Oracle® Communications Session Monitor

Release Notes

Release 4.3

F27700-01

March 2020

Oracle Communications Session Monitor Release Notes, Release 4.3

F27700-01

Contents

About This Guide

This document presents information about the Oracle Communications Session Monitor product family. The Session Monitor platform supports the following products:

- Oracle Communications Operations Monitor
- Oracle Enterprise Operations Monitor
- Oracle Communications Control Plane Monitor
- Oracle Communications Fraud Monitor
- Oracle Enterprise Telephony Fraud Monitor

Documentation Set

Document Name	Document Description
Developer Guide	Contains information for using the Session Monitor SAU Extension.
Fraud Monitor User Guide	Contains information for installing and configuring Fraud Monitor to monitor calls and detect fraud.
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 4.3 release, 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
March 2020	• Added OCSM 4.3 enhancements, features, Known Issues, and Resolved Issues.

1 Introduction

The Oracle Communications Session Monitor *Release Notes* provide information about new features, enhancements, and changed functionality in release 4.3

Session Monitor Supported Hardware

The products within the Oracle Communications Session Monitor suite are supported on Oracle, Sun, and HP systems.

Table 1-1 Supported Hardware for Oracle systems

Component	Requirement
Server	The following severs are supported: • Oracle Server X8-2 • Oracle Server X7-2 • Oracle Server X6-2 • Oracle Server X6-2L • Oracle Server X5-2 • Oracle Server X5-2L
Network Adapter	The following adapters are supported: • Oracle Quad Port 10GBase-T Adapter

> **Note:**
>
> The Oracle X7-2 and Oracle X8-2 server supports Session Monitor Installation using RPM installer only.

The following table lists the hardware supported for Oracle systems.

Table 1-2 Supported Hardware for Oracle Sun systems

Component	Requirement
Server	The following severs are supported: • Oracle Sun Server X4-2 • Oracle Sun Server X4-2L • Oracle Sun Server X3-2 • Oracle Sun Server X2-4
Network Adapter	The following network adapters are supported: • Sun Dual Port 10 GbE PCle 2.0 Networking Card with Intel 82599 10 GbE Controller • Sun Quad Port GbE PCIe 2.0 Low Profile Adapter, UTP • Sun Dual Port GbE PCIe 2.0 Low Profile Adapter, MMF

The following table lists the hardware supported for HP systems.

Table 1-3 Supported Hardware for HP Systems

Component	Requirement
Server	The following servers are supported: • HP DL580 G9 • HP DL380 G9 • HP DL380p G8 • HP DL580 G7
Network Adapter	The following network adapter s are supported: • HP NC365T PCIe Quad Port Gigabit Server Adapter • HP NC364T PCIe Quad Port Gigabit Server Adapter • HP Ethernet 1Gb 4-port 366FLR Adapter
Driver/Chipsets	The following drivers/chipsets are supported: • e1000 (82540, 82545, 82546) • e1000e (82571, 82574, 82583, ICH8..ICH10, PCH..PCH2) • igb (82575, 82576, 82580, I210, I211, I350, I354, DH89xx) • ixgbe (82598, 82599, X540, X550) • enic • i40e • Mellanox (mlx4, mlx5)

Hardware Requirements for Production Systems

For production systems, Oracle recommends completing a sizing exercise with Oracle Customer Support. Higher performance hardware may be required, for example, in cases with:

- High levels of monitored traffic
- High numbers of concurrent users
- High volumes of historical information

On the Mediation Engine machines, Oracle recommends using a RAID-10 array for the operating system and the database. A separate RAID-5 array is recommended for storing long-term data.

Hardware Requirements for Demonstration Systems

For development or demonstrations systems with little network traffic, the following table lists the minimum requirements to install any of the Session Monitor machine types.

Table 1-4 Hardware Requirements for Demonstration Systems

Component	Minimum Requirement
Processor	2.6 GHz Intel Xeon processor, 64-bit with 8 processing threads
Memory	8 GB RAM
Disk Space	80 GB storage on a hardware RAID controller

Table 1-4 (Cont.) Hardware Requirements for Demonstration Systems

Ports	2 Ethernet ports

Session Monitor Virtualization Support

This section describes the software and hardware requirements for Session Monitor virtualization.

