session request delay (all sessions)	Device, IP tag	-	Successful Session Request Delay (SSRD) is defined as the time interval from the first bit of the initial INVITE message containing the necessary information is sent by the originating user agent to the intended mediation or destination agent until the last bit of the first provisional response is received indicating an audible or visual status of the initial session setup request. Metric computed for all sessions passing through this device.
IETF metrics	Average failed session request delay	Device, IP tag	-	Failed Session Request Delay (FSRD) is defined as the time interval from the first bit of the initial INVITE message containing the necessary information sent by the originating agent or user to the intended mediation or destination agent until the last bit of the first provisional response or a failure indication response. A failure response is described as a 3XX (excluding 401, 402, and 407 non- failure challenge response codes), 5XX, or possible 6XX message. Sessions are only accounted for if they originated at this specific device.
IETF metrics	Average failed session request delay (all sessions)	Device, IP tag	-	Failed Session Request Delay (FSRD) is defined as the time interval from the first bit of the initial INVITE message containing the necessary information sent by the originating agent or user to the intended mediation or destination agent until the last bit of the first provisional response or a failure indication response. A failure response is described as a 3XX (excluding 401, 402, and 407 non- failure challenge response codes), 5XX, or possible 6XX message. Metric computed for all sessions passing through this device.
IETF metrics	Maximum successful session request delay	Device, IP tag	-	Successful Session Request Delay (SSRD) is defined as the time interval from the first bit of the initial INVITE message containing the necessary information is sent by the originating user agent to the intended mediation or destination agent until the last bit of the first provisional response is received indicating an audible or visual status of the initial session setup request. Sessions are only accounted for if they originated at this specific device.

Table 21-2 (Cont.) Device, Trunk and IP Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
IETF metrics	Maximum successful session request delay (all sessions)	Device, IP tag	-	Successful Session Request Delay (SSRD) is defined as the time interval from the first bit of the initial INVITE message containing the necessary information is sent by the originating user agent to the intended mediation or destination agent until the last bit of the first provisional response is received indicating an audible or visual status of the initial session setup request. Metric computed for all sessions passing through this device.
IETF metrics	Maximum failed session request delay	Device, IP tag	-	Failed Session Request Delay (FSRD) is defined as the time interval from the first bit of the initial INVITE message containing the necessary information sent by the originating agent or user to the intended mediation or destination agent until the last bit of the first provisional response or a failure indication response. A failure response is described as a 3XX (excluding 401, 402, and 407 non-failure challenge response codes), 5XX, or possible 6XX message. Sessions are only accounted for if they originated at this specific device.
IETF metrics	Maximum failed session request delay (all sessions)	Device, IP tag	-	Failed Session Request Delay (FSRD) is defined as the time interval from the first bit of the initial INVITE message containing the necessary information sent by the originating agent or user to the intended mediation or destination agent until the last bit of the first provisional response or a failure indication response. A failure response is described as a 3XX (excluding 401, 402, and 407 non-failure challenge response codes), 5XX, or possible 6XX message. Metric computed for all sessions passing through this device.
Advanced Metrics	Number of active sessions	Device, IP tag	Direction of the session Relevant call state	Number of call segments active in the given call direction and state.
Advanced Metrics	Number of established calls for each second	Device, IP tag	Direction of the call	Number of call segments for each second that got established, in the given call direction.
Advanced Metrics	Number of closed calls for each second	Device, IP tag	Direction of the call	Number of call segments for each second that finished, in the given call direction.
Advanced Metrics	Number of session timeout calls for each second	Device, IP tag	Direction of the call	Number of end-to-end calls (an end-to-end call can comprise of several correlated call legs) for each second that stopped being monitored because they were longer than the threshold (System setting, Session-timeout for calls).

