Oracle® Communications Session Monitor

Release Notes

Release 4.1
E99934-02
October 2019

Oracle Communications Session Monitor Release Notes, Release 4.1

E99934-02

Copyright © 2014, 2019, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

About this Guide

This document includes information about this release of the Oracle Communications Session Monitor product family. The Session Monitor products impacted by this release are:

- Operations Monitor
- Enterprise Operations Monitor
- Control Plane Monitor
- Fraud Monitor

For more information, see the following documents in the Session Monitor documentation set:

- *Oracle Communications Operations Monitor User's Guide*: Describes how to use Operations Monitor and Enterprise Operations Monitor to monitor, detect, and troubleshoot IP Multimedia Subsystem (IMS), Voice over Long-Term Evolution (VoLTE), and next-generation network (NGN) networks.
- *Oracle Communications Session Monitor Mediation Engine Connector User's Guide*: Describes how to configure and use Mediation Engine Connector.
- *Oracle Communications Session Monitor Developer's Guide*: Describes how to extend the Session Monitor product family by using the Oracle Communications Session Monitor SAU Extension.
- *Oracle Communications Session Monitor Security Guide*: Provides guidelines and recommendations for establishing a secure configuration and implementing security measures for the Session Monitor product family.

Revision History

Date	Description
March 2019	• Initial release
October 2019	• Adds "New Custom Call Merging Algorithms" to "New Features" chapter.

1

Release Notes

This chapter includes descriptions of the new and enhanced features introduced in Oracle Communications Session Monitor release 4.1.

New Features

Session Monitor release 4.1.0.0.0 includes the following new features, enhancements, and changed functionality:

- Fraud Monitor Enhancements
- New Platform-Wide KPIs
- Security Enhancement when Connecting Mediation Engine with Mediation Engine Connector or Fraud Monitor or Interactive Session Recorder
- Password Setting Enhancements

Fraud Monitor Enhancements

Following enhancements were made to Fraud Monitor:

- **Ratelimit:** Fraud Monitor evaluates the entries based on the Calls per Second, and Maximum Active Calls configured. Fraud Monitor raises warning or critical incidents when the entries exceeds these thresholds.
- **Redirect:** You can redirect the suspicious users based on the configured session agent, session agent group name, host name, and IP address.
- **Import/Export** the blacklists, ratelimit, and redirect lists.
- **Export** the whitelists.
- Automatically generate blacklists, ratelimit, and redirect list based on prefixes of phone numbers, hostnames, and IPs.

> **Note:**
>
> Fraud Monitor 4.1.0.0.0 supports only on Session Monitor 4.1.0.0.0.

For more information, refer to the *Fraud Monitor User's Guide*.

New Platform-Wide KPIs

Following new Platform-wide KPIs are added in this release. These KPIs can be accessed from Metrics library from Operations Monitor.

- Number of blacklisted calls

- Number of rate-limited calls
- Number of redirected fraudulent calls

For more information, see *Oracle Communications Operations Monitor User's Guide*.

New Custom Call Merging Algorithms

This topic lists new custom call merging algorithms in the 4.1 release.

The following new custom call merging algorithms have been added to this release:

- hf_uri_param_equals

Security Enhancement when Connecting Mediation Engine with Mediation Engine Connector or Fraud Monitor or Interactive Session Recorder

In 4.1.0.0.0, certificate validation is enabled for establishing HTTP connections secured by SSL (HTTPS). In order to establish secure and validated connections with each other, the machines need to be able to validate the certificate of each other. There is also an option if hostname should be validated.

When you connect Mediation Engine and Mediation Engineer Connector or Fraud Monitor, each machine must require a valid certificate for the other machine, so that machines can validate each other. This can be either the certificate found on the **Server Certificate** page of the other machine (self-signed) or the corresponding CA certificate (of the CA that signed the certificate).

When you connect Mediation Engine and Interactive Session Recorder, Mediation Engine requires a valid Interactive Session Recorder certificate to establish secure connection.

Post upgrade to 4.1.0.0.0, the connection between Mediation Engine and Mediation Engine connector or the connection between Mediation Engine and Interactive session recorder would not establish until each machine has valid certificates of the other.

For More information see, *Oracle Communications Operations Monitor User's Guide* and *Oracle Communications Mediation Engine Connector User's Guide*.

When you connect Mediation Engine with Mediation Engine Connector, it is mandatory to upload the Trusted Certificate of Mediation Engine to Mediation Engine Connector and Vice Versa. Similarly, the trusted certificate of Mediation Engine must be uploaded to Fraud Monitor and vice versa when connecting Mediation Engine to Fraud Monitor.

