Oracle® Communications Session Monitor

Release Notes

Release 5.1

F76352-03

August 2023

Oracle Communications Session Monitor Release Notes, Release 5.1

F76352-03

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 5.1

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.
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 5.1 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
April 2023	• Initial release.
July 2023	• Includes updates for P1 Release.
August 2023	• Includes updates for the supported versions of Google Chrome.

1 Introduction

The Oracle Communications Session Monitor *Release Notes* provide information about new features, enhancements, and changed functionality in release 5.1.

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 X9-2 • 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:**
>
> Session Monitor Release 5.1 supports installation using the 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
- AWS : c4.4xlarge

Session Monitor Operating System Requirements

Oracle Communications Sessions Monitor (OCSM) is offered as a set of Linux applications. The latest version of OCSM 5.1 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 8 x86-64 (64 bit)	Version 8.7 (with Oracle UE Kernel for Linux)	By default Oracle Linux installs Kernel 5. Oracle recommends that the latest Unbreakable Enterprise (UE) Kernel 5 is installed.
Red Hat Enterprise Linux 8	Version 8	See clarification above.

Note:

- You must configure a network device when installing Oracle Linux 8.
- 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
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	Supported versions: • 114.0.5735.199 or • 114.0.5735.201
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

Compatibility Matrix for Session Monitor

The following products can be configured with Session Monitor:

Product Name	Version
DPDK	21.11.2
ISR	6.4
SP-SBC	S-Cz9.2.0 Works with Operations Monitor and Enterprise Operations Monitor
E-SBC	S-Cz9.2.0 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	NNC90_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
Enterprise Session Border Controller (E-SBC)	• S-Cz9.2.0 • S-Cz9.1.0 • 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-Cz9.2.0 • S-Cz9.1.0 • 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 are supported by Oracle Communications Session Monitor.

MySQL Enterprise Edition

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

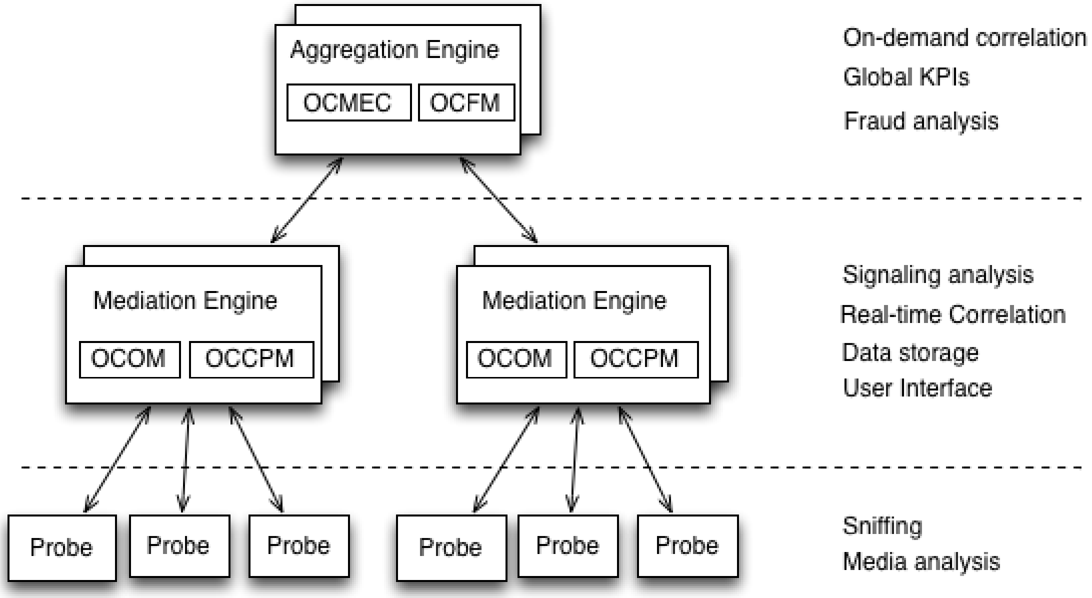
- MySQL 8.0.32

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 Release 5.1 Upgrade Guide*.

2 New Features

Session Monitor release 5.1 includes the following new features, enhancements, and changed functionality:

OJET Framework for the Mediation Engine Connector (MEC)

The Mediation Engine Connectpor (MEC) user interface has been transformed to improve user experience using the OJET framework. The new user interface does not change the functionality, but only provides an interactive new look and feel

CDR Support For ISUP and BICC Fields

OCSM Release 5.1 supports the following ISUP and BICC parameters in the CDR:

- Originating Point Codes (OPC)
- Destination Point Codes (DPC)
- Circuit Identification Code (CIC)
- NOA (Nature of address indicator) of calling party
- NOA (Nature of address indicator) of called party

End Timestamp Support in CDR

OCSM adds the End timestamp information from Calls to the CDR. In the CDR file, this value is written in UNIX Timestamp.