Table 21-2 (Cont.) Device, Trunk and IP Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
Advanced Metrics	Number of failed calls for each second	Device, IP tag	Direction of the call	Number of call segments for each second that failed, in the given call direction. This KPI is incremented for all response codes greater than 300. That is, 3xx,4xx,5xx and 6xx, except for codes 401 and 407.
Advanced Metrics	Number of calls completed/ established with a specific code for each second	Device, IP tag	Direction of the call Lower bound for the code Upper bound for the code	Number of SIP call segments for each second in the given direction that received a final response to the INVITE with a response code in the given range.
Advanced Metrics	Number of calls with Q.850 cause codes	Device, IP tag	Minimum Q.850 cause code Maximum Q.850 cause code	Number of SIP or ISUP call segments for each second where a Q.850 cause value in the given range was received, in a reason header (SIP) or in a cause parameter (ISUP).
Advanced Metrics	Number of SIP calls with Q.850 cause codes	Device, IP tag	Minimum Q.850 cause code Maximum Q.850 cause code	Number of SIP call segments for each second where a reason header with a Q.850 cause value in the given range was received.
Advanced Metrics	Number of ISUP calls with Q.850 cause codes	Device, IP tag	Minimum Q.850 cause code Maximum Q.850 cause code	Number of ISUP call segments for each second where a Q.850 cause value in the given range was received.
Advanced Metrics	Number of calls with a given length	Device, IP tag	Direction of the call Call length (milliseconds)>= Call length (milliseconds)<	Number or call segments for each second that finished after being established for a duration in the given range, in the given call direction.
Advanced Metrics	Number of session establishments	Device, IP tag	Direction of the call	Indicates the number of session establishments. A session is established when one of the following events occur: • A 180 response is received. • A 183 response is received. • A successful final response (2xx) is received. Counts for each call segment in the given direction.
Advanced Metrics	Number of closed calls with a Reason header in the BYE message (SDF)	Device, IP tag	Direction of the call	Number of call segments for each second in the given direction that were ended with a BYE message containing a reason header indicating Session Disconnect Failure (SDF). To count as SDF the reason header must contain a Q.850 cause value other than 16, 17, 18, 19, 21, or 31.
Advanced Metrics	Number of SIP call attempts	Device, IP tag	Direction of the call	Number of SIP call attempts for each second in the given call direction (for each call segment).

Table 21-2 (Cont.) Device, Trunk and IP Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
Advanced Metrics	Number of ISUP call attempts	Device, IP tag	Direction of the call	Number of ISUP call attempts for each second in the given call direction (for each call segment).
Advanced Metrics	Number of SIP calls that terminated abnormally	Device, IP tag	Direction of the call	Number of SIP call segments for each second that terminated abnormally, in the given call direction.
Advanced Metrics	Number of ISUP calls that terminated abnormally	Device, IP tag	Direction of the call	Number of ISUP call segments for each second that terminated abnormally, in the given call direction.
Advanced metrics	Rate of incoming SIP calls that terminated abnormally	Device, IP tag	-	Rate of incoming SIP call segments for each second that terminated abnormally. In percent of abnormally-terminated calls out of call terminated calls.
Advanced metrics	Rate of outgoing SIP calls that terminated abnormally	Device, IP tag	-	Rate of outgoing SIP call segments for each second that terminated abnormally. In percent of abnormally-terminated calls out of call terminated calls.
Advanced metrics	Rate of incoming ISUP calls that terminated abnormally	Device, IP tag	-	Rate of incoming ISUP call segments for each second that terminated abnormally. In percent of abnormally-terminated calls out of call terminated calls.
Advanced metrics	Rate of outgoing ISUP calls that terminated abnormally	Device, IP tag	-	Rate of outgoing ISUP call segments for each second that terminated abnormally. In percent of abnormally-terminated calls out of call terminated calls.
Advanced Metrics	Expired contacts	Device, IP tag	-	Number of contacts that were registered to the device and expired for each second.
Advanced Metrics	Number of new contacts for each second	Device, IP tag	-	Number of new contacts for each second that registered to the device (initial REGISTER).
Advanced Metrics	Refreshed contacts	Device, IP tag	-	Number of contacts registered to the device that refreshed the binding for each second (refreshing REGISTER).
Advanced Metrics	Failed registrations	Device, IP tag	-	Number of registration attempts to the device that failed for each second.
Advanced Metrics	Number of unauthorized registrations for each second	Device, IP tag	-	Number of registration attempts to the device that finally failed with REGISTER response code 401 or 407.
Advanced Metrics	Number of registered contacts gone for each second	Device, IP tag	-	Number of contacts that were gone for each second. A contact is gone if it is explicitly unregistered (expires=0). Additionally contacts that are not listed in a REGISTER response anymore are treated as gone if System setting, Registrations gone events is enabled.

