Oracle® Communications Session Monitor

Release Notes

Release 5.0

F41621-06

September 2022

Oracle Communications Session Monitor Release Notes, Release 5.0

F41621-06

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

Documentation Set

Table 1   Documentation Suite for OCSM 5.0

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 5.0 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
October 2021	• Initial release.
December 2021	• Adds updates for supported versions of Session Border Controller.
July 2022	• Updates the Session Monitor Virtualization Support section. • Adds updates for the section - Supported versions of Session Border Controller. • Adds updates for the section - Database Support
August 2022	• Updates the compatibility matrix for Fraud Monitor. • Adds KI for local help files.

1 Introduction

The Oracle Communications Session Monitor *Release Notes* provide information about new features, enhancements, and changed functionality in release 5.0.

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

Hardware	Supported Configurations
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

Table 1-2 (Cont.) Supported Hardware for Oracle Sun systems

Component	Requirement
Network Adapter	The following network adapters are supported: • Sun Dual Port 10 GbE PCIe 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 detailed sizing and traffic profile analysis excercise, please contact your sales representative. 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
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 7.0 VM
- 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	8 GB RAM
Disk Space	80 GB
NIC Card	1 Gbps vNIC

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 Cloud Deployment

The following mimimum shapes supported are as follows. For more information, see the Session Monitor Installation Guide.

- OCI Cloud : VM Standard 2.8
- Azure: Standard F8s

Session Monitor Operating System Requirements

Oracle Communications Sessions Monitor (OCSM) is offered as a set of Linux applications. The latest version of OCSM 5.0 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 7.9 (with Oracle UE Kernel for Linux)	By default Oracle Linux installs Kernel 3. Oracle recommends that the latest Unbreakable Enterprise (UE) Kernel 4 or above 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	27.0.1 or higher (on any operating system)
Apple Safari	Version 13.0.3 or higher (15608.3.10.1.4)
Google Chrome	Any version
Opera	17.0.1241.45 or higher (on any operating system)
Microsoft Edge	Microsoft Edge 44.18362.449.0 or higher Microsoft EdgeHTML 18.18362 or higher

Note:

Recent versions of Microsoft Edge and Google Chrome browsers may require a refresh of the online help links. Firefox browser is the recommend browser to view the Online Help.

Compatibility Matrix for Session Monitor

The following products can be configured with Session Monitor:

Product Name	Version
DPDK	19.11
ISR	6.4

Product Name	Version
SP-SBC	S-Cz9.0.0 Works with Operations Monitor and Enterprise Operations Monitor
E-SBC	S-Cz9.0.0 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
SP-SBC	For more information, see Session Border Controller Supported Versions. Works with Fraud Monitor and Enterprise Telephony Fraud Monitor.
E-SBC	For more information, see Session Border Controller Supported Versions. Works with Fraud Monitor and Enterprise Telephony Fraud Monitor.
SDM	NNC82_3

Session Border Controller Supported Versions

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

Table 1-8 Supported Session Border Controller Versions

Product	Versions
Enterprise Session Border Controller (E-SBC)	• S-Cz9.0.0 • S-Cz8.4.0 • S-Cz8.3.0 • S-Cz8.2.0 • E-Cz8.1.0 • E-Cz8.0.0 • E-Cz7.5.0 • E-Cz7.4.0 • E-Cz7.3.0
Session Border Controller (SBC)	• S-Cz9.0.0 • S-Cz8.4.0 • S-Cz8.3.0 • S-Cz8.2.0 • S-Cz8.1.0 • S-Cz8.0.0 • S-Cz7.5.0 • S-Cz7.4.0 • S-Cz7.3.0

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:

