Oracle® Communications Session Monitor

Release Notes

Release 4.4

F36099-01

December 2020

Oracle Communications Session Monitor Release Notes, Release 4.4

F36099-01

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 4.4 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
December 2020	• Initial release. • Added OCSM 4.4 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 4.4

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

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

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 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	8 GB RAM
Disk Space	80 GB
NIC Card	1Gbps 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 4.4 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 7.8 (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	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
SP-SBC	S-Cz8.4.0 Works with Operations Monitor and Enterprise Operations Monitor
E-SBC	S-Cz8.4.0 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	19.11
ISR	6.4

Product Name	Version
SP-SBC	S-Cz8.4.0 Works with Fraud Monitor and Enterprise Telephony Fraud Monitor.
E-SBC	S-Cz8.4.0 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
Enterprise Session Border Controller (E-SBC)	• S-Cz8.4.0 • S-Cz8.3.0 • S-Cz8.2.0 • E-Cz8.0.0 • E-Cz7.5.0 • E-Cz7.4.0 • E-Cz7.3.0
Session Border Controller (SBC)	• S-Cz8.4.0 • S-Cz8.3.0 • S-Cz8.2.0 • 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:

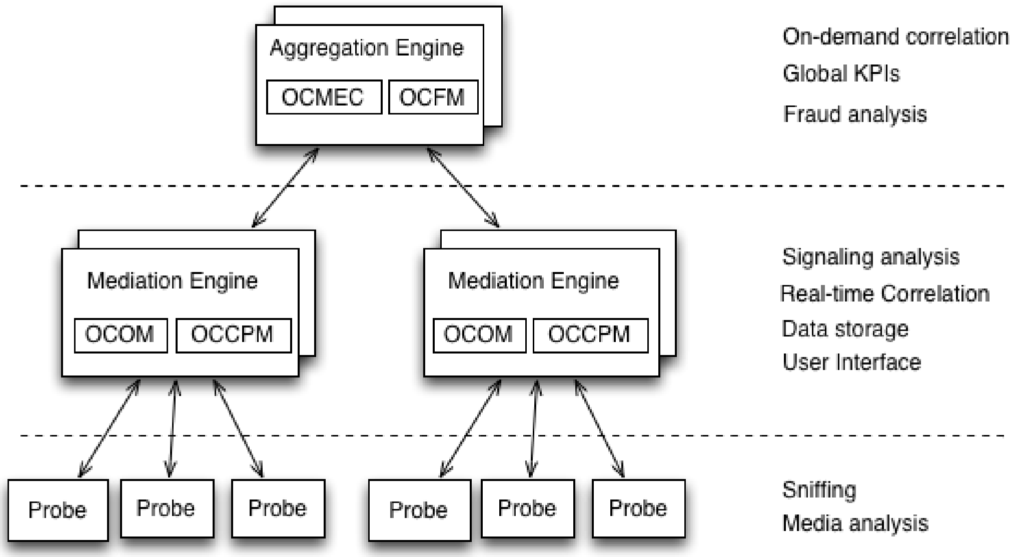
- 5.5.54
- 5.7.10
- 5.7.24

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 4.4 includes the following new features, enhancements, and changed functionality:

VSI Drop Enhancements

In older versions, Red bars indicate packet loss. To identify packets that are dropped by VSI or are dropped before reaching VSI, you need to perform a log analysis. If there are any packet drops before reaching the VSI module, such packet drops are identified by VSI by checking for any sequence-gaps that may appear due to packet drops between the APID and RAPID modules. These drops due to sequence-gaps are indicated by the Yellow bars introduced in the OCSM 4.4 release.

To summarize:

- Red bars: Indicate packet drops at VSI.
- Yellow bars: Indicate packet drops due to sequence-gaps before reaching VSI.
- Pink bars: Indicate that a few messages may have been lost and the call session information may not be accurate for the duration of the pink bars. Any occurrence of Yellow and Red bars are followed by pink bars.

