# Oracle® Communications Session Monitor

Installation Guide

Release 3.3.92

**E74347-01**

June 2016

ORACLE®

Oracle Communications Session Monitor Installation Guide, Release 3.3.92

E74347-01

# Contents

## 4 Session Monitor Post-Installation Tasks



## 5 Installing Operations Monitor Probe on Oracle Linux

# Preface

This guide provides instructions for installing Oracle Communications Session Monitor.

The Oracle Communications Session Monitor product family includes the following products:

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

## Audience

This guide is intended for the person or team that installs and maintains the Session Monitor products.

## Downloading Oracle Communications Documentation

Oracle Communications Session Monitor documentation and additional Oracle documentation is available from the Oracle Help Center Web Site:

http://docs.oracle.com

## Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

### Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

## Document Revision History

The following table lists the revision history for this document:

| Version | Date | Description |
|---|---|---|
| E74347-01 | June 2016 | Initial release. |

# 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

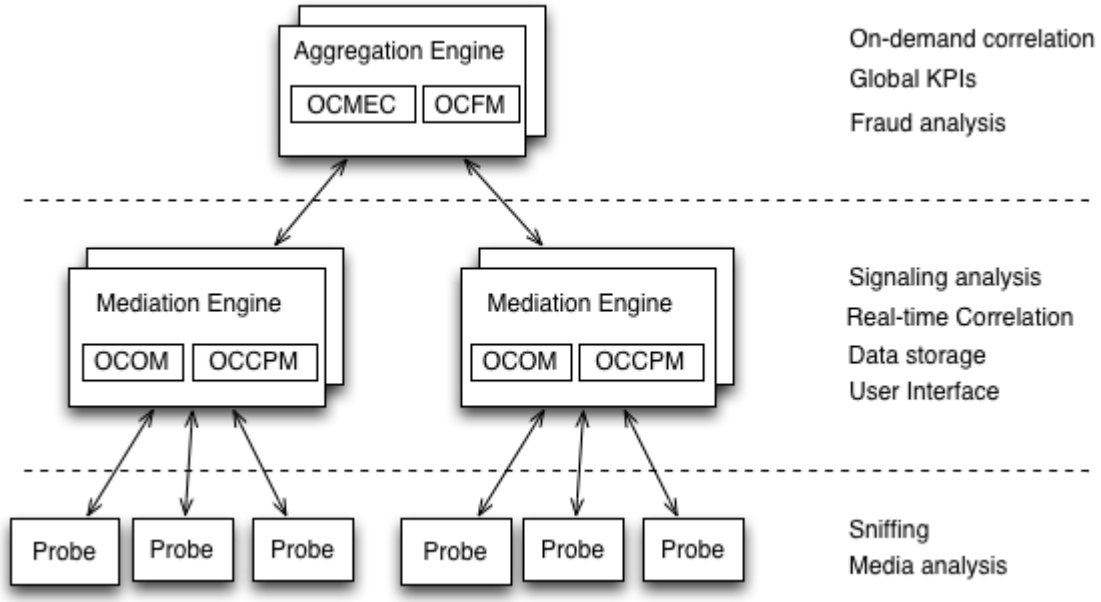
The Session Monitor system works by capturing the traffic from your network, correlating it in real-time, and storing it in indexed formats so that they are available for the various reports offered by the web interface.

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 (ME) layer**: This layer is responsible for understanding in real-time the traffic received, correlating it and storing it for future reference. This layer is also responsible for measuring, managing, and storing the KPIs. In the common case, there is one ME per geographical site. It is possible, however, to have the probes from multiple geographical sites sending the traffic to a single ME. It is also possible to have multiple ME installations in the same geographical site.
- **Aggregation Engine (AE) layer**: This layer is responsible for aggregating the global KPIs, on-demand correlation of calls passing multiple geographical sites, and for the global search features. In a typical setup, there is only one AE for the whole network.

Figure 1–1 shows the Session Monitor system architecture.

***Figure 1–1 Session Monitor System Architecture***




Each of the three layers supports high-availability by deploying two identical servers in active-passive or active-active modes of operation. For small setups, it is possible to run the probe layer and the ME layer on the same physical hardware. The AE layer always requires its own hardware.

From the Session Monitor products perspective, the Operations Monitor and the Control Plane Monitor (CPM) run on the Mediation Engine (ME) while the Mediation Engine Connector (MEC) and the Fraud Monitor products run on the Aggregation Engine (AE).

# 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

The following sections describe the system requirements for installing Session Monitor.

## Session Monitor Software Requirements

Table 1–1 lists the supported client browsers:

***Table 1–1 Supported Client Browsers***

| Browser | Version |
|---|---|
| Microsoft Internet Explorer | 8 or higher |
| Mozilla Firefox | 1.5 or higher (on any operating system) |

*Table 1–1 (Cont.) Supported Client Browsers*

| Browser | Version |
|---|---|
| Apple Safari | Any version, including Safari for iPad |
| Google Chrome | Any version |
| Opera | 9 or higher (on any operating system) |

## Session Monitor Supported Hardware

Session Monitor is supported on Sun and HP systems.

Table 1–2 lists the hardware supported for Sun systems.

*Table 1–2 Supported Hardware for Sun systems*

| Component | Requirement |
|---|---|
| Server | The following severs are supported:<br>■ Sun Server X2-4<br>■ Sun Server X3-2<br>■ Sun Server X4-2L<br>■ Sun Server X4-2<br>■ Sun Server X5-2<br>■ Sun Server X5-2L |
| Network Adapter | The following network adapters are supported:<br>■ Sun Dual Port 10 GbE PCIe 2.0 Networking Card with Intel 82599 10 GbE Controller<br>■ Sun Quad Port GbE PCIe 2.0 Low Profile Adapter, UTP<br>■ Sun Dual Port GbE PCIe 2.0 Low Profile Adapter, MMF |

Table 1–3 lists the hardware supported for HP systems.

*Table 1–3 Supported Hardware for HP Systems*

| Component | Requirement |
|---|---|
| Server | The following servers are supported:<br>■ HP DL380p G8, Embedded Smart Array P420i Controller<br>■ HP DL580 G7, Embedded Smart Array P410i Controller |
| Network Adapter | The following network adapter s are supported:<br>■ HP NC364T PCIe Quad Port Gigabit Server Adapter<br>■ HP NC365T PCIe Quad Port Gigabit Server Adapter<br>■ HP Ethernet 1Gb 4-port 366FLR Adapter |
| Capture Cards | The following capture cards are supported:<br>■ Napatech NT4E (4x 1Gbe ports)<br>■ Napatech NT20E2 (2x 10Gbe ports)<br>**Note:** Only one Napatech capture card per server is supported. |

## Session Border Controller Supported Versions

Table 1–4 lists supported Session Border Controller (SBC) versions.

*Table 1–4 Supported Session Border Controller Versions*

| Product | Versions |
|---|---|
| Enterprise Session Border Controller (E-SBC) | ■ EC640<br>■ EC710<br>■ EC720<br>■ EC730 |
| Session Border Controller (SBC) | ■ ECZ730 |

## Hardware Requirements for Demonstration Systems

For development or demonstrations systems with little network traffic, Table 1–5 lists the minimum requirements to install any of the Session Monitor machine types.

*Table 1–5 Hardware Requirements for Demonstration Systems*

| Component | Minimum Requirement |
|---|---|
| Processor | 2.6 GHz Intel Xeon processor, 64-bit with 8 processing threads |
| Memory | 8 GB RAM |
| Disk Space | 80 GB storage on a hardware RAID controller |
| Ports | 2 Ethernet ports |

## Hardware Requirements for Production Systems

For production systems, Oracle recommends to complete a sizing exercise together with your Oracle sales engineer. Higher performance hardware may be required, for example, in cases with:

- High levels of monitored traffic
- High numbers of concurrent users
- High volumes of historical information

On the Mediation Engine machines, Oracle recommends using a RAID-10 array for the operating system and the database. A separate RAID-5 array is recommended for storing long-term data.

## Session Monitor Virtualization Support

This section describes the software and hardware requirements for Session Monitor virtualization.

### Hypervisor Support

The following hypervisors are supported:

- Oracle VM version 3.2.7
- VMware vSphere ESXi 5.1

### Virtual Machine Requirements

Table 1–6 lists the minimum requirements for the virtual machines.

*Table 1–6 Hardware Requirements for Virtual Machines*

| Component | Requirement |
|---|---|
| Processor | 8 vCPUs |
| Memory | 8GB RAM |
| Disk Space | 80GB |
| NIC Card | 1Gbps vNIC |

In virtualized Mediation Engines, 50,000 concurrent calls (1 SIP leg per call) have been tested successfully.

### Host Machine Requirements

The physical machine that hosts the virtual machines should contain at a minimum the hardware resources that are required to host all the virtual machines, in addition to the hardware that is required for the hypervisor.

## Types of Installation Media

Session Monitor may be installed using a DVD or USB flash drive. If you are going to use a USB flash drive, make sure that its size is at least 1GB. See "Preparing Session Monitor Installation Media" for instructions on how to prepare a USB flash drive.

**Important:** When updating from a Palladion2.X installation, no data is carried over. If you want to keep the settings, create a configuration savepoint using the web interface and export it to a file. After completing the installation, you can upload the savepoint file and restore the settings.

**Note:** Oracle recommends the following:

- Use brand drives, as issues have been reported when using low-quality thumb drives.
- If the hardware on which Session Monitor is installed supports iLO or another out-of-band management technology, Oracle recommends to configure it before starting the installation.

# 2

# Installing Session Monitor

This chapter describes how to install Oracle Communications Session Monitor.

## Installing Session Monitor

To install Session Monitor:

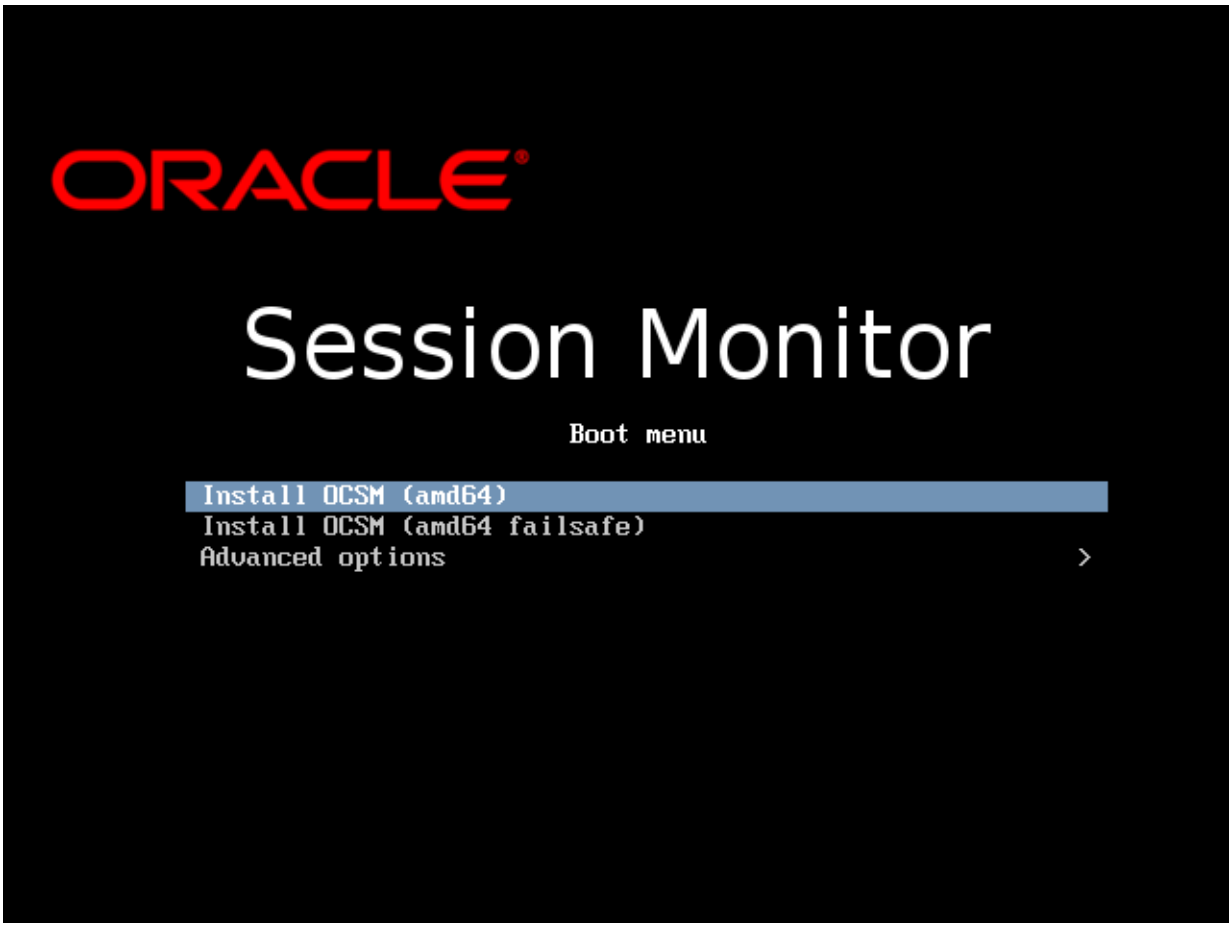
1. Insert the DVD or attach the USB flash drive and power on the system. Make sure that the machine boots from the installation media. This is usually done using a one-time boot option.

   **Note:** Booting from EFI without BIOS emulation is not supported.

   If booting from the installation media succeeds, you should see the Session Monitor installer Boot Menu screen.

   Figure 2–1 shows the Boot Menu screen.

***Figure 2–1 Session Monitor Boot Menu Screen***




Press ENTER on your keyboard to continue the installation. The installer is subsequently loaded which can take a few minutes.