Hypervisor Support

The following hypervisors are supported:

- Oracle VM version 3.4
- VMware vSphere ESXi 5.x/6.x
- Kernel-based Virtual Machine (KVM)

Virtual Machine Requirements

The following table lists the minimum requirements for the virtual machines.

Table 1-5 Hardware Requirements for Virtual Machines

Component	Requirement
Processor	8 vCPUs
Memory	8GB RAM
Disk Space	80GB
NIC Card	1Gbps vNIC

In virtualized Mediation Engines, 50,000 concurrent calls (1 SIP leg per call) have been tested successfully.

Host Machine Requirements

The physical machine that hosts the virtual machines should contain at a minimum the hardware resources that are required to host all the virtual machines, in addition to the hardware that is required for the hypervisor.

Session Monitor Operating System Requirements

Oracle Communications Sessions Monitor (OCSM) is offered as a set of Linux applications. The latest version of OCSM 4.3 is tested, benchmarked and certified on Oracle Linux platform. Oracle Linux is binary compatible with RHEL kernel, and OCSM has been tested with RedHat Compatible Kernel. Customers who want to use OCSM with RHEL are encouraged to load and test OCSM on the version of Linux on which they are planning to deploy. In this case, performance and capacity characteristics may vary from those tested while running OCSM on Oracle Linux. When OCSM is deployed on RHEL, Oracle will continue to support OCSM, and in case of issues that Oracle Support determines to be related to RHEL, the customer will be directed to work with RedHat support organization for issue resolution.

The following table lists the supported operating systems for running Session Monitor.

Table 1-6 Supported Operating Systems

Product	Version	Notes
Oracle Linux 7 x86-64 (64 bit)	Version 7 to Version 7.7 (with Oracle UE Kernel for Linux)	By default Oracle Linux installs Kernel 3. Oracle recommends that the latest Unbreakable Enterprise (UE) Kernel 4 for Linux is installed.
Red Hat Enterprise Linux 7	Version 7	See clarification above.

> **Note:**
>
> - You must configure a network device when installing Oracle Linux 7.
> - If required, update the DPDK drivers.

Session Monitor Connectivity

Following are Session Monitor connectivity details:

- One AE (OCOM's MEC feature): Supports up to 64 MEs
- One ME (OCOM, OCCPM): Supports up to
  - Native-Only Probes:
    - Media+Sig ; Signalling-Only: 128
    - Packet Inspector: 16
  - Embedded-Only Probes (SBC as a probe):
    - < 500 parallel calls per SBC: 1k (might require some manual tweaking, unlimit open files)
    - >= 500 parallel calls per SBC: 128
- Mixture of SBC and native probes: 128 (individual limits still apply)
- One Probe (OCOM, OCCPM) or SBC-probe can be connected to up to:
  - Probe: 2 MEs
  - SBC: 8 MEs
- One ME (OCOM, OCCPM): Connected to up to 1 AE

Session Monitor Software Requirements

The table lists the supported client browsers:

Table 1-7 Supported Client Browsers

Browser	Version
Microsoft Internet Explorer	8 or higher
Mozilla Firefox	1.5 or higher (on any operating system)

Table 1-7 (Cont.) Supported Client Browsers

Apple Safari	Any version, including Safari for iPad
Google Chrome	Any version
Opera	9 or higher (on any operating system)

Compatibility Matrix for Session Monitor

The following products can be configured with Session Monitor:

Product Name	Version
DPDK	19.08
ISR	6.3
SP-SBC	S-Cz8.3.0 Works with Operations Monitor and Enterprise Operations Monitor
E-SBC	S-Cz8.3.0 Works with Operations Monitor and Enterprise Operations Monitor

Compatibility Matrix for Fraud Monitor

The following products can be configured with Fraud Monitor:

Product Name	Version
DPDK	19.08
ISR	6.3
SP-SBC	SCZ 8.3.0 Works with Fraud Monitor and Enterprise Telephony Fraud Monitor
E-SBC	SCZ 8.3.0 Works with Fraud Monitor and Enterprise Telephony Fraud Monitor
SDM	8.2.1

Session Border Controller Supported Versions

The table lists supported Session Border Controller (SBC) versions.