Table 21-2 (Cont.) Device, Trunk and IP Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
Advanced Metrics	Number of registration attempts with a specific code for each second	Device, IP tag	Lower bound for the code Upper bound for the code	Number of registration attempts to the device that received a REGISTER response code in the given range.
Advanced Metrics	Total number of active calls	Device, IP tag	-	Sum of the numbers of incoming and outgoing established call segments on the device. This counts traversing calls twice.
Advanced Metrics	Total number of active calls (including traversing calls)	Device	-	Sum of the numbers of incoming, outgoing, and traversing established calls on the device. This counts traversing calls three times.
Advanced Metrics	SDP declared RTP transcoding	Device, IP Tag	Transcoding type Predicate type	Number of times each second when an RTP transcoding even was detected within a SIP call. RTP transcoding is detected by comparing the negotiated SDP between the SIP segments of the call.
Advanced metrics	Active calls with RTP transcoding	Device	Transcoding type Predicate type	Number of active SIP calls for each second in which RTP transcoding was detected. RTP transcoding is detected by comparing the negotiated SDP between the SIP segments of the call.
Advanced metrics / TCP counters	Number of active TCP connections to/from this device	Device, IP tag	-	Number of active TCP connections monitored on the device.
Advanced metrics/TCP counters	Number of created TCP connections to/from this device	Device, IP tag	-	Number of new TCP connections monitored on the device.
Advanced metrics/TCP counters	Number of timeout TCP connections to/from this device	Device, IP tag	-	Number of monitored TCP connections on the device that timed out.
Advanced metrics/TCP counters	Number of TCP SYN messages to/from this device	Device, IP tag	Direction of the message	Number of TCP packets of the respective type in the sent or received by the device (direction according to the KPI parameter).
Advanced metrics/TCP counters	Number of TCP ACK messages to/from this device	Device, IP tag	Direction of the message	Number of TCP packets of the respective type in the sent or received by the device (direction according to the KPI parameter).
Advanced metrics/TCP counters	Number of TCP RST messages to/from this device	Device, IP tag	Direction of the message	Number of TCP packets of the respective type in the sent or received by the device (direction according to the KPI parameter).
Advanced metrics/TCP counters	Number of TCP FIN messages to/from this device	Device, IP tag	Direction of the message	Number of TCP packets of the respective type in the sent or received by the device (direction according to the KPI parameter).
Advanced metrics/ SCTP counters	Number of active SCTP associations on this device	Device, IP tag	-	Number of active SCTP associations monitored on the device.

