Oracle® Communications Session Monitor

Installation Guide

Release 6.1

G41876-03

December 2025

Oracle Communications Session Monitor Installation Guide, Release 6.1

G41876-03

Contents

About This Guide

Revision History

1 Overview of Session Monitor Installation

Session Monitor System Architecture 1

About Installing Session Monitor 2

Session Monitor System Requirements 2

Network Monitoring Modes 2

2 Installing Session Monitor Using the My Oracle Support Website

Installing Session Monitor - Using MOS, with Internet Connectivity 1

- Installing Session Monitor Using the Zip File Downloaded from the MOS Website 1
  - Verifying the Contents of the Session Monitor Installation Bundle 2
  - Installing Session Monitor Software 3
  - Creating a Separate Partition for Data Storage and MySQL Storage 3
  - Enabling SELinux 5
  - Disabling SELinux 5
  - Adding Ports in the SELinux Port List 6
  - Troubleshooting Tips 6
- Configuring Proxies and Repos 7
- Configuring Reverse Proxy Server 7
- Session Monitor Post-Installation Tasks 8
  - About the Platform Setup Application 8
  - Virtual Machine Probe Cloning 13

Installing Session Monitor in an Offline Mode - Using the MOS Website 13

- Downloading Dependent RPMs on a Linux Machine with Internet Connectivity 14
- Installing Session Monitor using Method 1 15
- Installing Session Monitor using Method 2 17
- Tasks to be Performed after Session Monitor Installation - Offline 18
- Enabling SELinux - Offline 20

Disabling SELinux - Offline 21
Adding Ports in the SELinux Port List 21
Dependency RPMs 21

3 Installing Session Monitor Using the OSDC Website

Installing Session Monitor - with Internet Connectivity Using the OSDC Website 1
Downloading the Software from the Oracle eDelivery Website (OSDC) 1
Verifying the Contents of the Session Monitor Installation Bundle 2
Installing Session Monitor - Online 3
Configuring Proxies and Repositories 4
Creating a Separate Partition for Data Storage and MySQL Storage 5
Tasks to be Performed after RPM Installation 5
Enabling SELinux 6
Disabling SELinux 7
Adding Ports in the SELinux Port List 8
Troubleshooting Tips 8
Installing Session Monitor in an Offline Mode - Using the OSDC Website 9
Download Dependent RPMs on a Linux Machine with Internet Connectivity 9
Installing Session Monitor using Method 1 10
Installing Session Monitor using Method 2 12
Tasks to be Performed after Session Monitor Installation - Offline 13
Enabling SELinux - Offline 15
Disabling SELinux - Offline 16
Adding Ports in the SELinux Port List 16
Troubleshooting Tips 16

4 Configuring Session Monitor

About the Platform Setup Application 1
Platform Setup Application Initial Log In 1
Changing Your Password 1
Restarting or Powering Off Session Monitor 1
STIR/SHAKEN Monitoring 2
Enabling STIR/SHAKEN Support 2
Enabling the UCaaS CCaaS Extension 3
Selecting the Machine Type 4
Configuring Session Monitor 6
Mediation Engine Connection List 7
Typical Connection Scenarios 8
Secure Configuration 10
Server Certificate 10

Server Certificate 10
Trusted Certificates 14
Configuring the SMTP Settings 14
Setting Up the Mail Server 14
Setting Up the Email Notifications 14
Configuring the Capture Settings 15
Data Retention 15
Installing the Products 17

5 Session Monitor Post-Installation Tasks

Installing Software Update 1
Media Protocols 1
Filters 2
Status 2
Signaling Protocols 2
Packet Deduplication 3
Statistics per Protocol 3
Global Statistics 4
System Diagnostics 4
Creating a Report 4
Report Contents 4
Filter Syntax 5
Support for Backup and Restore 5

6 Configuring LDAP and RADIUS Authentication

Configuring External Authentication for Session Monitor with Radius Service 1
Troubleshooting External Authentication Issues for RADIUS on an SELinux Machine 1
Configuring Apache for Authenticating with RADIUS Server 1
RADIUS pld.conf File Details 5
Configuring RADIUS authentication over TLS (RadSec) 5
Getting Ready to Configure RadSec 6
Install the Module Files 7
Internal RADIUS Authentication (via nginx) 11
External Authentication Using RADIUS (via apache httpd) 12
Configure OCOM IP on the RadSec-enabled RADIUS Server 13
Enabling RadSec on FreeRADIUS Server 13
Support for Fail-Over 14
Logging 14
Configuring Apache for Authenticating with LDAP Service 15
pld.conf File Details 18

Configuring Secure LDAP (LADPS) Support 18

7 Installing and Configuring DPDK for Session Monitor

System Requirements 1
Hardware Requirements 2
Software Requirements 2
Installing and Configuring DPDK with Internet 2
Installing and Configuring DPDK without Internet 4
Updating DPDK 5
DPDK with Higher Throughput 6
Loading the igb_uio Module 6
Uninstalling DPDK 8

8 Downloading, Installing, and Configuring DPDK for Mellanox NIC Cards

Installing DOCA OFED 1
Installing and Configuring DPDK 2

9 Installing Skype for Business Agent

Overview 1
Pre-requisites 1
Installing Skype for Business Agent 1
Uninstalling Skype for Business Agent 2
Editing Mediation Engine Host Address 2
Configuring Skype for Business Agent for Monitoring Call Quality Information 3
Troubleshooting 4
Problems with Viewing Skype Call Data Information 4

10 Public Cloud Platforms

Create and Deploy Session Monitor on OCI 1
Deployment Checklist 1
Security Objects 2
Minimum Recommended Shapes 2
Deployment on OCI 3
Create and Deploy Session Monitor on Azure 5
Prerequisites to Azure Deployment 5
Deploying the Azure Instance 6
Creating a VM Instance for Azure Deployment 6
Azure Instance Deployment - Basics Configuration 6

Virtual Machines for Azure Deployment 6
Providing the Administrator Account Information 7
Inbound Port Information 7
Specifying Disk Options 7
Network Configuration 8
Completing the Instance Creation 8
Resizing the Root File System 9
Port Numbers for Importing Traffic 9
Changing Public and Private IP Address from Dynamic to Static 9
Create and Deploy Session Monitor on AWS 10
Prerequisites for AWS Deployment 10
Deploying the AWS Instance 11
Creating a VM Instance for AWS Deployment 11
Basic Configuration 11
Security Objects 12
Virtual Machines for AWS Deployment 13
Providing the Administrator Account Information 13
Configuring Network 13
Configure Storage 14
Completing the Instance Creation 15
Create and Deploy Session Monitor Session Monitor on GCP 15
Prerequisites for GCP Deployment 15
Deploying the GCP Instance 15
Security Objects 15
Virtual Machines for GCP Deployment 16
Completing the Instance Creation 16

A Palladion Ports Usage

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

Documentation Set

Table 1 Documentation Suite for Session Monitor Release 6.1

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.
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 Release 6.1, 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 2025	Initial Release. Includes documentation for new and enhanced features in the Oracle Communications Session MonitorRelease 6.1.

1

Overview of Session Monitor Installation

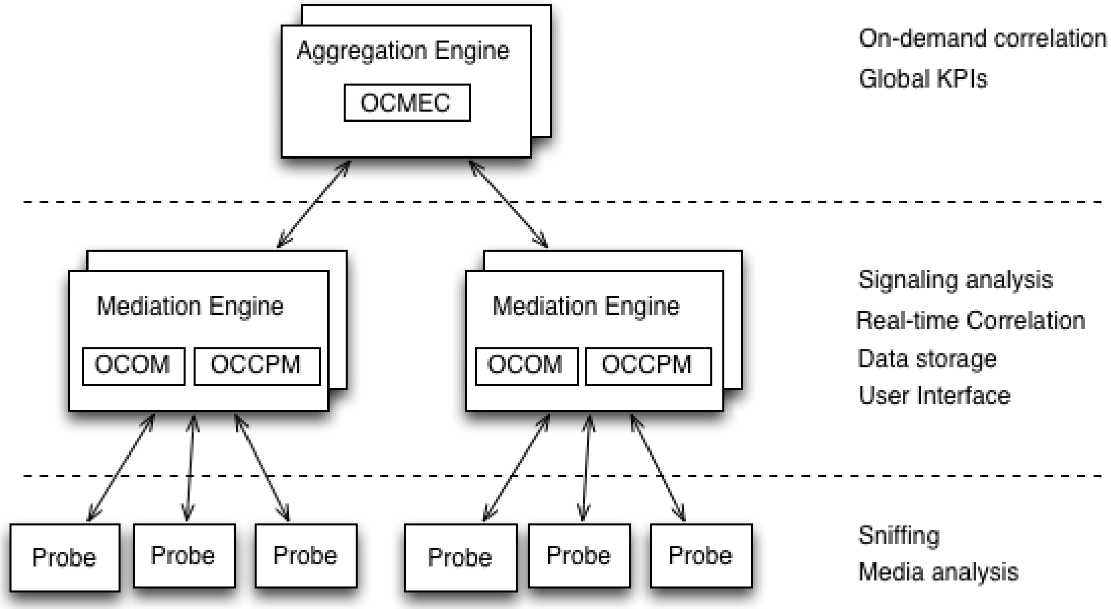
This chapter provides an overview of the Oracle Communications Session Monitor system architecture and the installation process.

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 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 Mediation Engine per geographical site. It is possible, however, to have the probes from multiple geographical sites sending the traffic to a single Mediation Engine. It is also possible to have multiple Mediation Engine installations in the same geographical site.
- **Aggregation Engine layer:** This layer is responsible for aggregating the global KPIs from all the Mediation Engine linked to it, and for the global search features. In a typical setup, there is only one AE for the whole network.



In the diagram above, acronyms have been used for the following products:

Table 1-1   Acronyms

Acronym	Product Name
OCCPM	Oracle Communications Control Plane Monitor
OCMEC	Oracle Communications Mediation Engine Connector
OCOM	Oracle Communications Operations Monitor
OCSM	Oracle Communications Session Monitor

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 Mediation Engine layer on the same physical hardware. The Aggregation Engine layer always requires its own hardware.

From the Session Monitor products perspective, the Operations Monitor and the Control Plane Monitor run on the Mediation Engine while the Mediation Engine Connector runs on the Aggregation Engine.

About Installing Session Monitor

The installation of Session Monitor includes these steps:

1. Reviewing the system requirements and selecting the hardware that is needed.
2. Using the Session Monitor Installer to do the software installation.
3. Using the Platform Setup Application for initial system configuration.

Session Monitor System Requirements

Before installing Session Monitor, ensure that partitions and disk size for the data (block) storage and MySQL storage are as per the desired retention period. It is recommended to complete a sizing exercise with assistance from your Oracle sales engineer.

Session Monitor System Requirements are found in the Release Notes.

Network Monitoring Modes

Session Monitor probes can use two modes of monitoring network mode:

- **mmpcap:** The **mmpcap** mode is based on the **libpcap** Packet Capture Library similar to **tcpdump**, using the Kernel's Packet Socket Interface. The network interface is set to promiscuous mode.
- **Data Plane Development Kit (DPDK):** DPDK is a set of data plane libraries and network interface controller drivers for fast packet processing. In this mode, the network interface is no longer accessible by the Kernel. You can find more information regarding the DPDK libraries in the website, http://dpdk.org.

By default, the installer enables the **mmpcap** mode which is recommended for small to medium installations (for up to 1400K pps depending on server capabilities). For higher network traffic solutions, you may choose to enable **DPDK** mode for better performance. For more information on DPDK, see Installing and Configuring DPDK for Session Monitor.

> **Note**
>
> The above number is only for reference. The actual decision on when to use DPDK depends on many factors. For consulting regarding this decision, Oracle recommends to complete a sizing exercise together with your Oracle sales engineer.

2 Installing Session Monitor Using the My Oracle Support Website

This section shall be used in the case that you want to install Session Monitor after downloading the Zip files from the My Oracle Support (MOS) website.

Topics:

- Installing Session Monitor from MOS with internet connectivity
- **Installing Session Monitor in an Offline Mode - Using the MOS Website**

Installing Session Monitor - Using MOS, with Internet Connectivity

This chapter describes how to install Session Monitor using the My Oracle Support Website, and with an internet connectivity.

> **Note**
>
> If you need separate partitions for data (block) storage and MySQL storage, see the section Creating a Separate Partition for Data and MySQL Storage.

Before installing Session Monitor, read the following:

- About Installing Session Monitor
- Session Monitor System Requirements

Installing Session Monitor Using the Zip File Downloaded from the MOS Website

This section describes installing the Session Monitor using Zip file downloaded from the My Oracle Support (MOS) website.

You have to set up the machine with Oracle Linux 9.6 operating system to install Session Monitor using the Zip file. Configurations are necessary for proxies and repos, if there are any, see Configuring Proxies and Repos.

To install Session Monitor using the Zip file:

1. Verify that the system hosting the Session Monitor is connected to the Internet.
2. Log on to the Session Monitor server as the root user or root privileged user.
3. Run this command to verify that Oracle Linux 9.6 has been installed.

   ```
   cat /etc/oracle-release
   ```

4. Install the Kernel version 5.15.0-302.167.6.
   a. Enable the ol9_UEKR7 repository:

      ```
      dnf config-manager --set-enabled ol9_UEKR7
      ```

   b. Install the kernel:

      ```
      dnf install -y kernel-uek-5.15.0-302.167.6.el9uek.x86_64
      ```

   c. Verify the grub configuration and check that the installed kernel is listed:

      ```
      grubby --info=ALL | grep -E "^kernel|^index"
      ```

   d. Set the default kernel:

      ```
      grubby --set-default=/boot/vmlinuz-5.15.0-302.167.6.el9uek.x86_64
      ```

   e. Reboot the system:

      ```
      reboot
      ```

   f. Verify the kernel version after reboot: uname -a
5. Once the VM or Server is up and running with 5.15 kernel, uninstall 6.x kernel and its associated dependencies by executing the following commands:

   ```
   rpm -qa | grep '^kernel-uek' | grep 6.12
   dnf remove <6.12 kernel packages>
   ```

6. If partitioning is required, refer to the section Creating a Separate Partition for Data and MySQL Storage.
7. Download the Session Monitor software:
   a. Create a temporary directory (temp_dir) on the system that hosts the Session Monitor.
   b. Download the software pack for your operating system from the MOS website.
   c. Download the Session Monitor installation software Zip file to temp_dir.
   d. Make sure you have the utility to extract the contents of the installation software Zip file. If you do not have the utility to extract, then install the utility before installing Session Monitor.
   e. Extract the Session Monitor installation software Zip file.

Verifying the Contents of the Session Monitor Installation Bundle

Verify the contents of the Session Monitor installation.zip bundle that you downloaded from the My Oracle Support website (MOS) or Oracle Software Delivery Cloud (OSDC).

Extract the bundle and verify that it has following contents:

1. README.txt
2. meta.nfo
3. ocsm-6.1.0.0.0-RPM-GA.zip
4. other_files/

5. other_files/my-8.0.cnf
6. other_files/ocsm-6.1.0.0.0.revision.txt
7. other_files/mysql-shell-commercial-8.4.6-1.1.el9.x86_64.rpm
8. scripts/
9. scripts/Install_OCSM_Rel_6.1.sh
10. scripts/Upgrade_OCSM_Rel_6.1.sh
11. scripts/Backup and Restore Scripts/
12. scripts/Backup and Restore Scripts/MySQLDeltaUpgrade.sh
13. scripts/Backup and Restore Scripts/backupAndRestoreBlockStorage.sh
14. scripts/Backup and Restore Scripts/backupAndRestoreOtherFiles.sh
15. scripts/Offline_Installation/
16. scripts/Offline_Installation/Download_rpms.sh
17. scripts/Offline_Installation/Offline_OCSM_Installation_Rel_6.1.sh
18. scripts/Offline_Installation/Offline_Repo_OCSM_Rel_6.1.sh
19. scripts/Offline_Installation/Offline_Repo_Server_preparation_Rel_6.1.sh
20. scripts/Offline_Installation/Offline_Upgrade_OCSM_Rel_6.1.sh

Installing Session Monitor Software

To install Session Monitor software:

1. Go to the directory where the Session Monitor Zip file is extracted and ensure that the installation script has the executable permission. If not, then set the execute permission using this command:

   ```
   chmod +x ./scripts/Install_OCSM_Rel_6.1.sh
   ```

2. Install the Session Monitor and its dependencies using this command:

   ```
   ./scripts/Install_OCSM_Rel_6.1.sh ocsm-<rn>-RPM-GA.zip
   ```

   > **Note**
   >
   > In this command, <rn> is the latest Session Monitor release number. For example, `ocsm-6.1.0.0.0-RPM-GA.zip`.

Creating a Separate Partition for Data Storage and MySQL Storage

Perform the following tasks to create a separate partition for data (block) storage and MySQL Storage

The following partitioning options are available:

- Single partition (default option)
- Secondary partition for data and MySQL storage

Perform the following tasks to create the partition for data storage MySQL Storage.

1. Run the following command to create a directory to mount the partition:

   ```
   mkdir -pv /opt/oracle/ocsm/var/vsi
   mkdir -pv /var/lib/mysql
   ```

2. Adjust /etc/fstab to mount the data storage partition. For example:

   ```
   For example,this entry may vary based on the environment:
   LABEL=PLD_DATA /opt/oracle/ocsm/var/vsi xfs
   defaults,nosuid,nodev,nofail 0 2
   LABEL=MYSQL_DATA /var/lib/mysql xfs
   defaults,nosuid,nodev,nofail 0 2
   ```

   During the MySQL and Session Monitor installation, partitions are detected by the product and the system uses these separate partitions.

Tasks to be Performed after Session Monitor Installation from the .Zip File

Perform the tasks given here after the Session Monitor installation.

1. Verify the installation by doing the following:
   a. Navigate to /var/log/.
   b. Verify whether the following log file exists: `ocsm_installed_*.log`
   c. Navigate to /var/log/ directory and verify that the file `ocsm_zip_install.log` is present.
2. Adjust the firewall to access the Session Monitor applications by doing the following tasks:
   a. Allow firewall to access the HTTPS service (port 443) by running the following command: `firewall-cmd --permanent --zone=public --add-service=https`.
   b. (Optional) If you are planning to configure the system as a Mediation Engine, allow the firewall to access the probe connection by doing these tasks:

      For SBC (embedded) probes:

      ```
      firewall-cmd --permanent --zone=public --add-port=4739/tcp
      firewall-cmd --permanent --zone=public --add-port=4740/tcp
      ```

      For standalone probes:

      ```
      firewall-cmd --permanent --zone=public --add-port=4741/tcp
      firewall-cmd --permanent --zone=public --add-port=4742/tcp
      ```

> **Note**
>
> Please note that the ports 4740/4742 are the preferred ports for connecting to SBC / standalone probes respectively. So, the firewall should be opened for ports 4739/4741 only if you are agree to have non-TLS connections.

3. Reload the configuration by running the following command: `firewall-cmd --reload`

> **Note**
>
> If you are planning to enable additional services, see the discussion about network security in the Oracle Communications Session Monitor Security Guide for a complete list of services and their respective ports.

4. Enable or Disable SELinux as per your requirement. For more information, see Enabling SELinux.

Enabling SELinux

Session Monitor currently supports the following top-level state of SELinux on a system – enforcing, permissive and disabled. The only supported SELinux type is **targeted**.

To enable SELinux:

1. Run the command to set the SELinux mode as **enforcing** and SELinux policy as **targeted**:

   ```
   sed -i -e "s/^SELINUX=.*/SELINUX=enforcing/" /etc/selinux/config
   sed -i -e "s/^SELINUXTYPE=.*/SELINUXTYPE=targeted/" /etc/selinux/config
   ```

2. Reboot the system using the command:

   ```
   reboot
   ```

3. After the reboot, run the command to verify the SELinux status:

   ```
   sestatus
   ```

   Verify the command output:

   ```
   SELinux status:        enabled
   SELinuxfs mount:                /sys/fs/selinux
   SELinux root directory:         /etc/selinux
   Loaded policy name:             targeted
   Current mode:                   enforcing
   Mode from config file:          enforcing
   Policy MLS status:              enabled
   Policy deny_unknown status:     allowed
   Max kernel policy version:      31
   ```

4. Install the customized SELinux policy modules for Session monitor using the command:

   ```
   cd /opt/oracle/ocsm/
   ./ocsm_ext.sh
   ```

Disabling SELinux

Use the following instructions to disable SELinux.

1. Set the SELinux mode as **disabled** using the command as a root user:

   ```
   sed -i -e "s/^SELINUX=.*/SELINUX=disabled/" /etc/selinux/config
   ```

2. Reboot the system using the command:

   ```
   reboot
   ```

3. Verify the SELinux status using the command:

   ```
   sestatus
   ```

4. Verify the output:

   ```
   SELinux status: disabled
   ```

Adding Ports in the SELinux Port List

On a SELinux enabled machine, in order to use any port other than the default ports in the Session Monitor, add the port in the SELinux port list using the following commands.

```
yum install -y setroubleshoot-server
semanage port -a -t <Service_Name> -p <Protocol> <Port_Number>
```

You can view all ports allowed in the SELinux using the command:

```
semanage port -l
```

For example: By default, SELinux allows http to listen on TCP ports 80, 443, 488, 8008, 8009, or 8443.

To configure http to run on a port other than the TCP ports listed above, such as 8001, then add the ports to the SELinux port list using the command:

```
semanage port -a -t http_port_t -p tcp 8001
```

Troubleshooting Tips

Following intructions will be helpful in solving issues in configuring SELinux.

To modify the mode in which SELinux runs in real-time, run the following commands:

Table 2-1 Modifying SELinux Mode

Mode	Command
To run SELinux in **permissive** mode (System prints warnings only but does not enforce SELinux policy)	`setenforce 0`
To run SELinux in the **enforcing** mode (SELinux security policy is enforced)	`setenforce 1`
Verify the status using command	`getenforce`

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 same to environment by doing the following.

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

```
proxy=<Your_Proxy>
```

where, <*your_proxy*> is the proxy server details.

Run the following command to export to the environment:

```
export http_proxy=<Your_Proxy>
export https_proxy=<Your_Proxy>
```

Configuring Reverse Proxy Server

⚠ **Caution**

Configuring reverse proxy server is optional.

The Session Monitor services are available to you through a reverse proxy web server. By default, the Session Monitor comes with a bundled copy of NGINX, the configuration files located at /opt/oracle/ocsm/etc/nginx file. However, you may choose to use another web server, such as Apache. A sample configuration file for Apache 2.4 is located at /opt/oracle/ocsm/etc/httpd/conf.d/pld.conf file.

Run the following commands to install the Apache Web Server and mod_ssl packages:

```
yum install -y httpd mod_ssl
```

After installing Apache, run the following commands to enable Apache as a front-end web server instead of NGINX:

```
systemctl stop pld-nginx.service
systemctl disable pld-nginx.service
ln -sf /usr/lib/systemd/system/{httpd,pld-webserver}.service
cp /opt/oracle/ocsm/etc/httpd/conf.d/pld.conf /etc/httpd/conf.d/
mv /etc/httpd/conf.d/ssl.conf{,.orig}
systemctl daemon-reload
systemctl start httpd.service
systemctl enable httpd.service
```

If you choose to authenticate users at the level of the reverse proxy, you must uncomment the sections in the sample Apache configuration file which configures LDAP or RADIUS authentication for the `/me/` and `/mec/` routes, and modify them as appropriate for your authentication provider. Additionally, you must enable external authentication in the Mediation

Engine and the Mediation Engine Connector. See the discussion on external authentication in the *Operations Monitor User's Guide*.

Session Monitor Post-Installation Tasks

This section provides instructions for the post-installation tasks for Session Monitor.

Before starting the post-installation tasks, verify that Session Monitor installation tasks are completed and all components are installed. See Installing Session Monitor Using the Zip File Downloaded from the MOS Website.

About the Platform Setup Application

The Platform Setup Application guides you through the Session Monitor configuration steps, including configuring the machine type, capture settings, and simple mail transfer protocol (SMTP) settings as follows:

1. Accept the license agreement to proceed with the Platform Setup Application.
2. The menu on the right shows your progress during configuration.
3. The Machine Type page sets which licensed Session Monitor applications are installed. In the Server Certificate page, you can upload your signed certificate for secure HTTPS connections.
4. Subsequent sections configure the Session Monitor server for your network. These steps are optional.
   Except for **Machine Type** and **Extensions**, you can review and change settings at any time by visiting the Platform Setup Application at **https://** *ip_address* **/setup/**, where *ip_address* is the IP address of the server that hosts a Session Monitor application. This URL is valid for any Session Monitor server.
5. In the final step, each selected Session Monitor application is installed.

After a successful installation, the log in page appears for each of your licensed Session Monitor application.

Platform Setup Application Initial Log In

All Session Monitor application interfaces are accessed through encrypted HTTPS connections. At the initial login, your web browser may not recognize the server and displays the warning: This Connection is Untrusted. Click **Confirm Security Exception** to proceed.

For information about how to protect connections to the system and avoid the untrusted certificate warning in the future, see Oracle Communications Session Monitor Security Guide.

This section describes how to configure Session Monitor using the Platform Setup Application.

To configure Session Monitor:

1. In a web browser, go to https://<ip_address>/setup.

   The **Platform Setup Application Login** page appears.
2. In the **Username** field, enter **sysadmin** and in the **Password** field, enter **oracle**.

   The License Terms agreement page appears.
3. Accept each Session Monitor application license terms agreement, by selecting the **I agree to the license terms** check box.
4. Click **Proceed**.

The **Change Password** dialog box appears.

The **Platform Setup Application** page appears.

5. Change the password by doing the following:
   a. In the **Set password** field, enter a new password.

      > ⓘ **Note**
      >
      > The password must have at least 8 characters. The password must contain at least one uppercase character. The password must contain a number. The password must contain a special character (@, #, -, _, .).

   b. In the **Repeat password** field, re-enter the password used in the previous step, which verifies that the password value was entered correctly.
   c. Click **Change**.

   The **Machine Type** page appears.

6. On the Machine Type page, select the machine type on which to install your licensed Session Monitor applications and components:
   - To install an Operations Monitor probe, select **Probe**.
   - To choose different Session Monitor applications, select the **Mediation Engine** and then select the required product (or applications) as per the license:
     - To install Operations Monitor, select the **Operations Monitor** check box.
     - To install Oracle Communications Control Plane Monitor, select the **Control Plane Monitor** check box.
     - To install an Operations Monitor embedded probe, select the **Probe (embedded)** check box.
     - To install Mediation Engine Connector, select the **Mediation Engine Connector** check box.

   Only the checked items are included in the installation.

   > ⓘ **Note**
   >
   > The Machine Type page only appears the first time you configure Session Monitor prior to the products installation. Machine type cannot be changed after the PSA installation is completed.
   >
   > You can select only one machine type for each installation process.
   >
   > Packet Inspector probe is not supported on a Session Monitor probe with SIP/RTP sniffing for the calls and VQ analysis.
   >
   > The products are machine-type specific and cannot be interchanged between machine types.
   >
   > For example, the Probe machine type requires a probe product, and the Mediation Engine machine type requires the Operations Monitor product.
   >
   > The machine type Mediation Engine Probe (embedded) must be chosen either with Operation Monitor or with Control Plane Monitor option selected.

7. Click **Continue**.

The machine type and application information appear in the status panel located on the right under the navigation list.

The **Configuration** page appears.

8. Configure the Session Monitor settings for the machine type you chose in step 5 in accordance with the terms of your license as follows:

   a. From the Capacity section in the Concurrent calls field, enter the number of concurrent calls printed on your license.

   b. If you have licensed RTP recording, select the RTP Recording check box.

   c. From the Capacity section in the Concurrent RTP streams field, enter the number of concurrent RTP streams printed on your license.

      > **Note**
      >
      > The number entered in the Concurrent RTP streams field can cause performance and stability issues if it is set higher than what your network hardware supports. Values above 20 are not recommended. Changes to the RTP recording setting take effect only after restarting the system.

   d. In the Additional Extensions section, select the **Non Calls** check box to see the Subscription panels in the user interface. You can edit this check box even after the installation is done.

   e. From the Extensions section, select all the product extensions you have licensed.

      > **Note**
      >
      > You cannot change the configured extensions after the installation. All Oracle Communications Session Monitor Enterprise users should select Media quality .

9. Click **Continue**.

   The Disk Usage page appears.

10. On the Disk Usage page, specify the maximum disk usage partition for the Packet Inspector.

    > **Note**
    >
    > On the Disk Usage page, specify the maximum disk usage partition for the shared file system containing the database/data storage (single raid systems). For systems with two raid arrays you can select the usage independently for both filesystems. For Probes with Packet Inspector feature you would be able to select the maximum storage capacity.

    The Mediation Engine Connection List page appears.

> **Note**
>
> The **ME Connection List** page appears only if you have selected machine type as Probe or Mediation Engine with Probe.

11. (Optional) If you selected Probe on the Machine Type page, set which mediation engines are connected to the Operations Monitor probe.

    a. Click **Add a new ME**.

    b. In the Hostname or IP field, enter the IP address of the machine that hosts the mediation engine.

    c. In the Port field, enter the port number of the mediation engine. For a Cleartext transmission enter 4741 and for TLS enter 4742.

    d. In the Name field, enter a name for the mediation engine.

    e. In the TLS field, select the check box for TLS transmissions or leave the check box unchecked for Cleartext.

       The Operations Monitor Probe can transmit data to one or more mediation engines with either transport layer security (TLS) encryption, or with un-encrypted Cleartext. A mediation engine can connect to more than one Operations Monitor Probe or more than one Session Border Controller Probe.

> **Note**
>
> Oracle recommends using TLS for connections between Standalone Probes and the Mediation Engine.

12. Click **Continue**.

    The Trusted Certificate page appears.

13. In the **Upload a trusted certificate** field, select **Browse** and locate the signed certificate file. Click **Continue**.

    (Optional) By default, the mediation engine machine accepts only encrypted transmissions, (unless the mediation engine and probe are on the same machine); for Cleartext transmissions select the **Accept insecure connections from remote probes** check box.

    Click **Continue**.

    The Server Certificate page appears.

14. All Session Monitor interfaces are accessed through encrypted (secure) HTTPS connections. Each Session Monitor machine uses a unique certificate to establish secure connections and to guarantee its authenticity and protect users' data.

    Do one of the following:

    - To use the self-signed certificate, click **Continue**.
    - To sign the server certificate with your organization's Public Key Infrastructure (PKI):

      a. Select **Download request**.

      b. Sign the certificate with the X.509 format.

      c. In the **Upload signed certificate** field, select **Browse** and locate the signed certificate file.

d. Click **Continue**. The SMTP Configuration page appears.

> **Note**
>
> - To regenerate a key and certificate on install, select **Regenerate key and self-signed certificate on install** and click **Continue**.
> - (Optional) Click **Download current certificate** to download the current self-signed certificate.

15. Session Monitor can send notifications and alerts directly to a user's email address. If you require notifications or alerts, select the Enable SMTP check box and fill in the relevant fields with your SMTP server details.
16. Click **Continue**.

    The Capture Settings page appears.
17. The **Capture Settings** page contains a list of configured network interfaces. Monitoring can be enabled and disabled. You should have configured network devices while installing Oracle Linux 8.
18. Click **Continue**.

    The Data Retention page appears. If you have enabled the **Non Calls** check box in the Configuration > Additional Extensions section, only then the Subscription Data - Subscriptions is enabled.
19. Click **Continue**.

    The Install page appears.
20. (Optional) Click **Download Configuration**, which downloads your configuration settings file in the default download location of your system.
21. Open the **psa_conf.json** configuration file and verify your settings.
22. Click **Install**.

    The **Did you select the right applications** dialog box appears.
23. Verify that you have chosen the correct Session Monitor applications and components for installation; after installation is complete, the selected applications and components cannot be changed.

    Click **OK**.

    The Platform Setup Application initiates the installation and reports its progress.

    The Installation Complete dialog box appears.
24. Do one of the following:
    - To go back to the Platform Setup Application, click **Back to Setup**.
    - To go to a Session Monitor application dashboard, click **Go to Application**.
25. The credentials for logging in to Session Monitor are:
    - For Platform Setup Application, enter the user name provided by Oracle and the password you set up in step 5.
    - For Operations Monitor and Control Plane Monitor, enter the login credentials provided by Oracle Sales Consultant.

