

Oracle® Communications Session Monitor Upgrade Guide



Release 5.0
F47891-01
October 2021

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Copyright © 2021, 2021, Oracle and/or its affiliates.

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 embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. 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, Java, and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside 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, Epyc, and the AMD 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

Revision History

1 Upgrading Session Monitor

Supported Upgrade Paths	1-1
Pre-requisites	1-1
Configuring Proxies and Repos	1-1
Creating a Backup before Upgrading	1-2
Altering Database Tables Before Upgrading to 5.0	1-3
Upgrading Session Monitor	1-3
Upgrading to Release 5.0 through PSA	1-4
Upgrading to Release 5.0 through ACLI	1-4
Upgrading DPDK	1-5
Uninstalling DPDK	1-5
Installing and Configuring DPDK with Internet	1-5
Installing and Configuring DPDK Without Internet	1-6
Upgrading Session Monitor without an Internet Connection	1-7
Post Upgrade	1-8

2 Upgrading MySQL

About this Guide

This guide provides guidelines and recommendations for setting up Oracle Communications Session Monitor in a secure configuration. The Oracle Communications Session Monitor product family includes the following products:

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

1

Upgrading Session Monitor

This document provides instructions for upgrading Oracle Communications Session Monitor from a previous version 3.x and 4.x to version 5.0.

Supported Upgrade Paths

This release has been tested for upgrades from specific prior releases. Verify that your current installed release is listed on a valid upgrade path. The possible upgrade paths to Session Monitor 5.0 are listed below.

Table 1-1 Supported Upgrade Paths

From	To	Mechanism
3.3	5.0	Migrate to 3.4 and then upgrade to 5.0
3.4	5.0	RPM Upgrade
4.0	5.0	RPM Upgrade
4.1	5.0	RPM Upgrade
4.2	5.0	RPM Upgrade
4.3	5.0	RPM Upgrade
4.4	5.0	RPM Upgrade



Note:

It is recommended to have both Probe and Mediation Engine in the same version of 5.0.

Pre-requisites

Before beginning with the process of upgrading, ensure that the following pre-requisites are fulfilled.

Configuring Proxies and Repos

You are required to configure the proxies and repos.

Configure the http proxy in `/etc/yum.conf` file and also export the proxy's address to the environment.

1. In `/etc/yum.conf`, add the following line:

```
proxy=<proxy_server>
```

2. Export the proxy's address.

```
export http_proxy=<proxy_server>
export https_proxy=<proxy_server>
```

3. Enable the required proxies in yum.conf.

```
curl -O https://yum.oracle.com/public-yum-ol7.repo
mv public-yum-ol7.repo /etc/yum.repos.d/public-yum-ol7.repo
yum-config-manager --enable ol7_latest ol7_UEKR4 ol7_developer_EPEL
ol7_optional_latest ol7_addons ol7_UEKR3 ol7_UEKR5 ol7_UEKR6
```

Creating a Backup before Upgrading

You must create a backup of the Mediation Engine (ME) and Mediation Engine Connector (MEC) before you begin upgrade.

For Mediation Engine

Session Monitor provides the feature of backing up the configuration of Mediation Engine (ME) servers by using Configuration Savepoints.

For more information, see Configuration Savepoints section in Settings chapter of *Operations Monitor User Guide*.

For Mediation Engine Connector



Note:

The backup procedure is not available for probes or Mediation Engine Connector (MEC).

Perform the following tasks to collect present data for comparing in case of any issues:

- Take Platform Setup Application (PSA) Screenshots
Go through each page of PSA and make screenshots of the page for comparing with post-upgrade in case of issues.
- Potential Customized Files
Ensure to make a backup copy of all the following potential customized files:
 - **/etc/mysql** - Configuration files for MySQL stored in this directory. Make a copy of the entire directory. This is not required for probes.
 - **/etc/iptego** for version 3.3 or **/opt/oracle/ocsm/etc/iptego** for version 3.4 and later - Configuration files for Session Monitor services are stored here. Make a copy of the entire directory.
- Any other configuration files that you consider to have changed on the server.
- Capture current system diagnostics with MySQL dumps and all the hardware system configuration.

Altering Database Tables Before Upgrading to 5.0

For any upgrade to 5.0, the following steps need to be followed. This has to be applied to all the nodes (Mediation Engine/Mediation Engine Connector/Fraud Monitor).