Table 21-2 (Cont.) Device, Trunk and IP Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
Advanced metrics/ SCTP counters	Number of SCTP associations created on this device	Device, IP tag	-	Number of new SCTP associations monitored on the device, for each second.
Advanced metrics/ SCTP counters	Number of SCTP DATA chunks to/from this device	Device, IP tag	Direction of the message	Number of SCTP chunks of the respective type sent or received by the device for each second (direction is a KPI parameter).
Advanced metrics/ SCTP counters	Number of SCTP INIT chunks to/from this device	Device, IP tag	Direction of the message	Number of SCTP chunks of the respective type sent or received by the device for each second (direction is a KPI parameter).
Advanced metrics/ SCTP counters	Number of SCTP INIT ACK chunks to/from this device	Device, IP tag	Direction of the message	Number of SCTP chunks of the respective type sent or received by the device for each second (direction is a KPI parameter).
Advanced metrics/ SCTP counters	Number of SCTP SACK chunks to/from this device	Device, IP tag	Direction of the message	Number of SCTP chunks of the respective type sent or received by the device for each second (direction is a KPI parameter).
Advanced metrics/ SCTP counters	Number of SCTP HEARTBEAT chunks to/from this device	Device, IP tag	Direction of the message	Number of SCTP chunks of the respective type sent or received by the device for each second (direction is a KPI parameter).
Advanced metrics/ SCTP counters	Number of SCTP HEARTBEAT ACK chunks to/from this device	Device, IP tag	Direction of the message	Number of SCTP chunks of the respective type sent or received by the device for each second (direction is a KPI parameter).
Advanced metrics/ SCTP counters	Number of SCTP ABORT chunks to/from this device	Device, IP tag	Direction of the message	Number of SCTP chunks of the respective type sent or received by the device for each second (direction is a KPI parameter).
Advanced metrics/ SCTP counters	Number of SCTP SHUTDOWN chunks to/from this device	Device, IP tag	Direction of the message	Number of SCTP chunks of the respective type sent or received by the device for each second (direction is a KPI parameter).
Advanced metrics/ SCTP counters	Number of SCTP SHUTDOWN ACK chunks to/from this device	Device, IP tag	Direction of the message	Number of SCTP chunks of the respective type sent or received by the device for each second (direction is a KPI parameter).
Advanced metrics/ SCTP counters	Number of SCTP ERROR chunks to/from this device	Device, IP tag	Direction of the message	Number of SCTP chunks of the respective type sent or received by the device for each second (direction is a KPI parameter).
Advanced metrics/ SCTP counters	Number of SCTP COOKIE ECHO chunks to/from this device	Device, IP tag	Direction of the message	Number of SCTP chunks of the respective type sent or received by the device for each second (direction is a KPI parameter).
Advanced metrics/ SCTP counters	Number of SCTP COOKIE ACK chunks to/from this device	Device, IP tag	Direction of the message	Number of SCTP chunks of the respective type sent or received by the device for each second (direction is a KPI parameter).
Advanced metrics/ SCTP counters	Number of SCTP ECNE chunks to/from this device	Device, IP tag	Direction of the message	Number of SCTP chunks of the respective type sent or received by the device for each second (direction is a KPI parameter).

Table 21-2 (Cont.) Device, Trunk and IP Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
Advanced metrics/ Sctp counters	Number of Sctp CWR chunks to/ from this device	Device, IP tag	Direction of the message	Number of Sctp chunks of the respective type sent or received by the device for each second (direction is a KPI parameter).
Advanced metrics/ Sctp counters	Number of Sctp SHUTDOWN COMPLETE chunks to/from this device	Device, IP tag	Direction of the message	Number of Sctp chunks of the respective type sent or received by the device for each second (direction is a KPI parameter).
Advanced metrics/ Traffic	Bandwidth consumed by SIP requests with the specified method	Device, IP tag	SIP Method	Bytes/second consumed by SIP requests with the given method sent or received by the device.
Advanced metrics/ Traffic	Bandwidth consumed by fragmented SIP requests with the specified method	Device, IP tag	SIP Method	Bytes/second consumed by SIP requests with the given method sent or received by the device, only counting the messages if they were a fragmented UDP datagram.
Advanced metrics/ Traffic	Number of UDP packets	Device, IP tag	Direction of the message	Number of UDP packets for each second sent or received by the device.
Advanced metrics/ Traffic	Bandwidth of the UDP packets	Device, IP tag	Direction of the message	Bytes/second of UDP packets sent or received by the device. This counts the packet starting with the transport header (not including the Ethernet and IP headers).
Advanced metrics/ Traffic	Number of TCP packets	Device, IP tag	Direction of the message	Number of TCP packets for each second sent or received by the device.
Advanced metrics/ Traffic	Bandwidth of the TCP packets	Device, IP tag	Direction of the message	Bytes/second of TCP packets sent or received by the device. This counts the packet starting with the transport header (not including the Ethernet and IP headers).
Advanced metrics/ Traffic	Number of Sctp packets	Device, IP tag	Direction of the message	Number of Sctp packets for each second sent or received by the device.
Advanced metrics/ Traffic	Bandwidth of the Sctp packets	Device, IP tag	Direction of the message	Bytes/second of Sctp packets sent or received by the device. This counts the packet starting with the transport header (not including the Ethernet and IP headers).
Advanced metrics/ Traffic	Number of fragmented UDP packets	Device, IP tag	Direction of the message	Number of fragmented UDP packets for each second sent or received by the device.
Advanced metrics/ Traffic	Number of fragmented IPv4 packets in memory	Device, IP tag	Direction of the message	Number of fragmented IPv4 packets sent or received by the device currently kept in memory.
Advanced metrics/ Traffic	Number of fragmented IPv6 packets in memory	Device, IP tag	Direction of the message	Number of fragmented IPv6 packets sent or received by the device currently kept in memory.
Advanced metrics/ Traffic	Number of IPv4 packets	Device, IP tag	Direction of the message	Number of IPv4 packets sent or received for each second.
Advanced metrics/ Traffic	Number of IPv6 packets	Device, IP tag	Direction of the message	Number of IPv6 packets sent or received for each second.