Graphing Library Revamp – GUI Enhancement for Charts

In OCSM Release 5.1, if you mouse-over on any graphs in a chart component the relevant KPI values are displayed, just like a Tooltip with information such as KPI name, Date, and Value.

Linking Email And Alert Notification To Trace And File Name

With this feature, the Trace file is linked to the Alert that caused the Trace to be created. This feature helps to link the Trace URL in the email notification along with Trace filename. A Search box added to the Traces table header in the GUI, makes the process of searching for the Trace file simpler.

Support for OCSM Deployment in AWS Cloud

In addition to the existing public cloud platforms OCI, and Azure, you can create, deploy and run OCSM on the AWS. For more details on the AWS support, see the Session Monitor Release 5.1 Installation Guide.

Support of X9-2 Hardware

OCSM Release 5.1 supports deployment on Oracle Server X9-2. OCSM Release 5.1 has been tested and benchmarked agianst the exisiting traffic benchmarks. The X9-2 hardware support adds to the support for all the existing hardware such as X7-2 and X8-2.

Backup and Restore

OCSM 5.1 provides enables you to Backup the Configuration, Database, Block Storage and other essential OCSM files of the OCSM Server by providing a Backup and Restore procedure. During the upgrade to Release 5.1 from an earlier Release, the Backup and Restore procedure can be used to take a Backup of your OCSM data and restore it if the upgrade does not complete successfully.

TLS v1.3 Support

The latest version of the TLS protocol is TLS 1.3, and is supported by OCSM Release 5.1.

Support for the Latest Tech Stack Components

OCSM Release 5.1 supports and must be run on the latest version of tech stack which include:

- Oracle Linux 8
- MySQL 8
- Python 3.9

> **Note:**
>
> The Tech stack compoments such as Orace Linux 7.X, Python 2.7.X, MySQL 5.X.X are no longer supported from Release 5.1.

> **Note:**
>
> OCSM Release 5.1 has been tested on the latest versions of Oracle Linux 8 (such as 8.5, 8.6, 8.7) and MySQL 8 (8.0.32) and Python 3.9.13.

3 Resolved Issues

The following table lists resolved issues in Oracle Communications Session Monitor 5.1.

ID	Fixed in Label	Severity	Description
30695091	5.1.0.0.0	2	OCOM ME: pld-diamond.service segfaults and crashes.
33408510	5.1.0.0.0	3	PRACK in the first leg is not correlated.
33364305	5.1.0.0.0	3	The Prefix Group column displays only one Tag for Realms assigned two Prefix Tags.
33124954	5.1.0.0.0	3	OCSM call information does not show the messages.
33296287	5.1.0.0.0	3	Getting Unknown Application Id (16777216) in message flow for Diameter.
33536824	5.1.0.0.0	2	Null IP and port information to OCOM in RTP QoS IPFIX meta.
33641362	5.1.0.0.0	3	The Message flow window does not display codecs in 200 OK.
33570155	5.1.0.0.0	3	UI problem after OCOM 5.0.0.0 upgrade.
33651145	5.1.0.0.0	3	Web Interface Message Flow not "saving" selected view properties.
33681051	5.1.0.0.0	3	pld-vsi.service crashed when "Non Calls Extension" is activated.
33578399	5.1.0.0.0	2	Frequent crash after upgrading to 5.0.
33694412	5.1.0.0.0	3	Unable to edit Trunk Devices imported using SBC Config Upload.
33302521	5.1.0.0.0	2	INTER-ME call Correlation Failure.
33739959	5.1.0.0.0	3	Changing password fails after upgrading to 5.0.0.0 (OCOM).
33739448	5.1.0.0.0	3	Web GUI issues after upgrading to 5.0.
33835207	5.1.0.0.0	3	5.0 || Source and Destination point codes not visible under messages tab of Call Info.