For more information, see *Oracle Communications Operations Monitor User's Guide*.

Password Setting Enhancements

Following password setting enhancements has been made in this release which includes:

- Supports a strong password.

  Password must contain at least one uppercase alphabet, at least one special character (such as !, @, #, $,%, ^, &, *, (), -, _, =, +), and at least one numeric digit between 0 and 9.
- Password expires after every 180 days and user is forced to change the password.
- User account gets locked after three unsuccessful login attempts.

Deprecated Support

With this release, the Session Monitor installation using ISO installer is deprecated.

Compatibility with Session Monitor 4.1.0.0.0

Session Monitor is now compatible with:

- DPDK version 17.05
- ISR 6.0 and higher
- MySQL Enterprise Edition release 5.7.10
- Oracle Linux 7.5
- SDM 8.1.1
- SP-SBC
  - OCOM and EOM works with SP-SBC 8.2 and lower
  - OCFM and OETFM works with SP SBC 8.2 and higher
- E-SBC
  - OCOM and EOM works with E-SBC 8.1 and lower
  - OCFM and OETFM works with 7.5 and higher

Fixes in This Release

Table 1-1 lists the service request (SR) issues reported and bug number, and provides a brief description of the resolution.

Table 1-1 Fixes in This Release

Service Request (SR) Number	Bug Number	Description
NA	28260436	Previously, the exported CSV report with call details does not have the prefix group. This has been fixed.
NA	28017157	Previously, there were discrepancies in the session count compared between the Mediation Engine and Session Border Controller. This has been fixed.
NA	2975644	Previously, there was a delay in displaying the call search results in the Mediation Engine. This has been fixed.
NA	27941411	Previously, when Skype for business extension is selected on the PSA page, the extension is not displaying as selected after the installation. This has been fixed.
NA	27928066	Previously, after upgrading from 3.4.0.2.0 to 4.0.0.2.0, user was unable to add the Number Determination Rules. This has been fixed.
3-17248978011	27925464, 27925413	Previously, multiple entries for block errors followed VSP crash in the application. This has been fixed.

Table 1-1 (Cont.) Fixes in This Release

Service Request (SR) Number	Bug Number	Description
3-17102467871	27724996	Previously, after enabling the system setting, **Allow regeneration of registration events for user updates** and running call, traffic core has been observed. This has been fixed.
3-16605515521	27723257	Previously, there was in a graph for two mediation engines having same probe generated at same time for similar values. This has been fixed.
3-16702781611	27706115, 27422870	Previously, 504 error encountered when logging into web interface of the application. This has been fixed.
3-17024002221	27665838	Now CSV exports the calls chart when there is a realm user with name containing umlaut characters.
NA	27635030	Previously, the alert message contains the **URL to source** parameter which was failing in few scenarios. Now the alert message contains the device details instead of the **URL to the source** parameter.
NA	27581166	Previously, when a traffic was sent with a VLAN tagging, the packets were sent only to one stream. This has been fixed.
NA	27502448	Previously, message details does not appear in a saved HTML file. This has been fixed.
NA	27496604	Previously, any user was able to change the local password in the application. The issue has been fixed.
3-16790330421	27487746	Previously, upgrade from 3.4.0.1.0 to 4.0.0.1.0 failed due to an DPDK error. This issue has been fixed.
NA	27475907, 26708680	Previously, there was an error when uploading blacklist file. This issue has been fixed.
NA	27458649	Previously, upgrade from 4.0.0.0 to 4.0.0.1 failed with an error **Error in PREIN** scriptlet. This has been fixed.
NA	27447890	Previously, when KPIs were added to **Favorites** panel, there was a delay for changes to appear in the **Favorite** Panel. This issue has been fixed.
3-16669909011	27444330	Previously, restarting the servers could not establish the connections between the Mediation Engines. This has been fixed.
NA	27432222	Previously, realm users could not create Synthetic KPI folder in KPI Metrics library. This issue has been fixed.
3-16710862634	27428462	Previously, there were errors in the system logs during heavy traffic. This issue has been fixed.
3-16608226991 3-16776373121	27374515, 27362237	Previously, VSI crashed after reaching the high memory usage of 364 GB. This issue has been fixed.
NA	27334265	Previously, the KPI alert mails were not sent successfully from PSA. This issue has been fixed.
3-16366822591 3-17777104681 3-16579309991	27305557	Previously, Enterprise Operations Monitor could not generated the requested certificate with the required data. This issue has been fixed.