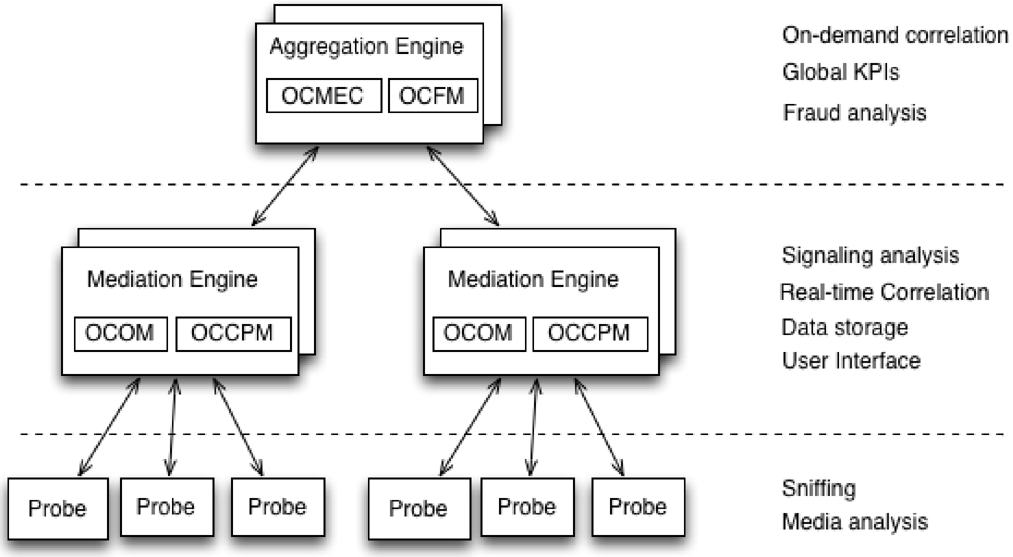
- 5.5.54
- 5.7.10
- 5.7.24
- 5.7.35
- 5.7.38

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

For upgrade related information, see the *Session Monitor Upgrade Guide*.

2
New Features

Session Monitor release 5.0 includes the following new features, enhancements, and changed functionality:

New and Improved User Experience Enabled by OJET

The user interface of OCSM 5.0 has been transformed to improve user experience using the OJET GUI Framework. The new user interface does not change the functionality, but only provides an interactive new look and feel.

> **Note:**
>
> The user interface for Mediation Engine Connector has not been changed to reflect OJET features.

Inclusive Terminology

Staying consistent with the Oracle-wide initiative to have a more inclusive and a culturally sensitive usage of terminologies across all software products, the OCSM 5.0 GUI, product documentation and marketing collaterals have been updated. We are moving away from the usage of terminologies such as 'Blacklist' and 'Whitelist'. You will now see the usage of inclusive terminology such as 'Blocklist' and 'Allowlist'.

Support for Monitoring Non-Call Events (Presence)

OCSM 5.0 supports monitoring of non-call events such as - Subscribe, Notify, and Publish. Non-call events form a critical part of network transactions and can impact the network performance. This feature enhances the level of information a user can access to identify and troubleshoot network issues. It also helps you debug issues related to non-call messages.

> **Note:**
>
> Monitoring of SIP MESSAGE and OPTIONS are not supported in this release.

A new page - **Subscriptions** has been added to OCSM 5.0. Using this page, you can monitor presence events for:

- Calls
- Alerts
- KPI definition
- User Tracking
- Devices
- IP Tracking

For more information, see the Subscriptions section in the Operations Monitor 5.0 User's Guide.

KPI Enhancements

This feature provides options to select only the required KPIs for a device or tag type, and to avoid the creation of unwanted and redundant KPIs by introducing templates. This enhancement provides an option to remove duplicate platform-wide KPIs created by multiple users with the Delete Common KPI option.

You can now choose to apply KPIs for a device or tag type using the Default KPI template or the Custom KPI Template. The admin user can now manage the unwanted KPI creation by assigning users with the four new permissions - KPI Management, Expand KPI, Shrink KPI, and View common KPI from other users. For more information, see the KPI Enhancements section in the Operations Monitor 5.0 User's Guide.

Support for Displaying Custom Logo on the User Interface

You can now select a custom logo file to be displayed on the application header using the **Custom logo for application header** option. You can upload and also customize the logo using different alignment positions.