ID	Fixed in Label	Severity	Description
33732497	5.1.0.0.0	3	SSRD and FSRD not shown under IETF metrics for Some Trunk Devices.
33739595	5.1.0.0.0	3	KPI calculation incorrect for ISUP devices.
33071906	5.1.0.0.0	3	OCOM ME - Sip Rel. Code 408 mapped incorrectly for Hairpin calls.
33904576	5.1.0.0.0	3	Feature change of alert definition configuration in 5.0.
33952583	5.1.0.0.0	1	GUI Interface slow - Reboot corrected.
33931074	5.1.0.0.0	2	SSR not considering 5xx response codes.
34122579	5.1.0.0.0	3	5.0 || "multiple Select" of the call legs In Call Transfer tab not working.
33881619	5.1.0.0.0	2	OCSM 5.0.0.1 slow performance web interface.
33836006	5.1.0.0.0	2	Performance/slowness issues after upgrade to 5.0.1
33634543	5.1.0.0.0	3	OCSM ME | Alert with the incorrect timestamp.
33871674	5.1.0.0.0	3	OCSM 5.0.0.1.0-428 Score and Metric graphs are not showing points calculation.
33823882	5.1.0.0.0	3	External authentication issue in 5.0.
34114817	5.1.0.0.0	2	VSI crash and KPI line stays flat.
34219173	5.1.0.0.0	3	Several bugs in OCOM 5.0.0.2.0 (continue of Bug 33570155).
33830399	5.1.0.0.0	2	Frequent crash after upgrading to 5.0 p1.
34200734	5.1.0.0.0	2	Messages for the hidden call leg appears under the Messages tab.
34224589	5.1.0.0.0	2	Drop in the graphs along with red bars.
34315106	5.1.0.0.0	4	Value of Maximum number of calls exported with bulk export not abided by.
34376549	5.1.0.0.0	2	Deviation Factor: Only integer values are accepted.
34379889	5.1.0.0.0	3	Several bugs in OCOM 5.0.0.x.0 (continue of Bug 34219173).
34336766	5.1.0.0.0	2	Advanced filter search issues.
34429792	5.1.0.0.0	2	REST API fails with multiple metrics.

ID	Fixed in Label	Severity	Description
33817254	5.1.0.0.0	3	OCOM is not always showing all call segments of a call.
34373158	5.1.0.0.0	3	disable TLS 1.0 (retaining TLS 1.2) on port 4740 and HTTPS webserver.
34204925	5.1.0.0.0	2	Crash in 4.4p1.
34487595	5.1.0.0.0	3	Command code for DIAMETER Msg not visible in GUI after upgrade to 5X from 4.4.
34629168	5.1.0.0.0	2	CDPN is incorrect in ISUP call.
34495474	5.1.0.0.0	3	Filter to a panel in the dashboard have been reset to default after a logout.
34664877	5.1.0.0.0	3	Selecting what looks like a 'select all' button greys out the icon in the Call Transfer tab.
34643928	5.1.0.0.0	3	Call Searches cannot be halted.
34684544	5.1.0.0.0	3	When we enable the show in groups, the devices under the trunk are not shown.
34451917	5.1.0.0.0	3	Media Recording Retention not Working
34684583	5.1.0.0.0	2	Calls opening with Details button is not working.
34703534	5.1.0.0.0	2	OneWayAudio Addon showing audio as OK for RTCP packets.
34733695	5.1.0.0.0	3	Issues arise when the name of a probe is changed.
34667532	5.1.0.0.0	2	Add Rights to the selected User Does not work properly.
34742740	5.1.0.0.0	2	Duplicate records seen under the Calls section of OCOM.
34781044	5.1.0.0.0	3	Unable to create a filter for initiator device.
34690868	5.1.0.0.0	3	OCSM App issues on 5.0.0.4.0 (Bug 34379889).
34666043	5.1.0.0.0	2	VSI crash after upgrading from 4.3 to 5.0p3.
34433329	5.1.0.0.0	2	VSI crash in 5.0p3.
34599305	5.1.0.0.0	2	VSI crash on 4.4.0.5.
34646929	5.1.0.0.0	2	Realm discrimination not working when custom pattern headers are used.
34618613	5.1.0.0.0	3	OCSM does not support DHE nor ECDHE based ciphers for IPFIX over TLS connection.
34753877	5.1.0.0.0	2	Is 5.7.40 MySql is compatible with OCOM 5.x or not.

ID	Fixed in Label	Severity	Description
34834673	5.1.0.0.0	3	Issue with User Tracking.
34840351	5.1.0.0.0	3	Display blank on current registration under user tracking
34835201	5.1.0.0.0	2	Direction of START RTP/RTCP packets is not correct in Message flow and Media Summary.
34788903	5.1.0.0.0	3	OCOM shows only 7 days of KPIs.
34822910	5.1.0.0.0	3	Search takes so much time with the advanced filter with a specific date.
35016058	5.1.0.0.0	2	OCOM Dashboards are not being displayed in the GUI after upgrade.
35112655	5.1.0.0.0	3	Starting from 5.0.0.5 release calls retention cannot be set in newsetup.