Virtual Machine Probe Cloning

A cloned probe is an exact replica of the original probe having the same UUID as the original probe. However, each probe requires a unique UUID to establish a connection with the Mediation Engine. If the Probe Virtual Machine has been cloned, you must change the Unique ID of the probe after cloning and before connecting the cloned probe. Follow the instructions after cloning the probe to generate random UUID.

Ensure that the following prerequisites are taken care of:

- Cloning of the probe has been successful.
- Cloned probe is not connected to the Mediation Engine. If it was connected, remove:
  - Mediation Engine details on the probe
  - Probe details on the Mediation Engine

1. Check for the UUID of both the probes under:

   ```
   /opt/oracle/ocsm/etc/iptego/psa/probe_uuid.conf
   ```

2. Run the script to change the UUID of cloned probe:

   ```
   /opt/oracle/ocsm/usr/share/pld/scripts/write_rapid_uuid.sh
   ```

3. Check the UUID and make sure that the UUID of the cloned probe has been changed after running the script in the `probe_uuid.conf` file
4. Connect the cloned probe to the Mediation Engine and make sure that the connection is successful.

> **Note**
>
> Connect the cloned probe to the Mediation Engine only after changing the UUID. The cloned probe newly connected to the Mediation Engine must be of the same version as the Mediation Engine. For example, if the Mediation Engine is on Release 6.1 version, then the probe version must also be Release 6.1 version.

Installing Session Monitor in an Offline Mode - Using the MOS Website

This chapter describes how to install Oracle Communications Session Monitor without an internet connection with files downloaded form the MOS website.

ⓘ **Note**

This procedure was tested on:

- Oracle Linux 9.6
- MySQL 8.4.6
- MySQL Connector 8.4.0

The versions of Dependency RPMs used in this procedure are the latest available versions at the time of this release based on Oracle Linux 9.6, MySQL 8.4.6, and the RPM file for the Session Monitor Release 6.1.0.0.0. Use the latest version of dependency RPMs for all future patch releases based on the Oracle Linux, and Session Monitor RPM used.

You can install Session Monitor in an offline mode using any one of the methods listed here:

- **Method 1**: Session Monitor node acts as the repo server.
- **Method 2**: A separate node acts as the repo server.

Session Monitor installation requires a temporary repo server to resolve the package dependencies. Henceforth, this server will be referred to as the Repo server in this document.

The Repo server can be a part of the Session Monitor node itself (Method 1) OR it can be separate node (Method 2). If it is a separate node, the Session Monitor node must be able to reach the Repo server.

If it is a separate node, the Session Monitor node must be able to reach the Repo server. In both methods, it is assumed that as Session Monitor node does not have an internet connectivity, so the dependency RPMs and packages would be first downloaded on a machine which has the internet connectivity.

⚠ **Caution**

Install the Session Monitor node with Oracle Linux 9.6.

Downloading Dependent RPMs on a Linux Machine with Internet Connectivity

Follow instructions in this section to download dependent RPMs on a Linux machine with internet connectivity. This Linux system should have 5 GB to 10 GB free disk space in the `/tmp` folder. Session Monitor.

1. Log in to the Linux machine as a root user OR root privileged user.
2. If the /tmp/ocsm folder already exists, take a backup of the /tmp/ocsm folder if required and delete the folder /tmp/ocsm.
3. Create a folder in /tmp/ocsm.

```
mkdir /tmp/ocsm
```

4. Copy the Session Monitor software Zip file, which is downloaded from My Oracle Support (MOS) or Oracle Software Delivery Cloud (OSDC) website, under the `/tmp/ocsm` folder on the Linux System.
5. Install the unzip package if not installed already.

   ```
   yum install -y unzip
   ```

6. Change to folder /tmp/ocsm.

   ```
   cd /tmp/ocsm
   ```

7. Unzip the software ZIP file which is copied here. For example:

   ```
   unzip ocsm-6.1.0.0.0-GA.zip
   ```

8. Execute below steps to copy the Offline installation scripts to /tmp/ocsm folder.

   ```
   cp -rf scripts/Offline_Installation/* /tmp/ocsm/
   ```

9. Set execute permission as:

   ```
   chmod +x Download_rpms.sh
   ```

10. Run the following command to download the script:

    ```
    ./Download_rpms.sh
    ```

    If you need to configure a proxy server for your system, run the same command with the following information:

    ```
    ./Download_rpms.sh "[PROTOCOL://]HOST[:PORT]"
    ```

    > ⓘ **Note**
    >
    > In the above command:
    >
    > - PROTOCOL is HTTP or HTTPS
    > - HOST is the IP address or FQDN of the proxy server
    > - PORT is the port number for the proxy server

Installing Session Monitor using Method 1

Install Session Monitor using Method 1 where the Session Monitor node acts as the Repo server.

1. Log in to the Session Monitor server installed with Oracle Linux 9.6 as a root user OR root privileged user
2. Ensure that 5 GB to 10 GB free space is available in the `/tmp` folder on this server.
3. If the `/tmp/ocsm` folder is already present, take a backup of the `/tmp/ocsm` folder if required and delete the folder `/tmp/ocsm`.

4. Create the folder `/tmp/ocsm` .

   ```
   mkdir /tmp/ocsm
   ```

5. Transfer the contents of the folder `/tmp/ocsm` from the Linux machine, where you have downloaded all the RPM files and scripts - to the `/tmp/ocsm` folder on the Session Monitor server.
6. Navigate to the folder `/tmp/ocsm` on the Session Monitor server.

   ```
   cd /tmp/ocsm
   ```

7. Install the Kernel version 5.15.0-302.167.6
   a. Install the kernel RPMs in order:

      ```
      rpm -ivh kernel-uek-core-5.15.0-302.167.6.el9uek.x86_64.rpm --oldpackage
      ```

      ```
      rpm -ivh kernel-uek-modules-5.15.0-302.167.6.el9uek.x86_64.rpm --
      oldpackage
      ```

      ```
      rpm -ivh kernel-uek-5.15.0-302.167.6.el9uek.x86_64.rpm --oldpackage
      ```

   b. Verify the grub configuration and check installed kernel is listed:

      ```
      grubby --info=ALL | grep -E "^kernel|^index"
      ```

   c. Set the default kernel:

      ```
      grubby --set-default=/boot/vmlinuz-5.15.0-302.167.6.el9uek.x86_64
      ```

   d. Reboot the system:

      ```
      reboot
      ```

   e. Verify the kernel version after reboot:

      ```
      uname -a
      ```

8. Navigate to the folder /tmp/ocsm on the Session Monitor server:

   ```
   cd /tmp/ocsm
   ```

9. Once the VM or Server is up and running with 5.15 kernel, uninstall 6.x kernel and its associated dependencies by executing the following commands

   ```
   rpm -qa | grep '^kernel-uek' | grep 6.12
   dnf remove <6.12 kernel packages>
   ```

10. Set execute permission as:

    ```
    chmod +x *.sh
    ```

11. Run the following command to install Session Monitor.

    ```
    ./Offline_Repo_OCSM_Rel_6.1.sh
    ```

Installing Session Monitor using Method 2

Install Session Monitor using Method 2 where the Repo server is a separate node. Session Monitor should be able to reach the Repo server.

1. Log in to the Repo server as a root user OR root privileged user and execute Steps 2 to 8.
2. Ensure that 5 GB to 10 GB free space is available in the `/tmp` folder on this server.
3. If the `/tmp/ocsm` folder is already present, take a backup of the `/tmp/ocsm` folder if required and delete the folder `/tmp/ocsm`.
4. Create the folder `/tmp/ocsm` .

   ```
   mkdir /tmp/ocsm
   ```

5. Navigate to the folder `/tmp/ocsm`.

   ```
   cd /tmp/ocsm
   ```

6. Transfer all the contents of the folder `/tmp/ocsm` from the Linux machine - where you have downloaded the RPM files and scripts - to the `/tmp/ocsm` folder on the Repo server.
7. Set execute permission as:

   ```
   chmod +x *.sh
   ```

8. Run the following command to prepare the Repo server.

   ```
   ./Offline_Repo_Server_preparation_Rel_6.1.sh
   ```

9. Log in to the Session Monitor server installed with Oracle Linux 9.6 as a root or root privileged user, and execute Steps 10 to 16.
10. Check if you have 5 GB to 10 GB free space available in the `/tmp` folder on the Session Monitor Server.
11. If the `/tmp/ocsm` folder is already present, take a backup of the `/tmp/ocsm` folder if required, and delete the folder `/tmp/ocsm`.
12. Create the folder `/tmp/ocsm` using this command:

    ```
    mkdir /tmp/ocsm
    ```

13. Transfer all the contents of the folder `/tmp/ocsm` on the Repo server machine to the folder `/tmp/ocsm` on the Session Monitor server.
14. Go to the folder `/tmp/ocsm`.

    ```
    cd /tmp/ocsm
    ```

15. Install the Kernel version 5.15.0-302.167.6:

a. Install the kernel RPMs in order:

```
rpm -ivh kernel-uek-core-5.15.0-302.167.6.el9uek.x86_64.rpm --oldpackage
```

```
rpm -ivh kernel-uek-modules-5.15.0-302.167.6.el9uek.x86_64.rpm --
oldpackage
```

```
rpm -ivh kernel-uek-5.15.0-302.167.6.el9uek.x86_64.rpm --oldpackage
```

b. Verify the grub configuration and check that the installed kernel is listed:

```
grubby --info=ALL | grep -E "^kernel|^index"
```

c. Set the default kernel:

```
grubby --set-default=/boot/vmlinuz-5.15.0-302.167.6.el9uek.x86_64
```

d. Reboot the system:

```
reboot
```

e. Verify the kernel version after reboot:

```
uname -a
```

16. Navigate to the folder /tmp/ocsm on the Session Monitor server:

```
cd /tmp/ocsm
```

17. Once the VM or Server is up and running with 5.15 kernel, uninstall 6.x kernel and its associated dependencies by executing the following commands

```
rpm -qa | grep '^kernel-uek' | grep 6.12
dnf remove <6.12 kernel packages>
```

18. Set the execute permission

```
chmod +x *.sh
```

19. Run the script `./Offline_OCSM_Installation_Rel_6.1.sh <REPO_SERVER_IP>` to install the Session Monitor.

```
./Offline_OCSM_Installation_Rel_6.1.sh <REPO_SERVER_IP>
```

where <REPO_SERVER_IP> is the IP address of the Repo server. For example:

```
./Offline_OCSM_Installation_Rel_6.1.sh 192.168.1.10
```

Tasks to be Performed after Session Monitor Installation - Offline

Perform the tasks provided here, after the RPM installation.

1. Run this command to verify the installation is successful:

   a. Go to the folder `/var/log/ocsm` file.
   b. Verify if the following log file exists: ocsm_installed_*.log

2. Adjust the firewall to access the Session Monitor applications:

   - Run this command to allow the firewall to access the HTTPS service (port 443):

     ```
     firewall-cmd --permanent --zone=public --add-service=https
     ```

   - (Optional) If you are planning to configure the system as a Mediation Engine, allow the firewall to access the probe connection by doing these tasks:

     - For SBC (embedded) probes:

       ```
       firewall-cmd --permanent --zone=public --add-port=4739/tcp
       ```

       ```
       firewall-cmd --permanent --zone=public --add-port=4740/tcp
       ```

     - For standalone probes:

       ```
       firewall-cmd --permanent --zone=public --add-port=4741/tcp
       ```

       ```
       firewall-cmd --permanent --zone=public --add-port=4742/tcp
       ```

     > **Note**
     >
     > The ports 4740 and 4742 are the preferred ports for connecting to SBC / standalone probes respectively. So, the firewall should be opened for ports 4739/4741 only if you are agree to have non-TLS connections.

3. Reload the configuration by running the following command:

   ```
   firewall-cmd --reload
   ```

   > **Note**
   >
   > If you are planning to enable additional services, see the content about network security in the Oracle Communications Session Monitor Security Guide for a complete list of services and their respective ports.

4. Enable or Disable SELinux as per your requirement. For more information, see Enabling SELinux - Offline.

Enabling SELinux - Offline

Session Monitor currently supports the following top-level states of SELinux on a system – enforcing, permissive, and disabled. The only supported SELinux policy type is **targeted**.

To enable SELinux:

1. Run the command to set the SELinux mode as enforcing and the SELinux policy as targeted:

   ```
   sed -i -e "s/^SELINUX=.*/SELINUX=enforcing/" /etc/selinux/config
   ```

   ```
   sed -i -e "s/^SELINUXTYPE=.*/SELINUXTYPE=targeted/" /etc/selinux/config
   ```

2. Reboot the system using the command:

   ```
   reboot
   ```

3. After the reboot, run the command to verify the SELinux status:

   ```
   sestatus
   ```

   - Verify the command output. The output should look like this:

     ```
     SELinux status: enabled
     SELinuxfs mount: /sys/fs/selinuxSELinux root
     directory: /etc/selinux
     Loaded policy name:targetedCurrent
     mode: enforcing
     Mode from config file:enforcing
     Policy MLS status: enabled
     Policy deny_unknown status: allowed
     Max kernel policy version:31
     ```

4. Install the customized SELinux policy modules for Session Monitor using the command:

   ```
   cd /opt/oracle/ocsm/
   ./ocsm_ext.sh
   ```

Disabling SELinux - Offline

Use the following instructions to disable SELinux.

1. Set the SELinux mode as disabled using the command as a root user:

   ```
   sed -i -e "s/^SELINUX=.*/SELINUX=disabled/" /etc/selinux/config
   ```

2. Reboot the system using the command:

   ```
   reboot
   ```

3. Verify the SELinux status using the command:

   ```
   sestatus
   ```

4. Verify the output:

   ```
   SELinux status:disabled
   ```

Adding Ports in the SELinux Port List

On a SELinux enabled machine, in order to use any port other than the default ports in the Session Monitor, add the port in the SELinux port list using the following commands.

1. Run this command that allows SELinux-specific service and adds the port number.

   ```
   yum install -y setroubleshoot-server
   semanage port -a -t <Service_Name> -p <Protocol> <Port_Number>
   ```

2. You can view all ports allowed in the SELinux using the command:

   ```
   semanage port -l
   ```

   For example: By default, SELinux allows HTTP to listen on the TCP ports: 80, 443, 488, 8008, 8009, or 8443.

3. To configure HTTP to run on a port other than the TCP ports listed above, such as 8001, then add the ports to the SELinux port list using the command:

   ```
   semanage port -a -t http_port_t -p tcp 8001
   ```

Dependency RPMs

This section describes the RPMs needed to install Session Monitor without an internet connection.

> **Note**
>
> The versions of Dependency RPMs used in this procedure are the latest available versions at the time of this release based on:
>
> - Oracle Linux 9.6
> - MySQL 8.4.6
> - The RPM file for Session Monitor Release 6.1.0.0.0.

> **Note**
>
> Use the latest versions of dependency RPMs for all future patch releases based on the Oracle Linux, MySQL and OCSM RPM used.

BaseOS Latest: https://yum.oracle.com/repo/OracleLinux/OL9/baseos/latest/x86_64/index.html.

1. pkgconf-m4-1.7.3-10.el9.noarch.rpm
2. libpkgconf-1.7.3-10.el9.x86_64.rpm
3. pkgconf-1.7.3-10.el9.x86_64.rpm
4. pkgconf-pkg-config-1.7.3-10.el9.x86_64.rpm
5. oracle-epel-release-el9-1.0-1.el9.x86_64.rpm
6. unzip-6.0-58.0.1.el9_5.x86_64.rpm
7. dejavu-serif-fonts-2.37-18.el9.noarch.rpm
8. freetype-2.10.4-10.el9_5.x86_64.rpm
9. glibc-2.34-168.0.1.el9.x86_64.rpm
10. libproxy-0.4.15-35.el9.x86_64.rpm
11. libpciaccess-0.16-7.el9.x86_64.rpm
12. freetype-2.10.4-10.el9_5.x86_64.rpm
13. libpng-1.6.37-12.el9.x86_64.rpm
14. graphite2-1.3.14-9.el9.x86_64.rpm
15. cups-libs-2.3.3op2-33.el9.x86_64.rpm
16. avahi-libs-0.8-22.el9_6.x86_64.rpm
17. glibc-2.34-168.0.1.el9_6.19.x86_64.rpm
18. glibc-common-2.34-168.0.1.el9_6.19.x86_64.rpm
19. glibc-gconv-extra-2.34-168.0.1.el9_6.19.x86_64.rpm
20. glibc-langpack-en-2.34-168.0.1.el9_6.19.x86_64.rpm
21. harfbuzz-2.7.4-10.el9.x86_64.rpm

AppStream Latest: https://yum.oracle.com/repo/OracleLinux/OL9/appstream/x86_64/index.html

1. perl-AutoLoader-5.74-481.el9.noarch.rpm

2. perl-Carp-1.50-460.el9.noarch.rpm
3. compat-openssl11-1.1.1k-5.el9_6.1.x86_64.rpm
4. perl-B-1.80-481.el9.x86_64.rpm
5. perl-Class-Struct-0.66-481.el9.noarch.rpm
6. perl-Data-Dumper-2.174-462.el9.x86_64.rpm
7. perl-Digest-1.19-4.el9.noarch.rpm
8. perl-Digest-MD5-2.58-4.el9.x86_64.rpm
9. perl-English-1.11-481.el9.noarch.rpm
10. perl-Errno-1.30-481.el9.x86_64.rpm
11. perl-Exporter-5.74-461.el9.noarch.rpm
12. openssl-devel-3.2.2-6.0.1.el9_5.1.x86_64.rpm
13. perl-Fcntl-1.13-481.el9.x86_64.rpm
14. perl-File-Basename-2.85-481.el9.noarch.rpm
15. perl-File-Copy-2.34-481.el9.noarch.rpm
16. perl-File-Find-1.37-481.el9.noarch.rpm
17. perl-Encode-3.08-462.el9.x86_64.rpm
18. perl-File-Path-2.18-4.el9.noarch.rpm
19. perl-File-Temp-0.231.100-4.el9.noarch.rpm
20. perl-FileHandle-2.03-481.el9.noarch.rpm
21. perl-Getopt-Long-2.52-4.el9.noarch.rpm
22. perl-File-stat-1.09-481.el9.noarch.rpm
23. perl-Getopt-Std-1.12-481.el9.noarch.rpm
24. perl-HTTP-Tiny-0.076-462.el9.noarch.rpm
25. perl-IO-1.43-481.el9.x86_64.rpm
26. perl-IO-Socket-IP-0.41-5.el9.noarch.rpm
27. perl-IO-Socket-SSL-2.073-2.el9.noarch.rpm
28. perl-IPC-Open3-1.21-481.el9.noarch.rpm
29. perl-MIME-Base64-3.16-4.el9.x86_64.rpm
30. perl-JSON-4.03-5.el9.noarch.rpm
31. perl-Math-Complex-1.59-481.el9.noarch.rpm
32. perl-Memoize-1.03-481.el9.noarch.rpm
33. perl-Math-BigInt-1.9998.18-460.el9.noarch.rpm
34. perl-Mozilla-CA-20200520-6.el9.noarch.rpm
35. perl-NDBM_File-1.15-481.el9.x86_64.rpm
36. perl-POSIX-1.94-481.el9.x86_64.rpm
37. perl-Net-SSLeay-1.94-1.el9.x86_64.rpm
38. perl-PathTools-3.78-461.el9.x86_64.rpm
39. perl-Pod-Escapes-1.07-460.el9.noarch.rpm

40. perl-Pod-Perldoc-3.28.01-461.el9.noarch.rpm
41. perl-Pod-Usage-2.01-4.el9.noarch.rpm
42. perl-Scalar-List-Utils-1.56-462.el9.x86_64.rpm
43. perl-Pod-Simple-3.42-4.el9.noarch.rpm
44. perl-SelectSaver-1.02-481.el9.noarch.rpm
45. perl-Socket-2.031-4.el9.x86_64.rpm
46. perl-Storable-3.21-460.el9.x86_64.rpm
47. perl-Symbol-1.08-481.el9.noarch.rpm
48. perl-Term-ANSIColor-5.01-461.el9.noarch.rpm
49. perl-Term-Cap-1.17-460.el9.noarch.rpm
50. perl-Sys-Hostname-1.23-481.el9.x86_64.rpm
51. perl-Text-ParseWords-3.30-460.el9.noarch.rpm
52. perl-Text-Tabs+Wrap-2013.0523-460.el9.noarch.rpm
53. perl-Time-1.03-481.el9.noarch.rpm
54. perl-Time-HiRes-1.9764-462.el9.x86_64.rpm
55. perl-Time-Local-1.300-7.el9.noarch.rpm
56. perl-URI-5.09-3.el9.noarch.rpm
57. perl-base-2.27-481.el9.noarch.rpm
58. perl-constant-1.33-461.el9.noarch.rpm
59. perl-if-0.60.800-481.el9.noarch.rpm
60. perl-interpreter-5.32.1-481.el9.x86_64.rpm
61. perl-libnet-3.13-4.el9.noarch.rpm
62. perl-mro-1.23-481.el9.x86_64.rpm
63. perl-overload-1.31-481.el9.noarch.rpm
64. perl-overloading-0.02-481.el9.noarch.rpm
65. perl-parent-0.238-460.el9.noarch.rpm
66. perl-podlators-4.14-460.el9.noarch.rpm
67. perl-subs-1.03-481.el9.noarch.rpm
68. perl-libs-5.32.1-481.el9.x86_64.rpm
69. perl-vars-1.05-481.el9.noarch.rpm
70. libnsl2-2.0.0-1.el9.x86_64.rpm
71. python3.11-3.11.11-2.el9.x86_64.rpm
72. mpdecimal-2.5.1-3.el9.x86_64.rpm
73. python3.11-setuptools-wheel-65.5.1-3.el9.noarch.rpm
74. python3.11-pip-wheel-22.3.1-5.el9.noarch.rpm
75. python3.11-libs-3.11.11-2.el9.x86_64.rpm
76. python3.11-pip-22.3.1-5.el9.noarch.rpm
77. python3.11-devel-3.11.11-2.el9.x86_64.rpm

78. createrepo_c-libs-0.20.1-2.el9.x86_64.rpm
79. createrepo_c-0.20.1-2.el9.x86_64.rpm
80. vsftpd-3.0.5-6.el9.x86_64.rpm
81. python3.11-devel-3.11.11-2.el9.x86_64.rpm
82. net-snmp-5.9.1-17.0.1.el9.x86_64.rpm
83. numactl-devel-2.0.19-1.el9.x86_64.rpm
84. python3.11-pyyaml-6.0-1.el9.x86_64.rpm
85. openssl-perl-3.2.2-6.0.1.el9_5.1.x86_64.rpm
86. wireshark-3.4.10-7.el9.x86_64.rpm
87. whois-5.5.9-4.el9.x86_64.rpm
88. libX11-1.7.0-11.el9.x86_64.rpm
89. boost-filesystem-1.75.0-10.el9.x86_64.rpm
90. boost-program-options-1.75.0-10.el9.x86_64.rpm
91. boost-system-1.75.0-10.el9.x86_64.rpm
92. libjpeg-turbo-2.0.90-7.el9.x86_64.rpm
93. lcms2-2.12-3.el9.x86_64.rpm
94. openjpeg2-2.4.0-8.el9.x86_64.rpm
95. libtiff-4.4.0-13.el9.x86_64.rpm
96. libwebp-1.2.0-8.el9_3.x86_64.rpm
97. libxcb-1.13.1-9.el9.x86_64.rpm
98. hicolor-icon-theme-0.17-13.el9.noarch.rpm
99. qt5-qtbase-5.15.9-10.el9_4.x86_64.rpm
100. qt5-qtbase-gui-5.15.9-10.el9_4.x86_64.rpm
101. qt5-qtmultimedia-5.15.9-1.el9.x86_64.rpm
102. qt5-qtbase-gui-5.15.9-10.el9_4.x86_64.rpm
103. wireshark-cli-3.4.10-7.el9.x86_64.rpm
104. xdg-utils-1.1.3-13.el9_6.noarch.rpm
105. whois-nls-5.5.9-4.el9.noarch.rpm
106. net-snmp-libs-5.9.1-17.0.1.el9.x86_64.rpm
107. net-snmp-agent-libs-5.9.1-17.0.1.el9.x86_64.rpm
108. net-snmp-libs-5.9.1-17.0.1.el9.x86_64.rpm
109. perl-Term-ReadLine-1.17-481.el9.noarch.rpm
110. libXau-1.0.9-8.el9.x86_64.rpm
111. fribidi-1.0.10-6.el9.2.x86_64.rpm
112. mariadb-connector-c-3.2.6-1.el9_0.x86_64.rpm
113. lm_sensors-libs-3.6.0-10.el9.x86_64.rpm
114. libX11-common-1.7.0-11.el9.noarch.rpm
115. desktop-file-utils-0.26-6.el9.x86_64.rpm

116. libsmi-0.4.8-30.el9.x86_64.rpm
117. wget-1.21.1-8.el9_4.x86_64.rpm
118. libglvnd-glx-1.3.4-1.el9.x86_64.rpm
119. qt5-qtdeclarative-5.15.9-3.el9.x86_64.rpm
120. alsa-lib-1.2.13-2.el9.x86_64.rpm
121. gstreamer1-plugins-base-1.22.12-4.el9.x86_64.rpm
122. gstreamer1-1.22.12-3.el9.x86_64.rpm
123. gstreamer1-plugins-bad-free-libs-1.22.12-4.el9_6.x86_64.rpm
124. openal-soft-1.19.1-16.el9.x86_64.rpm
125. pulseaudio-libs-15.0-3.el9.x86_64.rpm
126. libdrm-2.4.123-2.el9.x86_64.rpm
127. libglvnd-egl-1.3.4-1.el9.x86_64.rpm
128. libX11-xcb-1.7.0-11.el9.x86_64.rpm
129. mesa-libgbm-24.2.8-2.el9_6.x86_64.rpm
130. glx-utils-8.4.0-12.20210504git0f9e7d9.el9.x86_64.rpm
131. libICE-1.0.10-8.el9.x86_64.rpm
132. libSM-1.2.3-10.el9.x86_64.rpm
133. fontconfig-2.14.0-2.el9_1.x86_64.rpm
134. libinput-1.19.3-5.el9_6.x86_64.rpm
135. xcb-util-wm-0.4.1-22.el9.x86_64.rpm
136. xcb-util-image-0.4.0-19.el9.x86_64.rpm
137. xcb-util-keysyms-0.4.0-17.el9.x86_64.rpm
138. xcb-util-renderutil-0.3.9-20.el9.x86_64.rpm
139. libxkbcommon-x11-1.0.3-4.el9.x86_64.rpm
140. libxkbcommon-1.0.3-4.el9.x86_64.rpm
141. pcre2-utf16-10.40-6.0.1.el9.x86_64.rpm
142. qt5-qtbase-common-5.15.9-10.el9_4.noarch.rpm
143. xcb-util-0.4.0-19.el9.x86_64.rpm
144. libasyncns-0.8-22.el9.x86_64.rpm
145. libsndfile-1.0.31-9.el9.x86_64.rpm
146. mesa-dri-drivers-24.2.8-2.el9_6.x86_64.rpm
147. libwayland-server-1.21.0-1.el9.x86_64.rpm
148. xkeyboard-config-2.33-2.el9.noarch.rpm
149. libevdev-1.11.0-3.el9.x86_64.rpm
150. mtdev-1.1.5-22.el9.x86_64.rpm
151. libwacom-1.12.1-3.el9_4.x86_64.rpm
152. libXext-1.3.4-8.el9.x86_64.rpm
153. libglvnd-1.3.4-1.el9.x86_64.rpm

154. mesa-libGL-24.2.8-2.el9_6.x86_64.rpm
155. mesa-libEGL-24.2.8-2.el9_6.x86_64.rpm
156. cairo-1.17.4-7.el9.x86_64.rpm
157. emacs-filesystem-27.2-13.el9_6.noarch.rpm
158. flac-libs-1.3.3-10.el9_2.1.x86_64.rpm
159. graphene-1.10.6-2.el9.x86_64.rpm
160. gsm-1.0.19-6.el9.x86_64.rpm
161. iso-codes-4.6.0-3.el9.noarch.rpm
162. libdatrie-0.2.13-4.el9.x86_64.rpm
163. libogg-1.3.4-6.el9.x86_64.rpm
164. libthai-0.1.28-8.el9.x86_64.rpm
165. libtheora-1.1.1-31.el9.x86_64.rpm
166. libva-2.22.0-1.el9.x86_64.rpm
167. libvorbis-1.3.7-5.el9.x86_64.rpm
168. libwacom-data-1.12.1-3.el9_4.noarch.rpm
169. libwayland-client-1.21.0-1.el9.x86_64.rpm
170. libwayland-cursor-1.21.0-1.el9.x86_64.rpm
171. libwayland-egl-1.21.0-1.el9.x86_64.rpm
172. libXfixes-5.0.3-16.el9.x86_64.rpm
173. libXft-2.3.3-8.el9.x86_64.rpm
174. libXi-1.7.10-8.el9.x86_64.rpm
175. libXrender-0.9.10-16.el9.x86_64.rpm
176. libxshmfence-1.3-10.el9.x86_64.rpm
177. libXv-1.0.11-16.el9.x86_64.rpm
178. libXxf86vm-1.1.4-18.el9.x86_64.rpm
179. llvm-libs-19.1.7-2.el9.x86_64.rpm
180. mesa-filesystem-24.2.8-2.el9_6.x86_64.rpm
181. mesa-libglapi-24.2.8-2.el9_6.x86_64.rpm
182. mesa-vulkan-drivers-24.2.8-2.el9_6.x86_64.rpm
183. opus-1.3.1-10.el9.x86_64.rpm
184. orc-0.4.31-8.el9.x86_64.rpm
185. pango-1.48.7-3.el9.x86_64.rpm
186. pixman-0.40.0-6.el9_3.x86_64.rpm
187. xml-common-0.6.3-58.el9.noarch.rpm
188. vulkan-loader-1.4.304.0-1.el9.x86_64.rpm
189. python3.11-setuptools-65.5.1-3.el9.noarch.rpm
190. jbigkit-libs-2.1-23.el9.x86_64.rpm
191. urw-base35-bookman-fonts-20200910-6.el9.noarch.rpm

192. urw-base35-c059-fonts-20200910-6.el9.noarch.rpm
193. urw-base35-d050000l-fonts-20200910-6.el9.noarch.rpm
194. urw-base35-fonts-20200910-6.el9.noarch.rpm
195. urw-base35-fonts-common-20200910-6.el9.noarch.rpm
196. urw-base35-gothic-fonts-20200910-6.el9.noarch.rpm
197. urw-base35-nimbus-mono-ps-fonts-20200910-6.el9.noarch.rpm
198. urw-base35-nimbus-roman-fonts-20200910-6.el9.noarch.rpm
199. urw-base35-nimbus-sans-fonts-20200910-6.el9.noarch.rpm
200. urw-base35-p052-fonts-20200910-6.el9.noarch.rpm
201. urw-base35-standard-symbols-ps-fonts-20200910-6.el9.noarch.rpm
202. urw-base35-z003-fonts-20200910-6.el9.noarch.rpm

Developer EPEL Packages: https://yum.oracle.com/repo/OracleLinux/OL9/developer/EPEL/x86_64/index.html

1. libimagequant-2.17.0-1.el9.x86_64.rpm
2. libraqm-0.8.0-1.el9.x86_64.rpm
3. unittest-cpp-2.0.0-14.el9.x86_64.rpm

3

Installing Session Monitor Using the OSDC Website

This section shall be used in the case that you want to install Session Monitor after downloading the Zip files from the Oracle eDelivery website or the Oracle Software Delivery Cloud (OSDC) webiste.

Topics:

- Installing Session Monitor - with Internet Connectivity Using the OSDC Website
- Installing Session Monitor in an Offline Mode - Using the OSDC Website

Installing Session Monitor - with Internet Connectivity Using the OSDC Website

This chapter describes how to install Session Monitor after downloading the Session Monitorinstallation .ZIP bundle from the Oracle Software Delivery Cloud (OSDC) website or the Oracle eDelivery website.