To alter database tables:

1. Download the "db_update_script.sh" script delivered with RPM.
2. Set permissions to 777 for script:

```
chmod 777 db_update_script.sh
```

3. Run the db upgrade script "db_update_script.sh".

```
./db_update_script.sh
```

Note:

This script execution may take time, from a few minutes to several hours based on the number of database entries. As this runs, the GUI will be accessible. Some functions like downloading pap, message flow, and PDF download may not work in calls page.

4. Follow the normal upgrade procedure once script execution is successful as mentioned in "Upgrading Session Monitor."

Upgrading Session Monitor

Note:

It is not possible to directly upgrade from Session Monitor version 3.3 to Session Monitor version 3.4 or later as versions 3.4 and 4.x are built on Oracle Linux, and version 3.3 is Debian-based. To upgrade from 3.3 to 3.4 or 4.x, a re-install is required.

To upgrade Session Monitor:

1. Upgrade from Session Monitor release 3.3 to 3.4 or release 4.0 by referring to the Migration Guide provided in the 3.4, and 4.0 product documentation page on Oracle Help Center.

With this migration procedure, you can perform an upgrade without losing historic calls/ data.

2. After upgrading to Session Monitor release 3.4/4.0, upgrade to Session Monitor release 5.0 either by PSA or ACLI.
 - Upgrading to Release 5.0 through PSA
 - Upgrading to Release 5.0 through ACLI

Upgrading to Release 5.0 through PSA

Before upgrading, see [Altering Database Tables Before Upgrading to 5.0](#).

To upgrade to release 5.0

1. Open the PSA page of the ME by entering the URL address in the web browser:
`https://<IPofME>/setup/` where, `<IPofME>`

is the IP address of the ME. Contact your Oracle Representative for credentials.

2. Click browse and upload the software downloaded from Oracle

For Release 5.0, the software is an .rpm file:`ocsm-5.0.0.0-10243.x86_64.rpm`

3. After the upload is complete, click **Install**.
4. Accept the license agreement. The installation begins.
5. (Optional) You will receive the following error message if there is no enough disk space.

Cannot update. Not enough disk space. Please contact Support.

To free up the space, refer to the Document 1937398.1 in the Customer Support website.

The upgrade/installation may take 1 or more hours depending on the data on your machine. Once the installation gets completed, logout of the PSA page and re-login. Click Software Version from the right panel.

Result: The upgraded version is shown as Release 5.0.0.0 on the machine.

6. Log out of the application GUI and log in again to access new features.

Upgrading to Release 5.0 through ACLI



Note:

This section provides an example procedure for upgrading Mediation Engine (ME). The procedure for other machine types like Probe , and Mediation Engine Connector is the same.

Before upgrading, see [Altering Database Tables Before Upgrading to 5.0](#)

To upgrade Session Monitor to release 5.0 through ACLI:

1. Copy the RPM file `ocsm-5.0.0.0-10243.x86_64.rpm` to the system.
2. Set the correct environment by running the following command:

```
source /opt/oracle/ocsm/ocsm_env.sh
```

3. Run the following command to stop all the services on Operations Monitor:

```
pld-systemctl stop
```

4. Run the following command:

```
yum install ocsn-5.0.0.0.0-10243.x86_64.rpm
```

5. If Multi-VSP is enabled, then enable Multi-VSP again, and then restart all services using the command below: Else skip this step.

```
pld-systemctl start
```

6. The upgrade is complete. Run the following command to verify the Session Monitor software version:

```
cat /opt/oracle/ocsm/etc/iptego/display_version
```

Result: The output should be latest Session Monitor version. For example, 5.0.0.0.0.

7. Log out of the application GUI and log in again to access new features.

Upgrading DPDK

DPDK upgrade is required. Release 5.0 and above supports DPDK version 19.11 only. To update DPDK:

1. Follow the instructions in "Uninstalling DPDK"
2. Follow the instructions in "Installing and Configuring DPDK with Internet" or "Installing and Configuring DPDK without Internet" based on setup below.
3. Reboot the machine that hosts the probe, or mediation engine and probe.