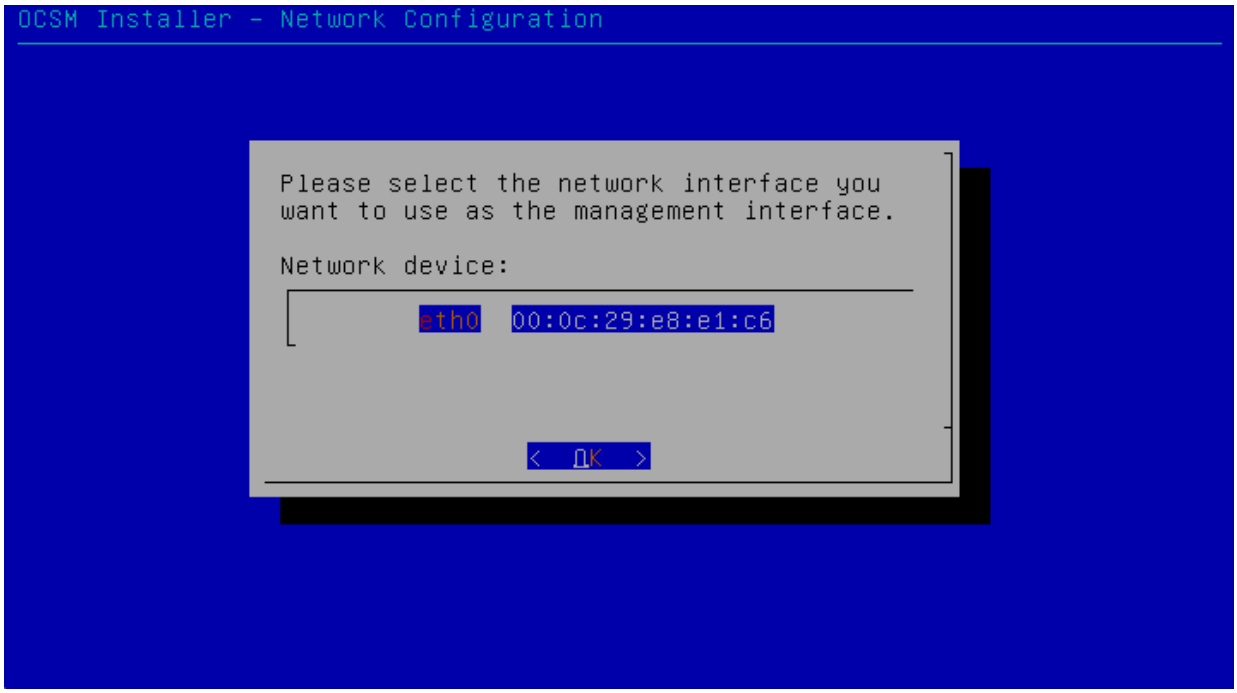
The installer checks whether the hardware passes the minimum system requirements for Session Monitor. If the minimum system requirements are not met, installation does not continue. See "Session Monitor System Requirements" or contact your Oracle sales engineer for more information about the system requirements.

2. Select the network adapter that is to be used for the management Web interface. A list of the supported network interfaces together with their hardware addresses (MAC) is shown.

   Figure 2–2 shows the network adapter selection screen.

   Choose the interface to use for accessing Session Monitor. Access via this interface is required to finish the installation. Refer to the documentation of the machine for further information about the location of network interfaces.

***Figure 2–2 Network Adapter Selection***

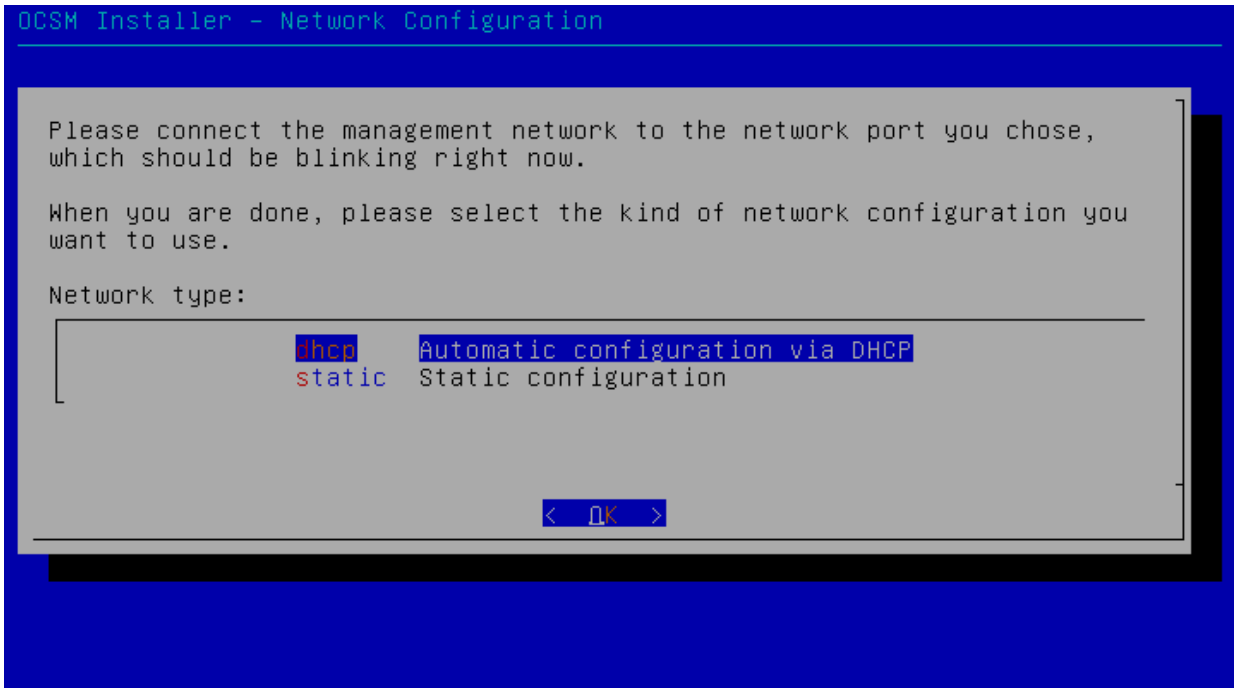



3. Select the IP configuration for the management network adapter. You can select to configure static IP settings manually or using DHCP.

   Figure 2–3 shows the network adapter IP configuration selection screen.

   **Note:** No error checking is performed to validate the network configuration; verify your inputs before proceeding.

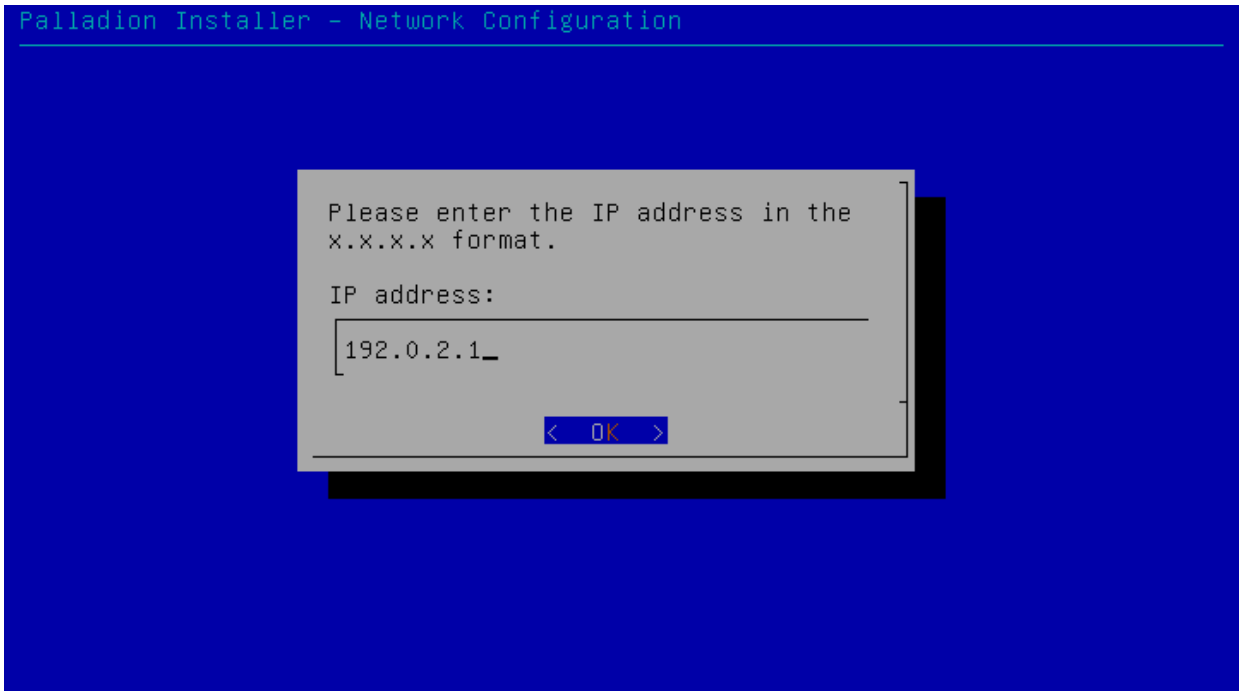
***Figure 2–3 Network Adapter IP Configuration Selection***




4. If you select static IP configuration, the installer prompts for the IP address, netmask, and the default gateway of your network.

   Figure 2–4 shows the network adapter IP address specification screen.

***Figure 2–4 Network Adapter IP Address Specification***



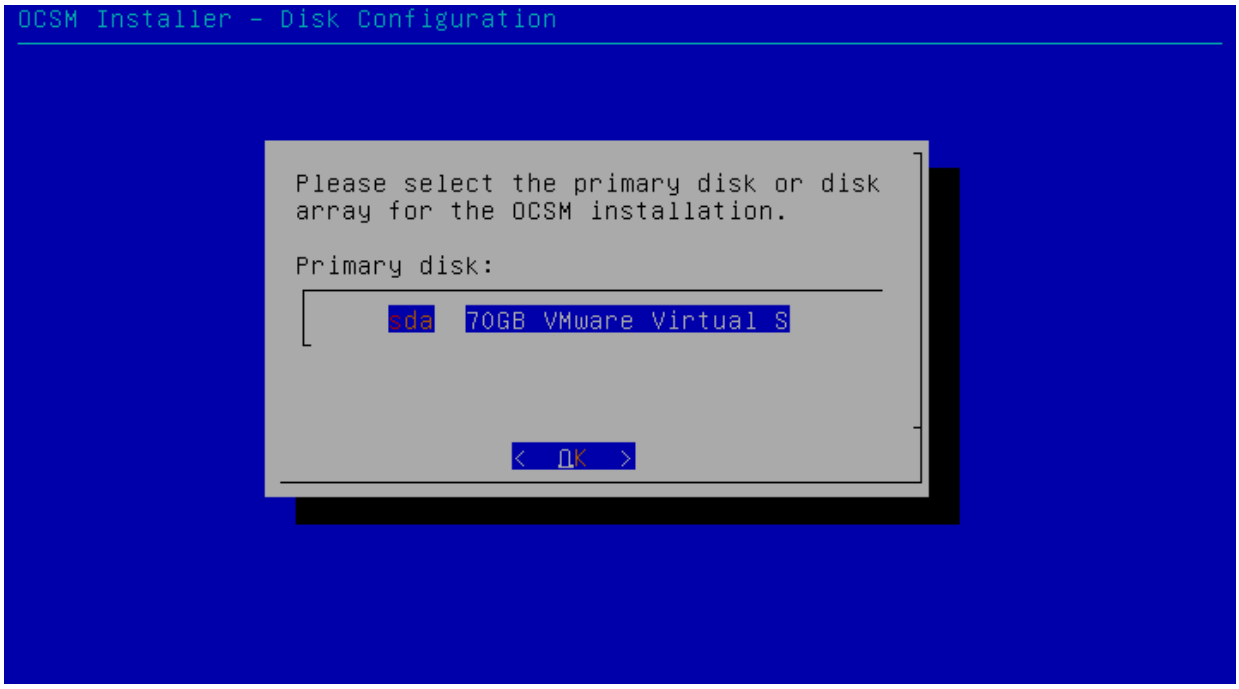

5. Select the primary disk or disk array for the installation. The primary disk will hold the Session Monitor operating system and the database. In the second step

you can choose to use another disk for long-term stored data or to keep all data on one disk.

**Caution:** Session Monitor installer erases any existing files on the disk to prepare the disk with the operating system. Make sure to back up any important files on the disk before proceeding with the installation.

Figure 2–5 shows the primary disk selection screen.

***Figure 2–5 Primary Disk Selection***



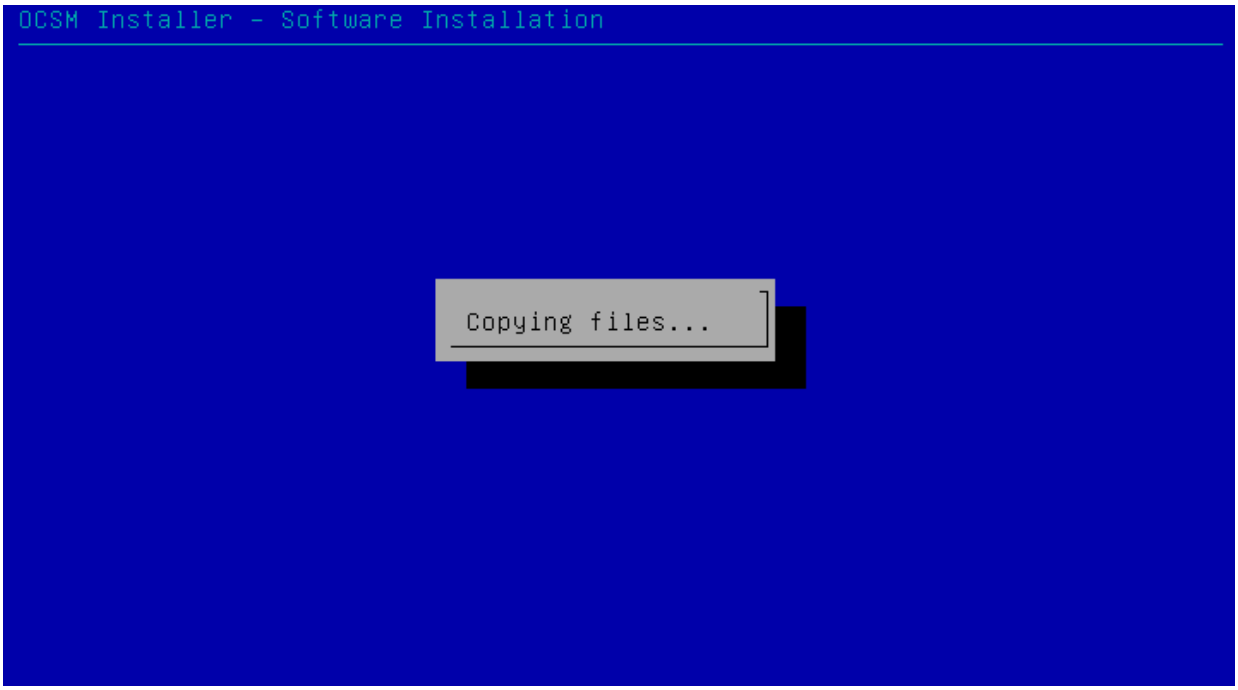

**Note:** The primary disk can have a size between 70GB and 2TB. If you want to use a larger disk array for data storage, configure it as a secondary disk.

**Important:** Configuring a machine with a secondary disk as a standalone Probe is not supported. Only Mediation Engine and Mediation Engine with embedded Probe machines can use a secondary disk.

6. The installer prepares the disks and sets up the system. This installation process usually takes about 10 minutes.

   Figure 2–6 shows the installation screen.