Table 21-2 (Cont.) Device, Trunk and IP Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
Advanced metrics/ Transactions	Number of incoming transactions with the given method name and response code	Device, IP tag	Transaction method Minimum answer code Maximum answer code	Number of transactions for each second where the device was the server (incoming transactions) and the method name and response code match the given parameters.
Advanced metrics/ Transactions	Number of outgoing transactions with the given method, name, and response code	Device, IP tag	Transaction method Minimum answer code Maximum answer code	Number of transactions for each second where the device was the client (outgoing transactions) and the method name and response code match the given parameters.
Advanced metrics/ Transactions	Number of incoming timed-out transactions with a certain method	Device, IP tag	Method to Monitor	Number of transactions for each second where the device received the request of the given type but did not send a final response in time.
Advanced metrics/ Transactions	Number of outgoing timed-out transactions with a certain method	Device, IP tag	Method to Monitor	Number of transactions for each second where the device sent the request of the given type but did not receive a final response in time.
Megaco/ H.248	Number of Megaco legs created	Device, IP tag	-	Number of new Megaco legs for each second on the Media Gateway.
Megaco/ H.248	Number of active Megaco legs	Device, IP tag	-	Number of active Megaco legs on the Media Gateway.
Megaco/ H.248	Number of Megaco legs that finished	Device, IP tag	-	Number of Megaco legs on the Media Gateway that finished for each second.
Megaco/ H.248	Number of Megaco legs that finished after a complete SDP negotiation	Device, IP tag	-	Number of Megaco legs on the Media Gateway that finished for each second, only counting those legs where a complete SDP negotiation happened before.
Megaco/ H.248	Percentage of finished Megaco connections with a complete SDP negotiation	Device, IP tag	-	Percentage of Megaco legs that finished after a complete SDP negotiation out of all finished Megaco legs on the Media Gateway.
Megaco/ H.248	Average millisecond response time for a Megaco request	Device, IP tag	-	Average response time for a Megaco request on the Media Gateway.
MGCP	Number of MGCP legs created	Device, IP tag	-	Number of new MGCP legs for each second on the Gateway.
MGCP	Number of active MGCP legs	Device, IP tag	-	Number of active MGCP legs on the Gateway.
MGCP	Number of MGCP legs that finished	Device, IP tag	-	Number of MGCP legs on the Gateway that finished for each second.
MGCP	Number of MGCP legs that finished after a complete SDP negotiation	Device, IP tag	-	Number of MGCP legs on the Gateway that finished for each second, only counting those legs where a complete SDP negotiation happened before.