Device Map Enhancements

This enhancement provides flexibility to select the required Platform devices to be enabled for a Device map. You can enable Device Map for a maximum of 50 Devices. You can also enable and display Trunks in a Device map. If you are upgrading from previous releases, where the **Device Map** flag is **True** and if the Device Map limit set earlier is less than or equal to 50, then the **Enabled Device Map** flag remains as **True** after the upgrade to OCSM 4.4. However, if the Device Map limit was greater than 50 before the upgrade, then the **Enabled Device Map** is set to **False**.

After upgrading to OCSM 4.4 set the **Enabled Device map** flag to **True** manually. Select the devices to be displayed in the map from the **Platform Device** settings. For more information, see the OCSM 4.4 Operations Monitor User Guide.

Support for OCSM Deployment in the Cloud

OCSM deployment is now supported in OCI and Azure cloud. For more information on the prerequisites and installation procedure, see the Session Monitor 4.4 Installation Guide.

Multiple-VSP Support

Enable the Multi-VSP feature to improve the concurrent user experience on the Mediation Engine user interface. The Multi-VSP feature faciltates creation of Multiple VSP instances. NGINX or HTTPD servers act as load balancers and the HTTP request load is distributed across multiple VSPs. For more details, see the OCSM 4.4 Operations Monitor User Guide.

Resetting the Password for Non Admin Users

Non-admin users can use the **Forgot password** link on the Mediation Engine GUI to reset the password. For more information, see the OCSM 4.4 Operations Monitor User Guide.

Fraud Monitor (OCFM) Notifications Enhancement

You can turn-off Email and SNMP notifications for Incidents. For more information, see the OCSM 4.4 Fraud Monitor User Guide.

Fraud Monitor (OCFM) Support for Multiple Mediation Engine Connections

A single Fraud Monitor can be connected to multiple Mediation Engines. For more information, see the OCSM 4.4 Fraud Monitor User Guide.

Capacity and Performance Improvements

OCSM 4.4 provides the following performance improvements:

- Operations Monitor performance improved to support higher signaling bandwidth.
- Support of higher number of registered users in the Mediation Engine.
- Fraud Monitor performance improvements.

Selinux Support

It is not mandatory anymore to disable Selinux post OCSM installations. Operations Monitor should function as usual with the SELINUX modes:

- Enforcing (Selinux type: Targeted)
- Permissive
- Disabled

For more information, see the OCSM 4.4 Session Monitor Installation Guide.

Virtual Probe Cloning Enhancements

The OCSM 4.4 release introduces a script to generate random UUIDs for cloned probes. After running the script, the cloned probes can be connected to the Mediation Engine successfully. For more information, see the OCSM 4.4 Session Monitor Installation Guide.

3

Interface Changes

The following topic summarizes changes for release 4.4. The additions, removals, and changes noted in these topics occurred since the previous release of Oracle Communications Session Monitor.

The interface changes in 4.4 are:

Change	Description
Yellow bars in the Mediation Engine pages.	Mediation Engine pages such as Active Calls, KPIs, Dashboard, Alerts, and so on display Red bars indicating about the message loss at EOM. This is also followed by a Pink bar indicating that the messages have been lost and VSI and the call session information may not be accurate until the duration of Pink bars. OCSM 4.4, Yellow bars indicate drops due to sequence-gap. If there are any packet drops before reaching the VSI module, such packet drops are identified by VSI by checking for any sequence-gaps that may generally appear due to the packet drops between the APID and RAPID modules.
Device Map	The **Device Map** button can be toggled to enable or disable the display of a device in a device map using the **Platform Devices** page. The maximum number of devices which can be enabled for the Device Map is 50. This can be configured in the **Device Map Limit** under **System Settings**. Trunks can also be enabled and displayed in Device map. The default status of the **Enabled Device Map** flag is **False**. To view a real-time map of the configured platform devices and the interactions between them, set this flag to **True**.
Resetting password for non-admin user	The **Forgot password** link on the Mediation Engine user interface allows non-admin users to reset passwords.
Notifications enhancement	In the Fraud Monitor user interface, a new option - **Do not revceive updates** has been added to turn-off email and SNMP notifications for Incidents. You can see this in the **Add email recipient** window.
Multiple Mediation Engine connection	In Fraud Monitor user interface, the **Setup** page displays connection status of all Mediation Engines simultaneously connected.