> **Note**
>
> If you need separate partitions for data (block) storage and MySQL storage, see the section Creating a Separate Partition for Data Storage and MySQL Storage .

Before installing Session Monitor, read the following:

- About Installing Session Monitor
- Session Monitor System Requirements

Downloading the Software from the Oracle eDelivery Website (OSDC)

The Oracle Software Delivery Cloud (OSDC) site allows you to download Oracle software products. The process of downloading software from OSDC includes following steps:

1. Go to the Oracle Software Delivery Cloud website http://edelivery.oracle.com/
2. Sign in with your Oracle account. If you do not have an Oracle account, you can register for an account here.
3. Search for the software by typing **OCSM** in the search bar and selecting it.
4. The selected products are then listed under **Download Queue**.
5. Click the X (cross) which is adjacent to the product in case you want to remove individual files or click **Remove All** if you want to remove all the listed items.
6. Click **Continue** to proceed to next screen; you will see a list of the selected software for downloading.

7. Choose the individual software components for download and click **Continue** if you wish to proceed or **Back** to review different software for downloading.
8. Read the license agreement carefully; mark the check box to agree with license agreements, and click **Continue**.
9. Click **Download** button to download the software or click the file name to individually download the files.
10. While you can save the file on any machine you choose, we recommend you save the file onto the machine where you plan to run it. You must extract the ZIP file on the platform for which it was intended. The length of time it takes to download an application depends on the size of the download, your connection speed, and the amount of traffic on the site.
11. Once the Download has completed, click **Return to Search** to search and download additional files or click **Sign Out** to log off Oracle Software Delivery Cloud.

Verifying the Contents of the Session Monitor Installation Bundle

Verify the contents of the Session Monitor installation.zip bundle that you downloaded from the My Oracle Support website (MOS) or Oracle Software Delivery Cloud (OSDC).

Extract the bundle and verify that it has following contents:

1. README.txt
2. meta.nfo
3. ocsm-6.1.0.0.0-RPM-GA.zip
4. other_files/
5. other_files/my-8.0.cnf
6. other_files/ocsm-6.1.0.0.0.revision.txt
7. other_files/mysql-shell-commercial-8.4.6-1.1.el9.x86_64.rpm
8. scripts/
9. scripts/Install_OCSM_Rel_6.1.sh
10. scripts/Upgrade_OCSM_Rel_6.1.sh
11. scripts/Backup and Restore Scripts/
12. scripts/Backup and Restore Scripts/MySQLDeltaUpgrade.sh
13. scripts/Backup and Restore Scripts/backupAndRestoreBlockStorage.sh
14. scripts/Backup and Restore Scripts/backupAndRestoreOtherFiles.sh
15. scripts/Offline_Installation/
16. scripts/Offline_Installation/Download_rpms.sh
17. scripts/Offline_Installation/Offline_OCSM_Installation_Rel_6.1.sh
18. scripts/Offline_Installation/Offline_Repo_OCSM_Rel_6.1.sh
19. scripts/Offline_Installation/Offline_Repo_Server_preparation_Rel_6.1.sh
20. scripts/Offline_Installation/Offline_Upgrade_OCSM_Rel_6.1.sh

Installing Session Monitor - Online

This section describes installing the Session Monitor - online using the ZIP bundle.

> ⚠ **Caution**
>
> Please read the installation instructions before beginning the installation process.

Complete the following tasks before installing Session Monitor:

- Set up the machine with Oracle Linux 9.6 operating system.
- Configure the proxy if required. For more information, see Configuring Proxies and Repositories.

1. Verify that the system hosting the Session Monitor is connected to the Internet.
2. Run this command to verify that Oracle Linux 9.6 has been installed.

   ```
   cat /etc/oracle-release
   ```

   The output of the command should show Oracle Linux version starting from version 8, for example: `Oracle Linux Server release 9.0`.
3. Install the Kernel version 5.15.0-302.167:
   a. Enable the ol9_UEKR7 repository:

      ```
      dnf config-manager --set-enabled ol9_UEKR7
      ```

   b. Install the kernel:

      ```
      dnf install -y kernel-uek-5.15.0-302.167.6.el9uek.x86_64
      ```

   c. Verify the grub configuration and check installed kernel is listed:

      ```
      grubby --info=ALL | grep -E "^kernel|^index"
      ```

   d. Set the default kernel:

      ```
      grubby --set-default=/boot/vmlinuz-5.15.0-302.167.6.el9uek.x86_64
      ```

   e. Reboot the system:

      ```
      reboot
      ```

   f. Verify the kernel version after reboot:

      ```
      uname -a
      ```

4. Once the VM or Server is up and running with 5.15 kernel, uninstall 6.x kernel and its associated dependencies by executing the following commands:

   ```
   rpm -qa | grep '^kernel-uek' | grep 6.12
   dnf remove <6.12 kernel packages>
   ```

5. Log on to the Session Monitor server as the root user or root privileged user.
6. If partitioning is required, refer to the section, Creating a Separate Partition for Data Storage and MySQL Storage
7. Create a temporary directory (`/tmp/ocsm_install`) on the system that hosts the Session Monitor.
   1. Copy the Session Monitor installation Zip bundle, downloaded from Oracle software delivery website, to the /tmp/ocsm_install directory
   2. Run this command to install unzip package:

      ```
      yum install -y unzip
      ```

   3. Change the working directory to /tmp/ocsm_install using command:

      ```
      cd /tmp/ocsm_install
      ```

   4. Extract the Session Monitor Installation bundle using command :

      ```
      unzip <Session Monitor Installation bundle .zip file>
      ```

   5. Set the execute permission for the installation scripts using command:

      ```
      chmod +x scripts/*.sh
      ```

   6. Run the Session Monitor online installation script using command:

      ```
      ./scripts/Install_OCSM_Rel_6.1.sh ocsm-6.1.0.0.0-RPM-GA.zip
      ```

Configuring Proxies and Repositories

Configure the proxies and repositories.

Configure the HTTP proxy in the `/etc/yum.conf` file and also export the same to environment by doing the following

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

   `proxy=<Your_Proxy>` where, you need to add the proxy server details in place of <your_proxy>.
2. Run the following commands to export the proxy server details to the environment:

   ```
   export http_proxy=<Your_Proxy>
   export https_proxy=<Your_Proxy>
   ```

Creating a Separate Partition for Data Storage and MySQL Storage

Perform the following tasks to create a separate partition for data (block) storage and MySQL Storage

The following partitioning options are available:

- Single partition (This is the default option)
- Secondary partition for data and MySQL storage

Perform the following tasks to create the partition for data storage MySQL storage:

1. Run the following command to create a directory to mount the partition:

```
mkdir -pv /opt/oracle/ocsm/var/vsi
mkdir -pv /var/lib/mysql
```

2. Adjust `/etc/fstab` to mount the data storage partition. For example:

> **Note**
>
> This entry may vary based on the environment:

```
LABEL=PLD_DATA /opt/oracle/ocsm/var/vsi xfs
defaults,nosuid,nodev,nofail 0 2
LABEL=MYSQL_DATA /var/lib/mysql xfs
defaults,nosuid,nodev,nofail 0 2
```

During the installation process of MySQL and Session Monitor, partitions are detected by the product and the system uses these separate partitions.

Tasks to be Performed after RPM Installation

Perform the tasks given here after the RPM installation.

1. Verify the installation by doing the following:
   a. Navigate to the /var/log/ocsm file
   b. Verify if the following log file exists: `ocsm_installed_*.log`
   c. Navigate to the /var/log/ directory and verify that the `ocsm_zip_install.log` is present.
2. Adjust the firewall to access the Session Monitor applications by doing the following tasks:
   - Run this command to allow the firewall to access the HTTPS service (port 443) by running the following command:

     ```
     firewall-cmd --permanent --zone=public --add-service=https
     ```

   - (Optional) If you are planning to configure the system as a Mediation Engine, allow the firewall to access the probe connection by doing these tasks:

For SBC (embedded) probes:

```
firewall-cmd --permanent --zone=public --add-port=4739/tcp

firewall-cmd --permanent --zone=public --add-port=4740/tcp
```

For standalone probes:

```
firewall-cmd --permanent --zone=public --add-port=4741/tcp

firewall-cmd --permanent --zone=public --add-port=4742/tcp
```

> **Note**
>
> The ports 4740/4742 are the preferred ports for connecting to SBC and standalone probes respectively. So, the firewall must be opened for ports 4739/4741 only if you agree to have non-TLS connections.

3. Run this command to reload the configuration:

   ```
   firewall-cmd --reload
   ```

   > **Note**
   >
   > If you are planning to enable additional services, see the discussion about network security in the Oracle Communications Session Monitor Security Guide for a complete list of services and their respective ports.

4. Enable or Disable SELinux as per your requirement. For more information, see Enabling SELinux.

Enabling SELinux

Session Monitor currently supports the following top-level states of SELinux on a system – enforcing, permissive, and disabled. The only supported SELinux policy type is **targeted**.

To enable SELinux:

1. Run the command to set the SELinux mode as enforcing and the SELinux policy as targeted:

   ```
   sed -i -e "s/^SELINUX=.*/SELINUX=enforcing/" /etc/selinux/config
   ```

```
sed -i -e "s/^SELINUXTYPE=.*/SELINUXTYPE=targeted/" /etc/selinux/config
```

2. Reboot the system using the command:

   ```
   reboot
   ```

3. After the reboot, run the command to verify the SELinux status:

   ```
   sestatus
   ```

   - Verify the command output. The output should look like this:

     ```
     SELinux status: enabled
     SELinuxfs mount: /sys/fs/selinuxSELinux root
     directory: /etc/selinux
     Loaded policy name:targetedCurrent
     mode: enforcing
     Mode from config file:enforcing
     Policy MLS status: enabled
     Policy deny_unknown status: allowed
     Max kernel policy version:31
     ```

4. Install the customized SELinux policy modules for Session Monitor using the command:

   ```
   cd /opt/oracle/ocsm/
   ./ocsm_ext.sh
   ```

Disabling SELinux

Use the following instructions to disable SELinux.

1. Set the SELinux mode as disabled using the command as a root user:

   ```
   sed -i -e "s/^SELINUX=.*/SELINUX=disabled/" /etc/selinux/config
   ```

2. Reboot the system using the command:

   ```
   reboot
   ```

3. Verify the SELinux status using the command:

   ```
   sestatus
   ```

4. Verify the output:

   ```
   SELinux
   status:disabled
   ```

Adding Ports in the SELinux Port List

On a SELinux enabled machine, in order to use any port other than the default ports in the Session Monitor,

1. Add the port in the SELinux port list using the following commands.

   ```
   yum install -y setroubleshoot-server
   semanage port -a -t <Service_Name> -p <Protocol> <Port_Number>
   ```

2. You can view all ports allowed in the SELinux using the command:

   ```
   semanage port -l
   ```

   For example: By default, SELinux allows HTTP to listen on the TCP ports: 80, 443, 488, 8008, 8009, or 8443.

3. To configure HTTP to run on a port other than the TCP ports listed above, such as 8001, then add the ports to the SELinux port list using the command:

   ```
   semanage port -a -t http_port_t -p tcp 8001
   ```

Troubleshooting Tips

This sections provides instructions that will be helpful in solving issues in configuring SELinux.

To modify the mode in which SELinux runs in real-time, run the following commands:

Table 3-1 Modifying SELinux Mode

Mode	Command
Run SELinux in permissive mode (System prints warnings only but does not enforce SELinux policy)	setenforce 0
Run SELinux in the enforcing mode (SELinux security policy is enforced)	setenforce 1
Verify the status	getenforce

Installing Session Monitor in an Offline Mode - Using the OSDC Website

This chapter describes how to install Session Monitor when the Session Monitor node is without an internet connection.

> **Note**
>
> This procedure was tested on:
>
> - Oracle Linux 9.6
> - MySQL 8.4.6
> - MySQL Connector 8.4.0
>
> The versions of the dependency RPMs used in this procedure are the latest available versions at the time of this release based on Oracle Linux 9.6 and MySQL 8.4.6 and the RPM file for Session Monitor Release 6.1.0.0.0. Use the latest version of dependency RPMs for all future patch releases based on the Oracle Linux, MySQL and Session Monitor RPM used.

You can install Session Monitor in an offline mode using any one of the methods listed here:

- **Method 1**: Session Monitor node acts as the repo server.
- **Method 2**: A separate node acts as the repo server.

Session Monitor installation requires a temporary repo server to resolve the package dependencies. Henceforth, this server will be referred to as the Repo server in this document.

The Repo server can be a part of the Session Monitor node itself (Method 1) OR it can be separate node (Method 2). If it is a separate node, the Session Monitor node must be able to reach the Repo server.

In both methods, it is assumed that as Session Monitor node does not have an internet connectivity, so the dependency RPMs and packages would be first downloaded on a machine which has the internet connectivity.

> ⚠ **Caution**
>
> Install the Session Monitor node with Oracle Linux 9.6.

Download Dependent RPMs on a Linux Machine with Internet Connectivity

Follow instructions in this section to download dependent RPMs on a Linux machine with internet connectivity:

1. Log in to the Linux machine as a root user OR root privileged user.

> **Note**
>
> Ensure that the Linux system has 5 GB to 10 GB free disk space in the `/tmp` folder.

2. If the `/tmp/ocsm` folder already exists, take a backup of the `/tmp/ocsm` folder if required, and delete the folder `/tmp/ocsm`.
3. Create a folder: `/tmp/ocsm`

   ```
   mkdir /tmp/ocsm
   ```

4. Copy the Session Monitor software Zip file which you downloaded from the OSDC Website to the `/tmp/ocsm` folder in the Linux System. For more information on downloading the Session Monitor Zip file, refer to the section Downloading the Software from the Oracle eDelivery Website (OSDC).
5. Install the unzip package.

   ```
   yum install -y unzip
   ```

6. Change to folder `/tmp/ocsm`:

   ```
   cd /tmp/ocsm
   ```

7. Extract the contents of the software Zip file which is copied here. For example:

   ```
   unzip ocsm-6.1.0.0.0-GA.zip
   ```

8. Execute below steps to copy the Offline installation scripts to /tmp/ocsm folder.

   ```
   cp -rf scripts/Offline_Installation/* /tmp/ocsm/
   ```

9. Set execute permission for the `Download_rpms.sh` script:

   ```
   chmod +x Download_rpms.sh
   ```

10. Run the `Download_rpms.sh` script to download the dependency RPMs:

    ```
    ./Download_rpms.sh
    ```

    If you need to configure a proxy server for your system, run the same command with the following information:

    ```
    ./Download_rpms.sh "[PROTOCOL://]HOST[:PORT]"
    ```

    - where PROTOCOL is HTTP or HTTPS
    - HOST is the IP address or FQDN of the proxy server
    - PORT is the port number for the proxy server

Installing Session Monitor using Method 1

Install Session Monitor using Method 1 where the Session Monitor node acts as the Repo server.

1. Log in to the Session Monitor server installed with Oracle Linux 9.6 as a root user OR root privileged user
2. Ensure that 5 GB to 10 GB free space is available in the `/tmp` folder on this server.

3. If the `/tmp/ocsm` folder is already present, take a backup of the `/tmp/ocsm` folder if required and delete the folder `/tmp/ocsm`.
4. Create the folder `/tmp/ocsm` .

   ```
   mkdir /tmp/ocsm
   ```

5. Transfer the contents of the folder `/tmp/ocsm` from the Linux machine, where you have downloaded all the RPM files and scripts - to the `/tmp/ocsm` folder on the Session Monitor server.
6. Navigate to the folder `/tmp/ocsm` on the Session Monitor server.

   ```
   cd /tmp/ocsm
   ```

7. Install the Kernel version 5.15.0-302.167.6
   1. Install the kernel RPMs in order:

      ```
      rpm -ivh kernel-uek-core-5.15.0-302.167.6.el9uek.x86_64.rpm --oldpackage
      ```

      ```
      rpm -ivh kernel-uek-modules-5.15.0-302.167.6.el9uek.x86_64.rpm --
      oldpackage
      ```

      ```
      rpm -ivh kernel-uek-5.15.0-302.167.6.el9uek.x86_64.rpm --oldpackage
      ```

   2. Verify the grub configuration and check installed kernel is listed:

      ```
      grubby --info=ALL | grep -E "^kernel|^index"
      ```

   3. Set the default kernel:

      ```
      grubby --set-default=/boot/vmlinuz-5.15.0-302.167.6.el9uek.x86_64
      ```

   4. Reboot the system:

      ```
      reboot
      ```

   5. Verify the kernel version after reboot:

      ```
      uname -a
      ```

8. Navigate to the folder /tmp/ocsm on the Session Monitor server:

   ```
   cd /tmp/ocsm
   ```

9. Once the VM or Server is up and running with 5.15 kernel, uninstall 6.x kernel and its associated dependencies by executing the following commands

   ```
   rpm -qa | grep '^kernel-uek' | grep 6.12
   dnf remove <6.12 kernel packages>
   ```

10. Set execute permission as:

    ```
    chmod +x *.sh
    ```

11. Run the following command to install Session Monitor.

    ```
    ./Offline_Repo_OCSM_Rel_6.1.sh
    ```

Installing Session Monitor using Method 2

Install Session Monitor using Method 2 where the Repo server is a separate node. Session Monitor should be able to reach the Repo server.

1. Log in to the Repo server as a root user OR root privileged user and execute Steps 2 to 8.
2. Ensure that 5 GB to 10 GB free space is available in the `/tmp` folder on this server.
3. If the `/tmp/ocsm` folder is already present, take a backup of the `/tmp/ocsm` folder if required and delete the folder `/tmp/ocsm`.
4. Create the folder `/tmp/ocsm` .

    ```
    mkdir /tmp/ocsm
    ```

5. Navigate to the folder `/tmp/ocsm`.

    ```
    cd /tmp/ocsm
    ```

6. Transfer all the contents of the folder `/tmp/ocsm` from the Linux machine - where you have downloaded the RPM files and scripts - to the `/tmp/ocsm` folder on the Repo server.
7. Set execute permission as:

    ```
    chmod +x *.sh
    ```

8. Run the following command to prepare the Repo server.

    ```
    ./Offline_Repo_Server_preparation_Rel_6.1.sh
    ```

9. Log in to the Session Monitor server installed with Oracle Linux 9.6 as a root or root privileged user, and execute Steps 10 to 16.
10. Check if you have 5 GB to 10 GB free space available in the `/tmp` folder on the Session Monitor Server.
11. If the `/tmp/ocsm` folder is already present, take a backup of the `/tmp/ocsm` folder if required, and delete the folder `/tmp/ocsm`.
12. Create the folder `/tmp/ocsm` using this command:

    ```
    mkdir /tmp/ocsm
    ```

13. Transfer all the contents of the folder `/tmp/ocsm` on the Repo server machine to the folder `/tmp/ocsm` on the Session Monitor server.
14. Go to the folder `/tmp/ocsm`.

    ```
    cd /tmp/ocsm
    ```

15. Install the Kernel version 5.15.0-302.167.6:

   a. Install the kernel RPMs in order:

      ```
      rpm -ivh kernel-uek-core-5.15.0-302.167.6.el9uek.x86_64.rpm --oldpackage
      ```

      ```
      rpm -ivh kernel-uek-modules-5.15.0-302.167.6.el9uek.x86_64.rpm --
      oldpackage
      ```

      ```
      rpm -ivh kernel-uek-5.15.0-302.167.6.el9uek.x86_64.rpm --oldpackage
      ```

   b. Verify the grub configuration and check that the installed kernel is listed:

      ```
      grubby --info=ALL | grep -E "^kernel|^index"
      ```

   c. Set the default kernel:

      ```
      grubby --set-default=/boot/vmlinuz-5.15.0-302.167.6.el9uek.x86_64
      ```

   d. Reboot the system:

      ```
      reboot
      ```

   e. Verify the kernel version after reboot:

      ```
      uname -a
      ```

16. Navigate to the folder /tmp/ocsm on the Session Monitor server:

    ```
    cd /tmp/ocsm
    ```

17. Once the VM or Server is up and running with 5.15 kernel, uninstall 6.x kernel and its associated dependencies by executing the following commands

    ```
    rpm -qa | grep '^kernel-uek' | grep 6.12
    dnf remove <6.12 kernel packages>
    ```

18. Set the execute permission

    ```
    chmod +x *.sh
    ```

19. Run the script `./Offline_OCSM_Installation_Rel_6.1.sh <REPO_SERVER_IP>` to install the Session Monitor.

    ```
    ./Offline_OCSM_Installation_Rel_6.1.sh <REPO_SERVER_IP>
    ```

    where <REPO_SERVER_IP> is the IP address of the Repo server. For example:

    ```
    ./Offline_OCSM_Installation_Rel_6.1.sh 192.168.1.10
    ```

Tasks to be Performed after Session Monitor Installation - Offline

Perform the tasks provided here, after the RPM installation.

1. Run this command to verify the installation is successful:

   a. Go to the folder `/var/log/ocsm` file.
   b. Verify if the following log file exists: ocsm_installed_*.log

2. Adjust the firewall to access the Session Monitor applications:
   - Run this command to allow the firewall to access the HTTPS service (port 443):

     ```
     firewall-cmd --permanent --zone=public --add-service=https
     ```

   - (Optional) If you are planning to configure the system as a Mediation Engine, allow the firewall to access the probe connection by doing these tasks:
     - For SBC (embedded) probes:

       ```
       firewall-cmd --permanent --zone=public --add-port=4739/tcp
       ```

       ```
       firewall-cmd --permanent --zone=public --add-port=4740/tcp
       ```

     - For standalone probes:

       ```
       firewall-cmd --permanent --zone=public --add-port=4741/tcp
       ```

       ```
       firewall-cmd --permanent --zone=public --add-port=4742/tcp
       ```

     > ⓘ **Note**
     >
     > The ports 4740 and 4742 are the preferred ports for connecting to SBC / standalone probes respectively. So, the firewall should be opened for ports 4739/4741 only if you are agree to have non-TLS connections.

3. Reload the configuration by running the following command:

   ```
   firewall-cmd --reload
   ```

   > ⓘ **Note**
   >
   > If you are planning to enable additional services, see the content about network security in the Oracle Communications Session Monitor Security Guide for a complete list of services and their respective ports.

4. Enable or Disable SELinux as per your requirement. For more information, see Enabling SELinux - Offline.

Enabling SELinux - Offline

Session Monitor currently supports the following top-level states of SELinux on a system – enforcing, permissive, and disabled. The only supported SELinux policy type is **targeted**.

To enable SELinux:

1. Run the command to set the SELinux mode as enforcing and the SELinux policy as targeted:

   ```
   sed -i -e "s/^SELINUX=.*/SELINUX=enforcing/" /etc/selinux/config
   ```

   ```
   sed -i -e "s/^SELINUXTYPE=.*/SELINUXTYPE=targeted/" /etc/selinux/config
   ```

2. Reboot the system using the command:

   ```
   reboot
   ```

3. After the reboot, run the command to verify the SELinux status:

   ```
   sestatus
   ```

   - Verify the command output. The output should look like this:

     ```
     SELinux status: enabled
     SELinuxfs mount: /sys/fs/selinuxSELinux root
     directory: /etc/selinux
     Loaded policy name:targetedCurrent
     mode: enforcing
     Mode from config file:enforcing
     Policy MLS status: enabled
     Policy deny_unknown status: allowed
     Max kernel policy version:31
     ```

4. Install the customized SELinux policy modules for Session Monitor using the command:

   ```
   cd /opt/oracle/ocsm/
   ./ocsm_ext.sh
   ```

Disabling SELinux - Offline

Use the following instructions to disable SELinux.

1. Set the SELinux mode as disabled using the command as a root user:

   ```
   sed -i -e "s/^SELINUX=.*/SELINUX=disabled/" /etc/selinux/config
   ```

2. Reboot the system using the command:

   ```
   reboot
   ```

3. Verify the SELinux status using the command:

   ```
   sestatus
   ```

4. Verify the output:

   ```
   SELinux status:disabled
   ```

Adding Ports in the SELinux Port List

On a SELinux enabled machine, in order to use any port other than the default ports in the Session Monitor, add the port in the SELinux port list using the following commands.

1. Run this command that allows SELinux-specific service and adds the port number.

   ```
   yum install -y setroubleshoot-server
   semanage port -a -t <Service_Name> -p <Protocol> <Port_Number>
   ```

2. You can view all ports allowed in the SELinux using the command:

   ```
   semanage port -l
   ```

   For example: By default, SELinux allows HTTP to listen on the TCP ports: 80, 443, 488, 8008, 8009, or 8443.

3. To configure HTTP to run on a port other than the TCP ports listed above, such as 8001, then add the ports to the SELinux port list using the command:

   ```
   semanage port -a -t http_port_t -p tcp 8001
   ```

Troubleshooting Tips

This sections provides instructions that will be helpful in solving issues in configuring SELinux.

To modify the mode in which SELinux runs in real-time, run the following commands:

Table 3-2 Modifying SELinux Mode

Mode	Command
Run SELinux in permissive mode (System prints warnings only but does not enforce SELinux policy)	setenforce 0
Run SELinux in the enforcing mode (SELinux security policy is enforced)	setenforce 1
Verify the status	getenforce

4

Configuring Session Monitor

This chapter describes how to configure Oracle Communications Session Monitor.

About the Platform Setup Application

The Platform Setup Application (PSA) guides you through the configuration steps to get the Session Monitor system running, including configuring the machine type, capture settings, DNS settings, and SMTP settings.

The menu on the right shows your progress in the overall configuration.

Platform Setup Application Initial Log In

This section provides how to log into Platform Setup Application initially.

1. Open the web browser and enter the URL provided by the System Administrator.
2. Confirm the security exception to proceed.

   The Log in page appears.
3. Enter the **Username** and **Password**. For default username and password, contact your Oracle representative.
4. Click **Sign in**.
5. **Review and Accept** the license of the software to continue.

   The Platform Application Setup page appears.

Changing Your Password

1. Click your username in the top right corner.
2. Select **Change Password** from the drop-down menu.
3. Enter the old and the new passwords.

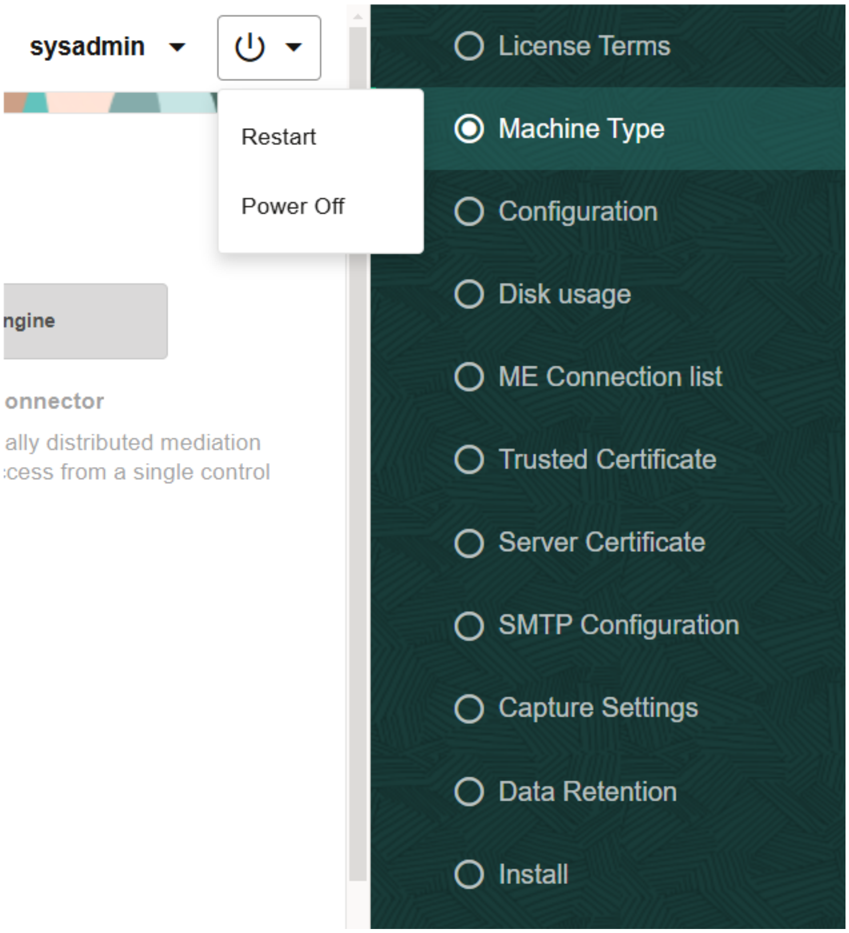
   Passwords must have the following characteristics:

   - At least 8 characters
   - At least one uppercase character
   - At least one digit
   - At least one special character
4. Click **Change**.

Restarting or Powering Off Session Monitor

The restart and power off buttons are accessible through the power button on the top right-hand corner of the screen.

Figure 4-1   Drop-Down Menu on Clicking the Power Button



After selecting an option, you are prompted a final time to confirm that you wish to proceed.

STIR/SHAKEN Monitoring

STIR/SHAKEN is a framework that integrates two protocol standards—Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted Information Using Tokens (SHAKEN)—to validate the legitimacy of caller identities in SIP-based voice calls.

The STIR/SHAKEN framework prevents caller ID spoofing and reduces unwanted robocalls by verifying caller legitimacy using digital signatures. Starting with the Release 6.1, Session Monitor introduces monitoring and reporting for STIR/SHAKEN-enabled calls.

Enabling STIR/SHAKEN Support

Enable STIR/SHAKEN in two places: In the Platform Setup Application, and under System Settings.

Platform Setup Application (PSA) > **Additional Extensions**. For STIR/SHAKEN monitoring, enable the PSA extension in the Enterprise Operations Monitor.

1. Using the Platform Setup Application:

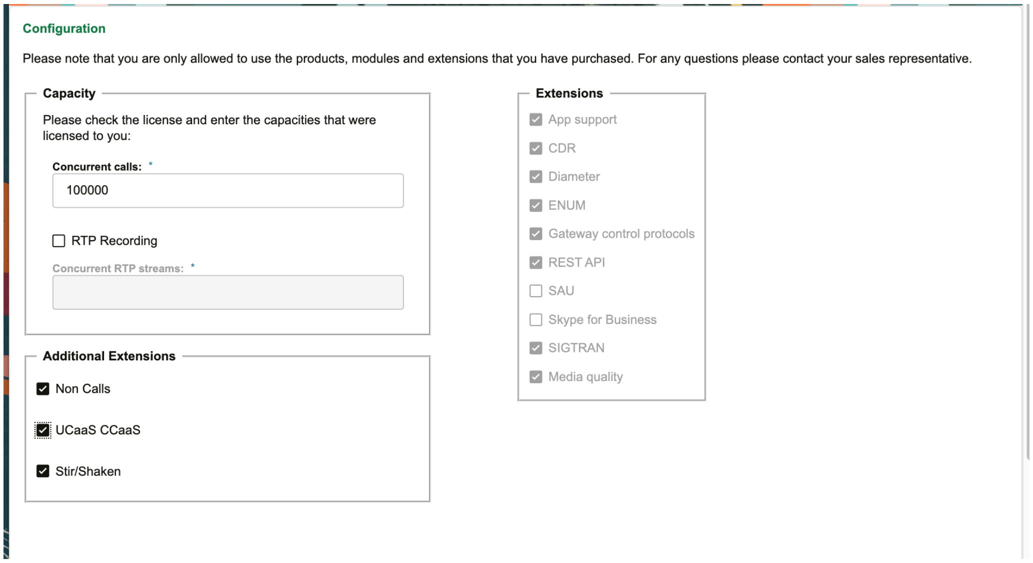
a. In a web browser, go to https://<ip_address>/setup or access the Platform Setup Application using the Mediation Engine GUI by clicking **admin** > **Setup**. The Platform Setup Application Login page appears.

b. Login to the Platform Setup Application.

c. Navigate to the **Configuration** page. Under the **Additional Extensions** area, select the **STIR/SHAKEN** check box.

d. Click **Apply**.

Figure 4-2 Enabling Stir/Shaken



Configuration

Please note that you are only allowed to use the products, modules and extensions that you have purchased. For any questions please contact your sales representative.