Table 1-8 Supported Session Border Controller Versions

Product	Versions

Table 1-8 (Cont.) Supported Session Border Controller Versions

Enterprise Session Border Controller (E-SBC)	• SCZ830 • SCZ820 • ECZ800 • ECZ750 • ECZ740 • ECZ730
Session Border Controller (SBC)	• SCZ830 • SCZ820 • SCZ800 • SCZ750 • SCZ740 • SCZ730

Database Support

The following databases run in concert with Oracle Communications Session Monitor.

MySQL Enterprise Edition

This release is compatible with the following versions of MySQL Enterprise Edition:

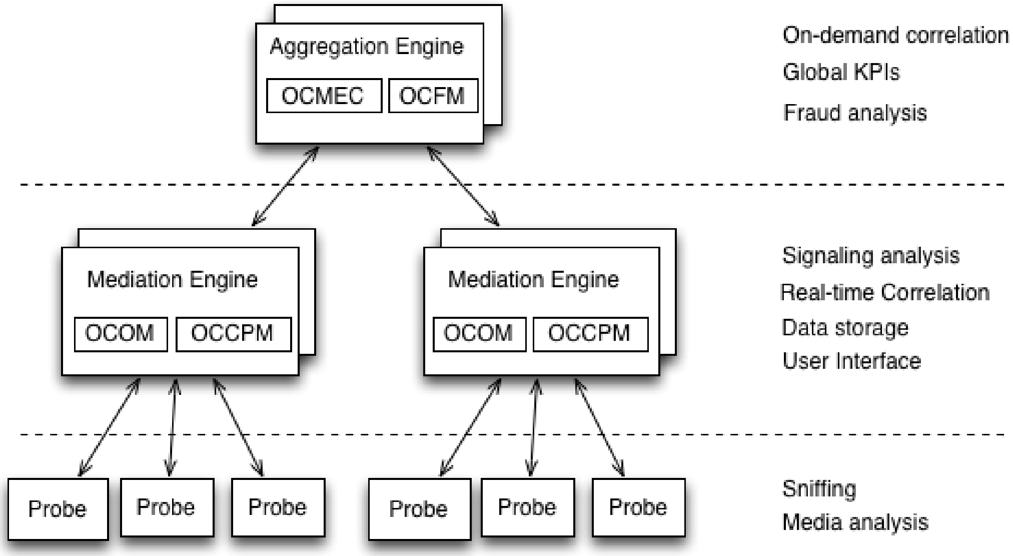
- 5.5.54
- 5.7.10
- 5.7.24

Session Monitor System Architecture

The Session Monitor system works by capturing the traffic from your network, correlating it in real-time, and storing it in indexed formats so that they are available for the various reports offered by the web interface.

The Session Monitor system architecture has three layers:

- **Probe layer:** This layer is responsible for capturing the traffic from your network and performing the Media Quality analysis. The probes send meta-data for each of the signaling messages to the Mediation Engine layer and analyze the RTP streams locally, sending the results of this analysis to the Mediation Engine layer.
- **Mediation Engine (ME) layer:** This layer is responsible for understanding in real-time the traffic received, correlating it and storing it for future reference. This layer is also responsible for measuring, managing, and storing the KPIs. In the common case, there is one ME per geographical site. It is possible, however, to have the probes from multiple geographical sites sending the traffic to a single ME. It is also possible to have multiple ME installations in the same geographical site.
- **Aggregation Engine (AE) layer:** This layer is responsible for aggregating the global KPIs from all the MEs linked to it, and for the global search features. In a typical setup, there is only one AE for the whole network.



Each of the three layers supports high-availability by deploying two identical servers in active-passive or active-active modes of operation. For small setups, it is possible to run the probe layer and the ME layer on the same physical hardware. The AE layer always requires its own hardware.

From the Session Monitor products perspective, the Operations Monitor and the Control Plane Monitor (CPM) run on the Mediation Engine (ME) while the Mediation Engine Connector (MEC) and the Fraud Monitor products run on the Aggregation Engine (AE).

Upgrade Information

DPDK upgrade is required. Release 4.3 supports DPDK version 19.08. After upgrading to 4.3, see the *Session Monitor Installation Guide* for information on upgrading DPDK.

Licensing Changes

Two licenses are available for Enterprise Operations Monitor :

- L107092 Enterprise Operations Monitor with Fraud Protection
- L107093 Enterprise Operations Monitor, Basic Edition

These changes affect the Enterprise product portfolio only.