***Figure 2–6 Session Monitor Installation***

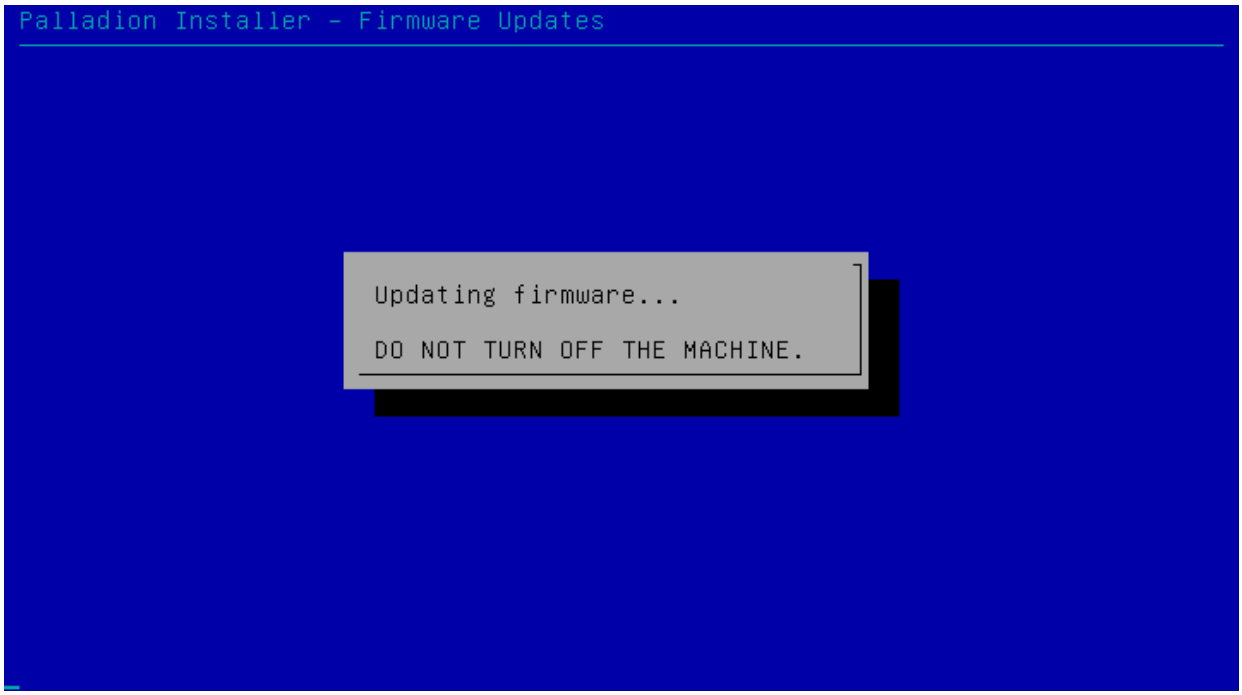



7. The installer updates the firmware required for the hardware components on the machine. This process can take several minutes to complete.

   **Note:** Do not power off the machine during this process, as this may leave components in an unusable state.

   Figure 2–7 shows the firmware update screen.

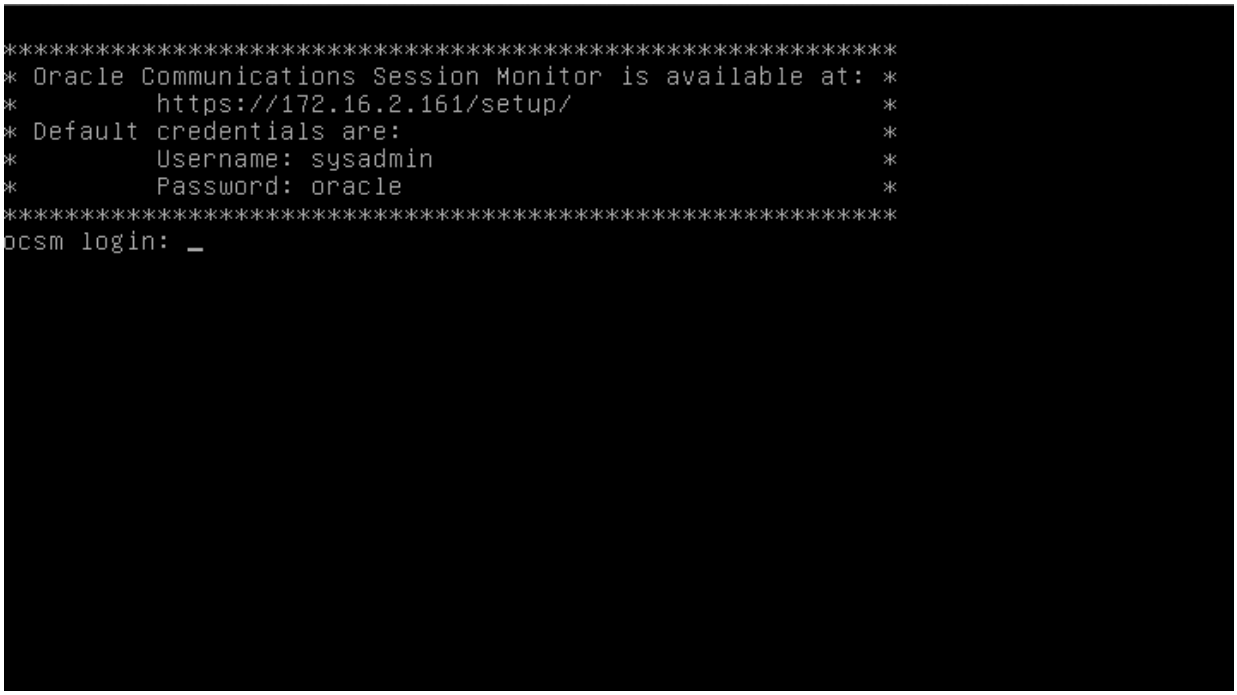
***Figure 2–7 Firmware Update***




8. The installer reboots the system. When instructed, remove the USB flash drive or DVD used for the installation. Make sure that the machine boots from the primary hard disk that you selected in the previous steps.

   Figure 2–8 shows the system reboot screen.

***Figure 2–8 System Reboot***



9. After rebooting, the machine shows the IP address that it uses. Open the URL https://*ip-address*/ in your Web browser to continue with the configuration of the Session Monitor system. You should see the login dialog to the Session Monitor Platform Setup Application (see "Configuring Session Monitor").

# 3

# 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, network settings, DNS settings, and SMTP settings.

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

The Machine Type page lets you choose the applications you want to install. In the License page you can upload a license file that also configures the applications.

The subsequent sections help you in configuring the machine for your network and time zone. These steps are optional and can be skipped by clicking on **Continue**.

You can review and change these settings at any time by visiting the Platform Setup Application at the https://*ip-address*/setup/ URL. This URL is valid for any Session Monitor server.

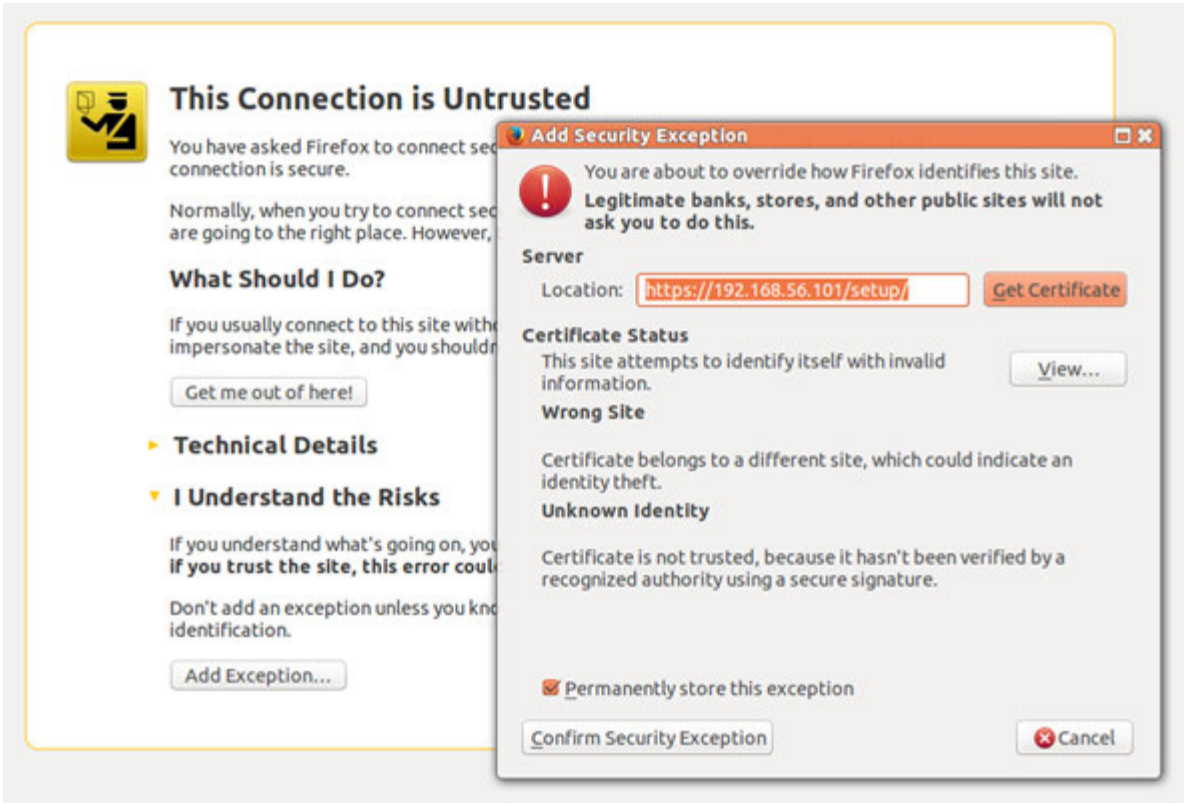
In the final step, the applications that are selected are installed. After the successful installation, you are taken to the applications.

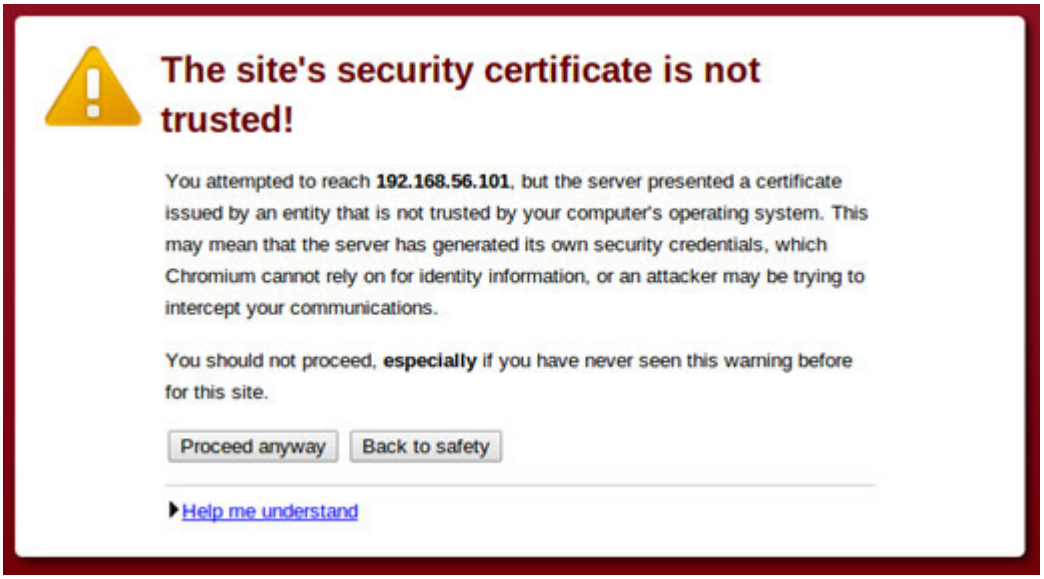
### Platform Setup Application Initial Log In

All Session Monitor interfaces can only be accessed through encrypted HTTPS connections. At initial login, your Web browser may not recognize the server and display the "This Connection is Untrusted" a warning message. Confirm the security exception to proceed.

Figure 3–1 shows the security exception confirmation screen.

***Figure 3–1 Security Exception Confirmation***



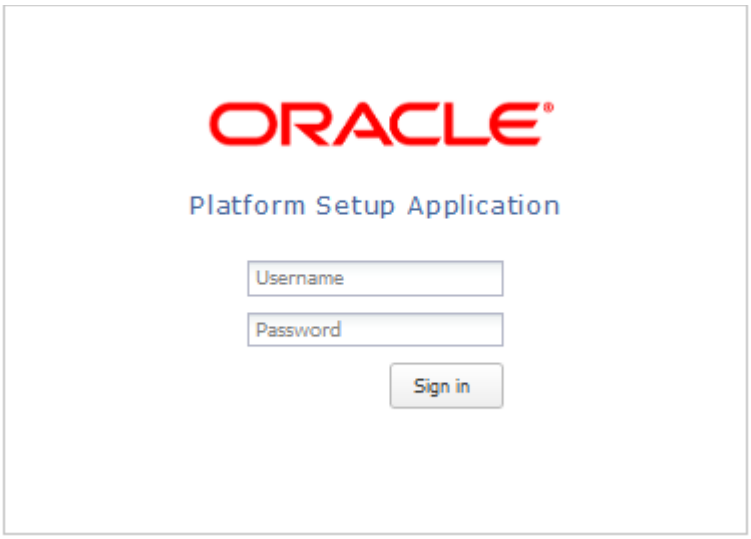




See "Secure Configuration" for information about how to protect connections to the system and avoid the untrusted certificate warning in the future.

The login page allows you to access the Platform Setup Application. Enter your user name and password into the indicated fields then click **Sign in**.

Figure 3–2 shows the Platform Setup Application Login page.

*Figure 3–2 Platform Setup Application Login Page*




If the user name or password entered are incorrect, a warning message appears below the login button and you'll have the opportunity to retry.

You can log into the Platform Setup Application using the default user name **sysadmin** and password **oracle**.

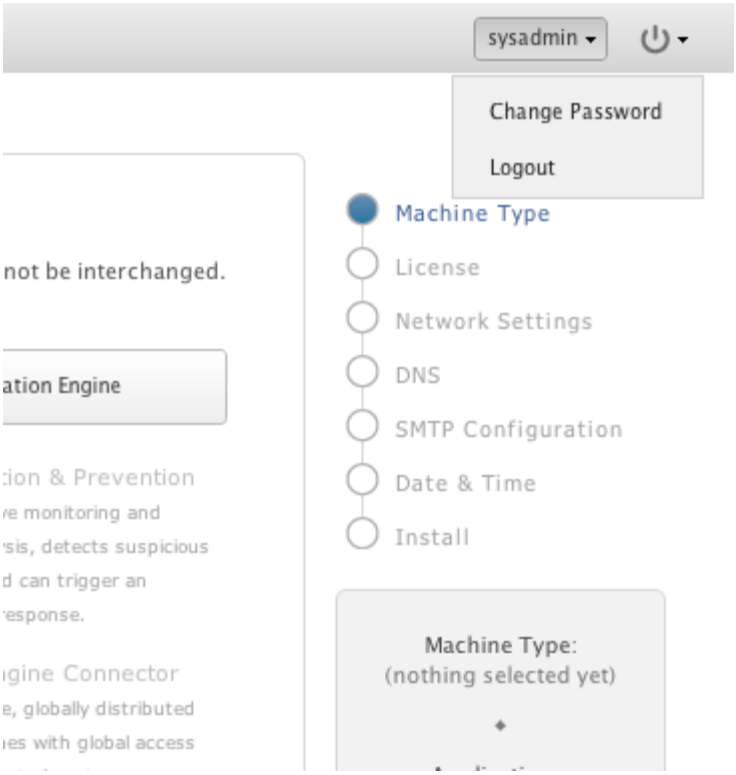
After you log in, you are prompted to review and accept the license of the software. You must agree to the license terms to continue.

## Changing Your Password

To change your password, click your user name in the top right-hand corner of the screen and select **Change Password** from the drop-down menu.