Capacity

Please check the license and enter the capacities that were licensed to you:

Concurrent calls: * 100000

□ RTP Recording

Concurrent RTP streams: *

Additional Extensions

☑ Non Calls

☑ UCaaS CCaaS

☑ Stir/Shaken

Extensions

☑ App support
☑ CDR
☑ Diameter
☑ ENUM
☑ Gateway control protocols
☑ REST API
□ SAU
□ Skype for Business
☑ SIGTRAN
☑ Media quality

- The STIR/SHAKEN extension, controls if STIR/SHAKEN calls are monitored.
- Enable this extension explicitly. The default setting is false.

> **Caution**
>
> Enabling/disabling the Stir/Shaken extension will start/stop the HTTP probe process and restart the counters process. It is recommended to perform this action during the maintenance window.

2. To view STIR/SHAKEN calls enable the below system setting:
   - **Support Stir/Shaken calls**
     This system setting controls whether STIR/SHAKEN calls are monitored. The default value is false. Enable this system setting after activating the extension in PSA.

Enabling the UCaaS CCaaS Extension

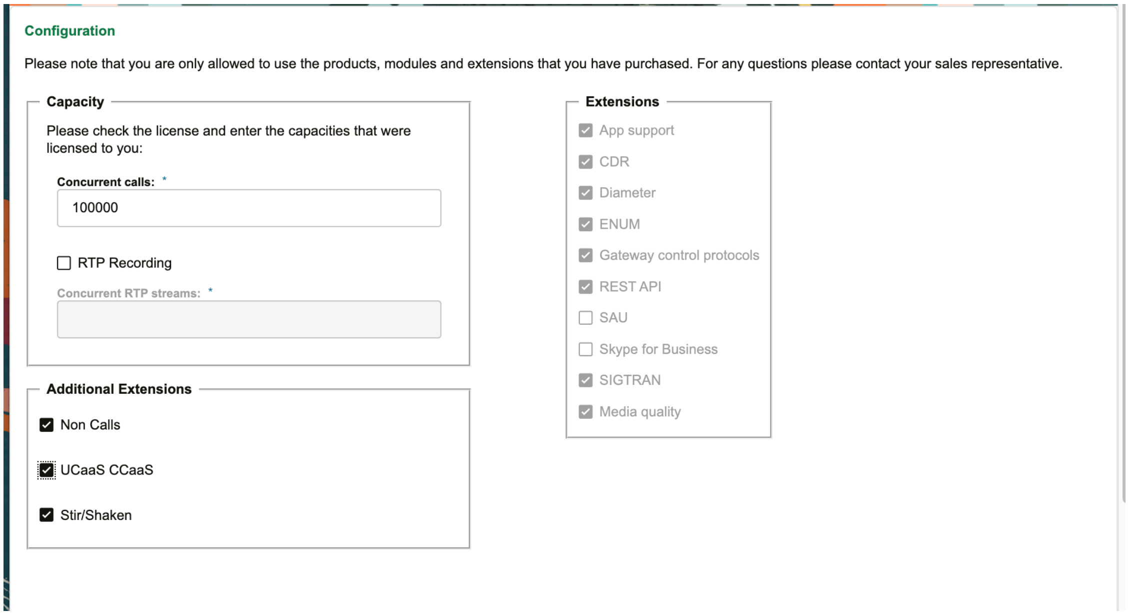
To activate UCaaS CCaaS monitoring, enable the UCaaS CCaaS Extension.

To enable the UCaaS CCaaS Extension:
The flag **UCaaS CCaaS** has been introduced in the Configuration section of the Platform Setup Application page to enable the UCaaS CCaaS Monitoring feature. This flag is disabled by default.

You can enable this flag during a fresh installation or even after the installation.

To activate the UCaaS CCaaS feature for upgraded systems, you need to enable this flag from the Platform Setup Application page after the upgrade.

Figure 4-3 UCaaS CCaaS Check Box



Configuration

Please note that you are only allowed to use the products, modules and extensions that you have purchased. For any questions please contact your sales representative.

Capacity

Please check the license and enter the capacities that were licensed to you:

Concurrent calls: * 100000

☐ RTP Recording

Concurrent RTP streams: *

Additional Extensions

☑ Non Calls

☑ UCaaS CCaaS

☑ Stir/Shaken

Extensions

☑ App support

☑ CDR

☑ Diameter

☑ ENUM

☑ Gateway control protocols

☑ REST API

☐ SAU

☐ Skype for Business

☑ SIGTRAN

☑ Media quality

After enabling this flag, you can view the following on the user interface:

- **UCaaS CCaaS Settings**
- **Metadata** tab in the Call Info page
- **UCaaS CCaaS** columns in the **Calls** Page
- **UCaaS CCaaS Legs in message flow**

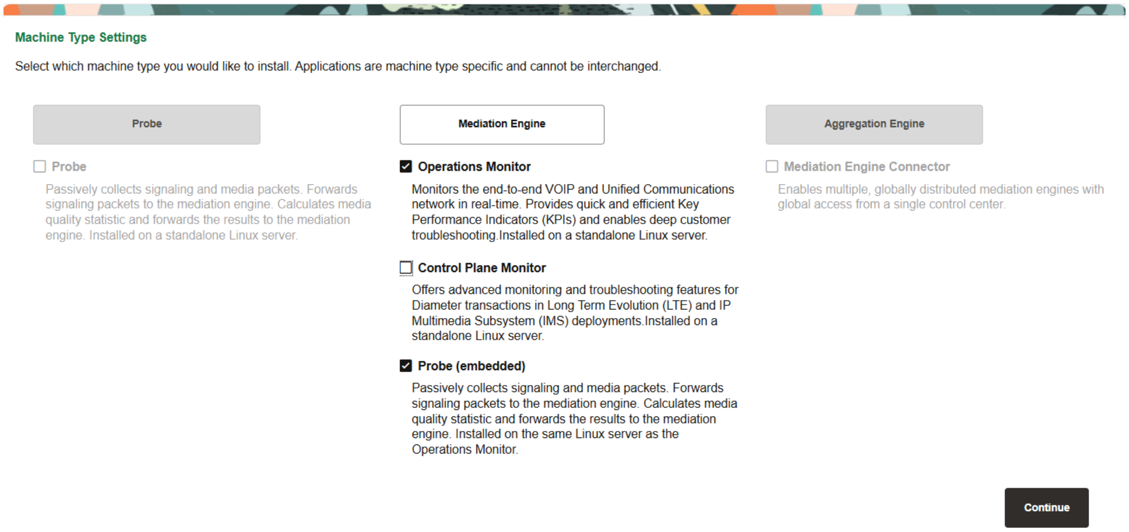
> **Note**
>
> To view correlated DR calls, enable the System Setting **Support UCaaS CCaaS Calls**.

The UCaaS CCaaS Monitoring feature is available only for Nodes installed as Mediation Engine and Mediation Engine + Probe. For more information, see the section Configuring Session Monitor in the Oracle Communications Session Monitor Installation Guide.

Selecting the Machine Type

The following figure shows the Machine Type Settings page.

Figure 4-4 Machine Type Settings pages



Machine Type Settings

Select which machine type you would like to install. Applications are machine type specific and cannot be interchanged.

□ Probe

Passively collects signaling and media packets. Forwards signaling packets to the mediation engine. Calculates media quality statistic and forwards the results to the mediation engine. Installed on a standalone Linux server.

☑ Operations Monitor

Monitors the end-to-end VOIP and Unified Communications network in real-time. Provides quick and efficient Key Performance Indicators (KPIs) and enables deep customer troubleshooting.Installed on a standalone Linux server.

□ Control Plane Monitor

Offers advanced monitoring and troubleshooting features for Diameter transactions in Long Term Evolution (LTE) and IP Multimedia Subsystem (IMS) deployments.Installed on a standalone Linux server.

☑ Probe (embedded)

Passively collects signaling and media packets. Forwards signaling packets to the mediation engine. Calculates media quality statistic and forwards the results to the mediation engine. Installed on the same Linux server as the Operations Monitor.

□ Mediation Engine Connector

Enables multiple, globally distributed mediation engines with global access from a single control center.

The Machine Type Settings page allows you to select which products you want to install. This page only appears the first time you configure Session Monitor prior to the products installation.

Select your machine type by clicking **Probe** or **Mediation Engine** or **Aggregation Engine** button. This will enable the corresponding product selection.

> **Note**
>
> - You can select only one machine type per installation.
> - Packet Inspector is not supported on the machine collocated with Operations Monitor or Probe with SIP/RTP sniffing for the calls and VQ analysis.

Next, select the check boxes next to the products that you want to install. Only checked items are included in the installation.

> **Note**
>
> The products are machine type specific and cannot be interchanged between machine types.
>
> For example, the Probe machine type requires a probe product, and the Mediation Engine machine type requires the Operations Monitor product.

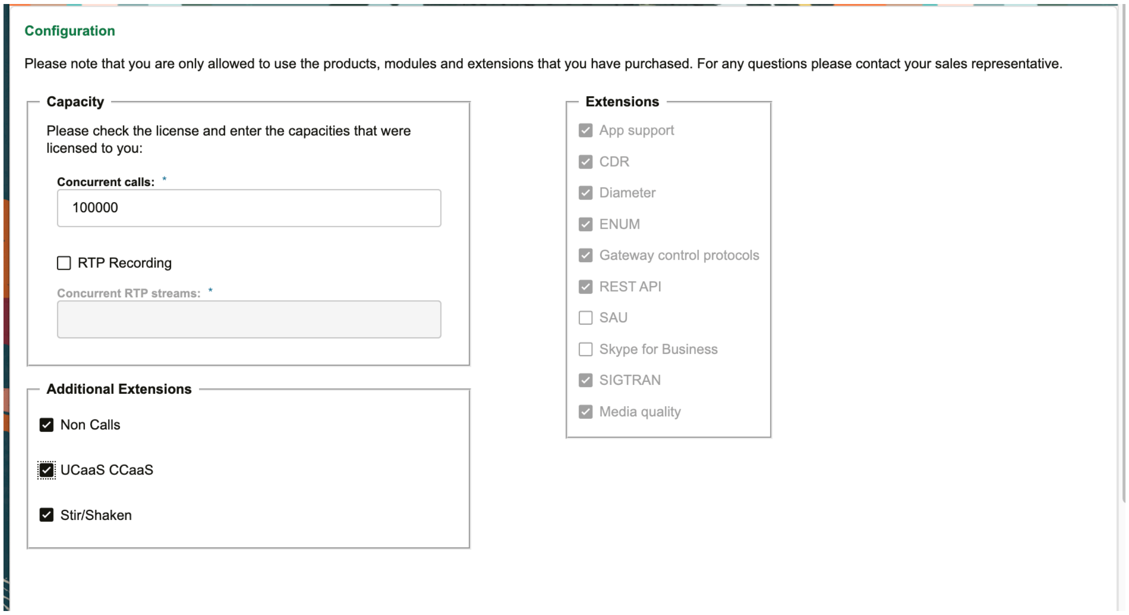
After selecting the products, click **continue** to proceed with the installation. Your machine type and product selections should appear in the status panel located on the right under the navigation menu.

Configuring Session Monitor

This step in the configuration process allows you to configure Session Monitor settings for this machine in accordance with the terms of your license.

> **Note**
>
> If you do not have a valid Session Monitor license, contact Oracle.

Figure 4-5 Configuration page



Configuration

Please note that you are only allowed to use the products, modules and extensions that you have purchased. For any questions please contact your sales representative.

Capacity

Please check the license and enter the capacities that were licensed to you:

Concurrent calls: * 100000

□ RTP Recording

Concurrent RTP streams: *

Additional Extensions

☑ Non Calls

☑ UCaaS CCaaS

☑ Stir/Shaken

Extensions

☑ App support
☑ CDR
☑ Diameter
☑ ENUM
☑ Gateway control protocols
☑ REST API
□ SAU
□ Skype for Business
☑ SIGTRAN
☑ Media quality

On the left side of the page you must enter the number of concurrent calls printed on your license. On the right side you must check the product extensions you have a license to use. All enterprise customers should automatically check **Media quality**.

> **Note**
>
> The number of Concurrent RTP streams can cause performance and stability issues if it is set higher than the hardware and the network permits. Values above 20 are not recommended. Changes to the RTP recording setting take effect only after a restart of the system. If you have multiple servers involved in your set up (additional standalone Probes servers connected to the Mediation Engine), this setting must be set on each Probe (unless certain Probe is not sniffing Media so that RTP recording is not really applicable for the Probe). In such scenarios, the value that is set should be same on each node, on the Mediation Engine (or the Mediation Engine with local Probe), and the Probes.

Click the **continue** button to navigate to the ME Connection List page.

Mediation Engine Connection List

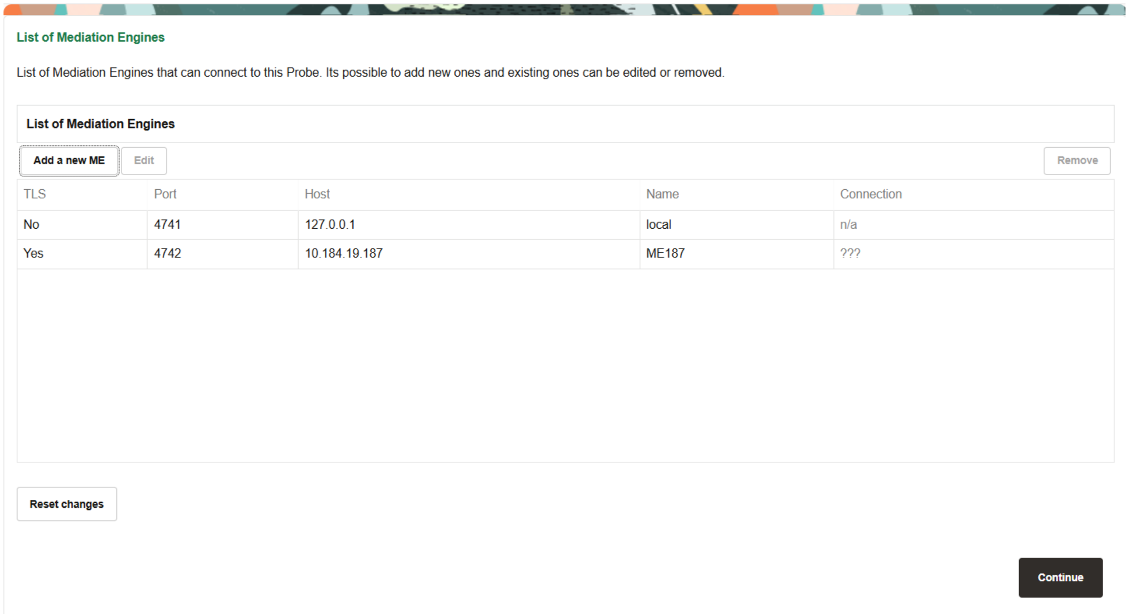
For a Probe machine type, the Mediation Engine Connection List page allows you to configure which Mediation Engines the Operations Monitor Probe connects to.

The following figure shows the ME Connection List page.

The Operations Monitor Probe can connect to one or more Mediation Engines, using TLS encryption, or with some configurations, also cleartext. Likewise, a Mediation Engine can connect to more than one Operations Monitor Probe (as well as Session Border Controller Probes).

On the Mediation Engine, cleartext connections are usually on port 4741 and encrypted connections on port 4742. For encrypted connections, the Operations Monitor Probe and the Mediation Engine need to be able to verify the certificate of the other party.

Figure 4-6   List of Mediation Engines



List of Mediation Engines

List of Mediation Engines that can connect to this Probe. Its possible to add new ones and existing ones can be edited or removed.

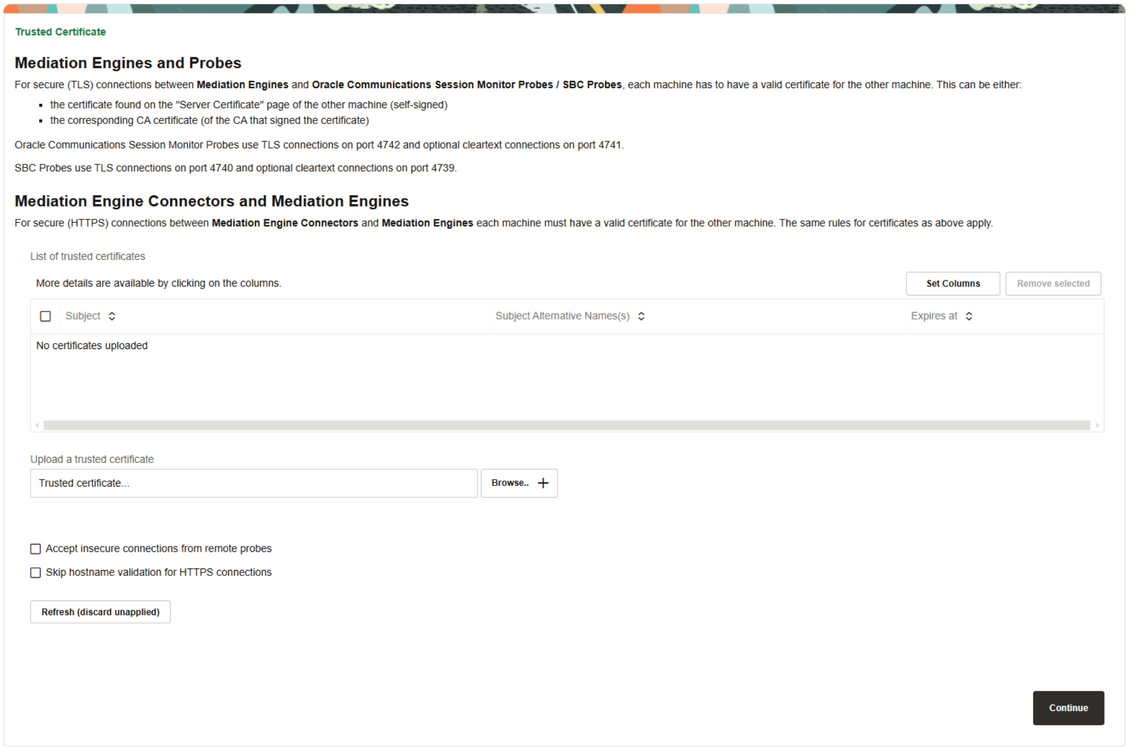
List of Mediation Engines

TLS	Port	Host	Name	Connection
No	4741	127.0.0.1	local	n/a
Yes	4742	10.184.19.187	ME187	???

The Mediation Engine machines by default only accept encrypted connections (unless the Mediation Engine and Probe are on the same machine); for unencrypted connections the check box Accept insecure connections from remote probes on the Trusted Certificate page must be checked.

The following figure shows the Trusted Certificate page.

Figure 4-7 Trusted Certificate page



Trusted Certificate

Mediation Engines and Probes

For secure (TLS) connections between **Mediation Engines** and **Oracle Communications Session Monitor Probes / SBC Probes**, each machine has to have a valid certificate for the other machine. This can be either:

- the certificate found on the "Server Certificate" page of the other machine (self-signed)
- the corresponding CA certificate (of the CA that signed the certificate)

Oracle Communications Session Monitor Probes use TLS connections on port 4742 and optional cleartext connections on port 4741.

SBC Probes use TLS connections on port 4740 and optional cleartext connections on port 4739.

Mediation Engine Connectors and Mediation Engines

For secure (HTTPS) connections between **Mediation Engine Connectors** and **Mediation Engines** each machine must have a valid certificate for the other machine. The same rules for certificates as above apply.

List of trusted certificates

More details are available by clicking on the columns.

□ Subject	Subject Alternative Names(s)	Expires at
No certificates uploaded		

Upload a trusted certificate

Trusted certificate...

□ Accept insecure connections from remote probes

□ Skip hostname validation for HTTPS connections

Typical Connection Scenarios

Mediation Engine and Operations Monitor Probe Are on the Same Machine

For setups with a Mediation Engine machine with an embedded Probe, a cleartext connection is automatically added to the ME connection list. For cleartext connections, no certificates are exchanged.

One Mediation Engine and Two Operations Monitor Probes

For setups with one Mediation Engine and two Operations Monitor Probes, the self-signed server certificates of both Operations Monitor Probes are uploaded as trusted certificates on the Mediation Engine, and the self-signed server certificate of the Mediation Engine is uploaded on both Operations Monitor Probes as a trusted certificate. On each Operations Monitor Probe, the IP of the Mediation Engine is added to the ME connection list with TLScheck box selected.

The following table describes the actions to configure the connections between one Mediation Engine and two Operations Monitor Probes.

Table 4-1 One Mediation Engine and Two Operations Monitor Probes

Machine	Action
Mediation Engine	• Download the Server Certificate. • Upload the Server Certificate of the Operations Monitor Probe1 to Trusted Certificate. • Upload the Server Certificate of the Operations Monitor Probe2 to Trusted Certificate.
Operations Monitor Probe 1	• Download the Server Certificate. • Upload the Server Certificate of the Mediation Engine to Trusted Certificate. • Add IP of the Mediation Engine to the ME Connection List, with TLS connection.
Operations Monitor Probe 2	• Download Server Certificate. • Upload Server Certificate of the Mediation Engine to Trusted Certificate. • Add IP of Mediation Engine to ME Connection List, with TLS connection.

Two Mediation Engines and One Operations Monitor Probe

For setups with two Mediation Engines and one Operations Monitor Probe, the self-signed server certificate of the Operations Monitor Probe is uploaded as trusted certificate on both Mediation Engines, and the self-signed server certificates of the Mediation Engine are uploaded on the Operations Monitor Probe as a trusted certificate. On the Operations Monitor Probe, the IPs of the Mediation Engines are both added to the ME connection list with TLScheck box selected.

The following table describes the actions to configure the connections between two Mediation Engines and one Operations Monitor Probe.

Table 4-2 Two Mediation Engines and One Operations Monitor Probe

Machine	Action
Mediation Engine 1	• Download the Server Certificate. • Upload the Server Certificate of the Operations Monitor Probe to Trusted Certificate.
Mediation Engine 2	• Download the Server Certificate. • Upload the Server Certificate of the Operations Monitor Probe to Trusted Certificate.
Operations Monitor Probe	• Download the Server Certificate. • Upload the Server Certificate of Mediation Engine 1 to Trusted Certificate. • Upload the Server Certificate of Mediation Engine 2 to Trusted Certificate. • Add IP of Mediation Engine 1 to ME Connection List, with TLS connection. • Add IP of Mediation Engine 2 to ME Connection List, with TLS connection.

All Other Scenarios

For setups with more than two Operations Monitor Probes or Mediation Engines, Oracle recommends that you use PKI (Public Key Infrastructure) with root certificates as described in *Oracle Communications Session Monitor Security Guide*.

Secure Configuration

To help protect users of Session Monitor and consumers' data, see the Session Monitor Security Guide for information on the security features of Session Monitor.

During the installation of a Session Monitor server, you will encounter the server certificate and trusted certificate pages.

Server Certificate

The Server Certificate page is used to see and change the certificate used by this server. This step is recommended to protect users' data.

For more information, see the discussion about encryption and certificates in the Session Monitor Security Guide.

Server Certificate

During a fresh installation, the Platform Setup Application automatically generates a self-signed certificate. You can sign a certificate signing request (CSR) with your own PKI and authenticate it on the Session Monitor server for trusted access or you can regenerate a new self-signed certificate.

It is recommended that you use CA-signed certificates. Starting with Release 6.1. the Server Certificate option allows you:

- Select one of these options:
  - Sign Certificate (for generating CSR)
  - Regenerate Key and Certificate
- Configure several parameters directly from the PSA page (Platform Setup Application) using the Advanced configuration dialog box
- Create key pairs with different configurations

To proceed further with the configuration, you must select any one of the options:

- Sign Certificate

or

- Regenerate key and Certificate

Generating a Self Signed Certificate

You can sign a certificate signing request (CSR) with your own PKI and authenticate it on the Session Monitor server for trusted access or you can also regenerate a new self-signed certificate.

1. **Sign Certificate**:

a. when you select the Sign Certificate option, the IP address of the machine is already added:
b. Click **Advanced Configuration**. For information, on the next steps, see the Advanced Configuration section.
c. Click **Download Request** to download the CSR. A new key pair is generated as per the configurations made in the previous step. The location is `opt/oracle/ocsm/etc/iptego/csr/CSR_KEY.key`.
d. Click **Upload** to upload the signed certificate.

> **Note**
>
> when signed certificates are uploaded or regenerated, all dependent TLS connections are interrupted and must be re-established using the new signed certificate.

2. **Regenerating Key and Certificate**:
   a. When you select this option, the IP address of the machine is already added.
   b. Click **Advanced Configuration**. For information, on the next steps, see the Advanced Configuration section.
   c. Click **Apply** to generate a new certificate using the settings made in the Advanced Configuration section and install the certificate on the system.

> **Note**
>
> Regenerating the key and self-signed certificate breaks the existing certificate pinnings and signatures.

Advanced Configuration

The **Advanced Configuration** dialog box enables you to configure certificate parameters.

The fields Organization, Organization Unit, Common Name, Key Algorithm, Key Size, and Digest Algorithm are mandatory. By default, these fields are populated with default values, but you can may edit these fields as needed. Advanced Configuration is optional.

1. In the pop-up dialog box, add details for the configurable fields:

Table 4-3 Configurable parameters

Parameter	Description	Values
Country Code	• Two-letter country code where the organization is located. • Required for X.509 certificates to specify the country in the certificate's distinguished name (DN).	Select a value from the drop down list.

Table 4-3 (Cont.) Configurable parameters

Parameter	Description	Values
State	• State or province name where the organization is located. • Used to further specify the organization's location in the certificate	Provide an appropriate value
Locality	• City or locality name where the organization is located. • Used to specify the city or locality in the certificate.	Provide an appropriate value
Organization	• Name of the organization that owns the certificate. • Required for organizational identification in the certificate	Default Value: Oracle Corporation. This can be edited.
Organization Unit	• Unit Department or unit within the organization. • To specify the organizational unit responsible for the certificate.	Default Value: Communications. This can be edited.
Common Name	• Fully Qualified Domain Name (FQDN) for which the certificate is issued. • Essential for SSL/TLS certificates to secure a specific domain.	Default Value: Oracle Communications Session Monitor. This can be edited.
Key Usage List	• Defines the purposes for which the key can be used. • Used to enforce proper usage of the certificate's key. • To restrict the key usage to specific purposes	• digitalSignature* • nonRepudiation* • keyEncipherment* • dataEncipherment • keyAgreement • keyCertSign • cRLSign • encipherOnly • decipherOnly * stands for Mandatory fields **Note** Either leave this blank or necessarily include: • digitalSignature • nonRepudiation • keyEncipherment

Table 4-3 (Cont.) Configurable parameters

Parameter	Description	Values
Extended Key Usage List	• Specifies additional purposes for the certificate. • Used for more granular control over the certificate's use cases.	• serverAuth* • clientAuth* • codeSigning • emailProtection • timeStamping • OCSPSigning • ipsecIKE • msCodeInd • msCodeCom • msCTLSign * stands for Mandatory fields **Note** Either leave this blank or necessarily include: • serverAuth • clientAuth
Key Algorithm	• Used when generating the key pair to determine the algorithm. • To specify the cryptographic algorithm for the key pair.	• RSA • ECDSA
Key Size	• Size of the cryptographic key in bits. • Used when generating the key pair for the certificate. • To determine the strength of the encryption	• RSA – 2048 – 3072 – 4096 • ECDSA: – p256 – p384
Digest Algorithm	• Hash function used for signing the certificate. • To ensure the integrity and security of the certificate	• SHA256 • SHA384 • SHA512

2. Click **OK** to apply the configuration changes. Clicking Reset sets all fields to their default values.

> ⓘ **Note**
>
> The **Key Usage List** and **Extended Key Usage List** parameters are used to specify the intended purposes of a certificate. Ensure that any modifications to these parameters comply with the Certificate Authority (CA) signing process guidelines and specifications required for Certificate Signing Request (CSR) generation.

Trusted Certificates

The Trusted Certificates page is used to configure the authentication of Session Border Controllers. This step is necessary before attempting to connect Session Border Controllers to Session Monitor.

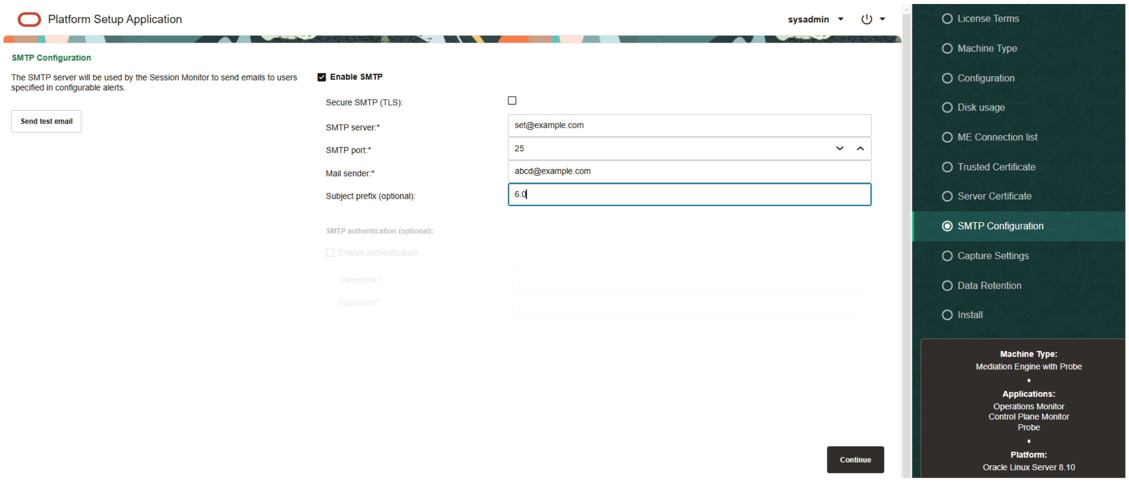
For secure (HTTPS) connections between Mediation Engine Connectors and Mediation Engines, each machine must have a valid certificate for the other machine. The same rules for certificates as for Mediation Engine and Probe.

For more information, see the discussion about connection with Oracle Session Border Controller in *Session Monitor Security Guide*.

Configuring the SMTP Settings

The following figure shows the SMTP Configuration page.

Figure 4-8   SMTP Configuration page



SMTP Configuration

The SMTP server will be used by the Session Monitor to send emails to users specified in configurable alerts.

☑ Enable SMTP

Secure SMTP (TLS): ☐

SMTP server:* set@example.com

SMTP port:* 25

Mail sender:* abcd@example.com

Subject prefix (optional): 6.0

SMTP authentication (optional):

☐ Enable authentication

Username:*

Password:*

Machine Type:
Mediation Engine with Probe

Applications:
Operations Monitor
Control Plane Monitor
Probe

Platform:
Oracle Linux Server 8.10

Session Monitor can send notifications and alerts directly to users' email addresses. Which notification to send to which address is configured in the relevant products. However, you first need to configure the SMTP settings properly for this feature to be available.

Setting Up the Mail Server

To use the email notification feature, select **Enable SMTP** check box. The system needs an SMTP server to send emails. Contact your network administrator to find out the address of the server your organization uses. The default port is the standard port 25.

If the server requires a valid email account, you will need to create one for Session Monitor. Then, select **Enable authentication** check box and enter the credentials.

Setting Up the Email Notifications

You can choose how the emails from Session Monitor will look like in the users' mailboxes. The field **Mail sender** is the email address Session Monitor will use; users will see this address in the **Sender:** or **From:** field of the emails. You can optionally specify a **Subject prefix** ; which appears at the beginning of the subject of the emails and make it easy to identify Session Monitor's emails in users' inbox.