The Enterprise Operations Monitor base capacity license (L98611) and the Fraud Monitor license (L106475) are not available for new purchases starting November 5 2019. Please refer to the Enterprise Operations Monitor licensing document for details on license descriptions/restrictions/dependencies for the new licenses.

Documentation Changes

The following information lists and describes the changes made to the Oracle Communications Session Monitor documentation set for release 4.3.

ePub and Mobi

The documentation no longer supports ePub and Mobi formats.

2 New Features

Session Monitor release 4.3 includes the following new features, enhancements, and changed functionality:

Skype For Business Enhancements

- **Visibility of Skype for Business Registration Events**
  For Skype for Business (SfB) Registration Events, Operations Manager processes both events - Register Request and 200 OK Response to display SfB registration events in the Operations Manager Registrations grid in the GUI.

  To support the display of an SfB registration event, the source IP address of the 200 OK Response message is updated with SfB server IP address and Destination IP address of the 200 OK Response message is updated with SfB Endpoint IP address, and this is sent to Operations Manager. Operations Manager processes both and displays the details in the **Registrations Details** window.

  Registration events of only those SfB users who sign in or sign out from the SfB Server after the upgrade are displayed in Registrations grid. SfB Registration events that existed before the upgrade are not displayed in the GUI.
- **Display of Media Statistics for a Skype for Business Call**
  The Media Summary tab for a SfB call displays the Media Type and the Codecs statistics in addition to other statistics. The Media Type and Codecs statistics are visible only for calls made after the upgrade to 4.3. Existing calls will not display this information in the Media Summary tab.
- **Visibility of Inbound and Outbound Legs of an SfB Call**
  Operations Monitor supports the visibility of both inbound and outbound legs of SfB calls.

  The SfB server needs to be configured as a platform device for the SfB calls to be correlated. Existing calls displayed in the Calls page before the upgrade will not be correlated.

Fraud Monitor Enhancements

- **Visibility into Dynamic Learning**
  Fraud Monitor users can view information on user call data that is captured over a period of time and how this information can be used to detect fraud scenarios. The Learning Period tab which is visible only to the Administrator, displays user information of the following metric type rules:
  - Destination-based traffic spikes
  - Destination-based call volume
  - Source-based traffic spikes
  - Source-based call volume

  The user listing shows a list of users and the rule type. Clicking on a user in the user listing shows the Learning Period graph. The data is shown for a period of last 7 days.

- **Automatic Deletion of Expired Subscriber Entries**
  All entries in the Blacklist, Whitelist, Ratelimit, and Redirect subscriber lists have an expiry time. The default expiry time is 48 hours from the time the subscriber is listed in the list. You can set the value for the expiry time in the range of 48-1440 hours.

  If Automatic Expiry Delete in System Settings is enabled, then 24 hours after the expiry, the entries are deleted. A warning or notification is sent at 03:23 every day in the form of either email or SNMP traps as configured.

  You can review the expired entries and choose to either delete the entries or extend the expiry time. For entries that existed before the upgrade to 4.3, you can use the Apply Automatic Expiry for Existing Entries option as a one time action.

- **New Source-Based Rules**
  Source Based traffic monitoring is a key enhancement to the fraud detection capabilities of Fraud Monitor. The Source-based Traffic Spikes and the Source-based Call Volume rules help in monitoring source based traffic. Traffic spike can be measured based on call duration. Call volume can be measured in number of calls per second and maximum active calls.

  As with Destination-based traffic rules, you can define Dynamic and Static methods of points accumulation. Fraud Monitor raises an incident when a source user generates an unusually high traffic. If the threshold is crossed, then source user accumulate points. These rules can be used to identify possible candidates for blacklisting source numbers.

Security Enhancements

- **Kill Specific UI Session**
  A privileged Linux user with root access can use the `Palladion logout <username>`command from the Mediation Engine Console to logout specific users, thereby killing the UI session.

- **User Administrator Role**
  The User Administrator role is a new role in the Mediation Engine which can be used to create a user meant to perform only user management task. The User Administrator user is created by Admin user, and there can be only one User Administrator user. The User Administrator user cannot perform any other tasks in the GUI.