Table 1-1 (Cont.) Fixes in This Release

Service Request (SR) Number	Bug Number	Description
3-16417250591	27304209	Previously, when a realm pattern exists before the system setting, **Allow regeneration of registration events** is being set to True, the setting has no affect to this realm pattern. This issue has ben fixed.
3-17777104681 3-16579309991 3-16366822591	27265090	Previously, CSR downloaded from PSA does not include SAN with FQDN, and IP address. This issue has been fixed.
3-16382705391	27263654, 27263654	Previously, the call flow data downloaded from PCAP does not include any data with call segments. This issue has been fixed.
NA	27253634	Previously, the KPI data is stored only up to 42 days. This issue has been fixed.
3-16364721734 3-15995467171	27239184	Previously, if a CSV file is opened before the download completes, error 404 is encountered. This issue has been fixed.
NA	27234006	Previously, the ISO file has default DNS configuration file. This issue has been fixed.
3-16364721549 3-16857278593	27233233	Previously, the exported CSV files contains a difference in timestamp for call data. The issue has been fixed.
3-16118361431	27177070, 27177028	Previously, the setting, **Device Map Limit** does consider the trunks to deactivate. This issue has been fixed.
3-16233507941 3-17257647691	27168382, 27840979	Previously, the Exception file contained spam logs for certain KPIs. This issue has been fixed.
3-16242462341 3-18038929741	27168173, 28461807	Previously, an error encountered when downloading PCAP file. The issue has been fixed.
3-16129745851		
3-16118361431	27102722	Previously, during an upgrade, if the disk space is full, then PSA does not display any message to the user and the error is logged as part of Pre-Check Script. This issue has been fixed.
3-15964648981	27076829	Previously, there is a latency issues with the search results for Registrations. The issue has been fixed.
3-15995467171	27041231	Previously, there were issues in the exported CSV report intermittently. The issue has been fixed.
NA	27037678	Previously, Enterprise Operations Monitor was querying to Oracle DNS server. This issue has been fixed.
NA	27037427	Previously, additional IP address were included in the user chronyc sources. This issue has been fixed.
3-15984525901 3-17399367461 3-17511747171	27008913	Previously, there were leaked counter errors in the call logs. This issue has been fixed.
NA	27008913	Previously, the **MySQL slow** log file did not rotate. The issue has been fixed.

Table 1-1 (Cont.) Fixes in This Release

Service Request (SR) Number	Bug Number	Description
3-15907324381	26960585	Previously, multiple DNS queries towards**teredo.ipv6.microsoft.com** correlated to the call were observed as ENUM messages are correlated with SIP.This issue has been fixed.
3-15854187011	26933528	Previously, when restoring the configuration savepoint with the manipulated KPI, then Probe KPI was not appearing in the KPI menu. This issue has been fixed.
NA	26831468	Previously, the VQ Statistics, Media Summary, and Media details were missing in the **merged.pcap** file. This issue has been fixed.
NA	26821331	Previously, VSI crashed frequently even after optimizing the increasing the server size capacity. This issue has been fixed.
NA	26785333	Previously, the **E-Mail Alert Notification** sent with incorrect timestamps. The issue has been fixed.
NA	26771219	Previously, the **Expected** field was not present in the final MDR report. The issue has been fixed.
3-15564906241 3-16766403911	26708680	Previously, lag error encountered at syslog when trying to upload Blacklist file. This issue has been fixed.
3-15396792091	26532659	Previously, could not login to Operations Monitor even after successful RADIUS authentication. This issue has been fixed.
NA	26495345	Previously, Megaco Packet Counters were reported as Diameter Packet Counters in the Signaling Protocols, in PSA. The issue has been fixed.
NA	25973426	Previously, the number of devices not involved in flow are affecting the correlation. The issue has been fixed.
NA	25910251	Previously, after VSI restart, the calls table gets locked and not displayed when MySQL query was executed. This issue has been fixed.
NA	24341980	Previously, an error encountered when searching from User Tracking page in the Mediation Engine Connector. This issue has been fixed.
NA	22174502	Previously, when you delete a Device, the counters associated with the device did not get deleted. The issue has been fixed.

Upgrading to Session Monitor 4.1.0.0.0 from a Previous Version

If you are using a Session Monitor version lower than 3.4.0.0.0, you need to migrate to Session Monitor 4.0.0.0.0. For migrating to 4.0.0.0.0 refer to the *Migration Guide* in Release 4.0 documentation on Oracle Help Center. After migrating to 4.0.0.0.0, you need to upgrade to 4.1.0.0.0. For more information, refer to *Session Monitor Upgrade Guide*.