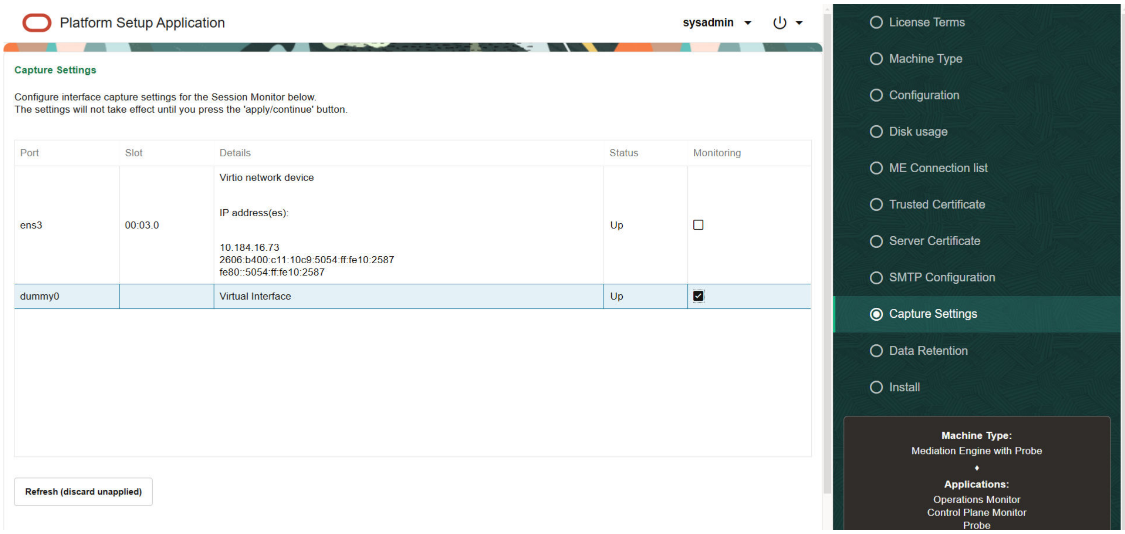
Configuring the Capture Settings

The Capture Settings page contains a list of configured network interfaces, with a toolbar for deleting interfaces, as well as a restore button to reset the last applied settings (usually, you want to add interfaces you didn't add during the installation procedure).

There's also a check box below the network list that can be checked if you wish to apply capture settings that won't allow you to reconnect to the Platform Setup Application again.

The following figure shows the Capture Settings page.

Figure 4-9 Capture Settings



Platform Setup Application

sysadmin

Capture Settings

Configure interface capture settings for the Session Monitor below.
The settings will not take effect until you press the 'apply/continue' button.

Port	Slot	Details	Status	Monitoring
ens3	00:03.0	Virtio network device IP address(es): 10.184.16.73 2606:b400:c11:10c9:5054:ff:fe10:2587 fe80::5054:ff:fe10:2587	Up	☐
dummy0		Virtual Interface	Up	☑

Refresh (discard unapplied)

Machine Type:
Mediation Engine with Probe

Applications:
Operations Monitor
Control Plane Monitor
Probe

Note

Monitoring is only enabled for machines that are configured as probes. On other machines, the monitoring check box is grayed out.

Important

Do not configure dummy interfaces with DHCP if there is no DHCP server to give an IP. When applying settings with a dummy interface using the DHCP method wait for the DHCP client to time out (usually one minute).

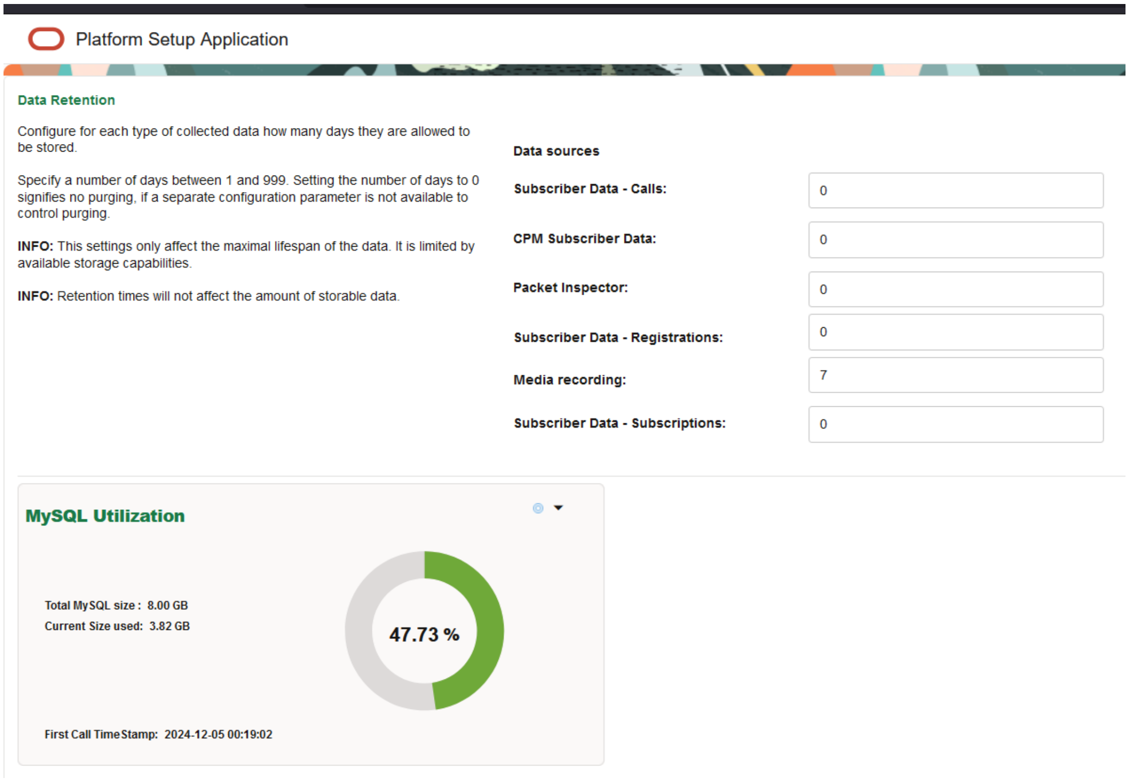
Data Retention

Data Retention allows you to get information on the utilization of MySQL. This feature is available for machine types of Mediation Engine + Probe or Mediation Engine.

Data Retention provides a graphical representation of the MySQL storage utilization. It provides an intuitive, and real-time insights into MySQL storage utilization. The Data Retention option in the Platform Setup Application, provides information on: :

- Total MySQL size
- Current size
- First call timestamp

Figure 4-10 Data Retention



Platform Setup Application

Data Retention

Configure for each type of collected data how many days they are allowed to be stored.

Specify a number of days between 1 and 999. Setting the number of days to 0 signifies no purging, if a separate configuration parameter is not available to control purging.

INFO: This settings only affect the maximal lifespan of the data. It is limited by available storage capabilities.

INFO: Retention times will not affect the amount of storable data.

Data sources

Subscriber Data - Calls:	0
CPM Subscriber Data:	0
Packet Inspector:	0
Subscriber Data - Registrations:	0
Media recording:	7
Subscriber Data - Subscriptions:	0

MySQL Utilization

Total MySQL size : 8.00 GB
Current Size used: 3.82 GB

First Call TimeStamp: 2024-12-05 00:19:02

You can view the graphical representation (a meter gauge) for the current size used against the total MySQL size. Session Monitor appropriately formats the size. The amount of storage used is displayed in GB if the database is smaller than 1 TB. Any database instance that is configured with more storage than 1 TB is displayed as an absolute value in TB. The meter gauge also indicates the percentage of the current MySQL size that is being used out of the total capacity. If there is no data available (when installed for the first time), the GUI displays "No data available" instead of the meter gauge. The interface provides a data refresh feature that includes options such as:

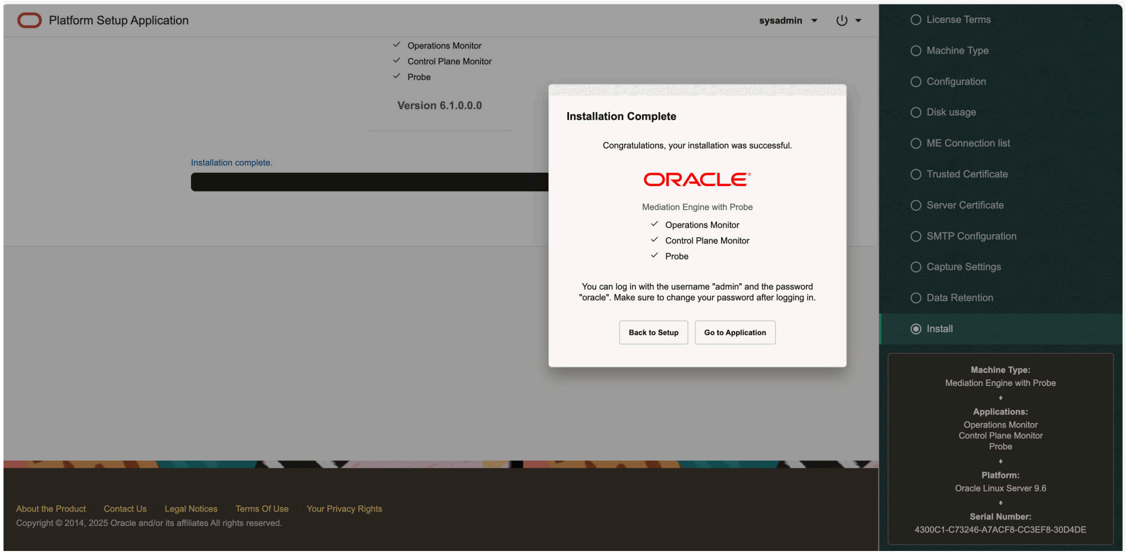
- 30 seconds
- 1 minute
- 2minutes
- 5 minute

Installing the Products

The Install page summarizes the components to install. Check that you selected the correct components; after the installation is complete, the selection of the components cannot be changed.

The following figure shows the Install page.

Figure 4-11 Install page



Platform Setup Application

✓ Operations Monitor
✓ Control Plane Monitor
✓ Probe

Version 6.1.0.0.0

Installation complete.

Installation Complete

Congratulations, your installation was successful.

Mediation Engine with Probe
✓ Operations Monitor
✓ Control Plane Monitor
✓ Probe

You can log in with the username "admin" and the password "oracle". Make sure to change your password after logging in.

Machine Type: Mediation Engine with Probe

Applications: Operations Monitor, Control Plane Monitor, Probe

Platform: Oracle Linux Server 9.6

Serial Number: 4300C1-C73246-A7ACF8-CC3EF8-30D4DE

Copyright © 2014, 2025 Oracle and/or its affiliates All rights reserved.

Click **Install** to start with the installation. The Platform Setup Application initiates the installation process and reports back the progress. The installation process might take a few minutes to complete.

You can click on the **Session Monitor** button when the installation is complete. This will bring you to the installed products' interface.

5

Session Monitor Post-Installation Tasks

This chapter provides instructions for Oracle Communications Session Monitor post-installation tasks.

Installing Software Update

After you log in to the product interface, you can see the status of the system or update the system. A system update will update all applications as well as the Platform Setup Application itself.

The Software Version page shows the currently installed components and the software version.

To install a software update, go to the Software Version page and select the update file (file type .rpm) that was provided by Oracle or your service provider. Click **Apply** to initiate the upload.

When the upload has finished, the page will show the version number and issue the date of the update. Click **Install** to proceed with upgrading the system. You can also abort the upgrade by clicking **Clear**.

> **Important**
>
> Session Monitor or parts of it may not be available during the update process.

Platform Setup Application will show the progress during the upgrade. You may click **Close** to hide the progress window.

After the successful upgrade, establish an SSH session with the product and execute the following command:

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

> **Note**
>
> If you have a setup with multiple servers (for example, Mediation Engine, Mediation Engine Connector, Probe(s)), upgrade all of them at the same time. Running different servers (Mediation Engine, Mediation Engine Connector, probe(s)) of the Session Monitor on different versions is not supported.

Media Protocols

The Media Protocols menu is available after the installation process has finished and only for machine type Probe (which includes the machine type Mediation Engine with Probe).

You use the Media Protocols page to identify the RTP traffic that the Probe looks for. The Probe accepts only the traffic that matches the BPF filter.

Filters

You can set the media protocols filter as follows:

- **Check all traffic for signaling:** When this check box is enabled, all traffic (including the traffic that matches the BPF filter rule) is passed to the signaling probes for filtering using the signaling protocols filters. When this check box is disabled, only the traffic that does not match the BPF filter rule is passed to the signaling probes. If you use Packet Inspector for media recording, you need to enable this option to filter the media packets using the Packet Inspector filter in **Signaling Protocols**.

  > ⓘ **Note**
  >
  > Packet Inspector supports STCP, TCP, and UDP as transport protocol for capturing the signaling network traffic or media. Due to the design limitation, other transport protocols such as ICMP are not supported.
  > Enabling this option may decrease system performance.

- **BPF filter:** This filter identifies the RTP traffic. Only the traffic that matches this filter rule is considered. You might want to configure the filter rule to pick up only the packets you are interested in. Ignoring the unwanted packets reduces the stress on the system and increases performance. The traffic that does not match this filter is passed to the signaling probes for filtering using the signaling protocols filters

See the Signaling Protocols section for more information about signaling protocols.

See the Filter Syntax section for more information about filters.

Status

The following status are shown for the RTP packets:

- **Active streams:** Specifies the number of RTP streams found. Only the traffic that matches the filter is counted.
- **Packets processed:** Specifies the packets that match the filter and processed successfully.
- **Packets dropped:** Specifies the packets that match the filter but not processed due to insufficient resources.

Signaling Protocols

The Signaling Protocols menu is available after the installation process has finished and only for machine type Probe (which includes the machine type Mediation Engine with Probe).

You use the Signaling Protocols page to identify the types of traffic the various probes (which sniff traffic) look for. The Probe accepts only the traffic that matches the filter rule and sends them to the Mediation Engine.

You might want to configure strict filtering rules for several reasons:

- The probes process all traffic that matches the filter. For most installations, the high volume of traffic makes inspecting every packet infeasible. Ignoring unnecessary packets, therefore, puts less stress on your system and makes subsequent analysis easier. For example, you may want to make sure the signaling probe, which monitors SIP, does not also get all the RTP traffic.
- You might not be interested in certain sources of traffic, even though the machine would pick it up.
- More complex VLAN configurations.

The default filters are sufficient for most installations and provide a good starting point.

After you configure the filters, it takes a few seconds for the probe(s) to reconfigure. The statistics on this page should show the totals for the new filters. The **Packets processed** statistic is a good indicator of how the filters are working.

> **Note**
>
> - Make sure to use vlan keywords in the filters when that is used on the network.
> - Make sure to change the default filters if you use non-standard ports or other options.
> - Traffic is first filtered using the media protocols setting. Only the traffic that does not match the media protocols BPF filter (except when **Check all traffic for signaling** filter option is enabled) is passed to the signaling probes.
> - If you use Packet Inspector for recording media, you need to include media packets in the Packet Inspector filter.
> - You need to ensure that there is sufficient disk space for storing media on the Probe machine. Media packets are initially stored on the Probe machine. The Probe forwards the packets to the Mediation Engine only when a user downloads the media to a PCAP file. When the disk is full, the Probe overwrites the calls stored on the disk with new calls. You can define the Packet Inspector filter to restrict the calls stored on the Probe and thus minimize calls that are overwritten.

For more information about filters, see the Filter Syntax section.

Packet Deduplication

You can select to turn on packet deduplication for the associated traffic type. If you turn on packet deduplication, you must also provide a time value in milliseconds. The value should be greater than zero.

Packet deduplication is done at L3 and above and it is best effort. Some types of traffic might not get deduplicated, for example, duplicates on nested VLANs, ipv6, and so on.

There is a System Setting to enable deduplication in the core, which should be enabled if there are multiple Probes connected to one Mediation Engine, and seeing the same traffic. If traffic is seen without and with vLAN tags, you should also disable VLAN awareness in **System Setting**.

Statistics per Protocol

The following statistics are shown for each protocol:

- **Rate:** Specifies the total number of packets accepted after the filtering.
- **Packets processed:** Specifies the number of packets processed in the last second. Only packets that match the filter are processed.

Global Statistics

The following statistics are shown for all devices:

- **Total sniffed:** Specifies the number of packets sniffed across all configured devices.
- **Total dropped:** Specifies the number of packets that were not processed. Packets were dropped either by the NICs or during processing due to system performance reasons. If possible, tighten the filter rules and disable the **Check all traffic for signaling**filter option in **Media Protocols** to ignore unnecessary packets and reduce stress on the system. If that is not possible, consider upgrading the machine.

System Diagnostics

The System Diagnostics menu allows the creation of a report with information on the installation. This report may be requested by the support team in case of issues.

Creating a Report

A report can be created by clicking **Create**. This may take several minutes to complete. Afterwards, the report can be downloaded as a file by clicking **Download**. This file can then be sent to the support team, for example by email.

If a report exists, its creation date will be shown. It can be downloaded as often as necessary, but there can be only one report at a time; creating a new report will overwrite any existing one.

Reports are deleted around midnight UTC.

Report Contents

The contents of a report include:

- Information on the available hardware of the machine that the monitoring solution is running on
- Log files
- Configuration of the monitoring solution
- Statistics about the performance and status of components of the system and of the monitoring solution
- If the check box **Include mysql dump...** is checked, the report includes a dump of most of the database tables. Note that the respective tables might be huge.
- If the check box **Include mysql dump...** is not checked, the report will include only minimal information about the database tables.

> ⓘ **Note**
>
> Sensitive information is removed before report creation, including, but not limited to, passwords, keys, and certificates.

Filter Syntax

The filter syntax used is the same as tcpdump or libpcap. For an example, see https://wiki.wireshark.org/CaptureFilters.

The following filters are also known as BPF filters:

- (tcp port 5060)
- ((udp or tcp) and port 5060)
- (vlan (udp or tcp) and port 5060)
- (tcp portrange 5060-5070)
- (not port 5060)
- (host 10.10.0.5 and port 5060)
- (not host 10.10.0.5 and port 5060)
- (not ether dst 12:34:56:78:90:ab)

Entries with a vlan keyword must be included for networks using VLANs. It is harmless to include them on networks which don't use VLANs, but do make sure there is a separate identical filter without the vlan. For example, (tcp port 5060) or (vlan and tcp port 5060).

Support for Backup and Restore

Session Monitor enables you to back up the Configuration, Database, and Potential Customized Files of the Session Monitor Servers using the Backup and Restore procedure.

You can use the Backup and Restore procedure to back up your older Session Monitor Release data during the upgrade to version Release 6.1 and restore it if the upgrade fails. For more information, see the Oracle Communications Session Monitor Release 6.1 Backup and Restore Guide.

6

Configuring LDAP and RADIUS Authentication

This section explains how to configure LDAP and RADIUS authentication to provide centralized user management and secure access control.

By integrating these two services, administrators can streamline authentication across systems and ensure consistent policy enforcement.

Configuring External Authentication for Session Monitor with Radius Service

This section explains how to configure the external authentication for Session Monitor with Radius Service using Apache Web Server.

For more information, refer to the following sections for configuring External Authentication with RADIUS service.

Troubleshooting External Authentication Issues for RADIUS on an SELinux Machine

On an SELinux-enabled machine, do not copy any modified `pld.conf` file from a different location and replace it with the existing file, as SELinux blocks access to such files. Instead, edit the `pld.conf` file contents directly using the vi/vim editor.

On an SELinux enabled machine, for External Authentication with the RADIUS Server, after copying the `mod_auth_xradius.so` file to the directory `/usr/lib64/httpd/modules/`, execute the this command to prevent SELinux from blocking access:

```
chcon -t httpd_modules_t /usr/lib64/httpd/modules/mod_auth_xradius.so
```

On a SELinux enabled machine, for External Authentication with Radius, perform the following tasks if you encounter this error after restarting HTTPD: `Permission denied: xradius: Cannot create DBM Cache at `/var/authxcache'`.

```
chcon -R -t httpd_cache_t /var/authxcache.dir
chcon -R -t httpd_cache_t /var/authxcache.pag
systemctl restart httpd.service
```

Configuring Apache for Authenticating with RADIUS Server

This section explains how to configure the external authentication for Session Monitor with the Radius Service using the Apache Web Server.

1. Log in to Session Monitor.
2. Click **Admin** and select **Settings**.
3. Enable the setting, **External authentication enabled** and set it to **True**.

4. **Log out** from Session Monitor.
5. If the current web service is NGINX, change to HTTPD by following the steps mentioned in Configuring Reverse Proxy Server.
   a. Run the following commands to install the Apache Web Server and mod_ssl packages:

   ```
   yum install httpd mod_ssl
   ```

   > **Note**
   >
   > If you have a proxy server, to complete the download, edit the proxy settings for the external downloads to be successful.

   b. Install the Apache Web Server and `mod_ssl packages` together as the HTTPD package executes a post-install script that uses `mod_ssl` to generate a localhost certificate. The localhost certificate is required for the default HTTPD service configuration. If the certificate is not generated, enter the following lines in the `/etc/httpd/conf.d/ssl.conf` file to start the HTTPD server:

   ```
   SSLCertificateFile /etc/pki/tls/certs/localhost.crt
   SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
   ```

6. If the localhost certificates are not generated, remove the `ssl.conf` file from the `/etc/httpd/conf.d` directory to start the Apache server.

   > **Note**
   >
   > When using HTTPD/Apache for web server due to external authentication configuration, if upgrade is applied ("dnf upgrade" OR HTTPD Upgrade) and httpd is updated, a new ssl.conf file is created. Hence, either remove, or move the ssl.conf file using this command and restart the HTTP service: :
   >
   > ```
   > mv /etc/httpd/conf.d/ssl.conf{,.orig}
   > ```

7. Run the following commands to install all additional packages:

   ```
   yum groupinstall "Development Tools"
   yum install httpd-devel
   ```

8. To install Apache modules for Radius authentication, run the following commands:

   ```
   wget http://www.outoforder.cc/downloads/mod_auth_xradius/
   mod_auth_xradius-0.4.6.tar.bz2
   tar -xvf mod_auth_xradius-0.4.6.tar.bz2
   cd mod_auth_xradius-0.4.6
   ```

9. A code change is required in the `xradius_cache.c` file, for the module to install properly:

   ```
   $ vi /root/mod_auth_xradius-0.4.6/src/xradius_cache.c
   ```

10. Copy the following lines into the editor and press the ENTER key:

    ```
    :%s/unixd_config/ap_unixd_config/g
    ```

11. Save the file.

12. To install the module files successfully, run the following commands:

    ```
    $ ./configure --with-apxs=/sbin/apxs
    $ make
    $ make install
    $ cd ..
    ```

13. Ensure that the `mod_auth_xradius.so` file is present in the `/usr/lib64/httpd/modules/` directory of your machine.

    ```
    #ls -lrt /usr/lib64/httpd/modules/mod_auth_xradius.so
    -rwxr-xr-x. 1 root root 193976 Mar 20 13:27 /usr/lib64/httpd/modules/
    mod_auth_xradius.so
    ```

14. To load the required modules into the HTTPD configuration, edit the file `/etc/httpd/conf/httpd.conf` and paste the following lines. Better to put under any 'Load Module' section or under any commented 'Load module' sample code) and save the file.

    ```
    LoadModule auth_xradius_module /usr/lib64/httpd/modules/mod_auth_xradius.so
    AuthXRadiusCache dbm /var/authxcache
    ```

15. Edit the `pld.conf` file:

    ```
    vi /etc/httpd/conf.d/pld.conf
    ```

16. Edit the following location in the file as below:

    ```
    <LocationMatch "^/me/(?!(proxy/|c/|r/|scripts/|/help/|logout\.html)).*$">
            #
            # BEGIN LDAP Auth
            # Uncomment and adjust the lines below for LDAP Auth
             AuthName "OCSM COM"
             AuthType basic
           AuthXRadiusAddServer "<Radius Server IP>:1812" "<Radius Shared
    Secret>"
             AuthXRadiusTimeout 2
             AuthXRadiusRetries 2
             AuthBasicProvider xradius
             Require valid-user
             RewriteEngine On
             RewriteCond %{SERVER_PORT} 443
             RewriteCond %{LA-U:REMOTE_USER} (.+)
             RewriteRule .* - [E=RU:%1,L]
            # AuthName should be the same as for /me/logout.html
            # AuthLDAPURL "ldap://ldap-server/dc=example,dc=org?uid?one"
            # AuthLDAPBindDN "cn=admin,dc=example,dc=org"
            # AuthLDAPBindPassword admin
             RequestHeader unset X-Forwarded-User
             RequestHeader set X-Forwarded-User %{RU}e
    ```

```
        # RequestHeader set X-Forwarded-User-Role ""
        # RequestHeader set X-Forwarded-User-Role %
{AUTHENTICATE_employeeType}e
        # RequestHeader unset X-Forwarded-User-Permission
        # RequestHeader set X-Forwarded-User-Permission %
{AUTHENTICATE_gecos}e
        # # Admin permission mask - all bits set
        # RequestHeader set X-Forwarded-User-Permission 4610266613338864839
        # Require valid-user
      # END LDAP Auth
    </LocationMatch>
```

> **Note**
>
> For Mediation Engine Connector, make similar changes under section <LocationMatch "^/mec/((?!(proxy/|r/|res/|help/|logout\.html)).*)$">

.

17. For a description of the parameters and information on the optional parameters in the RADIUS pld.conf file, see RADIUS pld.conf File Details.

> **Note**
>
> All Non admin users are required to be created on Operations Monitor first and then these users can log in via RADIUS Authentication.

18. If you have modified the Auth Name above, then modify the Auth Name in this section in the `pld.conf` file.

```
# Logout page for COM
    <Location /me/logout.html>
        AuthType basic
        # AuthName should be the same as for /me/
        AuthName "OCSM COM"
        AuthBasicProvider file
        AuthUserFile     "/opt/oracle/ocsm/etc/httpd/logout.htpasswd"
        Require           valid-user
        ProxyPass !
    </Location>
```

> **Note**
>
> Change the AuthName directive for Mediation Engine in <Location /me/logout.html> and for Mediation Engine Connector in <Location /mec/logout.html>

19. Run the following command to start and enable the HTTPD:

```
systemctl daemon-reload
systemctl restart httpd.service
```

The HTTPD server of Session Monitor has been configured for external authentication with RADIUS. When you open the Session Monitor in a web browser, the external authentication pop-up appears. On providing the correct RADIUS user credentials, you can log in successfully.

RADIUS pld.conf File Details

Edit the `pld.conf` file. Here, you can find the descriptions for the parameters that are edited and the optional parameters.

Table 6-1 RADIUS pld.conf file parameters

Parameters	Description
AuthXRadiusTimeout	The number of seconds to wait response from RADIUS Server.
AuthXRadiusRetries	The number of attempts to connect to server, expressed as positive integer value. Number of retries multiplied by timeout value should not exceed 30 (seconds)
AuthName	"OCSM COM" is the default name provided. It can be modified to any convenient name.
AuthBasicProvider	Type of authentication to use
<Radius Shared Secret>	This field must contain the secret that will be shared by Operations Monitor and the RADIUS server used for authentication.
<Radius Server IP>	The address of the RADIUS server against which Operations Monitor performs authentication.

Configuring RADIUS authentication over TLS (RadSec)

Session Monitor Release 6.1 offers secure RADIUS (RadSec) as an optional alternative to traditional UDP-based RADIUS. With RadSec, RADIUS messages are transmitted over TCP and secured using TLS, providing confidentiality, integrity, and certificate-based authentication, while avoiding the risks associated with legacy MD5 mechanisms.

Session Monitor employs the radsecproxy module to serve as an intermediary between the application and the RADIUS server. It receives local RADIUS requests from Session Monitor, encapsulates them within a TLS-protected TCP tunnel with certificate validation, forwards them to the external RADIUS server, and relays the responses back to Session Monitor.

Key Capabilities

> **Note**
>
> Use of RadSec is optional. There is no impact on current RADIUS authentication mechanisms.

- Secure RADIUS communication using TLS (RadSec) instead of traditional UDP.
- Support for both internal (nginx) and external (httpd) RADIUS authentication configurations within Session Monitor.
- Compatible with TLS 1.2 and TLS 1.3

- Seamless integration with existing RADIUS infrastructure using the radsecproxy module.
- Failover support with multiple RADIUS servers.

Getting Ready to Configure RadSec

Follow the steps given here to configure RadSec.

1. Log in to the Session Monitor CLI as the root user or root privileged
2. Install the necessary dependencies by running the following commands:

```
yum groupinstall "Development Tools"
yum install nettle-devel
```

3. Go to the official radsecproxy website using this link to download the radsecproxy source code:
   - Official website radsecproxy:
   - Download link: Download the radsecproxy source code.

> **Note**
>
> radsecproxy version 1.11.2 is the latest version validated by Session Monitor at the time of Release 6.1.

4. Run this command to extract the radsecproxy bundle with tar:

```
tar -xvf radsecproxy-1.11.2.tar.gz
```

5. (**Optional** radsecproxy has an idle timeout setting set to 300 seconds (5 minutes) by default. If a connection remains idle (there is no data transmitted between the Session Monitor and RADIUS server) for 5 minutes, radsecproxy automatically closes the connection and a new connection gets established when the next RADIUS request comes in. To make this connection remain open indefinitely from radsecproxy side, even if they are not actively being used, set `IDLE_TIMEOUT` parameter as 0 by making below code change in 'radsecproxy.h' file.

> **Note**
>
> The effective timeout also depends on your RADIUS server’s timeout settings; even if radsecproxy is configured for no timeout, the RADIUS server may still close idle connections based on its own timeout settings.

   a. Go to the radsecproxy directory.
   b. Run this command in the radsecproxy directory:

```
cd radsecproxy-1.11.2
sed -i 's/IDLE_TIMEOUT 300/IDLE_TIMEOUT 0/' radsecproxy.h
```

> **Note**
>
> Skipping this step does not affect authentication. radsecproxy automatically establishes a new connection when the next RADIUS authentication request is sent.

Install the Module Files

To install the module files successfully make sure that you are inside the radsecproxy-1.11.2 directory and build the package by running the following commands in order:

1. Run the following commands in order:

   ```
   cd radsecproxy-1.11.2
   ./configure
   make
   make install
   ```

2. If your RadSec-enabled RADIUS server is configured with a fully qualified domain name (FQDN), add an entry to the /etc/hosts file in the following format. Otherwise, you can skip this step.

   ```
   <_RADSEC_SERVER_IP>    _RADSEC_SERVER_FQDN
   ```

   For Example,

   ```
   123.4.5.6 myradiusserver.com
   ```

3. Create a configuration file named `radsecproxy.conf` in /etc/ location,

   ```
   vi /etc/radsecproxy.conf
   ```

4. Add the following content to the `/etc/radsecproxy.conf` file:

   ```
   # Master config file, all possible config options are listed below

   # First you may define any global options, these are:
   #
   # You can optionally specify addresses and ports to listen on
   # Multiple statements can be used for multiple ports/addresses
   ListenTCP       *:2083
   ListenUDP       localhost:1812


   # Optional log level. 3 is default, 1 is less, 5 is more
   LogLevel        3

   # Optional LogDestination, else stderr used for logging
   # Logging to file
   LogDestination      file:///var/log/radsecproxy.log


   # If we have TLS clients or servers we must define at least one tls block.
   ```

```
# You can name them whatever you like and then reference them by name when
# specifying clients or servers later. There are however three special
names
# "default", "defaultclient" and "defaultserver". If no name is defined for
# a client, the "defaultclient" block will be used if it exists, if not the
# "default" will be used. For a server, "defaultserver" followed by
"default"
# will be checked.
tls default {
    # You must specify at least one of CACertificateFile or
CACertificatePath
    # for TLS to work. We always verify peer certificate (client and
server)
    # CACertificatePath    /etc/radsecproxy/certs
    CACertificateFile    /etc/radsecproxy/certs/CA.pem

    # You must specify the below for TLS, we always present our certificate
    CertificateFile      /etc/radsecproxy/certs/CERT_PEM__
    CertificateKeyFile   /etc/radsecproxy/certs/CERT_KEY__

    # Optionally specify password if key is encrypted (not very secure)
    # CertificateKeyPassword  "_CERT_PASS"

    CipherList ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-
SHA384:ECDHE-RSA-AES128-GCM-
SHA256:TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_
SHA256:TLS_AES_128_CCM_SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-
CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES256-CCM:ECDHE-
ECDSA-AES128-CCM

    TLSVersion TLS1_2:TLS1_3
}


# Now we configure clients, servers and realms. Note that these and
# also the lines above may be in any order, except that a realm
# can only be configured to use a server that is previously configured.

# A realm can be a literal domain name, * which matches all, or a
# regexp. A regexp is specified by the character prefix /


client 127.0.0.1 {
    type    udp
    secret  radsec
}


server _RADIUS_SERVER {
    type    tls
    secret  radsec
    StatusServer on
# statusserver is optional, can be on or off. Off is default
}
```

```
# The realm below is equivalent to /.*
realm * {
    server _RADIUS_SERVER
}
```

Table 6-2 Field descriptions

Entry	Description
CACertificateFile	CA certificate file used to verify the peers certificate with the complete path
CertificateFile	Session Monitorclient certificate this radsecproxy will use
CertificateKeyFile	Specify the private-key file for the Session Monitor client certificate specified in CertificateFile
CertificateKeyPassword - (Optional)	The password to decrypt the private-key. Optionally specify password by replacing _CERT_PASS if key is encrypted (not very secure)
_RADIUS_SERVER	Replace _RADIUS_SERVER with IP address of the RadSec-enabled RADIUS Server, or a domain name (FQDN)
Secret	The secret must match the secret which you configured in your RadSec-enabled RADIUS server. Defaults to radsec as per RFC 6614.