3 Interface Changes

The following topic summarizes changes for release 4.3. The additions, removals, and changes noted in these topics occurred since the previous release of Oracle Communications Session Monitor.

The interface changes in 4.3 are:

Change	Description
Learning Period page	Added Learning Period page in the home page of Fraud Monitor.
Automatic Expiry Delete	Added the option to Fraud Monitor under Admin, System Settings to enable automatic deletion of expired entries in lists such as Blacklist, Whitelist, Redirect, and Ratelimit.
Apply Automatic Expiry for Existing Entries	Added the option to Fraud Monitor under Admin, System Settings to enable automatic deletion of expired entries for existing entries. This is a one time activity performed by the administrator.
Expiry Timer Value	Added the option to Fraud Monitor to set the expiry time for subscriber entries. The default value for the expiry timer configuration is 48 hours and it can be configured in a range of 48-1440 hours. This option is available in the configuration screen of all lists.
Review Expired	Added to Fraud Monitor to review the expired entries in the lists and as a follow up, administrator can delete the expired entries manually or extend the expiry time.
Extend Expiry Time	Added to Fraud Monitor to extend the expiry time of expired entries in the lists.
Receive Updates / Do Not Receive Updates	Added the option to Fraud Monitor under Settings, Notifications to enable notifications to be sent to the user about the expiry of list entries. Notifications are sent as email or SNMP traps if they have been configured.
Source-based Traffic Spike	New rule added in Fraud Monitor to detect source-based traffic spikes.
Source-based Call Volume	New rule added in Fraud Monitor to detect source-based call volume.
Call Volume	Call Volume rule has been renamed as Destination-based call volume.
User Administrator role	A new role has been added in the Mediation Engine to perform User Management tasks only.

4
Known Issues

The following table lists the known issues in version 4.3 of Oracle Communications Session Monitor.

ID	Description	Severity	Found In
30920564	Meditation Engine or Fraud Monitor installation shows error on the PSA GUI while installing on X8-2 server.	3	*4.3.0.0.0-103*. Workaround: Refresh the PSA GUI. After the refresh, the correct status of installation is shown.

Resolved Known Issues

The following table provides a list of previous known issues that are now resolved in 4.3 GA.

ID	Description
27862634	HTTP APP GET request failing with nginx 301 Moved Permanently response.
30089603	Fraud Monitor 4.1 reports less number of incidents as compared to 3.3.
29881497	Upgrade from 4.0.0.3.0 to 4.1.0.4.0 takes a very long time to upgrade.
30163935	The user role View Media Info cannot be assigned.
30173584	VSI shows dropped packets and is causing Red Bars. Need to understand why VSI is overloaded and dropping packets
30245588	In Operations Manager 4.2, non-preferred numbers are not greyed out, although the corresponding system setting is set to TRUE.
29395243	Some calls are missing in OCOM from the **Calls** section.
30233801	In OCSM 4.2, REST API does not work with TLSv1.
30161712	In OCSM 4.2, there is a delay of up to 1 hour between the alarm and the call
30051871	Secure LDAP (LDAPS) Support needs to be configured.
30385707	Broadsoft reported that Mediation Engine is down after upgrading from 4.1 to 4.2.
30398761	The DPDK script `configure_dpdk.py` which is listed in the Installation Guide to be used, fails.
30360536	ISUP body not decoded. Operations Manager is not able to parse and display the ISUP body in some cases.
26046378	Operations Manager 3PCC Call Correlation Support for 2 Outbound calls.
23188252	RFE: Chat Anonymization enhancements.
30655385	Maximum concurrent sessions do not work with external authentication.
30517390	Header and content privacy setting fails to anonymize contents of the message if the subject is not present.
30646618	RTP headers cannot be downloaded after V4.2 upgrade.
30644297	4.1: Not able to get login page and setup page.
30765160	Red bars can be seen and correlation failures after upgrade to 4.2 Release.
30727470	Red bars are seen after upgrading to 4.2 P1 UDP traffic.

ID	Description
30779429	The reason the header information is missing in the Call Summary Page.
30526923	OCSM encountered segfault in 4.2.
30202303	Filtered calls are not exported.
30760460	Unencrypted ESP packets support on OCOM.
30561182	Empty call flow diagram for few calls.
30968880	Message Flow RTP stats defect.