Table 21-2 (Cont.) Device, Trunk and IP Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
MGCP	Percentage of finished MGCP connections with a complete SDP negotiation	Device, IP tag	-	Percentage of MGCP legs that finished after a complete SDP negotiation out of all finished MGCP legs on the Gateway.
MGCP	Average millisecond response time for a MGCP request	Device, IP tag	-	Average millisecond response time for a MGCP request on the Gateway.
RTCP	Number of RTCP packets (all types)	Device	Direction	Number of RTCP packets sent or received by the device.
RTCP	Number of RTCP-XR packets	Device	Direction	Number of RTCP-XR packets sent or received by the device.
RTCP	Minimum jitter values reported in RTCP of finished streams	Device	Direction	Lowest jitter value (in milliseconds) from RTCP Receiver Reports of all streams that ended in a given second.
RTCP	Maximum jitter values reported in RTCP of finished streams	Device	Direction	Highest jitter value (in milliseconds) from RTCP Receiver Reports of all streams that ended in a given second.
RTCP	Average jitter values reported in RTCP of finished streams	Device	Direction	Average of the jitter values (in milliseconds) from RTCP Receiver Reports of all streams that ended in a given second.
RTCP	Minimum delay values reported in RTCP of finished streams	Device	Direction	Lowest delay value (in milliseconds) of all streams that ended in a given second. The delay for each stream is calculated or taken from RTCP-XR (preferring the latter).
RTCP	Maximum delay values reported in RTCP of finished streams	Device	Direction	Highest delay value (in milliseconds) of all streams that ended in a given second. The delay for each stream is calculated or taken from RTCP-XR (preferring the latter).
RTCP	Average delay values reported in RTCP of finished streams	Device	Direction	Average of the delay values (in milliseconds) of all streams that ended in a given second. The delay for each stream is calculated or taken from RTCP-XR (preferring the latter).
RTCP	Minimum MOScq values reported in RTCP of finished streams	Device	Direction	Lowest MOSCQ value from RTCP-XR VoIP Metrics Report Blocks of all streams that ended in a given second. Only streams which reported MOS are taken into account.
RTCP	Maximum MOScq values reported in RTCP of finished streams	Device	Direction	Highest MOSCQ value from RTCP-XR VoIP Metrics Report Blocks of all streams that ended in a given second. Only streams which reported MOS are taken into account.
RTCP	Average MOScq values reported in RTCP of finished streams	Device	Direction	Average of all MOSCQ values from RTCP-XR VoIP Metrics Report Blocks of all streams that ended in a given second. Only streams which reported MOS are taken into account.

Table 21-2 (Cont.) Device, Trunk and IP Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
RTCP Usage	Streams with RTCP	Device	Direction	Counter is increased for each RTP stream that ended and where at least one RTCP packet was seen (including RTCP-XR).
RTCP Usage	Streams with RTCP-XR Block Type 1 (Loss RLE Report Block)	Device	Direction	Counter is increased for each RTP stream that ended and where at least one RTCP-XR packet was seen.
RTCP Usage	Streams with RTCP-XR Block Type 2 (Duplicate RLE Report Block)	Device	Direction	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
RTCP Usage	Streams with RTCP-XR Block Type 3 (Packet Receipt Times Report Block)	Device	Direction	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
RTCP Usage	Streams with RTCP-XR Block Type 4 (Receiver Reference Times Report Block)	Device	Direction	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
RTCP Usage	Streams with RTCP-XR Block Type 5 (DLRR Report Block)	Device	Direction	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
RTCP Usage	Streams with RTCP-XR Block Type 6 (Statistics Summary Report Block)	Device	Direction	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
RTCP Usage	Streams with RTCP-XR Block Type 7 (Statistics Summary Report Block)	Device	Direction	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
RTCP Usage	Streams with RTCP-XR Block Type 8 (BT's Extended Network Quality Report Block)	Device	Direction	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
RTCP Usage	Streams with RTCP-XR Block Type 9 (Texas Instrument Extended VoIP Quality Report Block)	Device	Direction	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.