> **Note**
>
> Only the above mentioned configuration has been validated in Session Monitor lab testing. Any additional changes are considered experimental. For information on all the options available, see the official configuration file: radsecproxy.conf-example.

> **Warning**
>
> The name of the radius server must match the FQDN or IP address in the RADIUS server certificate.

5. Save the changes made.
6. Create a directory under the /etc folder to store the certificates (For example, `/etc/radsecproxy/certs/`),
7. Copy all certificate files referenced in the configuration into it and set secure ownership and permissions (private keys 600, certificates/CA bundles 644 and all files owned by root:root). For example:

```
$ mkdir -p /etc/radsecproxy/certs/


# After copying give necessary permissions to all certificates files
$ chmod 644 /etc/radsecproxy/certs/ocsm_CA.pem
$ chmod 644 /etc/radsecproxy/certs/ocsm_client.crt
$ chmod 600 /etc/radsecproxy/certs/ocsm_client.key
$ chown root:root /etc/radsecproxy/certs/*


# Verify the ownership and permissions
$ ls -lrRt /etc/radsecproxy/certs/
-rw-------. 1 root root 1679 Apr 17 13:06 ocsm_client.key
-rw-r--r--. 1 root root 1281 Apr 17 13:06 ocsm_client.crt
-rw-r--r--. 1 root root 1395 Apr 17 13:06 ocsm_CA.pem
```

> ⓘ **Note**
>
> Ensure the directories holding the certificates and radsecproxy.conf have secure permissions and ownership.

8. To load radsecproxy as a systemd service, create the file: `/usr/lib/systemd/system/radsecproxy.service`.

   ```
   vi /usr/lib/systemd/system/radsecproxy.service
   ```

9. Paste the following contents into the `radsecproxy.service` file:

   ```
   [Unit]
   Description=RADIUS proxy with RadSec support
   After=syslog.target network-online.target
   Documentation=man:radsecproxy(1)

   [Service]
   Type=forking
   User=root
   Group=root
   ExecStart=/usr/local/sbin/radsecproxy -c /etc/radsecproxy.conf
   ExecReload=/bin/kill -HUP $MAINPID
   ProtectSystem=full
   ProtectHome=true
   PrivateDevices=true
   PrivateTmp=true

   [Install]
   WantedBy=multi-user.target
   ```

10. Reload systemd and start the radsecproxy service by running the following commands:

    ```
    systemctl daemon-reload
    systemctl enable radsecproxy
    systemctl start radsecproxy
    ```

11. Check the radsecproxy status and verify that it is up and running:

    ```
    systemctl status radsecproxy
    ```

12. Continue configuring RADIUS authentication as you normally would. Depending on your setup, follow the typical steps for:

- Internal RADIUS authentication (via nginx) or
- External RADIUS authentication (via httpd)

During the configuration of the RADIUS authentication:

- use localhost IP **127.0.0.1** as the IP addresss of the RADIUS server.
- Set **radsec** as the shared secret for RADIUS authentication.

This configuration ensures that all outgoing RADIUS communication over UDP is directed to radsecproxy, which then converts it into RadSec requests over TLS.

Internal RADIUS Authentication (via nginx)

To configure Internal RADIUS Authentication (via nginx):

1. On your Operations Monitor, Navigate to **Radius Authentication** under **admin** → **Settings** → **External Devices**.
2. Click the **RADIUS authentication enabled** checkbox to enable RADIUS authentication.
3. Configure details as given here:

Table 6-3 Radius Authentication

Field	Value	Remarks
RADIUS server hostname	127.0.0.1	Hostname should be localhost for internal communication with radsecproxy
RADIUS server port number:	1812	The UDP port on which the radsecproxy server is listening
RADIUS shared secret	radsec	This field must contain the secret that is shared by Operations Monitor and the RADIUS server used for authentication. The recommended and default will be radsec
RADIUS NAS identifier	OCOM	a string identifier and is used by the RADIUS server to determine whether or not the request is coming from Operations Monitor.
RADIUS timeout	5	Number of seconds to wait response from RADIUS server.
Number of retries issued by RADIUS client	3	Number of retry attempts if a request to the RADIUS server fails

For more information on configuring internal RADIUS authentication, see the section RADIUS Authentication in the Oracle Communications Operations Monitor User Guide.

External Authentication Using RADIUS (via apache httpd)

Follow the typical steps to configure External Authentication Using RADIUS as before and modify the pld.conf. Add the below configuration changes in section '<LocationMatch "^/me/':

```
...
    <LocationMatch "^/me/(?!(proxy/|c/|r/|scripts/|/help/|logout\.html)).*$">
        AuthName "OCSM COM"
        AuthType basic
        AuthXRadiusAddServer "RADIUS_IP:RADIUS_PORT" "RADIUS_SHARED_SECRET"
        AuthXRadiusTimeout 5
        AuthXRadiusRetries 3
        AuthBasicProvider xradius
        Require valid-user
        RewriteEngine On
        RewriteCond %{SERVER_PORT} 443
        RewriteCond %{LA-U:REMOTE_USER} (.+)
        RewriteRule .* - [E=RU:%1,L]
        RequestHeader unset X-Forwarded-User
        RequestHeader set X-Forwarded-User %{RU}e

        ProxyPassMatch balancer://mycluster
        ProxyPassReverse  balancer://mycluster
    </LocationMatch>
....
```

Replace AuthXRadiusAddServer line as below:

```
AuthXRadiusAddServer "127.0.0.1:1812" "radsec"
```

Table 6-4   AuthXRadiusAddServer

Entry	Value	Remarks
RADIUS_IP	127.0.0.1	Hostname should be local host to internal communication with radsecproxy
RADIUS_PORT	1812	The UDP port on which the radsecproxy server is listening
RADIUS_SHARED_SECRET	radsec	This field must contain the secret that is shared by Operations Monitor and the RADIUS server used for authentication. The recommended and default will be radsec
AuthXRadiusTimeout	5	Number of seconds to wait response from RADIUS server.
AuthXRadiusRetries	3	Number of retry attempts if a request to the RADIUS server fails

For more information on configuring external RADIUS authentication, see the section Configuring Apache for Authenticating with RADIUS Server in the Oracle Communications Session Monitor Installation Guide Release 6.1Installation Guide.

Configure OCOM IP on the RadSec-enabled RADIUS Server

On the RadSec-enabled RADIUS server, ensure that the OCOM IP is configured as a valid client in the RADIUS server settings.

This step is necessary to allow the RADIUS server to accept requests from the radsecproxy and route them to the appropriate destination.

Enabling RadSec on FreeRADIUS Server

Follow the below steps to enable RadSec on FreeRADIUS Server:

1. This is a basic FreeRADIUS configuration example added for reference only.

   > ⚠ **Caution**
   >
   > Consult your vendor documentation or your IT team to enable and configure RadSec on your RADIUS server.

2. Before making any configuration changes, stop the radiusd service:

   ```
   systemctl stop radiusd
   ```

3. Enable the TLS virtual server:

   ```
   cd /etc/raddb/sites-enabled
   ln -s ../sites-available/tls
   ```

4. Copy your certificates under default directory (for example: `/etc/raddb/certs/ directory`).
5. Edit the `/etc/raddb/sites-available/tls configuration` file and add the certificate paths for **private_key_file**, **certificate_file**, **ca_file** inside the tls {} block under both the sections: listen {} and home_server tls {}.
6. Edit the tls virtual server configuration in the `/etc/raddb/sites-available/tls` file, in order to add definitions for the clients by extending the clients radsec {} section.

   ```
   vi /etc/raddb/sites-available/tls
   ```

   ```
   ...

   clients radsec {
      ...
      ...
          client _CLIENT_NAME {
                  ipaddr = _OCOM_IP
                  proto = tls
                  virtual_server = default
          }
   }

   ...
   ```

7. Replace:
   a. _CLIENT_NAME with any name of your choice
   b. Replace _OCOM_IP with the IP address of your OCOM
   c. A secret does not have to be specified for RadSec clients, as the default is radsec. If you specify a secret, then that will be used instead of radsec
8. Start radiusd service:

   ```
   systemctl start radiusd
   ```

9. Now your radius server accepts RadSec request from the Operations Monitor.

> ⚠ **Caution**
>
> Refer to the following official link for enabling RadSec with Enable RadSec.

Support for Fail-Over

RadSec supports fail-over by configuring multiple server options. Normally requests will be forwarded to the first server option defined.

If there are multiple server options, the proxy will do fail-over and use the second server if the first is down. If the two first are down, it will try the third etc. If the first server comes back up, it will go back to using that one. Detection of servers being up or down is based on the use of StatusServer (if enabled), and that TCP/TLS/DTLS connections are up. Otherwise unanswered requests are used to detect unresponsive servers.

Multiple RADIUS servers can be configured in radsecproxy.conf as shown below; ensure each server is also added under the realm section,

```
server radius-server-1 {
    ...
}

server radius-server-2 {
    ...
}

realm * {
    server radius-server-1
    server radius-server-2
}
```

Logging

RadSec supports logging mechanism, which shows information about successful and failed authentications and critical errors. By default (as per the configuration), logs are written to /var/log/radsecproxy.log.

LogDestination option in the configuration file (radsecproxy.conf) specifies where the log messages should go. Using this option, you may specify that logs must be written in a particular file. The value must be a file path. LogLevel option specifies the debug level. You can set it to 1, 2, 3, 4 or 5, where 1 logs only serious errors, and 5 logs everything. A logging level of 3 is the default and recommended log level.

Example log snippets showing successful and failed authentications,

```
Wed Apr 16 17:21:36 2025: Access-Reject for user userZ from apache-radius-
test to 127.0.0.1 (127.0.0.1)
Wed Apr 16 17:21:48 2025: Access-Accept for user userZ from apache-radius-
test to 127.0.0.1 (127.0.0.1)
```

Configuring Apache for Authenticating with LDAP Service

The NGINX Web Server provided with Session Monitor does not support the external authentication.
To enable external authorization you are required to have NGINX Web Server that provides external authentication and is optional. You can also have a webserver that supports External Authentication like Apache.

The default installation supports IPv6 only. Configurations are necessary for proxies and repos. If there are any, see Configuring Proxies and Repos.

> **Note**
>
> On a SELinux enabled machine, for External Authentication, do not copy any modified `pld.conf` file from a different location and replace it with an existing file as SELinux blocks access to such files.
>
> Instead, edit the `pld.conf` file contents directly using the VI editor.

The following procedure explains configuring external authentication using Apache Web Server as it is widely used.

To configure Apache in Session Monitor for authenticating with LDAP service:

1. Login to Session Monitor.
2. Click **Admin** and select **Settings**.
3. Enable the setting, **External authentication** enabled and set it to **True**.
4. Logout from Session Monitor.
5. If the current web service is NGINX, change to HTTPD by following all the steps mentioned in Configuring Reverse Proxy Server.

   - Run the following commands to install the Apache Web Server and mod_ssl packages:

     ```
     yum install -y httpd mod_ssl
     ```

   > **Note**
   >
   > If you have proxy server, to complete download, edit the proxy settings for the external downloads to be successful.

> **Note**
>
> Install Apache Web Server and **mod_ssl** packages together as the httpd package executes a post-install script which uses **mod_ssl** for generating a localhost certificate. The certificate is required for the default httpd service configuration. If the certificate is not generated, enter the following lines in the `/etc/httpd/conf.d/ssl.conf` file to start the httpd server:
>
> ```
> SSLCertificateFile /etc/pki/tls/certs/localhost.crt
> SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
> ```

If the localhost certificates are not generated, perform the following workaround to start the Apache server:

> **Note**
>
> - Remove the **ssl.conf** file from the **/etc/httpd/conf.d** directory.
>
> When using HTTPD/Apache for web server due to external authentication configuration, if upgrade is applied ("dnf upgrade" OR HTTPD Upgrade) and httpd is updated, a new ssl.conf file is created. Hence, either remove, or move the ssl.conf file using this command and restart the HTTP service:
>
> ```
> mv /etc/httpd/conf.d/ssl.conf{,.orig}
> ```

6. Run the following commands to install all additional packages:

   ```
   yum groupinstall "Development Tools" -y
   ```

7. Run the following command to install the required ldap modules:

   ```
   yum install mod_ldap
   ```

8. Edit the pld.conf file:

   ```
   vi /etc/httpd/conf.d/pld.conf
   ```

9. Edit the following location in the file as below:

   ```
     <LocationMatch "^/me/(?!(proxy/|c/|r/|scripts/|/help/|logout\.html)).*$">
           #
           # BEGIN LDAP Auth
           # Uncomment and adjust the lines below for LDAP Auth
            RewriteEngine On
            RewriteCond %{SERVER_PORT} 443
            RewriteCond %{LA-U:REMOTE_USER} (.+)
            RewriteRule .* - [E=RU:%1,L]
            AuthType basic
           # AuthName should be the same as for /me/logout.html
            AuthName "OCSM COM"
            AuthBasicProvider ldap
   ```

```
         AuthLDAPURL "ldap://ldap-server/dc=example,dc=org?uid?one"
         AuthLDAPBindDN "cn=admin,dc=example,dc=org"
         AuthLDAPBindPassword <password>
         RequestHeader unset X-Forwarded-User
         RequestHeader set X-Forwarded-User %{RU}e
        # RequestHeader set X-Forwarded-User-Role ""
        # RequestHeader set X-Forwarded-User-Role
{AUTHENTICATE_employeeType}e
        # RequestHeader unset X-Forwarded-User-Permission
        # RequestHeader set X-Forwarded-User-Permission %
{AUTHENTICATE_gecos}e
        # # Admin permission mask - all bits set
        # RequestHeader set X-Forwarded-User-Permission 4610266613338864839
         Require valid-user
        # END LDAP AUTH
</Location>
```

For a description of the parameters and information on the optional parameters in the pld.conf file, see pls.conf File Details.

> **Note**
>
> All Non admin users are required to be created on Operations Monitor first and then these users can log in using LDAP Authentication. However if permissions and roles are needed to be added for a user in LDAP, then these should be taken from Operations Monitor MySQL Database for the User and use them to provision on LDAP. This is optional.

10. If you have modified the `Auth Name` above, then modify the `Auth Name` in this section in the `pld.conf`

```
 # Logout page for COM
    <Location /me/logout.html>
        AuthType basic
        # AuthName should be the same as for /me/
        AuthName "OCSM COM"
        AuthBasicProvider file
        AuthUserFile     "/opt/oracle/ocsm/etc/httpd/logout.htpasswd"
        Require           valid-user
        ProxyPass !
    </Location>
```

11. Run the following command to start and enable the httpd

```
systemctl restart httpd.service
```

The httpd server of Session Monitor has been configured for external authentication.

When you open the Session Monitor in web browser, the external authentication pop-up appears. On providing the correct LDAP user credentials, the user will be logged in successfully.

pld.conf File Details

Configuring Apache for Authenticating with LDAP Service requires you to edit the `pld.conf` file. Here, you can find the descriptions for the parameters that are edited and the optional parameters.

Table 6-5 pld.conf file parameters

Parameters	Description
<LDAP_Server>	The LDAP server name
"ldap://ldap-server/dc=example,dc=org?uid?one"	The LDAP server IP address to which the authentication request is sent by Session Monitor. As DC and CN are LDAP specific, check the DC and CN values with your Local LDAP configuration.
<password>	The password for LDAP server to which authentication to the specific user is to be processed. It should be a Hashed Password.
AuthName	"OCSM COM" is the default name provided. It can be modified to any convenient name.
{AUTHENTICATE_gecos}e (optional)	`gecos` is a parameter on your LDAP Server that stores the permissions for the user. As this is LDAP specific, check your local LDAP configuration. If permissions are defined for your user, then you can umcomment this line and change the parameter name from gecos to the appropriate name defined in your LDAP. When you log in, Operations Monitor validates the permission received and then allows User Login.
{AUTHENTICATE_employeeType}e	Parameter on your LDAP Server that stores the Role for the User. As this is LDAP specific, check with your local LDAP configuration. If roles are defined for your user, then you can umcomment this line and change the parameter name from employee to the appropriate name defined in your LDAP. When you log in, Operations Monitor validates the role received and then allows User Login.

Configuring Secure LDAP (LADPS) Support

To configure LDAPS support, follow these steps:

Follow the instructions given in Configuring Apache for Authenticating with LDAP Service before executing the following steps to configure LDAPS:

1. Copy the CA certificate from the LDAP server and place it in a directory other than / root.

   ```
   /opt/certs/<CA Certificate>
   ```

2. Assign permissions for the directory which has the CA certificate.

   ```
   chmod -R 777 /opt/certs
   ```

3. Modify the `/etc/hosts` file with a fully qualified DNS.

   ```
   <DNS-IP> <Host Name> <Fully Qualified Host Name>
   ```

4. Modify `/etc/httpd/conf.d/pld.conf` to have the following line after **CustomLog**:

   ```
   LDAPTrustedGlobalCert CA_BASE64 </opt/certs/<CA Certificate>
   ```

5. Modify the **AuthLDAPURL** URL from ldap to ldaps.

   ```
   AuthLDAPURL ""ldaps ://ldap-server/dc=example,dc=org?uid?one""
   ```

7

Installing and Configuring DPDK for Session Monitor

This chapter provides instructions for installing and configuring Data Plane Development Kit (DPDK) for the Oracle Communications Session Monitor to monitor high volume of network traffic.

DPDK provides sniffing performance for some of the Intel network cards and network traffic patterns. If you have a compatible network card, you can enable DPDK.

> ⓘ **Note**
>
> See Oracle Communications Session Monitor Release Notes to verify if you need to update DPDK. If you need to update DPDK, verify if the DPDK requires latest Oracle Linux Platform.

DPDK is a special architecture supported by specific network card designs, drivers, and server architectures, that improves performance when processing network traffic. For high network traffic monitoring, you can select to enable DPDK option on Session Monitor Probes. DPDK uses NUMA architecture special feature to have faster access to traffic written from a Network Card and to enhance the performance.

DPDK architecture involves two parts for Session Monitor Probes. The daemon is responsible for network traffic analysis (rat) is compiled against a specific DPDK library, and is deployed upon Session Monitor installation. For DPDK to work, the DPDK driver must be downloaded and installed on the Probe, as well.

> ⓘ **Note**
>
> To install DPDK on a SELinux enabled machine, disable SELinux first and install DPDK. Enable SELinux after the installation of DPDK.

System Requirements

The following sections describe the hardware and software requirements for installing and configuring DPDK for Session Monitor.

> ⓘ **Note**
>
> The software and hardware details mentioned in this section are minimum requirements to enable DPDK for capturing high volume of network traffic. Contact Oracle Support for more assistance.

Hardware Requirements

This section describes the hardware requirements for installing and configuring DPDK.

Minimal Requirements

Following are the list of minimum hardware requirements:

- Probe machine (with DPDK) (2 Intel processors, each with 8 cores, 8 GB RAM, Intel based network card)
- Mediation Engine and Probe in one machine (at least 2 Intel processors and 24 cores in total, 24 GB RAM, Intel based network card)

Supported Servers

For supported servers, see the Session Monitor System Requirements section.

Supported Networking Cards

The following networking cards 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
- Mellanox ConnectX-5 EN network interface card, 100GbE dual-port QSFP28, PCIe3.0 x16, tall bracket

Software Requirements

Supported DPDK versions for Session Monitor

The following table lists the supported versions of DPDK.

Table 7-1 Table 5-1 Supported Versions DPDK for Session Monitor

DPDK Version	Session Monitor Release
21.11.2	Supported from Release 5.1.0.0.0
21.11.3	Supported from Release 5.2.0.0.0
23.11.2	Supported from Release 6.0.0.0.0
24.11.2	Supported from Release 6.1.0.0.0

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 X9-2 server has the following pre-requisite:

1. Log into the Platform Setup Application page:
   1. Select **Capture Settings**.
   2. Check the box in **Monitoring** column against each sniffing interface that you want to use for capturing the traffic.
2. Log into the machine that hosts the probe or mediation engine and probe as a **root** user.
3. (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, that will display system information:

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

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

   ```
   source /opt/oracle/ocsm/ocsm_env.sh
   python3 -m pip install meson
   python3 -m pip install ninja
   python3 -m pip install pyelftools
   yum install -y git
   yum install -y tar
   yum install -y gcc-toolset-14.x86_64
   ```

5. Edit /etc/default/grub and set "GRUB_ENABLE_BLSCFG" to False.
6. After making the changes in grub, run the command:

   ```
   sudo grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

7. Clone the DPDK kernel modules repository from the official source using the command below:

   Execute this command in the root folder:

   ```
   git clone http://dpdk.org/git/dpdk-kmods
   ```

8. Execute this command in the root folder.

   ```
   scl enable gcc-toolset-14 '/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.
9. (Optional) To view all the available advanced options, run the following command:

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

10. Reboot the machine that hosts the probe or mediation engine and probe.

Installing and Configuring DPDK without Internet

DPDK can be installed and configured without an internet connection.

1. Log into the Platform Setup Application page:
   a. Select **Capture Settings**.
   b. Check the box in Monitoring column against each sniffing interface that you want to use for capturing the traffic.
2. Log into the machine that hosts the probe or mediation engine and probe as a **root** user.
3. (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
```

4. Run the following command to download the Kernel:

> **Note**
>
> For offline installation of DPDK, check the Kernel version before downloading. The Kernel version in the `Download_rpms.sh` script is currently - "`kernel-uek-devel-5.15.0-302.167.6.el9uek.x86_64.rpm`". The Kernel dependency libraries are also present in the `Download_rpms.sh` script. The Kernel version is subject to change and hence we recommend you to check the `uname -r` and then download the corresponding RPM file and their dependencies from the YUM repository and place the appropriate Kernel version RPM file in the `Download_rpms.sh script`. Or, you can download and copy the RPM file and their dependencies to the existing offline REPO server. For more information, see **Installing Session Monitor in an Offline Mode - Using the MOS Website**.

5. After downloading the RPM file, run this command to install the Kernel.

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

6. Download the DPDK tar.gz file from https://fast.dpdk.org/rel into the folder `/var/cache/ocsm/dpdk/`.
7. Run the below commands on a linux terminal connected to internet and download the `dpdk-kmods` folder:

```
yum install git
git clone http://dpdk.org/git/dpdk-kmods
```

8. Copy the downloaded `dpdk-kmods` folder into **root** of the system where DPDK needs to be installed.
9. Download the latest `.whl` files for the meson, ninja and pyelftools libraries from the URLs mentioned below:

Table 7-2 Download URLs

Item	URL
meson-X.X.X-py3-none-any.whl	https://pypi.org/project/meson/#files
ninja-1.11.1-py2.py3-none-manylinux_X_XX_x86_64.manylinux20XX_x86_64.whl	https://pypi.org/project/ninja/#files
pyelftools-X.XX-py2.py3-none-any.whl	https://pypi.org/project/pyelftools/#files

10. Run the following commands as a **root** user:

```
source /opt/oracle/ocsm/ocsm_env.sh
pip3 install meson-X.X.X-py3-none-any.whl --no-index
pip3 install ninja-1.11.1-py2.py3-none-
manylinux_X_XX_x86_64.manylinux20XX_x86_64.whl --no-index
pip3 install pyelftools-X.XX-py2.py3-none-any.whl --no-
index
yum install -y gcc-toolset-14.x86_64
```

11. Edit /etc/default/grub and set "GRUB_ENABLE_BLSCFG" to False.
12. After making the changes in grub, run the command:

```
sudo grub2-mkconfig -o /boot/grub2/grub.cfg"
```

13. Execute this command in the root folder.

```
scl enable gcc-toolset-14 '/opt/oracle/ocsm/usr/share/pld/rat/
configure_dpdk.py'
```

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

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

15. Reboot the machine that hosts the probe or mediation engine and probe.

Updating DPDK

This section provides the instructions to update DPDK after a Kernel update.

> **Note**
>
> You must perform the instructions in this section if you have installed another Linux Kernel.

To update DPDK:

1. Reboot the system.
2. Follow the procedure detailed in: Installing and Configuring DPDK with Internet or Installing and Configuring DPDK without Internet depending on your setup. For DOCA NIC cards following instructions Installing DOCA OFED.
3. Reboot the machine that hosts the probe or mediation engine and probe.

DPDK with Higher Throughput

Starting with Session Monitor Release 5.1, both dynamic memory mode and legacy memory mode is supported. DPDK probe can reach up to 3.2 Mpps on a single port when legacy memory mode is enabled.

> **Note**
>
> This applies only for Intel NIC cards.

Legacy Memory Mode

Add the below configurations in the `rat.dpdk.conf`.

```
[dpdk]
mem_mode = 2

[sniffer/xx_xx_x]
dpdk_rx_ring_desc = 1024
```

After making the changes, restart the rat process using the command `systemctl restart pld-rat`.

Loading the igb_uio Module

Execute the following tasks **ONLY** if the igb_uio module is not loaded or if the DPDK ports are not bound with igb_uio properly.

In such cases, you will see error messages as shown here:

```
Jan 12 17:04:10 prodeomprobe2xdfw system_layout.py: unable to bind
0000:3b:00.3 to igb_uio
Jan 12 17:04:10 prodeomprobe2xdfw systemd: pld-rat.service: control process
exited, code=exited status=1
Jan 12 17:04:10 prodeomprobe2xdfw systemd: Failed to start OCSM Media Sniffer.
Jan 12 17:04:10 prodeomprobe2xdfw systemd: Unit pld-rat.service entered
failed state.
Jan 12 17:04:10 prodeomprobe2xdfw systemd: pld-rat.service failed.
```

To handle such errors, execute the following instructions which will load the igb_uio module:

> **Note**
>
> The DPDK version and the interface details will vary for each machine or server. Use the appropriate versions and interfaces while executing the following commands.

1. Run this command in the terminal as the root user to explicitly load the igb_uio module:

a. Command 1: Run this command to load the uio module:

```
modprobe uio
```

b. Command 2: Run this command to list a set of paths containing the igb_uio.ko file:

```
sudo find / -name igb_uio.ko
```

Example:

```
[root@iris ~]# sudo find / -name igb_uio.ko
/var/cache/ocsm/dpdk/dpdk-22.11.3/build/kmod/igb_uio.ko
/var/cache/ocsm/dpdk/dpdk-22.11.3/build/build/kernel/linux/igb_uio/
igb_uio.ko
/usr/lib/modules/5.4.17-2011.6.2.el7uek.x86_64/extra/igb_uio.ko [We
need to chose this path to load the igb_uio.ko. See next command
example]
```

c. Command 3: Run this command:

```
insmod <provide here the path of igb_uio.ko>
```

Example:

```
insmod /usr/lib/modules/5.4.17-2011.6.2.el7uek.x86_64/extra/igb_uio.ko
```

Ensure that there is no error after executing this command. And you must return to the terminal prompt.

2. Check if the igb_uio driver is correctly loaded. Run the command `lsmod | grep igb_uio` in the terminal. If the output shows igb_uio with value 1, it means that the module was successfully loaded.

   Example:

```
[root@iris ~]# lsmod | grep igb_uio
igb_uio                 20480  1
uio                     20480  3 igb_uio
```

3. Check the status of the interface using the command:

> **Note**
>
> Need to modify version details in the commands as per the appropriate versions of DPDK.

```
sudo /var/cache/ocsm/dpdk/dpdk-24.11.2/usertools/dpdk-devbind.py -s
```

- Let us assume the interface is 0000:3b:00.3, if the interface is bound properly to igb_uio, then the output looks like:

  ```
  "0000:3b:00.3 'Ethernet Controller XL710 for 40GbE QSFP+ 1583'
  drv=igb_uio unused=..."
  ```

- If the interface is still not bound to igb_uio, then the output looks like:

  ```
  "0000:3b:00.3 'Ethernet Controller XL710 for 40GbE QSFP+
  1583'unused=i40e,"
  ```

If the interface is still not bound to igb_uio, follow the below procedure:

a. Open the file /etc/rc.local in edit mode.

b. Paste this single line command, and exit from the file:

   ```
   sudo /var/cache/ocsm/dpdk/dpdk-24.11.2/usertools/dpdk-devbind.py -b
   igb_uio 0000:3b:00.3
   ```

c. Give execute permissions to the file using command:

   ```
   chmod +x /etc/rc.d/rc.local
   ```

4. Run the following commands to install DPDK and make igb_uio get persistent across reboot:

   ```
   Command 1 : source /opt/oracle/ocsm/ocsm_env.sh
   Command 2 : scl enable gcc-toolset-14 '/opt/oracle/ocsm/usr/share/pld/rat/
   configure_dpdk.py' ---> This will load igb_uio module and ensure
   persistance across reboot.
   Command 3 : reboot
   ```

   Once the setup is running, check if the igb_uio module is loaded using the command `lsmod | grep igb_uio`.

5. After this, check if the appropriate Ethernet interface is enabled in the PSA and if the DPDK installation is successful.

Uninstalling DPDK

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

1. Run the following commands:

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

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

2. Reboot the machine that hosts the probe or mediation engine and probe.

8

Downloading, Installing, and Configuring DPDK for Mellanox NIC Cards

Follow the instructions given in this section to install and configure DPDK for Mellanox NIC cards.

> **Note**
>
> Starting with DPDK 24.11.2, support for Mellanox OFED has been terminated and has been migrated to DOCA OFED. Follow the instructions to install the DOCA OFED.

1. Installing DOCA OFED
2. Installing and Configuring DPDK

Installing DOCA OFED

Complete the following tasks to download and install DOCA OFED package for Oracle Linux.

The supported networking cards are: Mellanox Technologies MT27800 Family [ConnectX-5].

Ensure that you have installed:

- Oracle Linux 9.6
- Session Monitor Release 6.1
- DPDK Version 24.11.2

1. Download the DOCA OFED based on OS distribution and architecture from the NVIDIA DOCA 3.1.0 Downloads page. Please follow the steps as mentioned below:

   ```
   Select "Host Server" >> "DOCA-Host" >>
   "Linux" >> "x86_64" >> "doca-ofed" >>
    "OracleLinux" >> "9.6" >> Select on "rpm(local)"
   ```

2. Run the commands:

   a. Run the following command to install the DOCA Host 3.1.0 package on the system:

      ```
      sudo rpm -i doca-host-3.1.0-091000_25.07_ol96.x86_64.rpm
      sudo dnf clean all
      ```

   b. Execute this command and verify if ol9_UEK7 repo is enabled or not.

      ```
      sudo dnf repolist all | grep -i uek
      ```

   c. If the repo ol9_UEK7 is disabled, enable it using command:

      ```
      sudo dnf config-manager --enable ol9_UEKR7
      ```

3. Install the DOCA OFED package to enable the required network drivers and libraries. Use the command below:

   ```
   sudo dnf -y install doca-ofed
   ```

   Reboot once the installation is complete.

4. Make sure that the `mlx kernel modules mlx5_ib`, `mlx5_core`, `ib_uverbs` are loaded.

   ```
   lsmod | grep mlx5
   lsmod | grep ib_uverbs
   ```

Installing and Configuring DPDK

Complete the following tasks to install and configure DPDK for Mellanox NIC cards.

1. Create a file `/opt/oracle/ocsm/etc/iptego/white_list_dpdk.local` with the value **mlx5_core** before starting the DPDK installation.
2. Log into the **Platform Setup** Application page.
   a. Select **Capture Settings**.
   b. Check the box in the **Monitoring** column against each sniffing interface that you want to use for capturing the traffic.
3. Log into the machine that hosts the probe or the mediation engine and probe as a **root** user.

   (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
   ```

   > **Note**
   >
   > If you observe a Python error while executing the .py files, run the command `update-alternatives --config python3` and select the `/usr/bin/python3.11` option.