Figure 3–3 shows the drop-down menu when you click your user name.

*Figure 3–3 Change Password Menu Item*




In the Change Password dialog box, enter the old and the new passwords in the indicated fields and click **Change** to complete the action.

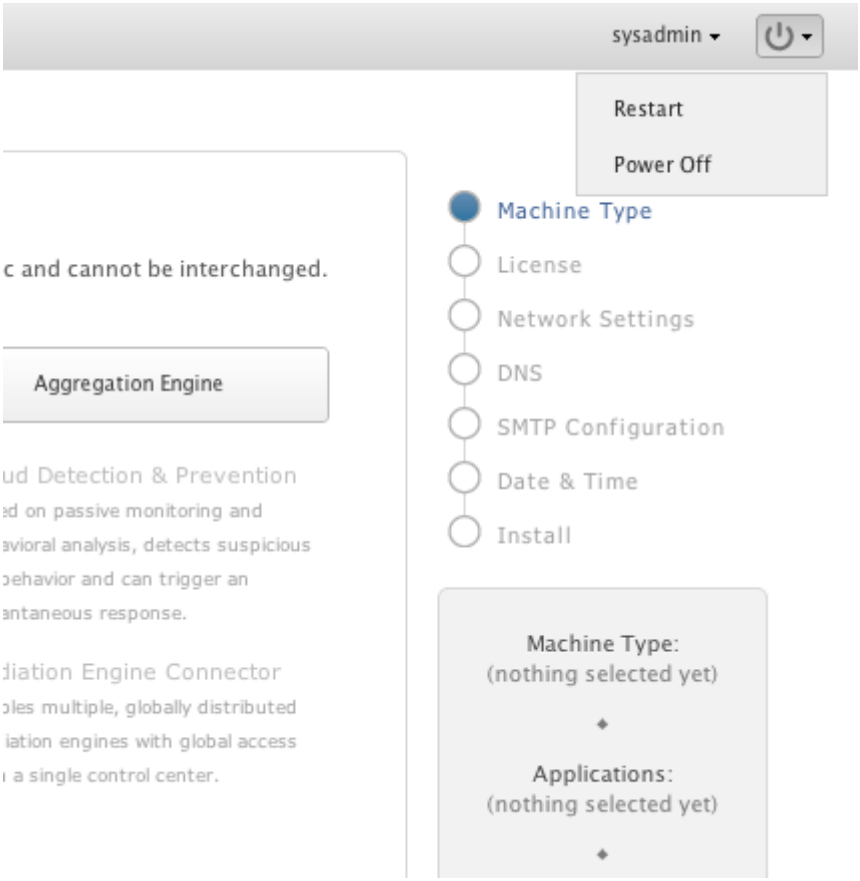
**Note:** The password can only contain digits, letters and white spaces.

## 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 3–4 shows the drop-down menu when you click the power button.

***Figure 3–4 Restarting or Powering Off Session Monitor***

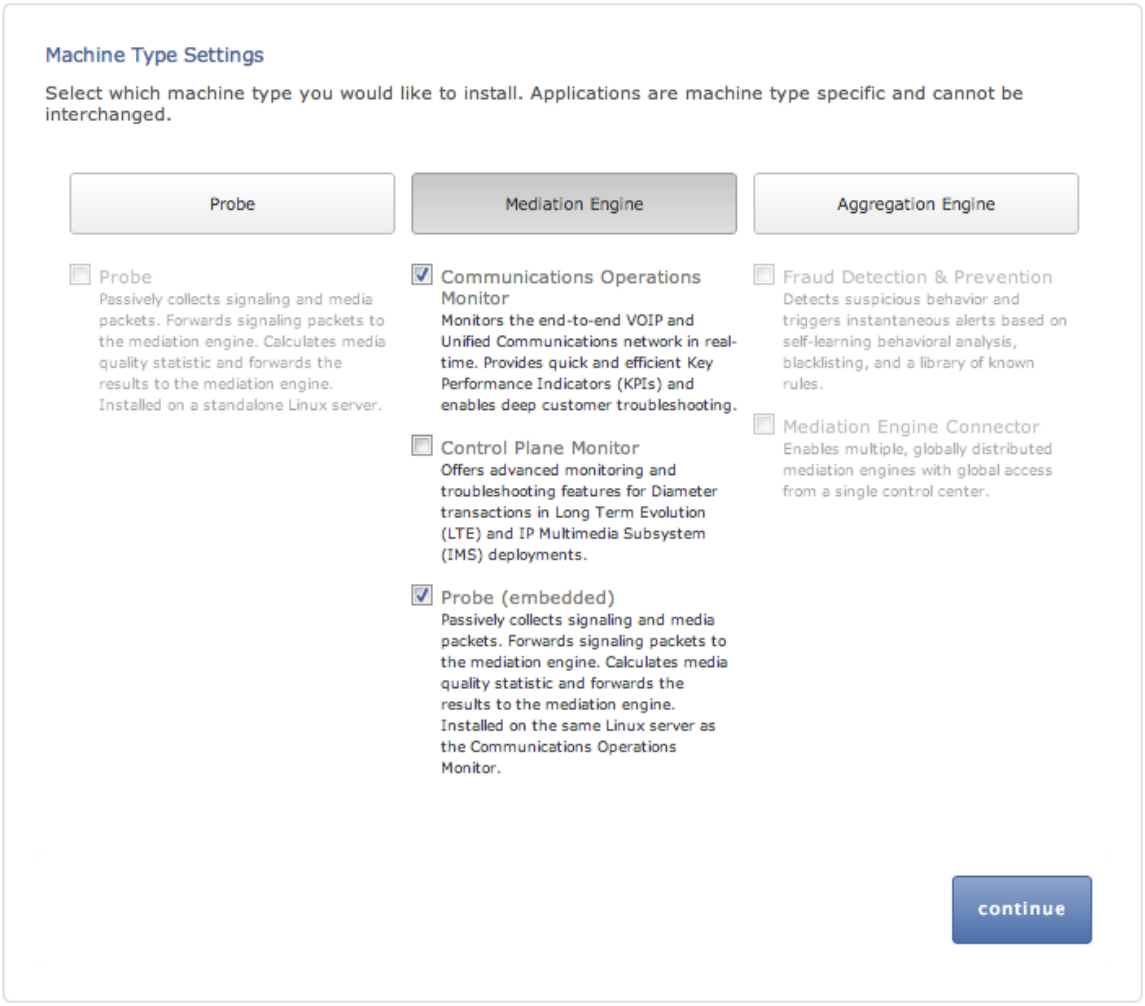



After selecting an option, you are prompted a final time to confirm that you wish to proceed.

## Selecting the Machine Type

Figure 3–5 shows the Machine Type Settings page.

***Figure 3–5 Machine Type Settings***




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.
- If you plan to use Packet Inspector for capturing network traffic, you need to install Operations Monitor and Probe on separate machines and then enable **Packet Inspector extension** on both machines. Packet Inspector is not supported on the machine where Operations Monitor and Probe are collocated.

---

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.

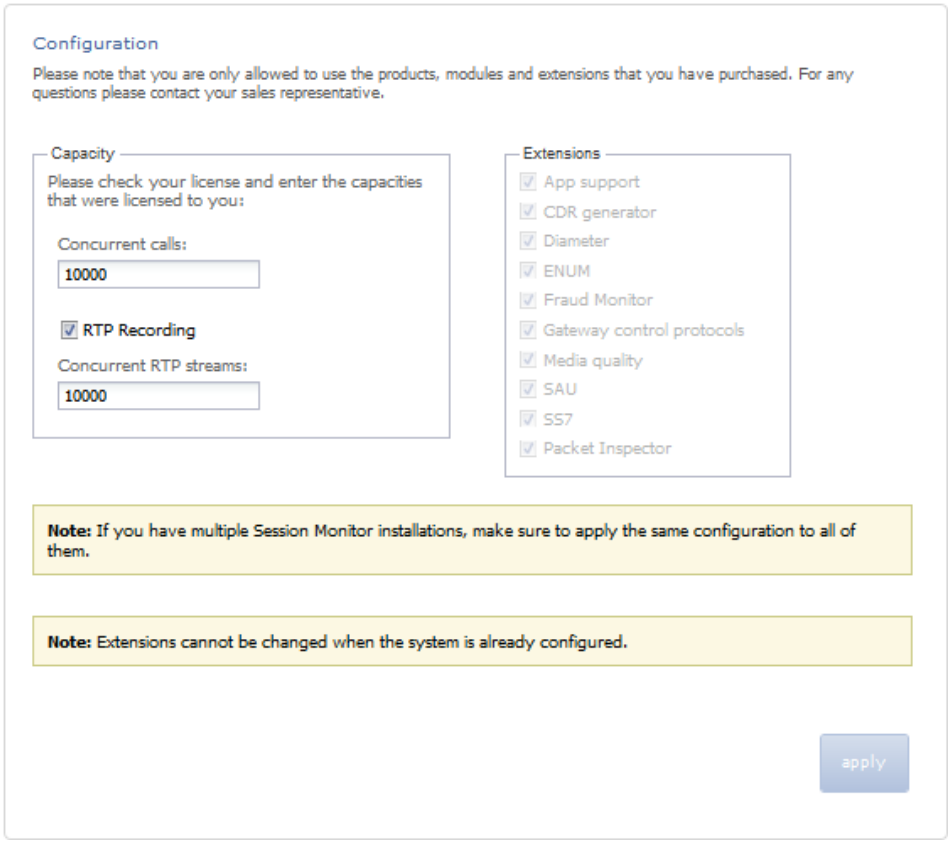
## Configuring Session Monitor

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 3–6 shows the Configuration page.

***Figure 3–6 Configuration Page***



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.

Click the **continue** button to navigate to the Network Settings page.

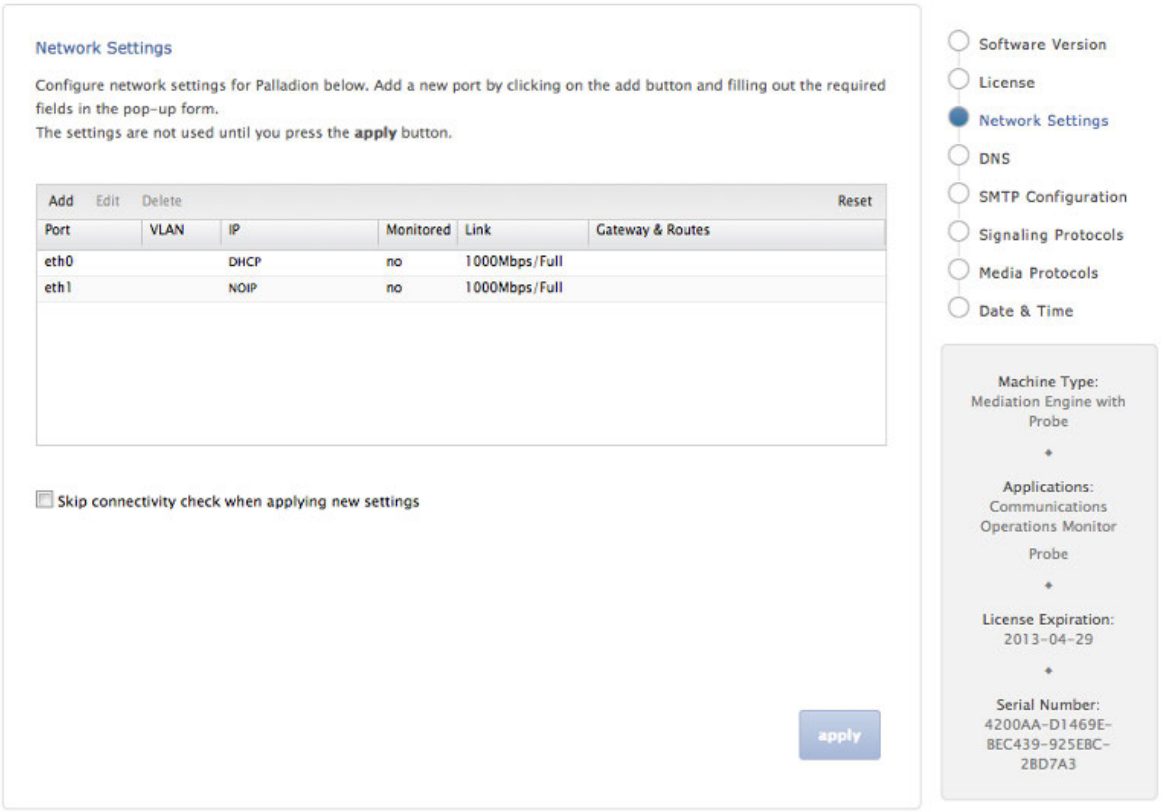
## Configuring the Network Settings

The Network Settings page contains a list of configured network interfaces, with a toolbar for adding, deleting, and editing 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 network settings that won't allow you to reconnect to the Platform Setup Application again.

Figure 3–7 shows the Network Settings page.

***Figure 3–7 Network Settings Page***

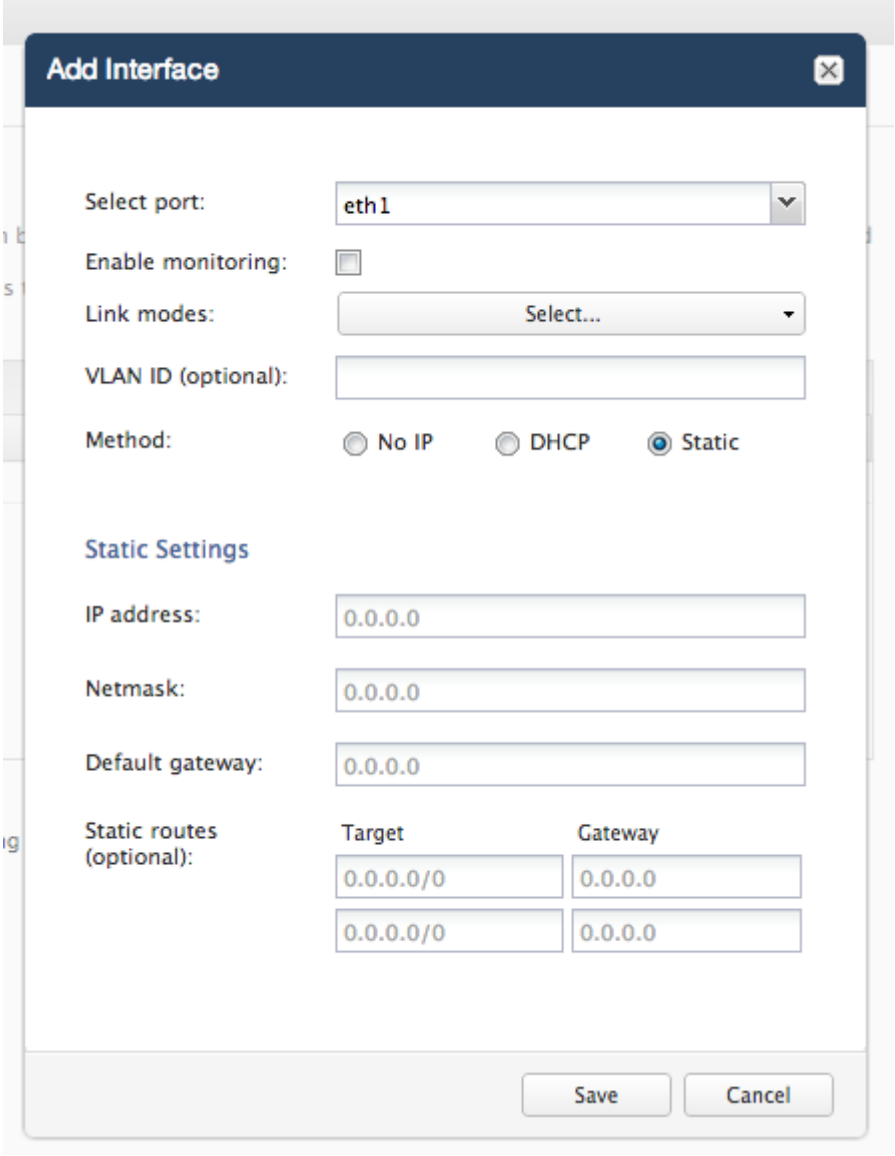


## Editing a Network Interface

To edit the settings of a network interface, select the entry in the list and click **Edit** in the toolbar (or double-click the entry).