Table 21-2 (Cont.) Device, Trunk and IP Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
RTCP Usage	Streams with RTCP-XR Block Type 10 (Port-repair Loss RLE Report Block)	Device	Direction	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
RTCP Usage	Streams with RTCP-XR Block Type 11 (Multicast Acquisition Report Block)	Device	Direction	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
RTCP Usage	Streams with RTCP-XR Block Type 12 (IDMS Report Block)	Device	Direction	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
RTCP Usage	Streams with RTCP-XR Block Type 13 (ECN Summary Report Block)	Device	Direction	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
RTCP Usage	Streams with RTCP-XR Block Type 14 (Measurement Information Report Block)	Device	Direction	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
RTCP Usage	Streams with RTCP-XR Block Type 15 (Packet Delay Variation Metrics Block)	Device	Direction	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
RTCP Usage	Streams with RTCP-XR Block Type 16 (Delay Metrics Block)	Device	Direction	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
RTCP Usage	Streams with RTCP-XR Block Type 17 (Burst/Gap Loss Summary Statistics Block)	Device	Direction	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
RTCP Usage	Streams with RTCP-XR Block Type 18 (Burst/Gap Discard Summary Statistics Block)	Device	Direction	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
RTCP Usage	Streams with RTCP-XR Block Type 19 (Frame Impairment Summary Statistics Block)	Device	Direction	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.

Table 21-2 (Cont.) Device, Trunk and IP Tag KPIs

Path	KPI Metric	Applicable	Parameter	Description
RTCP Usage	Streams with RTCP-XR Block Type 20 (Burst/Gap Loss Metrics Block)	Device	Direction	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
RTCP Usage	Streams with RTCP-XR Block Type 21 (Burst/Gap Discard Metrics Block)	Device	Direction	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
RTCP Usage	Streams with RTCP-XR Block Type 22 (MPEG2 Transport Stream PSI-Independent Decodability Statistics Metrics Block)	Device	Direction	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
RTCP Usage	Streams with RTCP-XR Block Type 23 (De-jitter Buffer Metrics Block)	Device	Direction	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
RTCP Usage	Streams with RTCP-XR Block Type 24 (Discard Count Metrics Block)	Device	Direction	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
RTCP Usage	Streams with RTCP-XR Block Type in range 25-254	Device	Direction	Counter is increased for each RTP stream that ended and where at least one RTCP-XR block of the given type was seen.
RTCP Usage	Streams with RTCP-XR Block Type 255	Device	Direction	Counter is increased for each RTP stream that ends and where at least one RTCP-XR block of the given type was seen.

A

Supported Codecs

The KPI for a negotiated codec is incremented ONLY if the corresponding negotiated codec is present.

The following tables provide the list of:

- [Table A-1](#)
- [Table A-2](#)
- [Figure A-1](#)

Supported codecs and their values, Negotiated codecs and the codec KPI incremented.

If the codec string does not match this list, then the KPI is not incremented. The codec name is however reflected in the **negotiated_codecs** column.

For example: For G726, there are variants such as:

- G726-40
- G726-32
- G726-24
- G726-16

But, if we receive the codecs like AAL2-G726-16, then it does not match with the G726 string "G726-16" and hence KPI is not incremented.

If you have created an 'UNKNOWN_CODEC' KPI, then this KPI is incremented if the codec does not match any of the below listed codec names.