4. Download the DPDK tar file from https://fast.dpdk.org/rel/ into the folder `/var/cache/ocsm/dpdk/`.
5. Run the following commands as a root user:

   ```
   source /opt/oracle/ocsm/ocsm_env.sh
   python3 -m pip install meson
   python3 -m pip install ninja
   python3 -m pip install pyelftools
   yum install -y tar
   yum  install gcc-toolset-14.x86_64
   ```

6. Edit /etc/default/grub and set “`GRUB_ENABLE_BLSCFG`” to False. Once the changes are made in grub, run the command:

   ```
   sudo grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

7. Run this command:

   ```
   scl enable gcc-toolset-14 '/opt/oracle/ocsm/usr/share/pld/rat/
   configure_dpdk_mlx.py'
   ```

8. Reboot the machine that hosts the probe or the mediation engine and probe.
9. MLNX drivers require root privileges for the Promiscuous Mode to be enabled. Assign **root** user privileges to the **ocsm** user.
10. Open file in edit mode: `/etc/passwd`
11. Change line `ocsm:x:998:996::/opt/oracle/ocsm:/sbin/nologin` to `ocsm:x:0:0::/opt/oracle/ocsm:/sbin/nologin`
12. Restart the RAT service (pld-rat): `systemctl restart pld-rat`

9

Installing Skype for Business Agent

This chapter explains how to install the Skype for Business Agent for Oracle Communications Enterprise Operations Monitor, and Oracle Communications Operations Monitor.

Overview

For Enterprise Operations Monitor (EOM) to monitor Skype for Business encrypted SIP messages, the user must install a Windows service (Agent) on the Skype for Business server. The Skype for Business Agent registers itself on the server and acts as a back-to-back user agent for the Skype for Business calls, obtaining access to the SIP message bodies. It then forwards the SIP messages to the EOM Mediation Engine, which analyzes them and displays them in the calls list alongside regular VoIP calls.

The Skype for Business Agent is distributed as a regular Windows .msi package which offers a wizard based installation.

Pre-requisites

Before installing Skype for Business Agent, ensure that you have the following:

- Mediation Engine is installed on Linux and the Skype for Business Server machine is able to connect to the Mediation Engine.

Installing Skype for Business Agent

To install Skype for Business Agent:

1. Download the Skype for Business installation file to a temporary directory (temp_dir).
2. Go to the *temp_dir* directory.
3. Unpack the **Skype for Business to Skype Agent** for Business (SFB) server.
4. Run the **Skype for Business Agent** file.

   The Oracle EOM Skype for Business Agent Setup wizard appears.
5. Click **Next**. The End-User License Agreement screen appears.
6. Accept the license agreement and click **Next**.

   The ME Connection Settings screen appears.
7. In the **ME Host Address** field, enter host address.
8. It is recommended not to deselect **Use TLS**. When selected, the connection to Mediation Engine is encrypted.

> **Note**
>
> If encryption is selected, you must generate a TLS certificate for the Skype for Business Agent which includes a Certificate. Upload the TLS certificate to the Enterprise Operations Monitor machine, and install it on the Skype Server in the local computer Trusted Certification Authorities store, and install the generated certificate including the private key permissions in the Personal Certificate store.

> **Note**
>
> **Important:**
>
> - Grant the read permissions for the private key to the OracleSkypeProbeUser account.
> - If encryption is not selected, the user must also select the Allow insecure connection checkbox in the Trusted certificates section in the Enterprise Operations Monitor setup.

The Ready to Install Oracle EOM Skype Agent screen appears.

9. Click **Install**.

   The installation sets up a service on the windows server and creates an user account,**OracleSkypeProbeUser** for the service.

10. Click **Finish**.

The Skype for Business Agent installation is now complete and the calls made from Skype will appears as a Skype call in the call details window.

Uninstalling Skype for Business Agent

To uninstall Skype for Business Agent:

1. From your machine, click **Start** and then click **Control Panel**.
2. Click **Programs**.
3. Click **Program and Features**.
4. In the list of currently installed programs, select **Oracle EOM Skype for Business Agent** and then click **Uninstall/Change**.
5. A confirmation dialogue box appears. Confirm Uninstallation.

The Skype for Business Agent is uninstalled.

Editing Mediation Engine Host Address

To edit the Mediation Engine host address:

1. Open the configuration file, **C:\Program Files\Oracle\Oracle EOM> Skype Probe\SkypeProbe.exe.config.**
2. Change the value of the tag having key, **apidAddr**.

For example:

```
<add key="apidAddr" value="192.168.123.120"/>
```

3. Save the **SkypeProbe.exe.config** file.
4. Place the cursor on the **Oracle EOM Skype Probe** service name and right click to restart.

Configuring Skype for Business Agent for Monitoring Call Quality Information

The Skype for Business Agent monitors only the SIP call flow. The call quality information is reported by the user agent, Skype for Business Desktop Client.

To get the call quality information:

1. Enable monitoring on the Skype server.

   See https://docs.microsoft.com/en-us/skypeforbusiness/deploy/deploy-monitoring/deploy-monitoring.

2. Install and configure the Skype for Business SDN API on the Skype Front-End Server, as described in the Skype for Business SDN API 2.4.1 Installation Admin Guide.

   See https://docs.microsoft.com/en-us/skype-sdk/sdn/articles/installing-sdn-interface.

3. After the installation, add the Mediation Engine machine to Skype for Business Server as a subscriber for the SDN API by running the following command in the Skype for Business Server console:

   ```
   SDNManager.exe /p s EOM submituri=https://<IP_address>/sfb/
   ```

   where *<IP_address>* is the IP address or the hostname of your Mediation Engine.

   The finished Skype calls show the MOS values and media summary.

4. Configure the SDN Manager to send QualityUpdate messages to the Mediation Engine by running the following command:

   ```
   SDNManager.exe /p s EOM "quality=True"
   ```

5. Operations Monitor reads the SDN Interface messages from the URL https://<Mediation Engine Host>/sfb/.

   ```
   cd "C:\Program Files\Microsoft Skype for Business Server\Microsoft
   Skype for Business SDN Manager\" SDNManager.exe /parameter
   subscriber ocom "submituri=https://<MediationEngine Host>/sfb/"
   ```

6. After configuring the SDN Dialog Listener and SDN Manager, run the following command for SDN Manager to forward the messages to Operations Monitor:

   ```
   cd "C:\Program Files\Microsoft Skype for Business Server\Microsoft Skype
   for Business SDN Manager\"
   SDNManager.exe /parameter subscriber ocom "submituri=https://
   <MediationEngineHost>/sfb/"
   ```

7. Verify the SDN Manager configuration:

   ```
   cd "C:\Program Files\Microsoft Skype for Business Server\Microsoft Skype
   for Business SDN Manager\"
   SDNManager.exe /download subscriber
   ```

   You should get an XML describing the configuration.

   > **Note**
   >
   > Make sure the value of the submituri parameter matches the address of the Enterprise Operations Monitor machine.

8. Check the SDN Manager and Dialog Listener log files at `%LOCALAPPDATA%\Local\Temp\SDN` after each Skype for Business call. Open the `SDNManager.log` file and search for the following:

   ```
   Starting to transmit the message?
   ```

   If the line does not exist, the SDN manager is configured incorrectly. Repeat the configuration process again.

Troubleshooting

This section provides guidelines for troubleshooting problems with Skype for Business Agent.

Problems with Viewing Skype Call Data Information

Perform the following if you are unable to view skype call data:

1. Verify that the **SkypeProbe.exe.config** file located in the installation directory has the correct IP address of Mediation Engine.
2. Verify Mediation Engine machine is reachable by pinging the Mediation Engine Machine from Skype for Business Server.
3. Verify the logs for any exceptions or connection errors in the following path:

   C:\ProgramData\Oracle EOM Skype Probe\Logs
4. Ensure that **OracleSkypeProbeUser** is a member of RTC Server Applications local group. If not, add the user by doing the following:
   1. From your computer, click **Start** and search for **Computer Management**.
   2. Click **Computer Management**.

      The Computer Management screen appears.
   3. Click **Local Users and Groups**.
   4. Select and right-click the **RTC Server Applications** group and click **Add to Group**.
   5. Locate and add the **OracleSkypeProbeUser** and click **OK**.

      The **OracleSkypeProbeUser** will be added to the RTC Server Applications group.
5. Verify the Enterprise Operations Monitor Skype for Business agent service is running in services.msc. by doing the following:

   a. From your computer, click **Start** and search for **Computer Management**.
   b. Click **Computer Management**.

      The Computer Management screen appears.
   c. Click **Services and Applications**.
   d. Click **Services**.
   e. Verify if Skype for Business Agent service is running, if not, right-click the service and click **Start**.

      The Skype for Business Agent will start running.

6. Verify if the connection between Mediation Engine and Skype for Business Server is blocked by firewall. If blocked, disable the setting depending on your Operating System.
7. If you have selected **Accept insecure connections from remote probes** during Enterprise Operations Setup, set the **UseTls** parameter to false in the **SkypeProbe.exe.config** file.

10

Public Cloud Platforms

You can run Oracle Communications Session Monitor on the following public cloud platforms:

- OCI
- Azure
- AWS
- GCP

> ⓘ **Note**
>
> Refer to the Session Monitor Release 6.1 Release Notes for confirmation on the public clouds supported and important details on the software version's support.

This section addresses requirements associated with running the Session Monitor as public cloud instances. It also provides basic instructions on deploying machine instances. Public Cloud providers maintain extensive product documentation. You must use those vendors' documentation for specifications, requirements, caveats, known issues, deployment details, and operation details prior to deploying the Session Monitor.

Create and Deploy Session Monitor on OCI

You can deploy the Mediation Engine, and Mediation Engine Connector nodes of the Session Monitor on Oracle Cloud Infrastructure (OCI). When deployed on the OCI platform, you configure and operate the Session Monitor as you would on any other platform. You can deploy the Session Monitor to use the environment's IP infrastructure, including the private and public addressing scheme.

Before installing Session Monitor components, SSH keys must be generated to access the Session Monitor VM instances.

For more information, see Generating an SSH Key Pair on Windows Using the PuTTYgen Program.

Deployment Checklist

Before starting the deployment, ensure that you have the following information handy.

Contact the OCI account administrator to assign the required privileges in IAM to create and/or use the following OCI resources:

- Identify and deploy to the correct OCI Region and compartment. This is typically a default component of the OCI Account.
- Identify and deploy to the correct OCI Availability Domain
- Identify and deploy to the correct OCI Fault Domain

- Prepare private and public key. For more information, see Generating an SSH Key Pair on Windows Using the PuTTYgen Program.
- Create Networks and Subnet - The OCI interface types include those hidden from the internet and those that are not. Oracle recommends creating regional subnets, which means the subnet can span across availability domains within the region. Refer to OCI's Regional Subnets documentation for further information about using these objects
- Identify and select or create the appropriate Virtual Cloud Network (VCN). Required VCN configuration includes:
  - Security list— these access control lists provide traffic control at the packet level.
  - Subnet configuration— Select a subnet as required
  - Internet Gateway—create a default internet gateway for the compartment and give it an appropriate name.
  - Route table (Use Default)—create a route table to route appropriate Subnet(s) through the Internet Gateway

Security Objects

Security lists specify the type of traffic allowed on a particular type of subnet.

Rules set on the security lists can be either stateful or stateless. Stateful rules employ connection tracking and have the benefit of not requiring exit rules. However, there is a limit to the number of connections allowed over stateful connections and there is a performance hit. Oracle, therefore, recommends stateless lists for media interfaces.

The security list for management ports can be stateful.

Port Numbers for Importing Traffic
Allow inbound traffic for the following ports.

Port no	Service	Protocol
22	SSH	TCP
111	rpcbind	TCP and UDP
80	Nginx	TCP
443	Nginx	TCP
4739-4742	apid	TCP
161	snmp	TCP and UDP

For more information, see the Oracle Communications Session Monitor Security Guide.

Minimum Recommended Shapes

Identify the shape, the minimum recommended shape is 4 OCPU, 8GB RAM, 80GB hard disk and 2 vNIC.

Table 10-1

Machine	Hardware Configuration	Shape Name in OCI
Mediation Engine	• 4v CPU • 30 GB RAM • 256 Gib HDD	VM.Optimized3.Flex

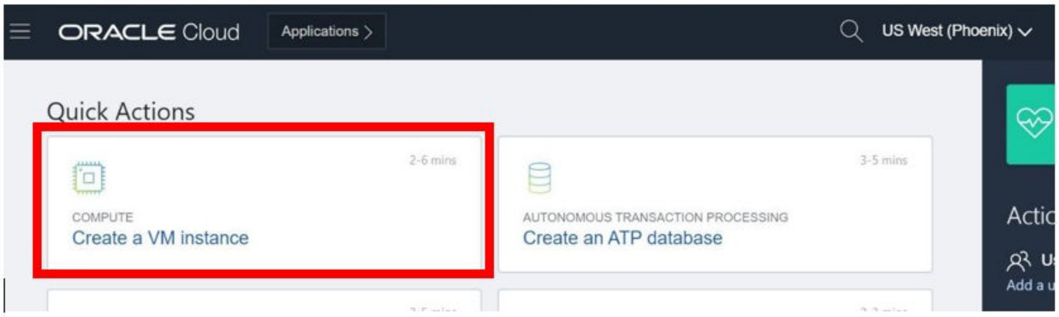
Table 10-1 (Cont.)

Machine	Hardware Configuration	Shape Name in OCI
Mediation Engine Connector	• 4v CPU • 30 GB RAM • 100 Gib HDD	VM.Optimized3.Flex

Deployment on OCI

The OCI instance configuration procedure includes a multi-dialog wizard that presents configuration options in sequence.

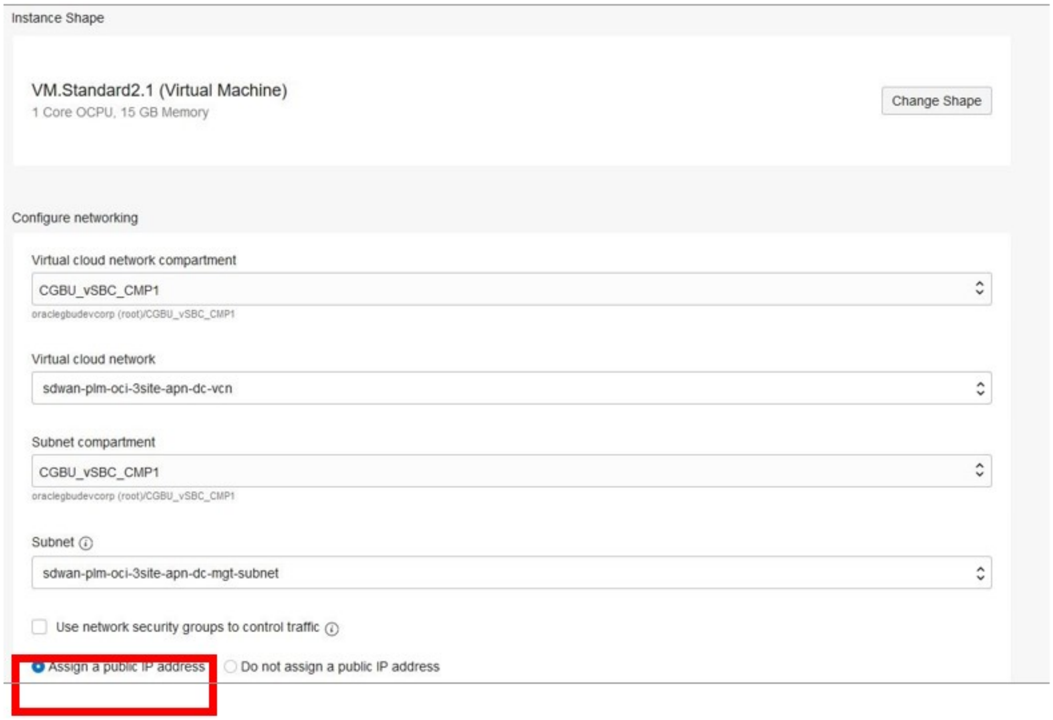
1. Login to the OCI console by selecting the appropriate region and compartment.
2. Click **Create a VM instance**.



3. In the **Create Compute Instance** page, provide a name for the instance.
   a. Select a compartment from the list of compartments.
   b. Select the appropriate Oracle Linux base image version that is required.
4. Click **Change Shape** to change the Instance shape.
   a. You can choose from two Standard Instance Types: a) Virtual Machine and b) Bare Metal Machine.
   b. Select a Shape. Select one option from the available options - `AMD Rome`, `Intel Skylake`, `Speciality and Legacy`.

   > **Note**
   >
   > In the Session Monitor Release 6.1, Session Monitor has been tested only with the `Intel` shape.

   c. Select a shape according to your requirement for the Virtual Machine created.
5. Select the **Virtual Cloud Network Compartment**.
6. Select **Virtual Cloud Network**.
7. Select **Subnet Compartment**.
8. Select a subnet as required and choose **Assign a Public IP Address**.



Instance Shape

VM.Standard2.1 (Virtual Machine)
1 Core OCPU, 15 GB Memory

Configure networking

Virtual cloud network compartment: CGBU_vSBC_CMP1
oraclegbudevcorp (root)/CGBU_vSBC_CMP1

Virtual cloud network: sdwan-plm-oci-3site-apn-dc-vcn

Subnet compartment: CGBU_vSBC_CMP1
oraclegbudevcorp (root)/CGBU_vSBC_CMP1

Subnet: sdwan-plm-oci-3site-apn-dc-mgt-subnet

☐ Use network security groups to control traffic

● Assign a public IP address ○ Do not assign a public IP address

9. In Configure boot volume screen, select **SPECIFY A CUSTOM BOOT VOLUME** and mention the required size.
10. In the **Add SSH keys** screen, choose the appropriate SSH key. Use one option to add the public key: `Generate SSH Key Pair`, `Upload Your Own Public Key`, `Paste own public key`.
11. In the **Show Advanced Options** screen, provide if any details are required.
12. Review the details which are selected or created in the previous steps, make changes if anything is required.
13. Click **Create** to start creating the instance.
14. After a delay of few minutes, the instance is created and the public and private IP addresses of the instance are displayed in the newly loaded page.
15. By default, the instance /(/root) file system has 40 GB only; even if you have defined the size in the earlier step. Follow the method explained in the document How To Create a Linux Instance With Custom Boot Volume and Extend The Root Partition in OCI: to increase the size.
16. After resizing the VM instances, follow the instructions in the Oracle Communications Session Monitor Installation Guide.

Note

If the disk size is increased after the Session Monitor installation and configuration, partitions space can be reconfigured by using script:

```
/opt/oracle/ocsm/usr/share/pld/scripts/admin/change-disk-usage.py
```

For example:. `/opt/oracle/ocsm/usr/share/pld/scripts/admin/change-disk-usage.py -d1 <new-size> -d2 <new size>`

Use d2 only if dual disks are being used. However, if the new partition space is lesser than the previous size then data is deleted. Ensure that the size is larger than the pre-configured size.

Create and Deploy Session Monitor on Azure

You can deploy Session Monitor on Azure public clouds.

Azure provides multiple ways of managing your environment(s), including using its web portal, using its powershell, and the CLI interfaces. This document focuses on the Web portal. The Web portal provides navigation using a web-page pane with links to specified functions on the left side of portal pages. These procedures also assume you have reviewed Azure documentation, and can access portal pages and navigation.

Before beginning, refer to the Oracle Communications Session Monitor Release 6.1 Release Notes to know details on the public clouds and important details on the software versions supported.

Prerequisites to Azure Deployment

This section addresses requirements associated with running the Session Monitor in public cloud instances.

The Azure cloud deployment infrastructure provides a flexible management system that allows users to create objects required during the instance deployment procedure prior to or during that deployment. When created prior to deployment, these objects become selectable, typically from drop-down lists in the appropriate deployment dialogs. These objects can be used for a single deployment or for multiple deployments.

The prerequisites for Azure deployment are:

- An account that has the privileges to create or use the resources.
- Azure Subscription details
- Information on the Region
- Resource Group details
- Public and Private subnet.
- Public and private keys. For more information, see Quick Steps - Create and use an SSH public-private key pair for Linux VMs in Azure.

Deploying the Azure Instance

The configuration procedure includes a multi-dialog wizard that presents configuration options in a sequence.

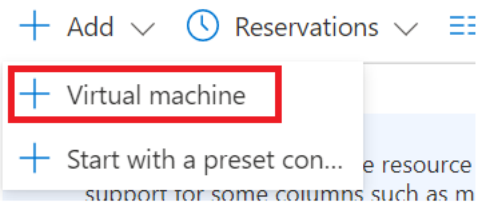
The instance deployment wizard sequence includes:

1. Creating a virtual machine
2. Perfoming disk configuration
3. Configuring networking
4. Management and Configuration
5. Reviewing

Creating a VM Instance for Azure Deployment

Perform the following tasks to create a VM instance.

In the Instance Deployment Wizard, click **Add**, and then click **Virtual Machine**.


+ Add
Reservations
+ Virtual machine
+ Start with a preset con...
e resource
support for some columns such as m

Azure Instance Deployment - Basics Configuration

The Azure instance deployment Basics configuration includes:

- Chose the appropriate subscription and resource group
- Specify the name as your Virtual machine name.
- Select your Region and Availability Option.
- Browse all public and private images and search for Oracle Linux 9.6
- Select the appropriate size of the image, and the minimum recommended shape.

Virtual Machines for Azure Deployment

The table lists the minimum recommended shapes and size for virtual machines to deploy Session Monitor on Azure.

Table 10-2 VM Shapes and Sizes

Machine	Hardware Configuration	Shape Name in Azure
Mediation Engine	• 8v CPU • 16 GB RAM • 80 Gib HDD	Standard F8s
Mediation Engine Connector	• 8v CPU • 16 GB RAM • 80 Gib HDD	Standard F8s

Providing the Administrator Account Information

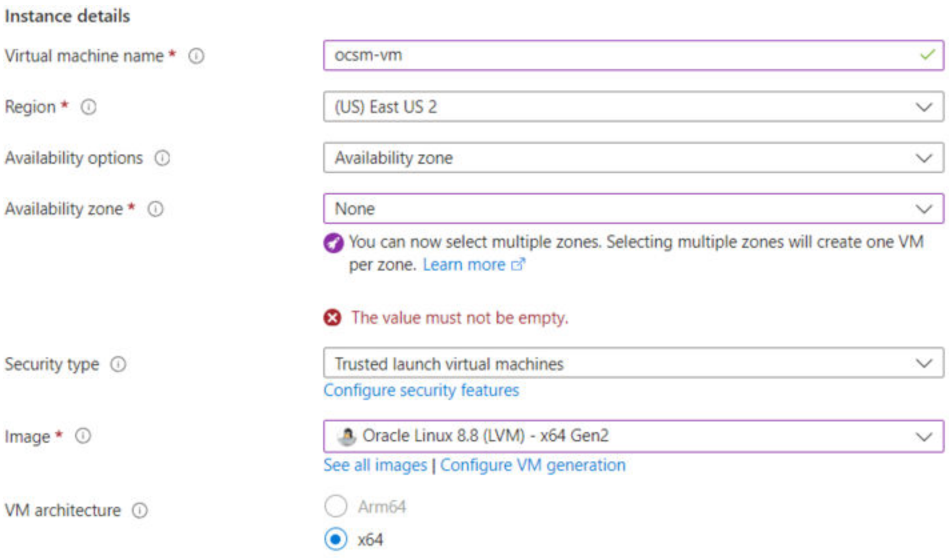
You can use either of the two methods to specify the Administrator Account information.

- Select Authentication Type as **Password**, create a user and assign any password to this user.
- The recommended method is to use the Authentication Type as **SSH public key**.
  - Create a user and provide the SSH public key from the machine you will use to log in to Session Monitor.
  - During the instantiation, this key is added to the **ssh-key** configuration element as an authorized-key for the user.

Inbound Port Information

Specifying your Inbound port rules external port access to interfaces.

Figure 10-1 Inbound Port



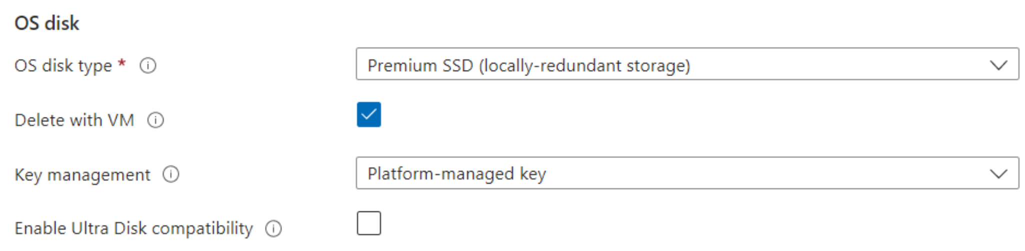
Instance details

Virtual machine name * ⓘ	ocsm-vm ✓
Region * ⓘ	(US) East US 2
Availability options ⓘ	Availability zone
Availability zone * ⓘ	None You can now select multiple zones. Selecting multiple zones will create one VM per zone. Learn more The value must not be empty.
Security type ⓘ	Trusted launch virtual machines Configure security features
Image * ⓘ	Oracle Linux 8.8 (LVM) - x64 Gen2 See all images | Configure VM generation
VM architecture ⓘ	○ Arm64 ● x64

Specifying Disk Options

Disk configuration for Azure Deployment includes setting the OS disk type to Premium SSD for better performance.

Figure 10-2   Disk Configuration



OS disk

OS disk type * ⓘ — Premium SSD (locally-redundant storage)

Delete with VM ⓘ — ☑

Key management ⓘ — Platform-managed key

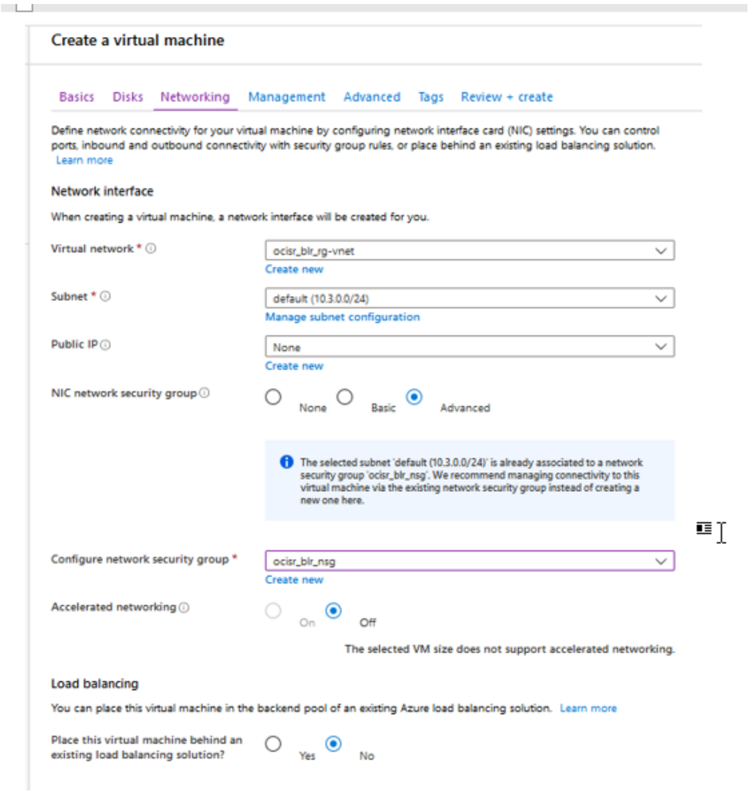
Enable Ultra Disk compatibility ⓘ — □

Network Configuration

Configure networking configuration for your Virtual Machine.

1. Select or create a new Virtual Network.
2. Select or create your Subnet.
3. Enter a name as your Public IP.
4. Select inbound ports (Required).

Figure 10-3   Network Configuration



Create a virtual machine

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. Learn more

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * ⓘ — ocisr_blr_rg-vnet
Create new

Subnet * ⓘ — default (10.3.0.0/24)
Manage subnet configuration

Public IP ⓘ — None
Create new

NIC network security group ⓘ — ○ None ○ Basic ● Advanced

The selected subnet 'default (10.3.0.0/24)' is already associated to a network security group 'ocisr_blr_nsg'. We recommend managing connectivity to this virtual machine via the existing network security group instead of creating a new one here.

Configure network security group * — ocisr_blr_nsg
Create new

Accelerated networking ⓘ — ○ On ● Off

The selected VM size does not support accelerated networking.

Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more

Place this virtual machine behind an existing load balancing solution? — ○ Yes ● No

Completing the Instance Creation

Complete the creation of your instance by retaining the default values.

In the **Management**, **Advanced** and **Tags** tabs, leave the default values as is. You can define tags to clarify details about the instance objects. You do not need to configure anything on the **Tags** tab.

In the **Review and Create** tab, review your settings, and click **Create** to complete instance creation.

The VM instance is ready for Session Monitor installation. For information on the installation of Session Monitor components, see Oracle Communications Session Monitor Installation Guide.

Resizing the Root File System

By default, the instance /(/root) file system will have 30 GB only.

If you need to resize the root file system, see Expand an Azure Managed Disk.

Port Numbers for Importing Traffic

Allow inbound traffic for the following ports.

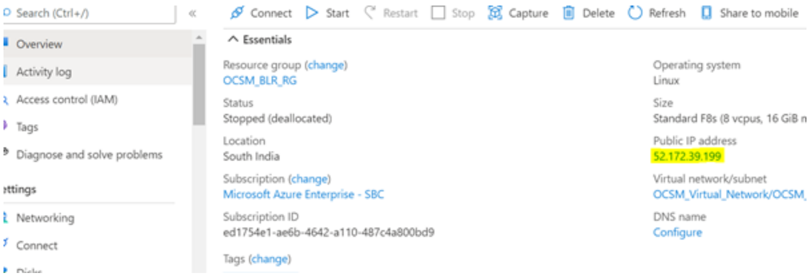
Port no	Service	Protocol
22	SSH	TCP
111	rpcbind	TCP and UDP
80	Nginx	TCP
443	Nginx	TCP
4739-4742	apid	TCP
161	snmp	TCP and UDP

Changing Public and Private IP Address from Dynamic to Static

By default, the Azure VM has a dynamic IP address which changes during the reboot. Hence you need to change from dynamic to static.

1. Click the Public IP address under the **Overview** section.
2. See the accompanying screenshot:

Figure 10-4 Public IP Address



Resource group (change)
OCSM_BLR_RG

Status
Stopped (deallocated)

Location
South India

Subscription (change)
Microsoft Azure Enterprise - SBC

Subscription ID
ed1754e1-ae6b-4642-a110-487c4a800bd9

Tags (change)

Operating system
Linux

Size
Standard F8s (8 vcpus, 16 GiB n

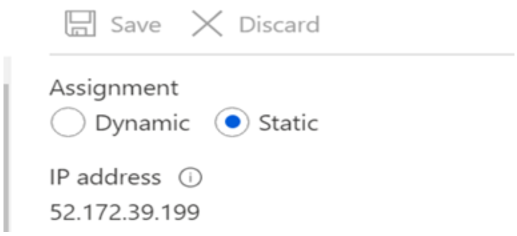
Public IP address
52.172.39.199

Virtual network/subnet
OCSM_Virtual_Network/OCSM_

DNS name
Configure

3. Choose Static or Dynamic as per your requirement then click **Save**.

Figure 10-5 Save IP address



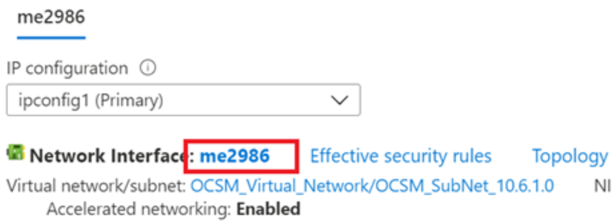
Save Discard

Assignment
○ Dynamic ● Static

IP address ⓘ
52.172.39.199

4. Click Networking on the side panel.
5. Click on the network interface as shown in the graphic.

Figure 10-6 Network Interface



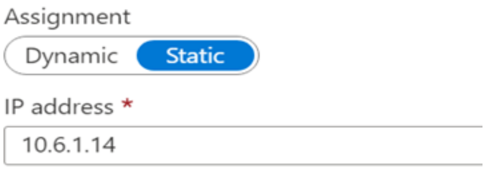
me2986

IP configuration ⓘ
ipconfig1 (Primary)

Network Interface: me2986 Effective security rules Topology
Virtual network/subnet: OCSM_Virtual_Network/OCSM_SubNet_10.6.1.0 NI
Accelerated networking: Enabled

6. Click **Private IP** under **IP Configuration**.
7. Assign the Dynamic or Static IP address.

Figure 10-7 Static and Dynamic Address



Assignment
Dynamic **Static**

IP address *
10.6.1.14

Create and Deploy Session Monitor on AWS

This section provides information on the process for creating an AWS VM.

You must use those vendors' documentation for specifications, requirements, caveats, known issues, deployment details, and operation details prior to deploying the Session Monitor.

Prerequisites for AWS Deployment

The prerequisites for AWS deployment are:

- An account that has the privileges to create or use the resources.
- AWS Account ID and credential details
- Information on the Region
- Resource Group details

- Public and Private subnet.
- Public and private keys. For more information, see Create a key pair using Amazon EC2.

Deploying the AWS Instance

The configuration procedure includes a multi-dialog wizard that presents configuration options in a sequence.

The instance deployment wizard sequence includes the following steps:

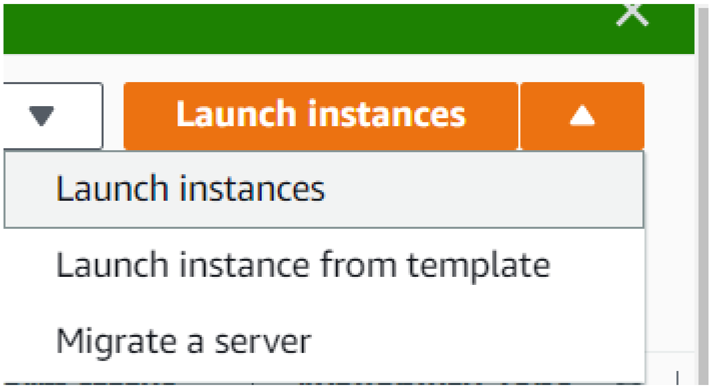
1. Creating a virtual machine
2. Preforming disk configuration
3. Configuring networking
4. Management
5. Reviewing configuration

Creating a VM Instance for AWS Deployment

Perform the following tasks to create a VM instance:

1. In the **Instance Deployment** wizard, click **Launch Instances**.
2. Click **Launch Instances**.

Figure 10-8 Launch Instances menu option

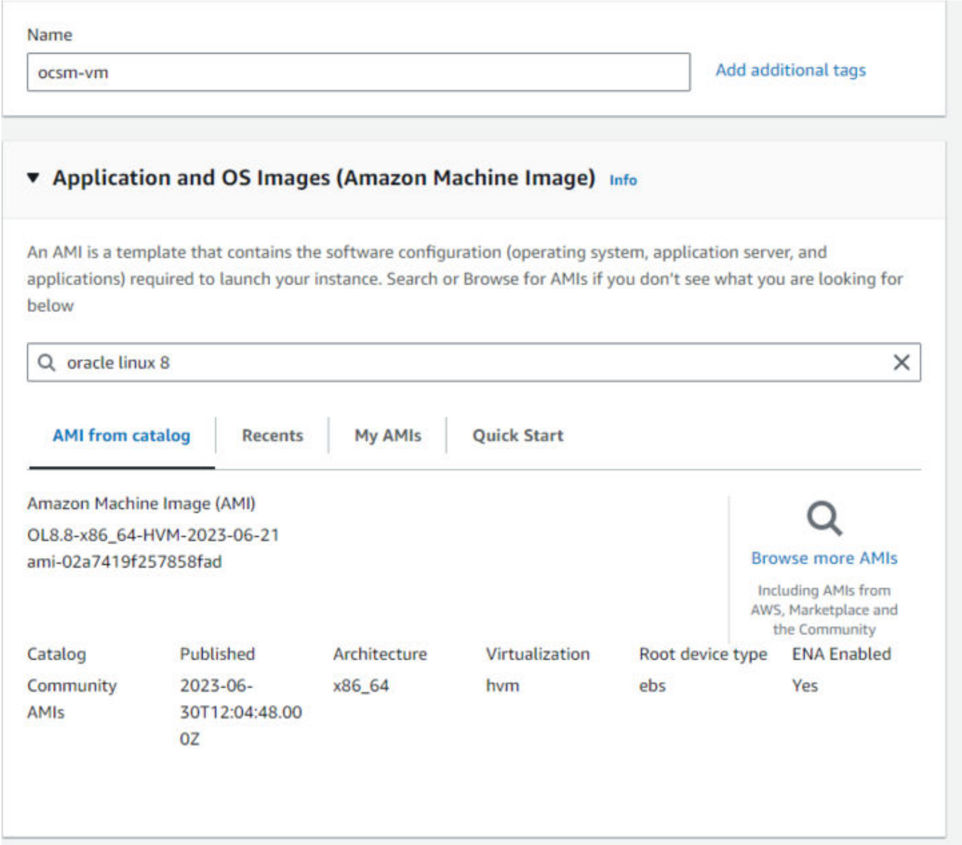


Basic Configuration

The basic configuration for the AWS instance deployment includes:

- Get started by completing the tasks outlined in the **Launch Instances** dialog box.
  - Chose the appropriate region
  - Specify the name as your Virtual machine name
  - Browse all public and private images and search for Oracle Linux 9.6
  - Select the appropriate size of the image, and the minimum recommended shape.

Figure 10-9 Launch an Instance



Name

ocsm-vm

▼ Application and OS Images (Amazon Machine Image)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

oracle linux 8

Amazon Machine Image (AMI)
OL8.8-x86_64-HVM-2023-06-21
ami-02a7419f257858fad

Catalog	Published	Architecture	Virtualization	Root device type	ENA Enabled
Community AMIs	2023-06-30T12:04:48.000Z	x86_64	hvm	ebs	Yes

Security Objects

Security lists specify the type of traffic allowed on a particular type of subnet.

Rules set on the security lists can be either stateful or stateless. Stateful rules employ connection tracking and have the benefit of not requiring exit rules. However, there is a limit to the number of connections allowed over stateful connections and there is a performance hit. Oracle, therefore, recommends stateless lists for media interfaces.

The security list for management ports can be stateful.

Port Numbers for Importing Traffic
Allow inbound traffic for the following ports.

Port no	Service	Protocol
22	SSH	TCP
111	rpcbind	TCP and UDP
80	Nginx	TCP
443	Nginx	TCP
4739-4742	apid	TCP
161	snmp	TCP and UDP

For more information, see the Oracle Communications Session Monitor Security Guide.

Virtual Machines for AWS Deployment

The minimum recommended shapes and size for virtual machines to deploy Session Monitor on AWS:

Machine	Hardware Configuration	Shape Name in AWS
Mediation Engine	• 16v CPU • 32 GB RAM • 400 Gib HDD	c5.4xlarge
Mediation Engine Connector	• 16v CPU • 32 GB RAM • 400 Gib HDD	c5.4xlarge

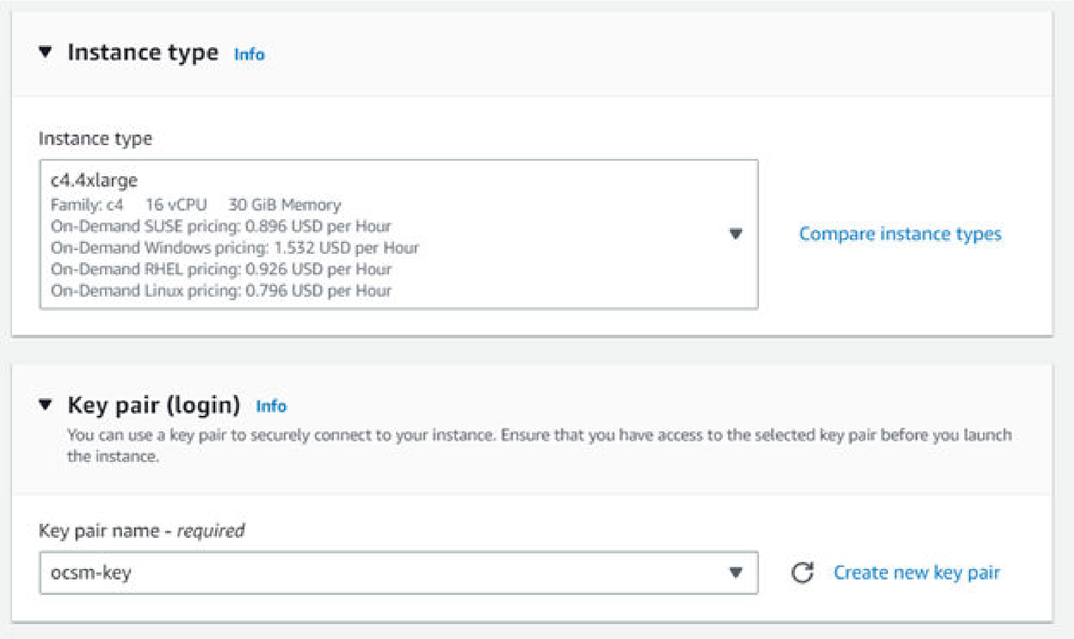
Providing the Administrator Account Information

Use a key-pair to connect to your instance securely. Before you launch the instance, ensure that you have access to the key-pair.

- Select the key pair name created in the previous section. or create a new key pair for the machine you will use to log in to the Session Monitor instance.

  During the instantiation, this key is added to the SSH-key configuration element as an authorized-key for the user.

Figure 10-10 Select the key pair name



▼ Instance type Info

Instance type

c4.4xlarge
Family: c4 16 vCPU 30 GiB Memory
On-Demand SUSE pricing: 0.896 USD per Hour
On-Demand Windows pricing: 1.532 USD per Hour
On-Demand RHEL pricing: 0.926 USD per Hour
On-Demand Linux pricing: 0.796 USD per Hour

▼ Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

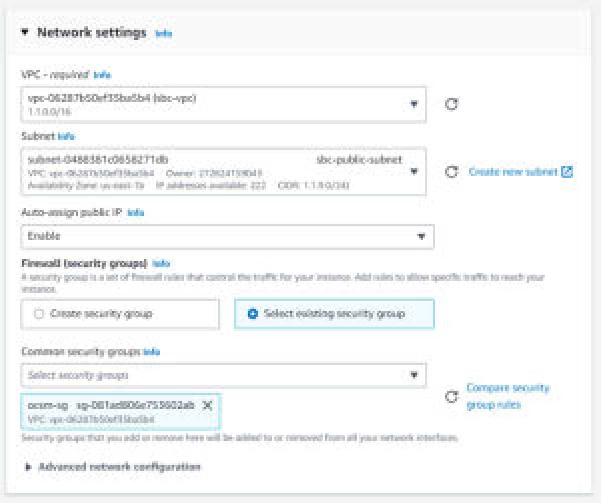
ocsm-key

Configuring Network

Configure networking for your Virtual Machine.

- Configure the following networking components for your Virtual Machine:
  - Select or create a new Virtual Network(VPC).
  - Select or create your Subnet.
  - Enter a name as your Public IP.
  - Select or create the security group.

Figure 10-11   Network Settings



▾ Network settings Info

VPC - required Info

vpc-06287b50ef35ba5b4 (sbc-vpc)
1.1.0.0/16

Subnet Info

subnet-0488381c0658271db sbc-public-subnet
VPC: vpc-06287b50ef35ba5b4 Owner: 272624159048
Availability Zone: us-east-1b IP addresses available: 223 CIDR: 1.1.0.0/24

Create new subnet

Auto-assign public IP Info

Enable

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

○ Create security group ● Select existing security group

Common security groups Info

Select security groups

ocsm-sg sg-081ad806e755602ab ✕
VPC: vpc-06287b50ef35ba5b4

Compare security group rules

Security groups that you add or remove here will be added to or removed from all your network interfaces.

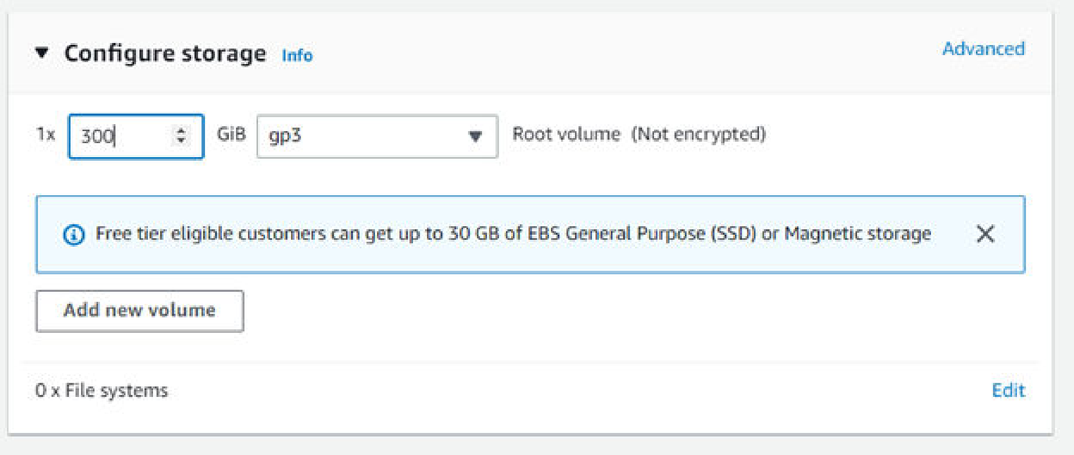
▸ Advanced network configuration

Configure Storage

Disk configuration for AWS Deployment includes setting the OS disk type to SSD for better performance.

- See the Configure Storage screen for information on the values that need to be specified

Figure 10-12   Configure Storage



▾ Configure storage Info

Advanced

1x 300 GiB gp3 Root volume (Not encrypted)

ⓘ Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage ✕

Add new volume

0 x File systems

Edit

Completing the Instance Creation

Complete the creation of your instance by retaining the default values.

1. In the **Advanced** tab, leave the default values as is.
2. You can define tags to clarify details about the instance objects. You do not need to configure anything on the Tags.

Create and Deploy Session Monitor Session Monitor on GCP

You must use those vendors' documentation for specifications, requirements, caveats, known issues, deployment details, and operation details prior to deploying the Session Monitor Session Monitor.

Prerequisites for GCP Deployment

The prerequisites for GCP deployment are:

- An account that has the privileges to create or use the resources.
- Information on the Region
- Public and Private subnet.
- Public and private keys. For more information, see https://cloud.google.com/compute/docs/connect/create-ssh-keys

> **Note**
>
> Only online installation of Session Monitor is supported.

Deploying the GCP Instance

The configuration procedure includes a multi-dialog wizard that presents configuration options in a sequence.

The instance deployment wizard sequence includes the following steps:

1. Creating a virtual machine
2. Preforming disk configuration
3. Configuring networking
4. Management
5. Reviewing configuration

Security Objects

Security lists specify the type of traffic allowed on a particular type of subnet.

Rules set on the security lists can be either stateful or stateless. Stateful rules employ connection tracking and have the benefit of not requiring exit rules. However, there is a limit to the number of connections allowed over stateful connections and there is a performance hit. Oracle, therefore, recommends stateless lists for media interfaces.

The security list for management ports can be stateful.

Table 10-3 Port Numbers for Importing Traffic

Port Number	Service	Protocol
22	SSH	TCP
111	rpcbind	TCP and UDP
80	Nginx	TCP
443	Nginx	TCP
4739-4742	apid	TCP
161	snmp	TCP and UDP

For more information, see the Oracle Communications Session Monitor Security Guide.

Virtual Machines for GCP Deployment

The minimum recommended shapes and size for virtual machines to deploy Session Monitor on GCP.

Table 10-4 Virtual Machines for GCP

Machine	Hardware Configuration	Shape Name in GCP
Mediation Engine	• 8 vCPU • 32 GB RAM • 150 Gib HDD	n2-standard-8
Mediation Engine Connector	• 8 vCPU • 32 GB RAM • 150 Gib HDD	n2-standard-8

Completing the Instance Creation

Complete the creation of your instance as per requirements.

A

Palladion Ports Usage

This document provides information on port numbers, protocols, and endpoints. This information is meant for the operators deploying Session Monitor to configure the required firewalls/ACLs.

Node	Transport	Port	Protocol	Encrypted	Function	Remote Endpoint	Remote Port
Mediation Engine, RM	TCP	80	HTTP	No	Access to Web interface	Any	Random
Mediation Engine, RM	TCP	443	HTTPS	Yes	access to Web interface	Any	Random
Mediation Engine, Probes, RM	TCP	22	SSH	Yes	access to CLI interface	Any	Random
Mediation Engine	TCP	21	FTP	No	access to FTP interface	Any	Random
Probes	TCP	8084-8086	ZMQ	No	RPC server for VQ records of the RTP probes	Mediation Engine	Random
Probes	TCP	18084-18086	XML-RPC	No	publishers for VQ records of RTP probes	Mediation Engine	Random
Probes	TCP, UDP	4004 - 4006	ZMQ	No	control interfaces server of RTP probes	Mediation Engine	Random
Probes	TCP	18000-18020	ZMQ	No	publishers for signaling messages	Mediation Engine	Random
Mediation Engine	TCP	5005	ZMQ	No	publisher for RTP streams description	Probes	Random
Mediation Engine, Probes	UDP	123	NTP	No	time synchrnoization	Time server	123
Mediation Engine	UDP	53	DNS	No	domain name resolution	Name server	53

Node	Transport	Port	Protocol	Encrypted	Function	Remote Endpoint	Remote Port
Mediation Engine, Probes	TCP	8071	XML-RPC	No	RPC server of raw traffic dumper	Probes	Random
Mediation Engine	TCP	8888	XML-RPC	No	RPC config port for rtpanalyzer	Probes	Random
Mediation Engine	UDP	1062	SNMP	No	binds counters	Not applicable	Not applicable
Mediation Engine	TCP	3306	MYSQL	No	MySQL Server TCP connection connects vsi, acd, diamond, meco, ccalls, vsp, counters, regs	Not applicable	Not applicable
Mediation Engine	TCP	4739	IPFIX	No	IPFIX communication with the SBC	SBC	Random
Mediation Engine	TCP	4740	IPFIX	YES	IPFIX communication with the SBC	SBC	Random
Mediation Engine	TCP	4741	IPFIX	No	IPFIX communication with the probe	probes	Random
Mediation Engine	TCP	4742	IPFIX	YES	IPFIX communication with the probe	probes	Random
Mediation Engine	TCP	5090	SIP	No	port to send SIP publish to the Vqcollector	Any	Random
Mediation Engine	TCP	5555-5559	ZMQ-RPC	No	Counters manager publishes cnt changes to counters	Internal(vsi, meco, acd, diamond, apid)	Random
Mediation Engine	TCP	6379-6389	REDIS	No	redis connects to vsi diamond and sau	Not applicable	Not applicable
Mediation Engine	TCP	8077	XML-RPC	No	counter connects to vsp	Not applicable	Not applicable

Node	Transport	Port	Protocol	Encrypted	Function	Remote Endpoint	Remote Port
Mediation Engine	TCP	8080	XML-RPC	No	vsi connects to vsp, vsictl.py	Mediation Engine, Probe	Not applicable
Mediation Engine	TCP	8081 - 8086	HTTP	No	VSP connects nginx	Not applicable	Not applicable
Aggregation Engine	TCP	8095	HTTP	No	SAU REST interface, only bound on LO binds - sau connect - external	External	Not applicable
Mediation Engine	TCP	8184	XML-RPC	No	apid XMLRPC listener connects to VSP	Internal(Apid)	Random
Mediation Engine	TCP	8186	ZMQ-RPC	No	Counter manager publishes cnt changes to VSI binds - vsi connects - counter manager	Internal(VSI)	Random
Mediation Engine	TCP	8188	ZMQ-RPC	No	Megaco probe ZMQ-PB-RPC port	Internal	Random
Mediation Engine	TCP	8189	ZMQ-RPC	No	MGCP probe ZMQ-PB-RPC port	Internal	Random
Mediation Engine	TCP	8190	ZMQ-RPC	No	ENUM probe ZMQ-PB-RPC port	Internal	Random
Mediation Engine	TCP	8191	ZMQ-RPC	No	DIAMETER probe ZMQ-PB-RPC port	Internal	Random
Probe	TCP	8192	ZMQ-RPC	No	rat (RTP sniffer) ZMQ-PB-RPC port	Internal	Random
Mediation Engine	TCP	8193	ZMQ-RPC	No	ccalls probe ZMQ-PB-RPC port	Internal	Random

Node	Transport	Port	Protocol	Encrypted	Function	Remote Endpoint	Remote Port
Mediation Engine	TCP	8194	ZMQ-RPC	No	apid probe ZMQ-PB-RPC port	Internal	Random
Probe	TCP	8195	ZMQ-RPC	No	rapid ZMQ-PB-RPC port	Internal	Random
Mediation Engine	TC	10001	ZMQ-RPC	No	Megaco probe XMLRPC configuration bind - megaco_probe, connect - vsp	Internal	Random
Mediation Engine	TCP	10002	XML-RPC	No	acd connects to vsp(ACD correlation XMLRPC configuration) binds - acd connects - vsp	Internal	Random
Mediation Engine	TCP	10005	XML-RPC	No	MGCP probe XMLRPC configuration bind - mgcp_probe, connect - vsp	Internal	Random
Mediation Engine	TCP	10009	XML-RPC	No	ENUM probe XMLRPC configuration binds - enum_probe connects - vsp	Internal	Random
Mediation Engine	TCP	10013	XML-RPC	No	DIAMETER probe XMLRPC configuration bind - diameter_probe, connect - vsp	Internal	Random
Mediation Engine	TCP	10017	ZMQ-DATPUB	No	vsi counter publish (ZMQ-JSON) endpoint	Internal	Random

Node	Transport	Port	Protocol	Encrypted	Function	Remote Endpoint	Remote Port
Mediation Engine	TCP	10019	XMLRPC	No	usd XMLRPC interface	Internal	Random
Mediation Engine	TCP	10021	ZMQ-RPC	No	vsi alias update publish endpoint (ZMQ-ProtoBuf interface vsi-usd)	Internal	Random
Mediation Engine	TCP	10023	XMLRPC	No	meco (Media Correlator) XMLRPC server port meco connects to vsp	Internal	Random
Mediation Engine	TCP	10024	ZMQ-RPC	No	Counter manager publiches cnt changes to meco meco connects to counter manager	Internal	Random
Mediation Engine	TCP	10025	ZMQ-DATPUB	No	meco connects to vsi meco (Media Correlator) ZMQ publisher (meco to VSI). This port is used by MECO to publish media leg reports (VQsummary data) to VSI.	Internal	Random

Node	Transport	Port	Protocol	Encrypted	Function	Remote Endpoint	Remote Port
Mediation Engine	TCP	10026	ZMQ-DATPUB	No	vsi connects to meco VSI ZMQ publisher for Media Leg Updates (VSI to meco). This port is used by VSI to send media related data about a call (by checking the SDP pairs) to MECO so that MECO can correlate it with RTP data.	Internal	Random
Mediation Engine	TCP	10027	ZMQ-DATPUB	No	meco to counters_reader meco (Media Correlator) counter publish (ZMQ-JSON) endpoint port	Internal	Random
Mediation Engine	TCP	10028	ZMQ-DATPUB	No	Diamond counter publish (ZMQ-JSON) endpoint port Diamond connects to counter_reader	Internal	Random
Mediation Engine	TCP	10030	ZMQ-DATPUB	No	apid connects to vsi apid (ZMQ-JSON) endpoint port (subscribed by VSI for VQ data	Internal	Random

Node	Transport	Port	Protocol	Encrypted	Function	Remote Endpoint	Remote Port
Mediation Engine	TCP	10038	ZMQ-DATPUB	No	sdnp connects to vsi sdnp (ZMQ-JSON) endpoint port (subscribed by VSI for VQ data	Internal	Random
No NODE	TCP	10034	XMLRPC	No	diamond XMLRPC server port	Internal	Random
Mediation Engine	TCP	10555	XMLRPC	No	counters reader connects to counters manager Counters manager retrieves counter values from reader cvd1 (counters values daemon of vsi cnts)	Internal	Random
Mediation Engine	TCP	10556	XMLRPC	No	counters reader connects to counters manager Counters manager retrieves counter values from reader cvd2 (counters values daemon of meco cnts)	Internal	Random

Node	Transport	Port	Protocol	Encrypted	Function	Remote Endpoint	Remote Port
Mediation Engine	TCP	10557	XMLRPC	No	counters reader connects to counters manager Counters manager retrieves counter values from reader cvd3 (counters values daemon of meco cnts)	Internal	Random
Mediation Engine	TCP	10558	XMLRPC	No	counters reader connects to counters manager Counters manager retrieves counter values from reader cvd4 (counters values daemon of diamond cnts)	Internal	Random
Mediation Engine	TCP	10559	XMLRPC	No	counters reader connects to counters manager Counters manager retrieves counter values from reader cvd5 (counters values daemon of apid cnts)	Internal	Random
Mediation Engine	TCP	12010	XMLRPC	No	export-metrics XMLRPC server (used by VSP for configuration injection)	Internal	Random

Node	Transport	Port	Protocol	Encrypted	Function	Remote Endpoint	Remote Port
Mediation Engine	TCP	18010	ZMQ-PKTPUB	No	apid SIP publisher apid (binds) connects to vsi	Internal	Random
probe	TCP	18015	ZMQ-PKTPUB	No	binds rat, connects rapid, ZMQ SIP publisher	Internal	Random
probe	TCP	18018	ZMQ-PKTPUB	No	binds rat, connects rapid, ZMQ Enum publisher (frames)	Internal	Random
probe	TCP	18019	ZMQ-PKTPUB	No	binds rat, connects rapid, ZMQ diameter publisher (frames)	Internal	Random
Probe	TCP	18027	ZMQ-DATPUB	No	rat daemon (RTP sniffer) RTP statistics publisher Publish statistics related to RTP and RTCP. Rat(bind) rapid(connect)	Internal	Random
Mediation Engine	TCP	18028	ZMQ-DATPUB	No	megaco_probe(bind) acd (connect) Megaco Control to acd	Internal	Random
Mediation Engine	TCP	18029	ZMQ-DATPUB	No	mgcp_probe(bind) acd (connect) Mgcp Control to acd	Internal	Random
Mediation Engine	TCP	18030	ZMQ-DATPUB	No	Enum_probe(bind) acd (connect) Enum Control to acd	Internal	Random

Node	Transport	Port	Protocol	Encrypted	Function	Remote Endpoint	Remote Port
Mediation Engine	TCP	18031	ZMQ-DATPUB	No	diameter_probe(bind) acd (connect) Diameter(CX) Control to acd	Internal	Random
Probe	TCP	18032	ZMQ-PKTPUB	No	rat(bind) rapid(connect)rat daemon packet publisher. Publish recorded RTP/RTCP packets.	Internal	Random
Probe	TCP	18033	ZMQ-DATSUB	No	rat(bind) rapid(connect) rat daemon listen port for RecordRequest subscriber	Internal	Random
Mediation Engine	TCP	19016	ZMQ-PKTPUB	No	megaco_probe(bind) acd (connect) MEGACO frames forwarded to acd	Internal	Random
Mediation Engine	TCP	19017	ZMQ-PKTPUB	No	mgcp_probe(bind) acd (connect) MGCP frames forwarded to acd	Internal	Random
Mediation Engine	TCP	19018	ZMQ-PKTPUB	No	enum_probe(bind) acd (connect) ENUM frames forwarded to acd	Internal	Random
Mediation Engine	TCP	19019	ZMQ-PKTPUB	No	diameter_probe(bind) acd (connect) Diameter_cx frames forwarded to acd	Internal	Random

Node	Transport	Port	Protocol	Encrypted	Function	Remote Endpoint	Remote Port
Mediation Engine	TCP	10031	ZMQ-DATPUB	No	acd(bind) vsi (connect) acd to vsi protocol leg report	Internal	Random
Mediation Engine	TCP	10032	ZMQ-DATPUB	No	vsi(bind) acd(connect) vsi to acd call leg updates	Internal	Random
Mediation Engine	TCP	10035	ZMQ-DATPUB	No	acd(bind) counter(connect) acd counter publishing port, counters daemon connects to it	Internal	Random
Mediation Engine	TCP	10036	ZMQ-DATPUB	No	apid(bind) counter(connect)apid counter publishing port	Internal	Random
Mediation Engine	TCP	10037	ZMQ-DATPUB	No	apid(bind)meco(connect) apid (ZMQ-Protobuf) endpoint port (subscribed by MECO for VQ chunks)	Internal	Random
Mediation Engine	TCP	10033	ZMQ-RPC	No	acd(bind) counters manager(connect) counter manager publishes cnt changes to acd	Internal	Random

Node	Transport	Port	Protocol	Encrypted	Function	Remote Endpoint	Remote Port
Mediation Engine	TCP	18054	ZMQ-PUBSUB	No	Encapsulated frames as a result of a forward_cmd message.. Pint(bind) meco(connect)	Internal	Random
Mediation Engine	TCP	18060	ZMQ-DATPUB	No	ZMQ vsi publisher (DB calls update data) (vsi publishes, ccalls subscribes)vsi(bind) ccalls(connect)	Internal	Random
Mediation Engine	TCP	18061	ZMQ-DATPUB	No	ZMQ vsi publisher (DB registration event data (vsi publishes, ccalls subscribes)vsi(bind) ccalls(connect)	Internal	Random
Mediation Engine	TCP	18062	ZMQ-DATPUB	No	ZMQ vsi publisher (DB subscription event data(vsi publishes, ccalls subscribes) vsi(bind) ccalls(connect)	Internal	Random
Mediation Engine	TCP	18115	ZMQ-PKTPUB	No	ZMQ SIP publisher apid(bind) vsi (connect)	Internal	Random

Node	Transport	Port	Protocol	Encrypted	Function	Remote Endpoint	Remote Port
Mediation Engine	TCP	18116	ZMQ-PKTPUB	No	ZMQ Megaco publisher (frames) apid(bind) megaco_probe (connect)	Internal	Random
Mediation Engine	TCP	18117	ZMQ-PKTPUB	No	ZMQ mgcp publisher (frames) apid(bind) mgcp_probe (connect)	Internal	Random
Mediation Engine	TCP	18118	ZMQ-PKTPUB	No	ZMQ enum publisher (frames) apid(bind) enum_probe (connect)	Internal	Random
Mediation Engine	TCP	18119	ZMQ-PKTPUB	No	ZMQ diameter publisher (frames) apid(bind) diameter_probe (connect)	Internal	Random
Mediation Engine	TCP	18127	ZMQ-DATPUB	No	rat daemon (RTP sniffer) RTP statistics publisher Publish statistics related to RTP and RTCP. Apid(bind) meco(connect)	Internal	Random
Mediation Engine	TCP	18132	ZMQ-PKTPUB	No	rat daemon packet publisher. Publish recorded RTP/RTCP packets. Apid(bind) meco(connect)	Internal	Random

Node	Transport	Port	Protocol	Encrypted	Function	Remote Endpoint	Remote Port
Mediation Engine	TCP	18133	ZMQ-DATSUB	No	rat daemon listen port for RecordRequest subscriber Apid(bind) meco(connect)	Internal	Random
Mediation Engine	TCP	18150	ZMQ-DATPUB	No	Packet inspector info publisher. Apid(bind) pint(connect)	Internal	Random
Mediation Engine	TCP	18151	ZMQ-DATPUB	No	Packet inspector search interface. Apid(bind) pint(connect)	Internal	Random
Mediation Engine	TCP	18200	ZMQ-PKTPUB	No	apid Diameter publisher for DSC integration with CPM apid(bind) diameter(connect)	Internal	Random
Mediation Engine, probe, Aggregation Engine	TCP	18300	HTTPS	Yes	Skype for Business SDN API updates subscriber port sdnp(bind) nginx(connect)	Internal	Random