Figure 3–8 shows the dialog box to edit the network interface.

***Figure 3–8 Edit Network Interface***




To change the IP method, select the radio button. If you select **Static** IP configuration, you will get additional options.

The following fields are compulsory for static IP configuration:

- IP Address
- Netmask
- Default Gateway

Static routes are optional; the left column contains the target IP/netmask in CIDR format and the right one the target IP.

> **Note:** You can save yourself filling out the netmask by typing in CIDR format in the IP address field, for example 192.168.0.1/24, and the netmask field will get 255.255.255.0 filled in automatically.

Link modes can be changed by clicking **Link modes** and the text **Select...**. This will open a pane with check boxes. There's usually no reason to touch this setting.

Monitoring can be enabled by checking the corresponding check box. This option is only available if your machine is a probe.

To save the network interface setting, click **Save**. The settings are not used until you click **Apply/Continue**.

To use and keep any changes you made in the Edit Interface dialog box, you have to click **Apply/Continue** in the lower-right corner. The settings are applied and the browser will try to connect to the machine. If the browser fails to connect to the machine within a given amount of time, the settings are reverted. This is to prevent locking yourself out. If you want to change the interface settings so that you won't be able to connect (for example, to deploy the server on another network), check the check box **Skip connectivity check when applying new settings** before clicking **Apply/Continue**.

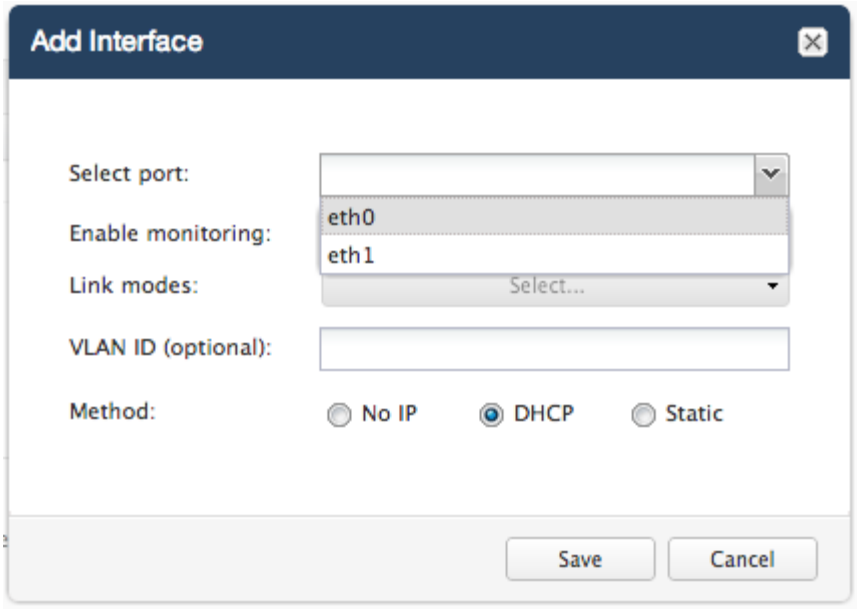
If you are configuring Session Monitor for the first time you are guided to "Configuring the SMTP Settings".

## Adding a Network Interface

To add a new network interface, its physical port has to be already configured on the machine. Press **Add** on the toolbar. Then select an interface from the drop-down menu. You can also create a VLAN interface by entering a VLAN ID in the VLAN port.

Figure 3–9 shows the dialog box to add an interface.

*Figure 3–9 Add Network Interface*




## Deleting a Network Interface

To delete a network interface, select the interface in the list and click **Delete** on the toolbar.

## Resetting the Network Interface Settings

To reset your network settings to the last state before you clicked **Apply/Continue**, click **Reset** in the toolbar.

**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).

# 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.

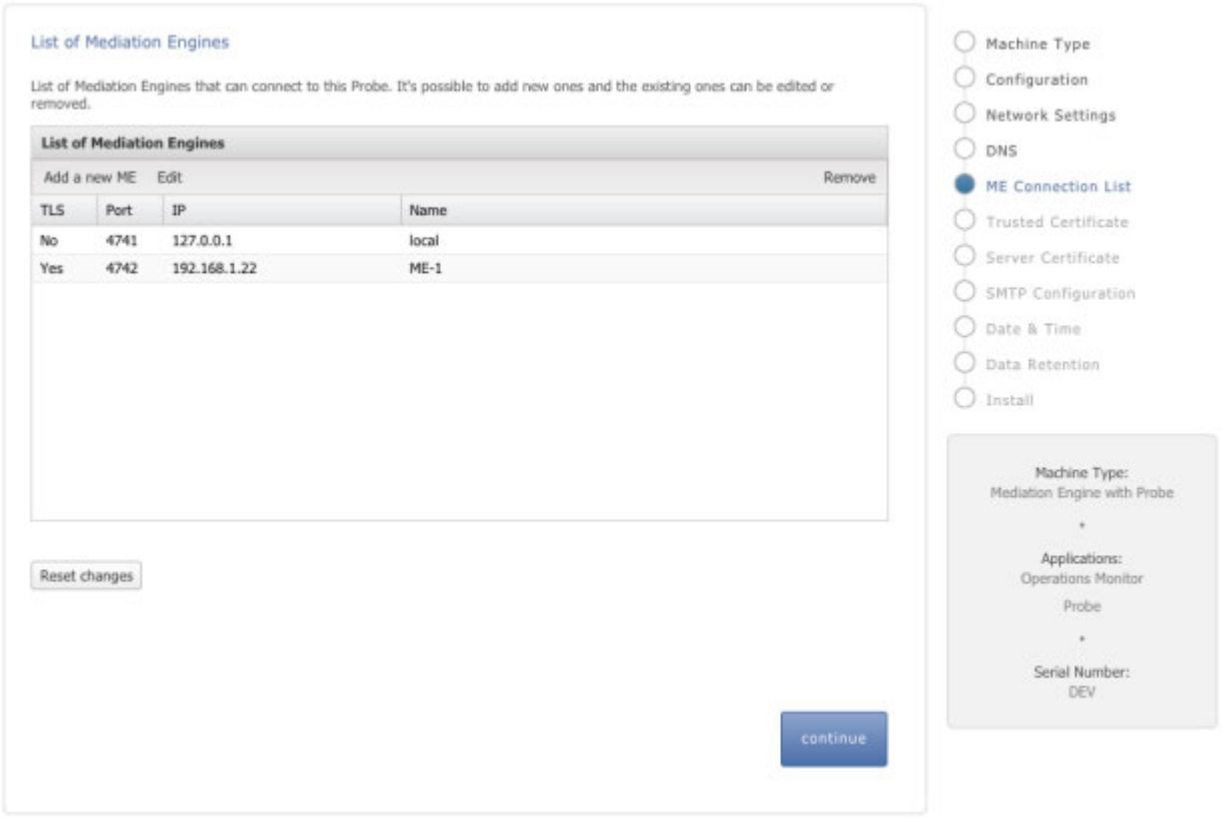
Figure 3–10 shows the ME Connection List page.

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. See "Secure Configuration" for more information.

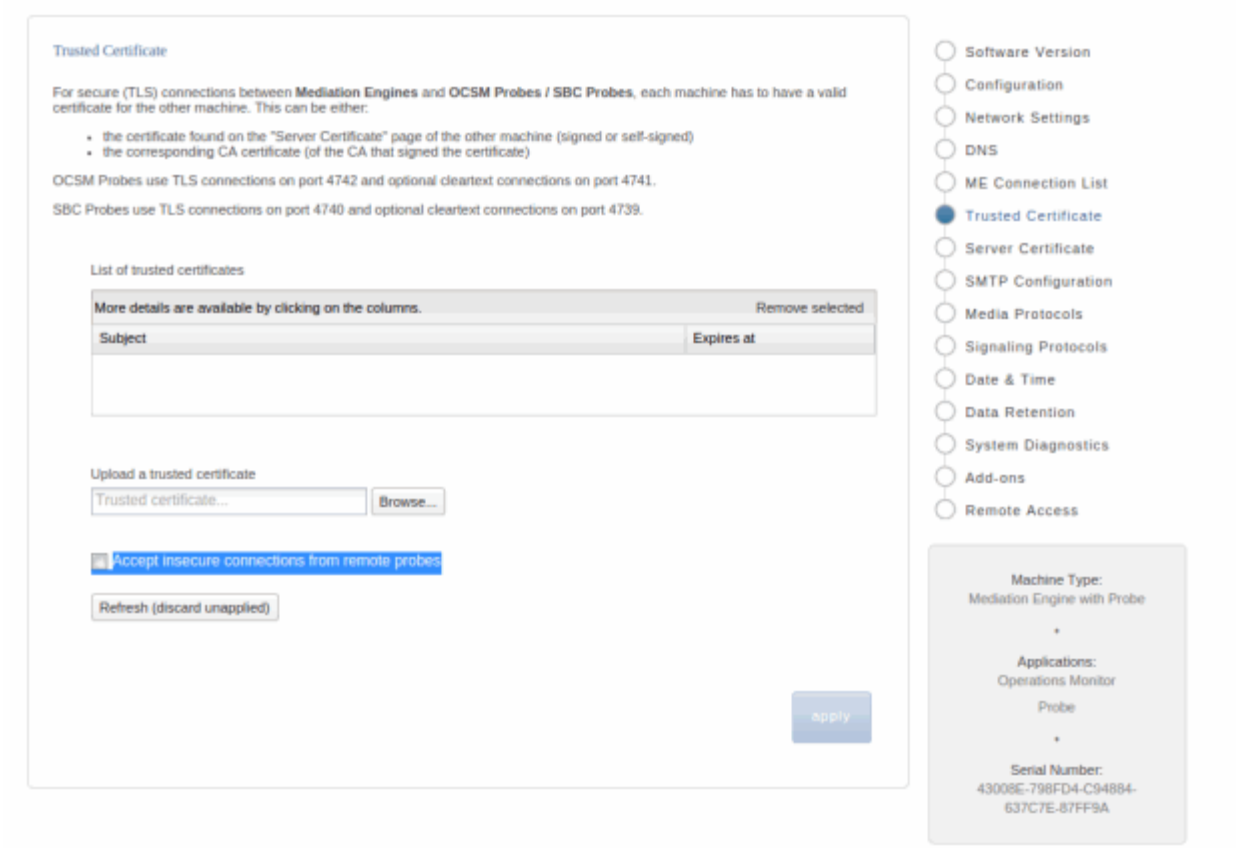
***Figure 3–10 ME Connection List Page***




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.

Figure 3–11 shows the Trusted Certificate page.

*Figure 3–11 Trusted Certificate Page*




## 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 **TLS** check box selected.

Table 3–1 describes the actions to configure the connections between one Mediation Engine and two Operations Monitor Probes.

*Table 3–1 One Mediation Engine and Two Operations Monitor Probes*

| Machine | Action |
|---|---|
| Mediation Engine | ■ Download the Server Certificate.<br>■ Upload the Server Certificate of the Operations Monitor Probe1 to Trusted Certificate.<br>■ Upload the Server Certificate of the Operations Monitor Probe2 to Trusted Certificate. |
| Operations Monitor Probe 1 | ■ Download the Server Certificate.<br>■ Upload the Server Certificate of the Mediation Engine to Trusted Certificate.<br>■ Add IP of the Mediation Engine to the ME Connection List, with TLS connection. |
| Operations Monitor Probe 2 | ■ Download Server Certificate.<br>■ Upload Server Certificate of the Mediation Engine to Trusted Certificate.<br>■ 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 **TLS** check box selected.

Table 3–2 describes the actions to configure the connections between two Mediation Engines and one Operations Monitor Probe.

*Table 3–2 Two Mediation Engine and One Operations Monitor Probe*

| Machine | Action |
|---|---|
| Mediation Engine 1 | ■ Download the Server Certificate.<br>■ Upload the Server Certificate of the Operations Monitor Probe to Trusted Certificate. |
| Mediation Engine 2 | ■ Download the Server Certificate.<br>■ Upload the Server Certificate of the Operations Monitor Probe to Trusted Certificate. |
| Operations Monitor Probe | ■ Download the Server Certificate.<br>■ Upload the Server Certificate of Mediation Engine 1 to Trusted Certificate.<br>■ Upload the Server Certificate of Mediation Engine 2 to Trusted Certificate.<br>■ Add IP of Mediation Engine 1 to ME Connection List, with TLS connection.<br>■ Add IP of Mediation Engine 2 to ME Connection List, with TLS connection. |

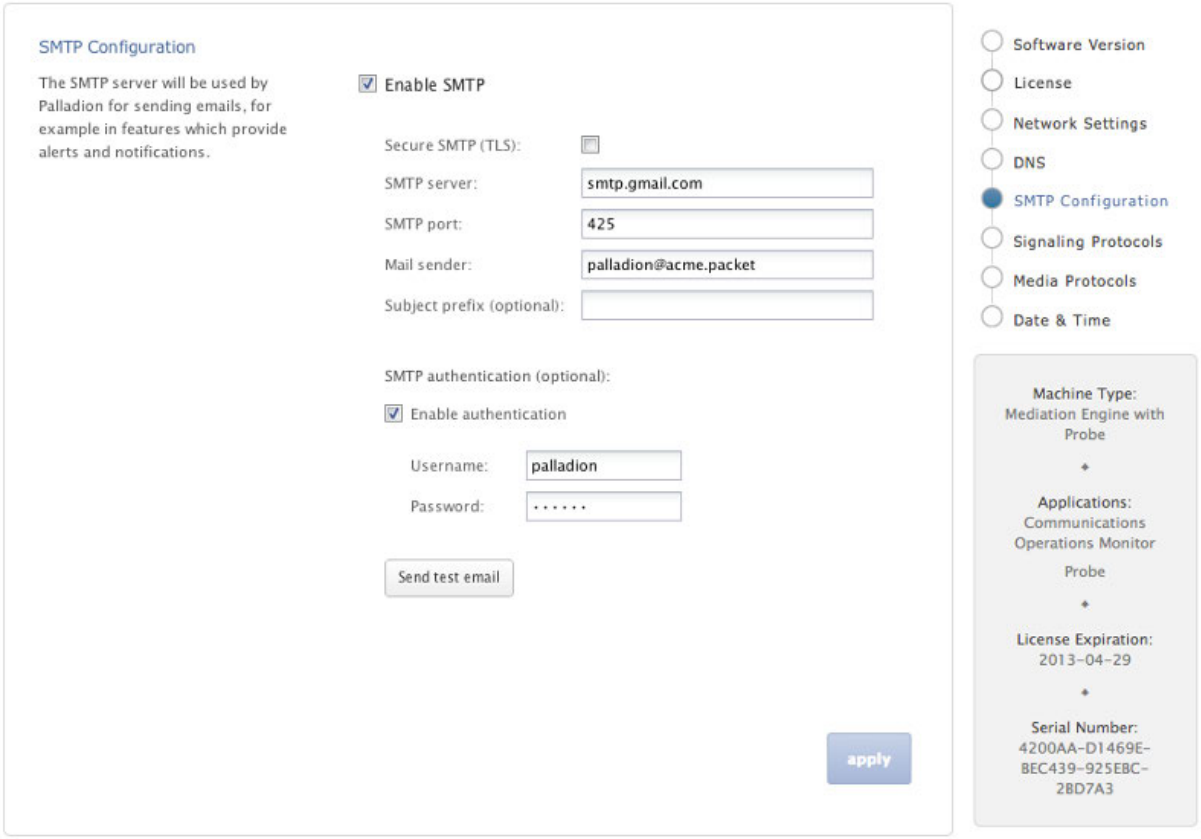
### All Other Scenarios

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 *Session Monitor Security Guide*.