4 Known Issues

The following tables list the known issues and resolved known issues in Oracle Communications Session Monitor 4.4.

Known Issues

The following table provides a list of known issues in 4.4 GA.

ID	Description	Severity	Found In
ACMEESBC-1027331673420	In local, self contained online help, the arrows and contract/ expand, used for help navigation do not display as expected. **Workaround**: Click the box-like character.	4	OCSM 4.4

Resolved Known Issues

The following table provides a list of previous known issues that are now resolved in 4.4 GA.

ID	Description
25891854	syslog reports CRITICAL leaked counters
28139926	Performance Issues Slow ME GUI after upgrade to 4.0.0.2.0
29323444	Red bars in "calls Summary" page
29405884	VMware probe cloning support process and clarification
30430395	Support for Mellanox NIC on DPDK Probe
30446543	FDP 4.2 Incidents are not Reported for Static Call Volume Rule
30531418	Swisscom pld-vsi.service crash, out-of-memory
30561182	Empty call flow diagram for few calls
30568547	balance-irqs command in pld-scripts cron script is incorrect
30682796	vsi drops and red bars after upgrade to 4.2.0.1.0
30727463	Redbars in TCP based based traffic.
30727480	VSP performance improvement in external authentication based systems
30844829	Swisscom Reported vsi crashes in Custom Patch equivalent to 4.2p2
30878442	Segmentation fault in zmq library

ID	Description
30931997	File Transfer is not anonymized
31003911	No VQ graphs or media details after upgrade to 4.2.0.2.0
31035831	OCOM : ME DIP in graph - segfault - error 4 in libxmlrpc_abyss.so.3.51
31161454	OCSM : Add Right and Remove Right not working in MEC
31161589	OCSM : MEC || Stringent password rules disabled, User getting suspended after 3 invalid attempts
31180430	OCSM DPDK probe - pld-rat.service failing - code=dumped, status=4/ILL
31187885	installation of Skype for Business Agent got error
31219988	Voice Quality Graph shows severe drops\Media Details Tab not populated
31231855	MEC Graph Timescale Issue
31232208	Max concurrent sessions limits reached need Error Message on Web GUI
31262299	Stuck Calls in OCOM
31303699	Device Name Not Visible when configured with VLAN.
31381396	Trunk Devices are displayed as using Call Merging Algorithms
31440966	VSI unable to parse End of call VQ reports
31493497	DPDK Probe rat segfault almost everyday.
31510972	rat-mmpcap crash with red bars and flat 400 calls on GUI
31622120	'whois' package required but not part of RPM installation
31692805	pld-rat.service failing - code=dumped, status=4/ILL
31717465	4.1 FM Upgrade to 4.3.1 caused multiple issues, expire events, SDM/SBC updates
31719769	PI Filter Syntax Issue
31777478	FDP-Automatic Review Trigger: Blacklist gives errors and service restarts in log
31849109	In-dialog SIP MESSAGE not processed
31853084	Synthetic KPI cannot be added, throws error: Adding counter failed: Trying to add a duplicate counter
31859715	CSV Export doesnÂ´t work via MEC
31860240	OCOM is not displaying PRACK messages.
31916955	'OCFM: Notification for expired list entries' email has formatting errors
31939117	No ISUP Message Details via advanced search on the MEC
31983809	The error message “c= line found in SDP” is displayed in ME.
32040427	Synthetic KPI Expression with Brackets

ID	Description
32148906	Filtered calls are note exported correctly with CSV export and advanced filters set