Table A-1 Supported Codecs and their Values

Supported Codec	Value
PCMA	0
PCMU	1
G726_40	2
G726_32	3
G726_24	4
G726_16	5
G729/G.729	6
G729A/G.729A	7
G729B/G.729B	8
G729AB/G.729AB	9
G723/G.723	10
G7231/G.723.1	11
G7231-H/G.723.1-H	12
G7231A-H/G.723.1A-H	13
G7231-L/G.723.1-L	14

Table A-1 (Cont.) Supported Codecs and their Values

Supported Codec	Value
G7231A-L/G.723.1A-L	15
G729E/G.729E	16
G728/G.728	17
iLBC	18
GSM-FR	19
AMR/AMR-NB	20
AMR-WB	21
clear-channel	22
T.38	23
G722/G.722	24
OPUS	25
SILK	26
EVS	27
EVRC	28
EVRCB/EVRCB0/EVRCB1	29
EVRCC/EVRCC0/EVRCC1	30
EVRCD/EVRCD0/EVRCD1	31
EVRCE/EVRCE0/EVRCE1	32
UNKNOWN-CODEC	33

Matrix of Negotiated Codecs and Codec KPIs Incremented**Table A-2 Negotiated Codecs and the Respective Codec KPI Incremented**

Negotiated Codecs in Call	Negotiated Codec KPIs Incremented
PCMA, PCMA, PCMA	PCMA KPI
PCMA/G729, PCMA, PCMA	G729 and PCMA KPIs
PCMA/G729/PCMA, PCMA, PCMA	PCMA KPI
PCMA/G729/PCMA/AMR telephone-event, PCMA, PCMA	AMR and PCMA KPIs
G722/EVS/PCMA , iLBC/GSM/G729	PCMA and G729 KPIs
AMR telephone-event/PCMA telephone-event, iLBC/GSM	PCMA and GSM KPIs
G722 tone/EVS, iLBC/GSM tone	EVS and GSM KPIs

Negotiated Codecs and Data in the Respective Columns of the Calls Page

This table provides examples of how negotiated codecs and transcoded calls are identified and listed. The information provided here serves as a reference guide on how to read the **Negotiated codecs** column in the Calls table to determine the codec negotiation across multiple call legs. The **Negotiated codecs** column shows the negotiated codecs per RTP leg of a call and is separated by comma (.). If the codec renegotiation happens during the call, renegotiated codecs are displayed in the **Negotiated Codecs** column separated by a (/) forward slash.

Figure A-1 Negotiated Codecs and Data in the Respective Columns of the Calls Page

No.	Negotiated Codecs in Call	Negotiated codecs	Transcoded Call
1	A SBC1 SBC2 B <-----PCMA-----><-----PCMA-----><-----PCMA----->	PCMA, PCMA, PCMA	No
2	A SBC1 SBC2 B <-----PCMA-----><-----PCMA-----><-----PCMA-----> <-----G729-----><-----PCMA-----><-----PCMA----->	PCMA/G729, PCMA, PCMA	Yes
3	A SBC1 SBC2 B <-----PCMA-----><-----PCMA-----><-----PCMA-----> <-----G729-----><-----PCMA-----><-----PCMA-----> <-----PCMA-----><-----PCMA-----><-----PCMA----->	PCMA/G729/PCMA, PCMA, PCMA	Yes
4	A SBC1 SBC2 B <-----PCMA-----><-----PCMA-----><-----PCMA-----> <-----G729-----><-----PCMA-----><-----PCMA-----> <-----PCMA-----><-----PCMA-----><-----PCMA-----> <--AMR telephone-event--><-----PCMA-----><-----PCMA----->	PCMA/G729/PCMA/AMR telephone-event, PCMA, PCMA	Yes
5	A SBC B <-----G722-----><-----iLBC-----> <-----EVS-----><-----GSM-----> <-----PCM-----><-----G729----->	G722/EVS/PCMA, iLBC/GSM/G729	Yes
6	A SBC B <-----AMR telephone-event-----><-----iLBC-----> <-----PCMA telephone-event-----><-----GSM----->	AMR telephone- event/PCMA telephone- event, iLBC/GSM	Yes
7	A SBC B <-----G722 tone-----><-----iLBC-----> <-----EVS-----><-----GSM tone----->	G722 tone/EVS, iLBC/GSM tone	Yes