Oracle® Communications Session Monitor

Release Notes

Release 4.2

F16848-01

December 2019

Oracle Communications Session Monitor Release Notes, Release 4.2

F16848-01

Contents

About This Guide

Revision History

1 Introduction

Session Monitor Supported Hardware 1-1

Hardware Requirements for Production Systems 1-2

Hardware Requirements for Demonstration Systems 1-2

Session Monitor Virtualization Support 1-3

Session Monitor Operating System Requirements 1-3

Session Monitor Connectivity 1-4

Session Monitor Software Requirements 1-4

Compatibility Matrix for Session Monitor 1-5

Compatibility Matrix for Fraud Monitor 1-5

Session Border Controller Supported Versions 1-6

Database Support 1-6

Session Monitor System Architecture 1-6

Upgrade Information 1-7

Licensing Changes 1-8

Documentation Changes 1-8

Patches Included In This Release 1-8

2 New Features

3 Interface Changes

4 Known Issues

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 4.2 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
July 2019	• Initial release
Aug 2019	• Corrections to compatibility matrix and supported versions
Sept 2019	• Adds Red Hat statement • Updates supported drivers and chipsets in "Session Monitor Supported Hardware"
Nov 2019	• Adds "Licensing Changes" section
Dec 2019	• Adds notes about upgrading to 4.2p1 to "Upgrade Information."

1 Introduction

The Oracle Communications Session Monitor *Release Notes* provide information about new features, enhancements, and changed functionality in release 4.2

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 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 server supports only Session Monitor Installation using RPM installer.

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
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 4.2 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

Table 1-6 (Cont.) Supported Operating Systems

Oracle Linux 7 x86-64 (64 bit)	7 or higher (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	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)
Apple Safari	Any version, including Safari for iPad

Table 1-7 (Cont.) Supported Client Browsers

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	18.11
ISR	6.0, 6.2*
SP-SBC	8.3 or lower Works with Operations Monitor and Enterprise Operations Monitor
E-SBC	8.3 or lower Works with Operations Monitor and Enterprise Operations Monitor

> **Note:**
>
> The * marked version recordings at ISR should not be segmented.

Compatibility Matrix for Fraud Monitor

The following products can be configured with Fraud Monitor:

Product Name	Version
DPDK	18.11
ISR	6.0, 6.2*
SP-SBC	8.3 or lower Works with Fraud Monitor and Enterprise Telephony Fraud Monitor
E-SBC	7.5 or higher Works with Fraud Monitor and Enterprise Telephony Fraud Monitor
SDM	8.2

> **Note:**
>
> The * marked version recordings at ISR should not be segmented.

> **Note:**
>
> Fraud Monitor 4.2 is supported only with Session Monitor 4.2.

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)	• 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

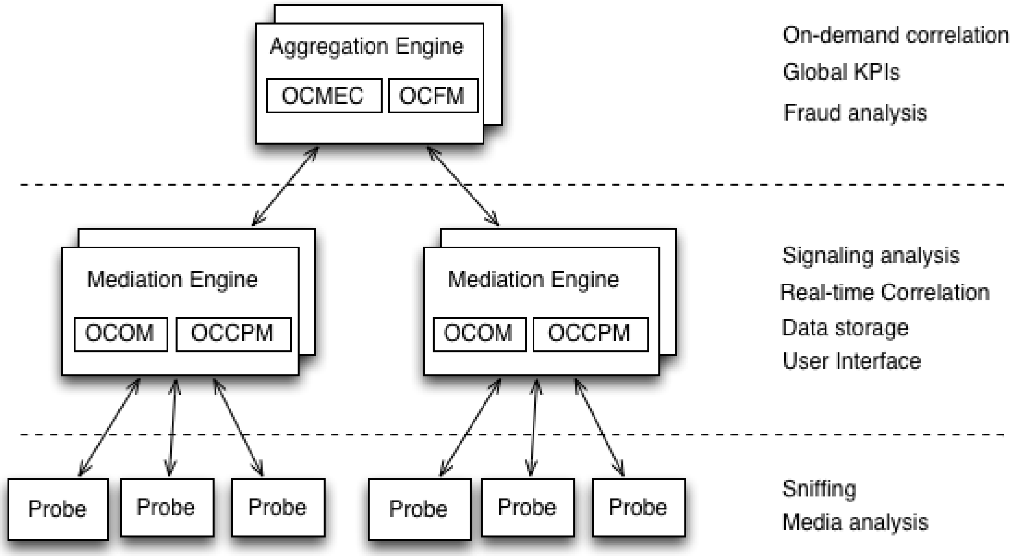
The Session Monitor system works by capturing the traffic from your network, correlating it in real-time, and storing it in indexed formats so that they are available for the various reports offered by the web interface.

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 4.2 and above supports DPDK version 18.11 only. After upgrading to 4.2, see the *Session Monitor Installation Guide* for information on upgrading DPDK.

> **Note:**
>
> Please check the pre-requisites in the Upgrade Guide before upgrading to 4.2p1.

> **Note:**
>
> It is recommended to have both Probe and Mediation Engine in the same version of 4.2p1.