Uninstalling DPDK

This section describes the instructions for uninstalling DPDK. To uninstall DPDK:

- Run the following commands:

```
source /opt/oracle/ocsm/ocsm_env.sh  
/opt/oracle/ocsm/usr/share/pld/rat/configure_dpdk.py --remove
```

Installing and Configuring DPDK with Internet

This section describes the procedure for installing and configuring DPDK for Session Monitor.

Note:

You must be connected to the internet before starting the installation. Running the following command installs, downloads the required files, and configures the DPDK automatically.

For DPDK installation, for Oracle X7-2 server has the following pre-requisite:

1. Create a file, `/opt/oracle/ocsm/etc/iptego/white_list_dpdk.local` with the value **i40e** before triggering DPDK installation.
1. Log into the Platform Setup Application page.
2. Select **Capture Settings**.
3. Check the box in **Monitoring** column against each sniffing interface that you want to use for capturing the traffic.
4. Log into the machine that hosts the probe or mediation engine and probe as a root user.
5. (Optional) For better understanding of the network, CPU, and NUMA nodes of the server, you can run the following command to review the output of the `system_layout.py` script. It will display system information:

```
source /opt/oracle/ocsm/ocsm_env.sh
/opt/oracle/ocsm/usr/share/pld/rat/system_layout.py
```

6. Run the following commands which guides you through the installation:

```
source /opt/oracle/ocsm/ocsm_env.sh
/opt/oracle/ocsm/usr/share/pld/rat/configure_dpdk.py
```

The `configure_dpdk.py` script downloads and installs the required DPDK driver, the corresponding Kernel headers required for compiling DPDK driver, compiles, installs the driver, and creates server and Session Monitor DPDK related configuration.

7. (Optional) To view all the available advanced options, run the following command:

```
/opt/oracle/ocsm/usr/share/pld/rat/configure_dpdk.py -h
```

Installing and Configuring DPDK Without Internet

DPDK can be installed and configured without an internet connection.

1. Log into the Platform Setup Application page.
2. Select **Capture Settings**.
3. Check the box in **Monitoring** column against each sniffing interface that you want to use for capturing the traffic.
4. Log into the machine that hosts the probe or mediation engine and probe as a root user.
5. (Optional) For better understanding of the network, CPU, and NUMA nodes of the server, run the `system_layout.py` script to display system information.

```
source /opt/oracle/ocsm/ocsm_env.sh
/opt/oracle/ocsm/usr/share/pld/rat/system_layout.py
```

6. Run the following command:

```
yum install kernel-uek-devel-$(uname -r)
```

7. Download the DPDK tar file from <http://git.dpdk.org/dpdk/refs/> into the folder `/var/cache/ocsm/dpdk/`.

8. Run the following commands as a root user:

```
source /opt/oracle/ocsm/ocsm_env.sh
/opt/oracle/ocsm/usr/share/pld/rat/configure_dpdk.py
```

9. (Optional) To view all the available advanced options, run the following command:

```
/opt/oracle/ocsm/usr/share/pld/rat/configure_dpdk.py -h
```

Upgrading Session Monitor without an Internet Connection

If your OCSM server is located on an isolated network that does not have a direct connection to the internet, set up a repo server on that same network using the procedure in the *Downloading the RPMs* section and the *Configuring a Repo Server* section of the *Installation Guide*.

1. Log in to the OCSM node as the root user
2. Confirm the `baseurl` parameter in the `/etc/yum.repos.d/ocsm.repo` file points to the IP address of the repo server on the same network as the OCSM server.

```
[OCSM]
name=OCSM dependencies
baseurl=ftp://<REPO_SERVER_IP>/pub/ocsm/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=0
enabled=1
proxy=_none_
```

3. Clean the repo details in the client.

```
yum clean all
```

4. Verify the repo list.

```
[root@ocsm]$ yum repolist
Loaded plugins: ulninfo
repo id repo name status
OCSM OCSM dependencies 89
repolist: 89
```

5. Log into the OCSM web interface.
6. Navigate to **Software Version**.
7. Select the RPM file to update.
8. Click **Apply** to start the upload.
9. Click **Install** to start the upgrade.

Post Upgrade

After upgrading the system, complete the following steps.

Certificate Exchange

Before logging into the system, exchange certificates between the Mediation Engine (ME) and the Mediation Engine Connector (MEC). See the "Connecting Mediation Engine with Mediation Engine Connector" section in the MEC User Guide.