## Configuring the SMTP Settings

Figure 3–12 shows the SMTP Configuration page.

***Figure 3–12 SMTP Configuration Page***




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 will need 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

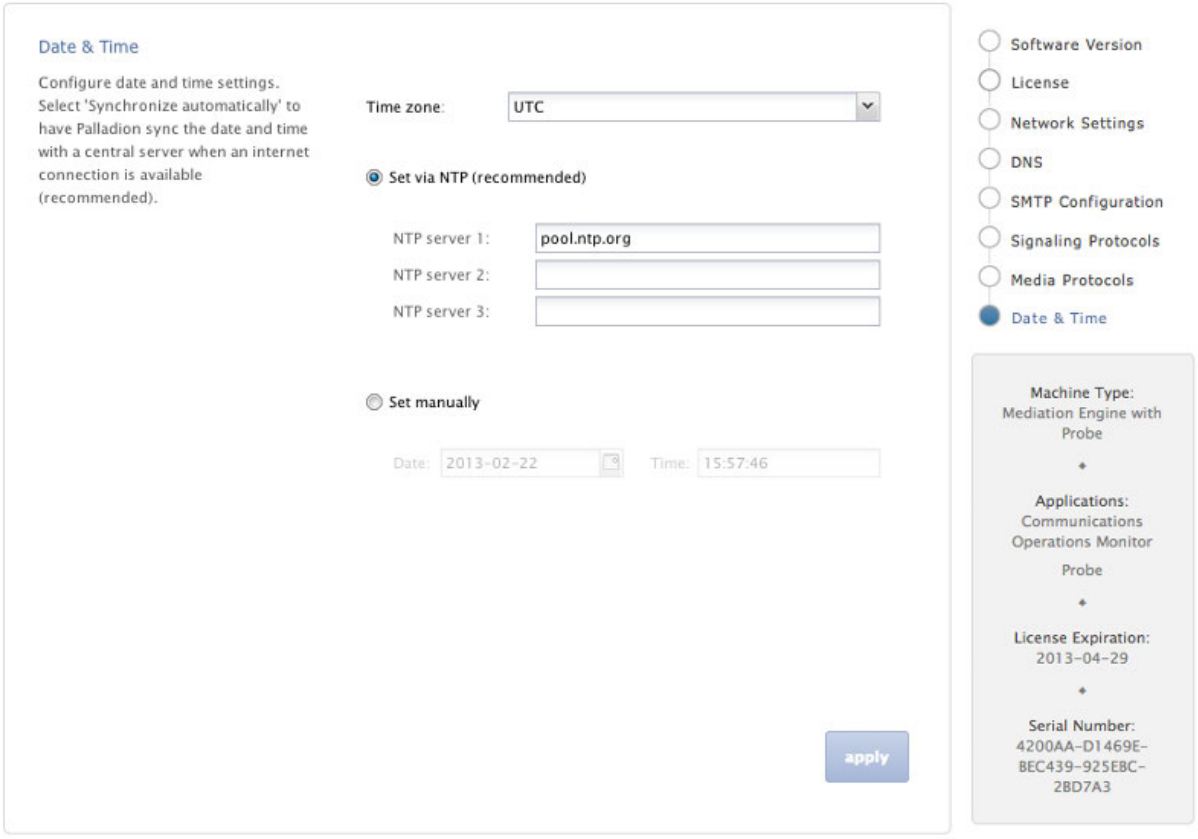
You can choose how the emails from Session Monitor will look like in the users' mailboxes.The field **Mail sender** is the email address Session Monitor will use; users will see this address in the **Sender:** or **From:** field of the emails. You can optionally specify a **Subject prefix**; this will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

If you are configuring Session Monitor for the first time you will be guided to "Setting the System Date and Time".

# Setting the System Date and Time

Figure 3–13 shows the Date and Time Settings page.

***Figure 3–13 Date and Time Settings Page***




In the Date and Time Settings page you can choose how the system will synchronize its time. Make sure that the correct method will be used, as it is important to have a correct and stable time:

- For correctness of the data recorded by Session Monitor
- To have automatic maintenance running during the night
- To have correct journals to diagnose potential problems

It is recommended to use automatic time synchronization by choosing the NTP method (default). This will set the time automatically and keep it synchronized with the global internet time.

**Note:** In setups with multiple Session Monitor machines, make sure to use the exact same time source for all machines. Some features might not work as expected if the machines clocks differ from each other.

### Setting the System Time Using the Internet Time

Session Monitor system needs a time server to synchronize with. Session Monitor is configured to use a public server pool by default (0.pool.ntp.org). This requires that the Session Monitor machine has access to the Internet. More specifically, make sure that the system is able to resolve network names with DNS (see Network Settings) and to communicate over the UDP port 123 through your internet gateway and firewall. You can specify up to three servers, in case one of them is unreachable or gives erroneous times.

### Setting the System Time Using your Local Network Time

If your organization runs an NTP server (ask your network administrator about this), use that instead of a public one. To do so, select **Set via NTP**, and enter the network name or the IP address of this relay.

### Setting the System Time Manually

If the system does not have access to any time server, you need to set the current time manually. It will then use the server's internal clock, but this will slowly drift away from the real time the rest of the world is on (for instance, 1 second more difference per day). Therefore, you should come back to the Date and Time Settings page and adjust it every week or so. To do so, get a reliable time yourself (such as a computer using network synchronization), select **Set manually**, and enter the correct date (YYYY-MM-DD) and time (HH:MM:SS).

Make sure to apply the settings by clicking **Apply/Continue** button, and wait for the synchronization to complete.

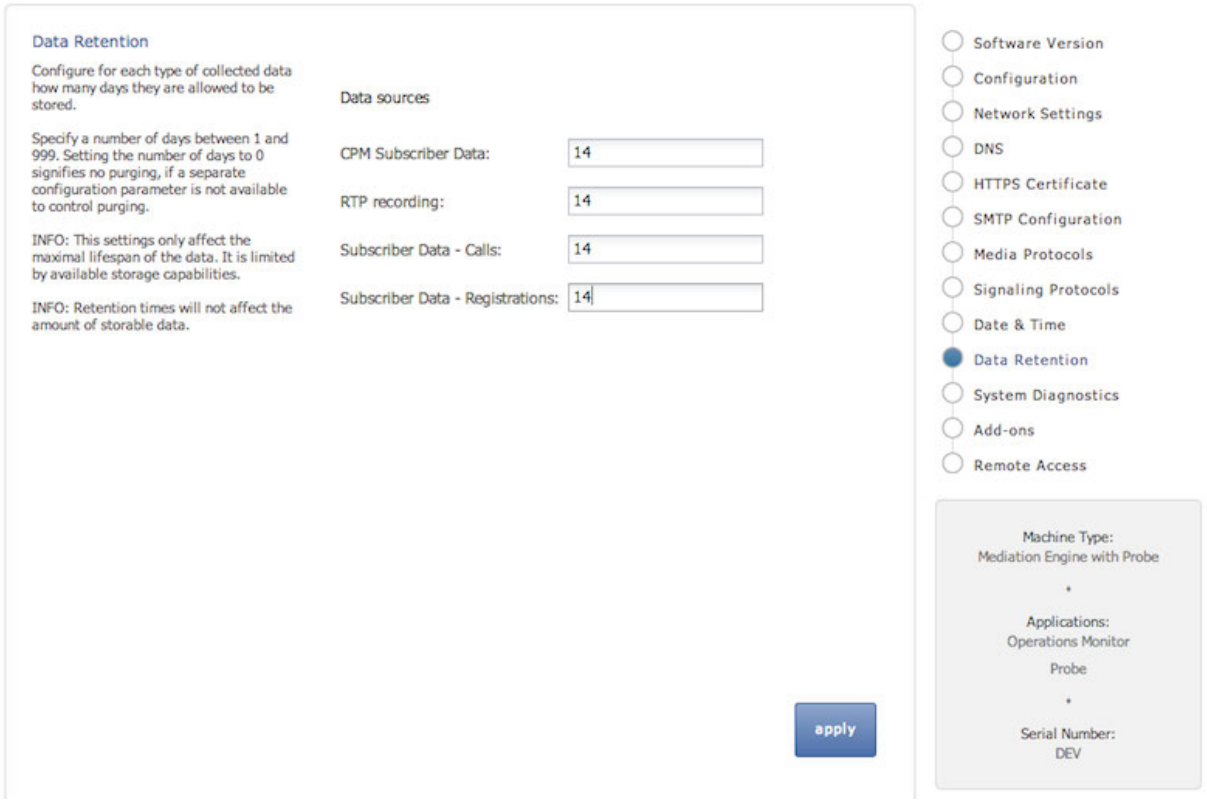
If you are configuring Session Monitor for the first time, you will be guided to "Installing the Products".

## Configuring Data Retention

The Data Retention page is used for configuring data retention in database for different data sources. Some settings depend on the license settings and will be available only if the associated configuration is set.

Figure 3–14 shows the Data Retention page.

***Figure 3–14 Data Retention Page***




Data retention is configured in days per data type. A value of **0** disables time based data retention.

> **Note:** The settings only affect the maximal lifespan of the data. Data availability is limited by available storage capabilities.

> **Note:** Retention times does not affect the amount of storable data.

You can configure data retention times for the following data types:

- **CPM Subscriber Data**: Delete Diameter S6 transaction data. Enabled by the CPM module.
- **RTP Recording**: Delete RTP Recordings. Enabled by RTP recording configuration.
- **Subscriber Data - Calls**: Delete call meta data and signaling.

> **Note:** Saved calls are not deleted by this option. Saved calls must be deleted by operators. (Optional) Disable user permissions for saved call functionality.

- **Subscriber Data - Registration**: Delete registration events.

**Note:** CDR/MDRs are not supported. Data retention affects data in the database only. For deleting CDR/MDRs, use FTP to delete files after downloading.

# 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*.

## Trusted Certificates

The Trusted Certificates page is used to configure the authentication of session border controllers (SBCs). This step is necessary before attempting to connect SBCs to Session Monitor.

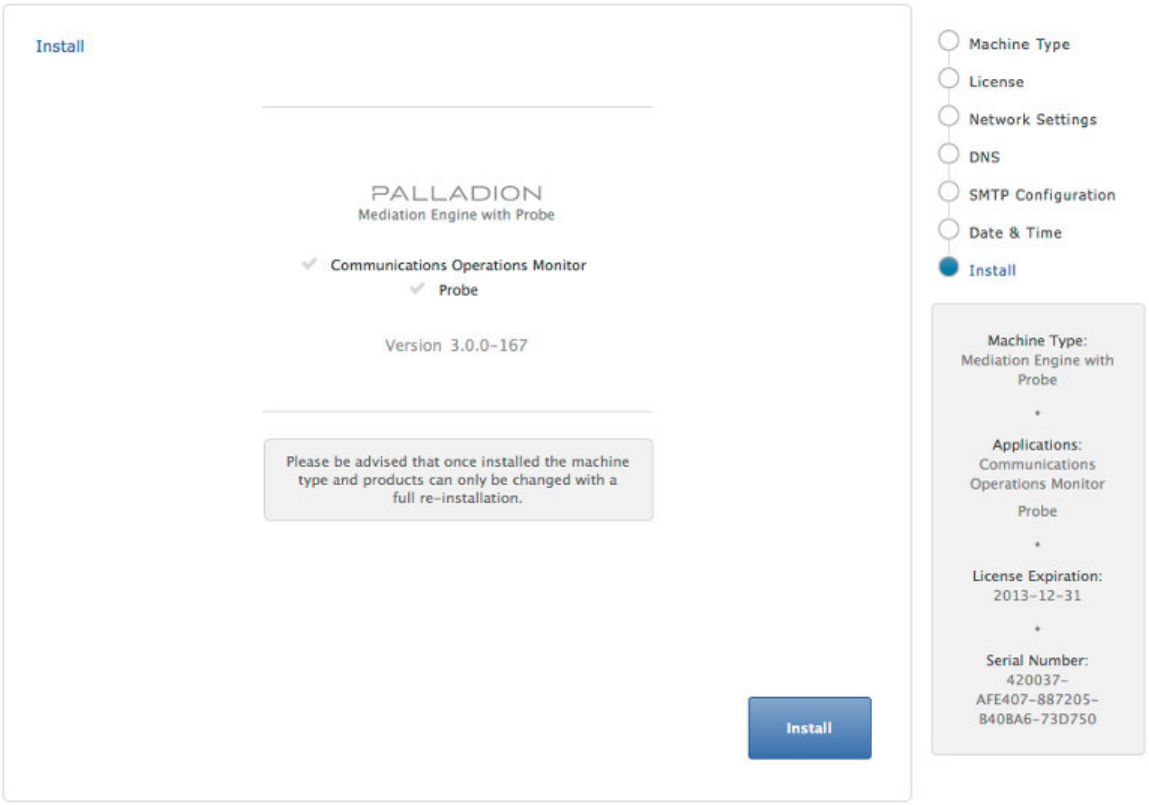
For more information, see the discussion about connection with Oracle Session Border Controller in *Session Monitor Security Guide*.

# 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.

Figure 3–15 shows the Install page.

***Figure 3–15 Install Page***




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.

# 4

# Session Monitor Post-Installation Tasks

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

## Access to Session Monitor by Oracle Support

To authorize Oracle Support access to your Session Monitor servers, you must provide direct shell access using Secure Shell (SSH). Shared desktop access is not direct shell access.

Oracle Support provides you the SSH credentials for authentication and authorization. You configure the credentials on the Remote Access page in Platform Setup Application (PSA). You can modify the credentials or disable shell access at anytime in PSA.