Licensing Changes

As of November 5, 2019, two new licenses for Enterprise Operations Monitor are available:

- 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. 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 4.2

ePub and Mobi

The documentation no longer supports ePub and Mobi formats.

Patches Included In This Release

2 New Features

Session Monitor release 4.2 includes the following new features, enhancements, and changed functionality.

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.

Third-Party Call Control (3PCC)

Third-Party Call Control (3PCC) servers initiate two outgoing legs to establish a single call between two parties. OCSM 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.

Password Enhancement

Software release version 4.2 and later support complexity requirements for passwords. After upgrading to 4.2 or later, the system will accept old passwords but force users to reset their password to meet the complexity requirements.

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.

3

Interface Changes

The following topic summarizes changes for release 4.2. The additions, removals, and changes noted in these topics occurred since the previous release of Oracle Communications Session Monitor.

Settings

Change	Description
SFB Filter Configuration	Added the following configuration checkboxes to support the SFB filter: • Video • IM • Conference • Desktop Sharing • File Transfer
Search on Enter	Added the Search on Enter key to filtering in the following windows: • Recent Calls • User Calls • Calls
Privacy Setting for Chat	Added the ability to anonymize content and select SIP headers.

4 Known Issues

The following table lists the known issues in version 4.2 of Oracle Communications Session Monitor.

ID	Description	Severity	Found In
29757880	The default active calls graph is not displaying as expected.	4	4.2.0.0.0
29823958	Packet inspector is not masking supported headers	3	4.2.0.0.0
29835976	When Mediation Engine is connected to Mediation Engine Connector via ext authentication, Mediation Engine alerts are not displayed on the connector	3	4.2.0.0.0
29895638	Call info is not displayed when a call is run in an Established state	3	4.2.0.0.0
29946916	Mediation Engine does not display the device KPI Call Attempts per Second	3	4.2.0.0.0
29947559	IMSI search only returns exact match results	3	4.2.0.0.0
29965117	In Fraud Monitor, configuring to username filter creates an incident	4	4.2.0.0.0
29999562	When exporting devices to CSV format, 3PCC does not save as Enabled. JSON export continues to function as expected	3	4.2.0.0.0

Resolved Known Issues

The following table provides a list of previous known issues that are now resolved in 4.2 GA.

ID	Description
29952724	Ensure users can view and add panels only for what they have permission to manage
29939401	Web session inactivity time-out is enforced as according to configuration

ID	Description
29743505	Cannot search for users that are not on the main user page
29899590	OCOM username does not allow special characters
29754178	FDP crash observed when running call with To/From headers missing the "userinfo" field
29606673	Diagnostics do not include PSA Version Table Entry
29724786	VSI crash observed when call event publisher is to be enabled
28364504	Skype probe installation fails on machines in a server pool
29439407	Unable to access Web GUI on MEC after upgrading to 4.1.0.2.0
29434370	Multilib library version incompatibility while installing OCSM 4.1.0.2.0
29327721	Fraud Monitor "to-phone-number" filter type does not allow regex
29232952	Ensure voice quality modules are not accessible to users with no voice quality permission
29231708	Ensure users cannot add alerts for modules they are not permitted to use
29209386	MEC-ME-SSL connection using regenerated self-sign certificates fails for second ME node
29199158	Restoring large configuration savepoints fails with "transaction aborted" or "504 gateway timeout" messages
29041454	pld-vsi.service restarts due to memory cghealth with customer traffic (SCTP)
29031775	OCSM: (mgcp_probe) crash results in drop in OCSM graph
28895459	Slow performance and messages log full with "WSGIControllerComponent.py" exception
28816572	MEC : Not able to log in when "Remember Me" is checked
28814340	OOCM 4.0 has invalid cron job "killall vsi" under pld-scripts
28805519	Counter: Total number of active calls Keyerror:0
28726653	On the user tracking page, search is not working as expected
28696863	Red bars and pld-diamond.service crashing
28461807	Unable to download pcap. "Sorry, an error occurred while processing your request" error displays.
28417903	Link quality showing exception error when adding an IP
28366322	"Failed to find probe on ME" error

ID	Description
28360801	OCOM does not correlate From-URI user part (using uri_user test) AND x-to parameter of From header (using hf_param_equals test). These values can now be correlated with the hf_uri_param_equals test. See the Call Merging Algorithms chapter in the Operations Monitor User Guide
28250113	MEC admin unable to delete users created by admin
28186912	Blank "Recent call stats repartition" panel on Dashboard
28077766	All media legs are visible from "Media Summary" and "Media Details" even when user is configured for limited traffic visibility
27823620	Calls no longer stored on disk: "int exceeds XML-RPC limits" error
27686830	"The selected call is no longer stored on disk" error occurring for recent calls
27659806	E-Mail Alert Notification from OCFM is always in UTC timezone
27627444	Register Message Correlation for same endpoint towards more than one Registrars
27596954	Intel X710/i40e driver support
27302448	SIP response 404 cannot be seen under Calls for TCP flows
27143434	Too many streams error even with concurrent streams being recorded not on max
20922461	PI tries to reach non configured probes
23213095	Display vlan tags in message flow (toggle option) for SIP and RTP flows