External Authentication

Post the upgrade, it is mandatory the pld.conf template from `/opt/oracle/ocsm/etc/httpd/conf.d/pld.conf` to `/etc/httpd/conf.d/` folder and configure External Authentication details. This ensures new fixes and any changes in the pld.conf template to be applied on the system.

2

Upgrading MySQL

This chapter provides the instructions for upgrading MySQL.

The upgrade paths are:

- From release 5.5.54 to 5.7.35
- From 5.7.10/5.7.24 to 5.7.35

Upgrading MySQL from Release 5.5.54 to Release 5.7.35

Note:

Session Monitor version 5.0 supports MySQL 5.5.54, 5.7.10, 5.7.24 and 5.7.35 versions. If you have upgraded from a previous Session Monitor version, your system will be running MySQL 5.5.

Upgrading MySQL will not create any loss of data. But all the services will be stopped during this upgrade. The upgrade time depends on the size of the database.

Note:

Before upgrading MySQL, configure yum proxies and repos as yum must connect to the configured repos. Refer to "Configuring Proxies and Repos".

To upgrade to MySQL 5.7.35 for the latest performance updates and improvements, perform the following steps in the maintenance window:

1. Log in to the Session Monitor server console as the root user and run the following command to load the environment variables.

```
source /opt/oracle/ocsm/ocsm_env.sh
```

2. Stop the Session monitor services.

```
pld-systemctl stop
```

3. From MOS, download the below patch from Patches and Updates section:

p33133319: MySQL Database 5.7.35 RPM for Oracle Linux / RHEL 7 x86 (64bit)

4. Download the zip file p33133319_570_Linux-x86-64.zip and place it under /root or any directory on the system.

5. Unzip the file.

```
[root@ocsm ~]# unzip p33133319_570_Linux-x86-64.zip
```

6. Install all the rpms extracted from the zip file.

```
yum install -y mysql-commercial*.rpm
```

7. Complete all the MySQL table migrations from release 5.5 to the latest release 5.7.35.

```
mysql_upgrade
```

This command may take some time to complete depending on the DB size.

8. Once complete, run the following command to move MySQL configuration file, **my.cnf**:

```
cp /opt/oracle/ocsm/etc/iptego/my-5.7.cnf /opt/oracle/ocsm/etc/iptego/my.cnf
```

9. Restart the mysqld service.

```
systemctl restart mysqld.service
```

10. Start the Session Monitor services.

```
pld-systemctl start
```

11. (Optional) Verify the MySQL version installed.

```
mysql --version
```

Upgrading MySQL from Release 5.7.10/5.7.24 to Release 5.7.35

Note:

Session Monitor version 5.0 supports MySQL versions 5.5.54, 5.7.10, and 5.7.24. 5.7.35.

Upgrading MySQL will not create any loss of data. But all the services will be stopped during this upgrade. The upgrade time depends on the size of the database.

Note:

Before upgrading MySQL, configure yum proxies and repos as yum must connect to the configured repos. Refer to "Configuring Proxies and Repos".

To upgrade to MySQL 5.7.35 for the latest performance updates and improvements, perform the following steps in the maintenance window:

1. Log in to the Session Monitor server console as the root user and run the following command to load the environment variables.

```
source /opt/oracle/ocsm/ocsm_env.sh
```

2. Stop the Session monitor services.

```
pld-systemctl stop
```

3. From MOS, download the below patch from Patches and Updates section:

Patch 33133319: MySQL Database 5.7.35 RPM for Oracle Linux / RHEL 7 x86 (64bit)

4. Download the zip file `p33133319_570_Linux-x86-64.zip` and place it under `/root` or any directory on the system.
5. Unzip the file.

```
[root@ocsm ~]# unzip p33133319_570_Linux-x86-64.zip
```

6. Install all the rpms extracted from the zip file.

```
yum install -y mysql-commercial*.rpm
```

7. Complete all the MySQL table migrations from release 5.5 to the latest release 5.7.35.

```
mysql_upgrade
```

This command may take some time to complete depending on the size of the database.

8. Restart the mysqld service.

```
systemctl restart mysqld.service
```

9. Start the Session Monitor services.

```
pld-systemctl start
```

10. (Optional) Verify the MySQL version installed.

```
mysql --version
```