Oracle Support connects to your Session Monitor server using a VPN connection. Ensure that a VPN connection is created and tested, in the event that Oracle Support needs to use the VPN connection for an urgent issue.

## 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 .bin) 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.

**Note:** If you have a setup with multiple servers (for example, one ME and multiple Probe servers), upgrade all of them at the same time. Running different servers of the Session Monitor at 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:** 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 "Signaling Protocols" for more information about signaling protocols.

See "Filter Syntax" 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.

## Implementation

If the machine has a Napatech card installed, this card performs the filtering. Detection of this card is automatic; you do not need to configure it.

# 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 "Filter Syntax".

### 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 ME, 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 http://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).

# 5

# Installing Operations Monitor Probe on Oracle Linux

This chapter provides instructions for installing and configuring the Oracle Communications Operations Monitor probe on Oracle Linux.

## Operations Monitor Probe for Oracle Linux System Requirements

The following sections describe the hardware and software requirements for installing the Operations Monitor probe on Oracle Linux.

### Hardware Requirements

#### Supported Servers

The following Oracle servers are supported:

- Oracle Server X5-2
- Oracle Server X5-2L

Additionally, the following are minimum requirements:

- 2 Intel processors, each with 8 cores
- Intel based network card

#### 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

### Software Requirements

#### Data Plane Development Kit

Table 5–1 lists the supported versions of Data Plane Development Kit (DPDK).

*Table 5–1 DPDK Software Requirements*

| DPDK Version | Operations Monitor Release |
|---|---|
| 2.0.0 | Supported from 3.3.90.2.0. |
| 1.7.0 | Supported from 3.3.70.0.0 to 3.3.90.1.0. |

### Operating System

The Operations Monitor probe can run on the Oracle Linux 7 operating system. Ensure that you are running Oracle Linux 7 and that the packages are up to date.

> **Note:** If you prefer to use the installation image to install the Operations Monitor probe, see "Installing Session Monitor" and "Configuring Session Monitor".

To update the packages, execute:

```
yum update
```

Reboot the system if the packages have been updated since the last reboot.

### Dependencies

Some of the needed libraries are not available in the Oracle Linux 7 repositories. However, the libraries are made available by the EPEL (Extra Packages for Enterprise Linux) Special Interest Group from the Fedora Project.

To add their repository to your system, execute:

```
curl -f -O http://www.mirrorservice.org/sites/dl.fedoraproject.org/\
pub/epel/7/x86_64/e/epel-release-7-5.noarch.rpm
rpm -ivh epel-release-7-5.noarch.rpm
```

In addition to this, it will be necessary to install the package **vrb**.

### Required Kernel Modules

Operations Monitor probe needs direct access to the Intel network interfaces. You need to unload the normal network driver for selected ports and associate them with a different driver that allows direct access. There are two options to accomplish this.

The Linux kernel as of version 3.6 provides a module named **vfio-pci** which fits the needs of DPDK. However, this solution has some limitations. The alternative solution is the **igb_uio** driver provided by Intel. It is more versatile than the native solution but requires extra steps to set up.

### Using the igb_uio Kernel Module

Verify that the **igb_uio** loadable kernel module is installed on your system. The following command either displays information about the installed module or informs about the absence of the module:

```
modinfo igb_uio
```

If the module is not installed on your system, follow these steps to install the module:

1. Download the Intel Data Plane Development Kit (DPDK) from http://dpdk.org.

   **curl -f -O http://dpdk.org/browse/dpdk/snapshot/dpdk-***version_number***.tar.gz**

Where *version_number* is the DPDK software version required for your installed release of Operations Monitor. For more information, see "Software Requirements".

2. Install the development tools on the machine.

   ```
   yum group install Development tools
   ```

3. Install the kernel development files.

   ```
   yum install kernel-uek-devel
   ```

4. Navigate to the download location of the DPDK and unpack the files.

   ```
   tar xzf dpdk-version_number.tar.gz
   ```

5. Change to the folder where the DPDK files are extracted.

   ```
   cd dpdk-version_number
   ```

6. Configure and build the module.

   ```
   make config T=x86_64-native-linuxapp-gcc && make
   ```

7. Install the **igb_uio** loadable kernel module:

   ```
   install build/kmod/igb_uio.ko /lib/modules/$(uname -r)/extra
   depmod -a
   ```

8. Load the kernel modules **uio** and **igb_uio** to be persistent (see "Persistent Loading of a Kernel Module".)

### Using the vfio-pci Kernel Module

Verify that you are running the Red Hat compatible kernel and that it is used as the default kernel when booting using the following command:

```
grub2-editenv list
```

The command should return:

```
saved_entry=Oracle Linux Server, with Linux 3.10...
```

If you are not running a Red Hat compatible kernel, do the following:

1. Obtain the list of kernels currently configured on your system using the following command:

   ```
   grep "^menuentry" /boot/grub2/grub.cfg | cut -d "'" -f2
   ```

2. Select the line that starts with:

   ```
   Oracle Linux Server, with Linux 3.10
   ```

3. Set the new default using the following command:

   ```
   grub2-set-default "line picked in previous step"
   ```

4. Add the kernel command line option (see "Adding a Kernel Command Line Option").

   ```
   intel_iommu=on
   ```

5. Set the kernel module to be loaded when the system boots (see "Persistent Loading of a Kernel Module").

```
vfio-pci
```

# Updating Software for DPDK Based Probes

This section describes the procedure for updating software for DPDK based probes.

Ensure that you are running Oracle Linux 7 and that the packages are up to date.

To update the packages, execute:

```
yum update
```

> **Note:** Before updating the probes, see the Oracle Communications Session Monitor Release Notes to verify if the update package requires new packages to be installed.

To update the probes:

1. Run the following command to check for dependencies:

   ```
   # rpm -ivh ocsmxxxxxxxxxxx
   ```

   If dependencies exist, you will see an error message. The message provides the following details:

   [*xxx-yyy*] **is needed by ocsmxxxxx**

   > **Note:** Download the .rpm file each time you update your system.

2. See the Oracle Communications Session Monitor Release Notes to verify if the update requires a newer DPDK version.
   - If you require a newer DPDK version, see the topic "Using the igb_uio Kernel Module". Complete the procedure before moving to step 4.
   - If you do not require a newer DPDK version, continue to step 4.
3. Stop the daemons to prevent the interruption of current data processing.

   To stop the daemons, enter the following command:

   ```
   systemctl stop pld-rat
   systemctl stop pld-rapid
   ```

4. Upgrade the DPDK based probes package, enter:

   **rpm -Uvh** *xxxx*.**rpm**

5. To restart the upgraded daemons, execute:

   ```
   systemctl start pld-rapid
   systemctl start pld-rat
   ```

# System Configuration

The following sections describe the system configurations.

## Setting Up Huge Pages

The Operations Monitor probe needs huge pages provided by the Linux kernel. Each port or each configured sniffer (see "Section sniffer/name") needs at least 1GB of huge pages. Furthermore, the Operations Monitor probe requires a huge page size of 1GB.

For example, to set up 8GB of huge pages each of 1GB size, add the following options to your kernel command line options (see "Adding a Kernel Command Line Option"):

```
default_hugepagesz=1G hugepagesz=1G hugepages=8
```

To configure a different amount of memory:

1. Replace the **8** with the desired number of huge pages.

   ```
   default_hugepagesz=1G hugepagesz=1G hugepages=8
   ```

2. Create the following directory:

   ```
   mkdir -p /mnt/huge
   ```

3. Edit **/etc/fstab** and add the following line:

   ```
   hugetlbfs  /mnt/huge  hugetlbfs  defaults,pagesize=1G  0  0
   ```

4. Reboot the system for the changes to apply.

## Making CPUs Exclusive

This step is optional but leads to a better performance of the Operations Monitor probe.

To hide the CPUs used by Operations Monitor probe from the Linux scheduler, add the following Kernel command line option (see "Adding a Kernel Command Line Option"):

**isolcpus=***a,b,c,d...*

where *a,b,c,d...* are selected CPU IDs provided by the **/usr/share/pld/rat/system_layout.py** utility.

> **Note:** Do not add CPU IDs 0 and 1.

## Network Connectivity

Ensure that the Operations Monitor Probe can establish a TCP connection on port 4741 or 4742 (depending on the configuration described later) of the Mediation Engine.

Additionally, the daemons **rat** and **rapid** use some ports on localhost for internal communication; therefore, it is necessary to ensure that no other services use these same ports. The port numbers used by these daemons can be obtained from their configuration files.

# Installing and Configuring Operations Monitor Probe

Download the Operations Monitor probe rpm package **ocsm-3.3.90.0.0.x86_64.rmp**. The package and its dependencies can be installed using the following command:

```
yum install ocsm-3.3.90.0.0.x86_64.rpm
```

## Adjusting Configurations in the RAT Configuration File for Your System

The default RAT configuration file is in the directory **/etc/iptego/rat.conf**.

You may need to adjust some of the configurations to fit your system configuration. The configuration file is divided into several sections, each containing options and possible references to other sections of the file, so be careful and make sure you write a valid configuration. A section is denoted by brackets and contains one or several assignment statements.

After adjusting the configurations you can enable the daemon using the following commands:

```
systemctl enable pld-rat
systemctl start pld-rat
```

### Section dpdk

The dpdk section is denoted by:

```
[dpdk]
```

Table 5–2 lists and describes the entries in the dpdk section.

***Table 5–2 Entries in the dpdk Section***

| Entry | Description |
|---|---|
| **mem_channels =** *N* | Sets the number, *N*, of memory channels per processor socket. |
| **mem_layout =** *X, Y* | Sets the memory allocated using huge pages per memory channel, measured in megabytes. This must be a colon separated list with one entry per specified memory channel. An entry must be a multiple of 1024 including 0. |
| **rat_cpu_id =** *I* | Sets the CPU ID, *I*, to which the main thread will be pinned. CPU IDs start at 0. Use the **/usr/share/pld/rat/system_layout.py** utility to get an overview of the available CPUs.<br>The selected CPU ID should not be 0 or 1. |
| **driver =** *kernel_module_name* | Sets the kernel module to use. This can be either **vfio-pci** or **igb_uio**. See "Required Kernel Modules" for further information. |

Ensure that the specified amount of huge pages is available on your system. The Linux kernel distributes huge pages equally across memory channels. For example, the following configuration would be valid if you set up 8 huge pages of size 1024MB on a system with 2 memory channels:

```
[dpdk]
mem_channels = 2
mem_layout = 2048,2048
rat_cpu_id = 3
driver = vfio-pci
```

However, the following would be invalid, since the 8 huge pages are distributed between two channels:

```
mem_channels = 2048,6144
```

### Section sniffer/name

The sniffer section specifies a sniffer and a name for this sniffer. You can later use this name to refer to this sniffer.

The section is denoted by:

```
[sniffer/name]
```

For example, if port1 is the sniffer name, the section would be denoted by:

```
[sniffer/port1]
```

Table 5–3 lists and describes the entries in a sniffer section.

***Table 5–3 Entries in the sniffer Section***

| Entry | Description |
|---|---|
| **type = dpdk** | Specifies to use the Intel DPDK to access the networking cards. This entry must be set to **dpdk**. |
| **port_masks =** X+Y | Specifies the ports that are used by the sniffer. It can either be a single PCI ID or multiple PCI IDs combined by using a + sign. A valid PIC ID consists of 5 (lower case) hexadecimal digits with the following layout:<br>`AA:BB.C`<br><br>Use the **/usr/share/pld/rat/system_layout.py** utility for an overview of the available cards and their PCI IDs. For example, to listen only on the port with the PCI ID 88:00.0, set the entry as follows:<br>`port_masks = 88:00.0`<br><br>To listen on ports 88:00.0, 88:00.1 and a0:00.2 using only one sniffer, set the entry as follows:<br>`port_masks = 88:00.0+88:00.1+a0:00.2`<br><br>**Note**: Do not put white spaces between a port and the + sign and always use lower case characters for hex numbers. |
| **disable_rtp = 0** | Specifies whether media traffic should be analyzed. Setting this to **1** disables media traffic analyzing. |
| **all_traffic_signaling = 0** | Setting this to **1** passes all traffic to the signaling analyzer, regardless if it is categorized as media traffic.<br>**Note**: Enabling this entry may result in a notable decrease of performance. |
| **rtp_filter =** *pcap filter expression* | Specifies a filtering rule to categorize packets as media traffic. Only packets for which the filter applies will be passed to the media analyzer, except when **all_traffic_signaling** is enabled. |
| **buf_size =** *M* | Sets the buffer size for the sniffer, measured in packets. Ensure that the combined amount of buffers do not conflict with the configured memory layout. The amount of huge pages memory a sniffer requires depends on this buffer size. The amount of memory a single sniffer requires with a buffer size of *M* is about *2304 x M / 2^20* (internal paddings and alignments on memory allocation that depend on the machine configuration may increase this amount). |
| **buf_size_mb** = *X* | Sets the buffer size for the sniffer, expressed in megabytes. The program will estimate the buffer size in packets. Usually *X* is the memory layout for this NUMA node divided by the number of ports*streams. This parameter overwrites **buf_size**. |
| **workers =** *N* | Sets the number of media traffic worker threads to create for this sniffer. |

*Table 5–3 (Cont.) Entries in the sniffer Section*

| Entry | Description |
|---|---|
| **worker_cpus** = *X Y Z* | Specifies the CPU IDs *X,Y,Z* to use for the media traffic threads. Assign a list of the length according to the configured number of workers and streams. |
| **filter_cpus =** *X Y* | Sets the CPU IDs, *X, Y...* for the signaling analyzer thread. Assign a list of the length according to the configured number of streams. |
| **filter_timer_ms** = *MS* | Specifies the internal buffer in MS for signaling traffic. More memory is required for larger values. Values between 1 and 20 usually perform well. |
| **sniffer_cpus =** *X Y* | Sets the CPU IDs, *X, Y...* for the main threads of this sniffer. Assign a list of the length according to the configured number of streams.<br>**Note:** Ensure that you select CPU IDs that belong to the same NUMA node that the configured port belongs to. Assign each CPU ID only once for best performance. Hyperthread cores can be used, but keep in mind that you are using hyperthreading and not real cores in that case. You must not configure ports on different NUMA nodes in a single sniffer. |
| **n_streams** = *N* | Specifies the number of sniffing streams running in parallel. Sniffer, filter, and workers cpus are needed for each stream. **buf_size** or **buf_size_mb** must be considered as well. |

### Section signaling/name

There are multiple signaling sections, one for each supported protocol plus some additional. Following is a list of the valid signaling sections:

```
[signaling/sip]
[signaling/rudp]
[signaling/diameter]
[signaling/megaco]
[signaling/mgcp]
[signaling/enum]
[signaling/pinted]
```

Table 5–4 lists the entries in a signaling section.