Fraud Monitor Enhancements

- **Expiry Timer Enhancement**
  This features allows you to set the **Never Expire** option for the expiry timer that never expires for subscribers added to the Blocklist, Rate limit, Redirect, and Allowlist lists.
- **Rule Broken Enhancement**
  The **Rule Broken** column displays the name of the rule that was broken or violated for an incident in the Fraud Monitor Incidents page.
- **Comments on the Incident tab**
  This feature enables you to add, edit, search, and delete comments for incidents. This feature helps the Fraud detection team know if an action needs to taken over an incident by providing comments for a single or multiple incidents.

BICC Support

You can now distinguish between ISUP and BICC messages by the protocol name looking at the Ladder Diagram section. To enable the capture of BICC messages, enable SIP/ISUP from the Signaling Protocols page in PSA.

3
Known Issues

The following tables list known issues and resolved issues in Oracle Communications Session Monitor 5.0.

Known Issues

The following table provides a list of known issues in 5.0 GA.

ID	Severity	Description
34267143	4	No left-side index/search in local help files.

Resolved Issues

The following table lists resolved known issues in Oracle Communications Session Monitor 5.0.

ID	Fixed in Label	Severity	Description
33175267	5.0.0.0.0	2	Upgrade fails due to pre-install script logic.
32956182	5.0.0.0.0	2	No alert when multiple address under "SNMP trap target address(es)".
32866629	5.0.0.0.0	2	OCOM 4.3 || Issue with RTP recording.
32859478	5.0.0.0.0	2	Performance issue after upgrading to 4.4p1.
32449092	5.0.0.0.0	2	VSI Segfault '0000000000523fbd sp 00007f45cfe7cb20 error 4 in vsi'.
32245978	5.0.0.0.0	2	OCOM : OCOM ME - Probe shows connected but no data received.
32169611	5.0.0.0.0	2	Failing to send email using TLS
33405160	5.0.0.0.0	3	Incorrect login logging.
33357650	5.0.0.0.0	3	No SDP codecs printed in message flow when compact form header i.e. "c: application/sdp" is used in SDP.
33083042	5.0.0.0.0	3	CSV export not working if filter "start timestamp = ON(any day)" and "Edit Advanced".

ID	Fixed in Label	Severity	Description
33060650	5.0.0.0.0	3	CSV Export not exporting all calls for User Tracking but Bulk Export does.
32970304	5.0.0.0.0	3	4.4 Outdated 3rd party libraries
32970263	5.0.0.0.0	3	4.4 No security-relevant HTTP headers are present on the web service.
32896053	5.0.0.0.0	3	4.4 Cross-Site Scripting (XSS) payload turned into a Denial of Service (DoS) for the current user.
32856465	5.0.0.0.0	3	Correlation based on Replaces header in INVITE Missing.
32845718	5.0.0.0.0	3	Cross-Site Scripting (XSS) and Cross-Site-Request-Forgery attacks.
32841772	5.0.0.0.0	3	Information Disclosure: Software Versions.
32497799	5.0.0.0.0	3	User Agent (UA) field is sometimes not exported to CSV.
32447232	5.0.0.0.0	3	CSV Export shows call legs that are restricted under realm access.
32358991	5.0.0.0.0	3	Realm Access Broken for Platform Devices with IP address Range, not spefific IP
32241439	5.0.0.0.0	3	OCOM : Session Establishment Ratio - Incorrect Calculation.
32175998	5.0.0.0.0	3	MEC is showing coded message when there are UTF-8 Characters in sip message.
32040493	5.0.0.0.0	3	"Custom Name Tag" not there when creating/ editing user through MEC.
31939439	5.0.0.0.0	3	Fraud Monitor 'RightClick' options with 'Advanced Filter' does not work .
31897570	5.0.0.0.0	3	Insecure PATH settings in /opt/oracle/ocsm/ ocsm_env.sh

ID	Fixed in Label	Severity	Description
31747908	5.0.0.0.0	3	Score and Metric graphs are not showing points calculation.
31357761	5.0.0.0.0	3	RTP Streams not visible - VQ analysis missing.
31309802	5.0.0.0.0	3	MEC Active Calls Count Issue.
30202303	5.0.0.0.0	3	Filtered calls are not exported.