*Table 5–4 Entries in the signaling Sections*

| Entry | Description |
|---|---|
| **filter =** *pcap_filter_expression* | Specifies a filtering rule that a packet has to fulfill to be categorized into the protocol type of this signaling section. |
| **deduplication_timelimit =** *X* | Specifies the maximal delta in which a duplication packet can be recognized.<br>**Note**: Setting this to a value larger than **0** may decrease the performance. |

### Section base

In the base section, you specify which sniffers you want to activate and which signaling types you want to analyze.

```
[base]
sniffer = <name1> <name2> ...
signaling = sip ...
```

For example, if you configured a sniffer section for a sniffer named **port1** and you want to activate the sniffer, then the list of sniffer would contain port1 as follows:

```
[base]
sniffer = ... port1 ...
```

Valid elements of the signaling list are:

```
sip rudp diameter megaco mgcp enum pinted
```

They are valid only if the according signaling/*name* section has been configured correctly.

## RAPID Configuration Files

The communication between this probe and the Mediation Engines is handled by the service **pldrapid**. After the service is configured, you must enable it using:

```
systemctl enable pld-rapid
systemctl start pld-rapid
```

### Basic Configuration

Rapid's configuration file is **/etc/iptego/rapid.conf**. It may not be necessary to edit this file; however, you need to configure the list of Mediation Engines in the file **/etc/iptego/psa/probe_me.conf**, which is included in **/etc/iptego/rapid.conf** file.

The following example shows the configuration for a list of Mediation Engines:

```
[MEList]
names = me1

[MEList/me1]
ip = aaa.bbb.ccc.ddd
name = ME
tls = no
port = 4741
```

where *aaa.bbb.ccc.ddd* is the IP address of the Mediation Engine. The value of the **name** field is arbitrary.

In the above example configuration, the Probe connects using an unencrypted connection to the Mediation Engine. Unencrypted connections must be enabled on the Mediation Engine. For an encrypted connection, the **tls** field must be set to **yes** and the port must be set to **4742**. For encrypted connections, additional configuration is necessary (see "Configuring Encrypted Communication").

If connections to more Mediation Engines are desired then further sections, say MEList/me2 and MEList/me3, have to be added for those, and they have to be referenced in the **names** field of the MEList section as in the following example:

To configure connections to additional Mediation Engines (for example, me2 and me3), add the Mediation Engines to the **names** field in the MEList section and add the corresponding MEList/me2 and MEList/me3 sections.

```
[MEList]
names = me1 me2 me3
```

For proper operation, a valid **/etc/iptego/psa/probe_uuid.conf** file is also necessary. This file is created during packet installation. Otherwise, the **write_rapid_uuid.sh** script can be used to perform this task.

## Configuring Encrypted Communication

If encrypted (TLS) communication with one or several Mediation Engines is enabled, then you must set up appropriate certificates.

For encrypted connections, it is required that the Probe authenticate the Mediation Engine and vice versa. Therefore, both the Probe and the Mediation Engine needs a signed (possibly self-signed) certificate and corresponding secret key, as well as the certificate of the Certification Authority (CA) that signed the peer's certificate. A machine which uses a certificate signed by a CA needs the CA's certificate to build its own certificate chain.

All of the needed certificates are stored in an Oracle Wallet. The wallet must reside in a disk file whose standard location (configured in **rapid.conf**) is **/etc/iptego/wallet**. Several tools are available from Oracle that allow the creation and manipulation of wallets. Since a wallet is a directory that contains only the file **ewallet.p12** in PKCS #12 format, it is also possible to create and maintain the wallet using third-party tools.

If a password is necessary to open the wallet, then that password must be stored in a separate file whose standard location (configured in **rapid.conf**) is **/etc/iptego/apid.key**. This is a text file containing only the password.

## Changing SELinux Context for Network Traffic Capture

SELinux is enabled by default for Oracle's Unbreakable Linux Kernel (UEK). When capturing network traffic with PCAP, processing issues can arise if Security Enhanced Linux (SELinux) is enabled. If you are using SELinux, before capturing packets from Oracle Communications Mediation Engine Connector, change the SELinux context file type for **tcpdump** in the Oracle Enterprise Linux (OEL) probe.

To change the security context for Network traffic capture, enter the following command:

```
chcon -t bin_t /usr/sbin/tcpdump
```

## Setting Storage Values for Packet Inspector

Storage values must be set before starting Packet Inspector.

To set storage values for Packet Inspector:

1. Create a new directory called **pinted**, in which to save your stored packets.

   ```
   mkdir -p /home/pinted
   ```

   Where *home* is the path to the directory where Packet Inspector saves data packets.

2. Open the **/etc/iptego/pinted.conf** Packet Inspector configuration file.
3. Search for the following section:

   ```
   [storage]
   ```

4. Enter the storage values you require for the following entries:
   a. **limit_mb**, enter the amount of space you require for saved packets.

---

**Note:** If you use Packet Inspector for capturing and storing media, ensure that there is sufficient disk space on the Probe machine to store the media.

---

b. **storage_path**, enter the path and directory name, which is used by Packet Inspector to save your stored data packets. The default path is */home***/pinted**.

5. Save the file.

### Enabling and Starting Packet Inspector

By default, Packet Inspector is disabled. You can enable this feature by running the following command:

```
system enable pld-pinted
```

Once enabled you can start Packet Inspector with the following command:

```
System start pld-pinted
```

**Note:** Running Packet Inspector can degrade system performance.

## Common System Settings

The following sections describe common system settings.

### Adding a Kernel Command Line Option

To add a kernel command line option, follow these steps:

1. Open the **/etc/default/grub** file in an editor (for example, vi).
2. Locate the line that begins with:

   ```
   GRUB_CMDLINE_LINUX
   ```

   If the line does not exist, add it to the file.
3. Append the command line option to the end of the line inside double quotes. For example:

   ```
   GRUB_CMDLINE_LINUX="... ... option_a"
   ```

   where *option_a* is the command line option you want to add.
4. Save the file and close your editor.
5. Generate the new grub configuration file using one of the following commands:
   - For BIOS based systems:

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

   - For UEFI-based systems:

     ```
     grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
     ```

The new kernel command line option will be used the next time you restart the system.

### Persistent Loading of a Kernel Module

To load a loadable kernel module on boot, follow these steps:

1. Create a start up script with the following name.

   **/etc/sysconfig/modules/***module_name***.modules**

where *module_name* is the name of your module.

2. Add the following to the script's content.

```
#!/bin/sh
/sbin/modprobe module_name
```

3. Make the script executable with the **chmod** command.

```
chmod +x /etc/sysconfig/modules/module_name.modules
```

# Troubleshooting

This section contains optional procedures. You can perform these procedures to gather additional data about the Operations Monitor Probe on Oracle Linux. You can refer this data to troubleshoot performance issues.

## Periodic Logging

You can enable periodic logging of the Operations Monitor Probe on Oracle Linux. You can use these logs to review historical system resources and the use of resources to run processes.

Periodic logging involves:

- Verifying atop is Installed on Oracle Linux
- Installing atop
- Enabling Periodic Logging

### Verifying atop is Installed on Oracle Linux

To verify if atop is installed, from the command line, enter the verification query:

```
rpm -q atop
```

If atop is not installed, see "Installing atop".

If atop is installed, see "Enabling Periodic Logging".

### Installing atop

To install atop:

1. Enter the following command:

```
yum install atop
```

2. Verify that the installation has been successful. Enter the following command:

```
rpm -q atop
```

If the installation has been successful, you will see text verifying the installed version.

### Enabling Periodic Logging

You can enable periodic logging at any desired interval.

**Note:** When enabling logging, consider the disk space requirements for your long term needs.

To enable periodic logging:

1. In the **/etc/default** directory, create a new file called **atop**.
2. Add the following lines to the file:

```
INTERVAL=600
LOGPATH="/var/log/atop"
OUTFILE="$LOGPATH/daily.log"
```

3. Set the **INTERVAL=** value to the desired frequency (in seconds).
4. Restart the atop process. At the command line, enter:

```
systemctl restart atop.service
```

# A

# Preparing Session Monitor Installation Media

This appendix provides instructions for creating the Oracle Communications Session Monitor installation media.

## Preparing the Installation Media

Session Monitor may be installed using a DVD or USB flash drive. If you are going to use a USB flash drive, make sure that its size is at least 1GB. Oracle recommends using brand drives, as issues have been reported when using low-quality thumb drives.

Download the Session Monitor Installer ISO image from the repository indicated to you by Oracle or your service provider. If you want to use the DVD installation method, create a new DVD from the image. Otherwise follow the instructions below to create a bootable USB flash drive.

**Caution:** Following the instructions writes the image directly to the device, which can be very dangerous when done without care, if you give the wrong device name, for example, the one representing your internal hard drive instead of the one representing the USB flash drive, all data from the running system can be deleted.

### Preparing a USB Flash Drive Using UNetBootin

**Note:** Using UNetBootin is the recommended way to prepare a USB flash drive for the installation. For Linux and Mac OS X, if this approach fails, an alternative preparation method is described in "Preparing a USB Flash Drive (alternative, Linux/Mac OS X)".

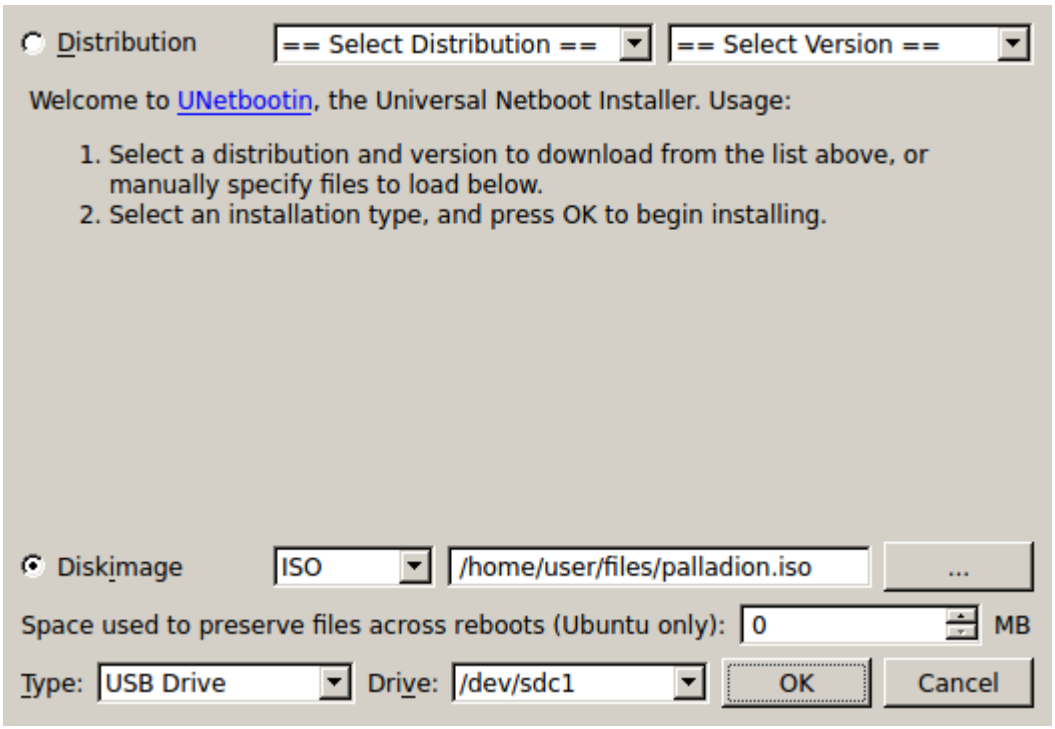
1. Download the UNetBootin tool matching your operating system from:

   `http://unetbootin.sourceforge.net/`

   This site also contains more information on using and troubleshooting the tool.
2. Plug the USB flash drive into the computer.
3. Start UNetBootin. Select **Diskimage** and **ISO** as the source. Click **...** next to the empty text entry and select the Session Monitor ISO image.
4. Select the type **USB Drive** and the USB flash drive you just plugged in.
5. Double check the selections you have made. If they are all correct, click **OK** to start the writing process. UNetBootin informs you about the progress.

Figure A–1 shows the UNetbootin dialog box.

***Figure A–1 Using UNetBootin to Prepare a USB Flash Drive for the Installation***




## Preparing a USB Flash Drive (alternative, Linux/Mac OS X)

**Important:** The method described below only applies to Linux and Mac OS X and should only be used if the preferred method using UNetBootin does not work.

1. Plug the USB flash drive into the computer.
2. Find out which device name has been given to the USB flash drive:

   **Linux** Execute **lsblk** on the command line. A tree of devices with their names, sizes and other information is shown. If **lsblk** is not available on your system, you can use **dmesg**.

   Example output:

```
scsi 8:0:0:0: Direct-Access USB Flash Disk PMAP PQ: 0 ANSI: 0 CCS
sd 8:0:0:0: Attached scsi generic sg2 type 0
sd 8:0:0:0: [sdb] 7827456 512-byte hardware sectors (4008 MB)
sd 8:0:0:0: [sdb] Write Protect is off
sd 8:0:0:0: [sdb] Mode Sense: 23 00 00 00
sd 8:0:0:0: [sdb] Assuming drive cache: write through
sdb: sdb1
```

   In this example, **sdb** is the device name to use. A tree of devices with their names, sizes and other information is shown.

   **Mac OS X** Execute **diskutil** list on the command line. A list of devices with their names, sizes and other information is shown.

3. Unmount the partitions of the USB flash drive in case any have been mounted automatically.

   On **Linux**, execute:

   **umount** *USB device name*

   For example:

   ```
   umount /dev/sdb1
   ```

   On **Mac OS X,** execute:

   **diskutil unmountdisk** *USB device name*

   For example:

   ```
   diskutil unmountdisk /dev/disk1
   ```

4. Write the image to the USB flash drive:

   **dd if=***/path/to/ocsm-3.3.90.0.0.iso* **of=***USB device name* **bs=1m**

   where */path/to/ocsm-3.3.90.0.0.iso* is the path to the image file.

   **Important:** All data from the USB flash drive will be deleted.

5. Synchronize the disk caches and wait until disk activity stops to assure that all data has been completely written to the USB flash drive:

   - On **Linux**, execute **sync** on the command line.
   - On **Mac OS X,** execute:

     **diskutil eject** *USB device name*

     For example:

     ```
     diskutil eject /dev/disk1
     ```

## Creating a Bootable USB on Windows

- If running Windows 7, use the Windows7 USB/DVD Download Tool.
  1. Download the Windows 7 USB/DVD Download Tool from:

     http://www.microsoft.com/en-us/download/windows-usb-dvd-download-tool
  2. In the Setup Wizard, click **Next**> **Install**.
  3. After installing, click **Finish** and open the program.
  4. Click **Browse** and locate the ISO file.
  5. Click **USB device**.
  6. Locate your USB device and click **Begin copying**.
  7. If prompted, click **Erase USB Device** and then **Yes**.
- If running Windows XP, use UNetbootin.
  1. Download UNetbootin from:

     http://unetbootin.sourceforge.net/

2. Open the downloaded file and click **Run**.
3. When the program opens, click **Diskimage** and set to **ISO**.
4. Click **. . .** and locate the ISO file.
5. Set the **Type** to **USB Drive**, and set the **Drive** to the drive where the USB is mounted.
6. Click **OK**.

# Glossary

### Napatech card

A specialized network card which does part of the packet filtering and processing in dedicated hardware, as opposed to doing filtering and processing on the CPU.

### Probe

A machine which filters and processes network traffic. It does not calculate the statistics.

### RTP

RTP (Real-time Transport Protocol) is the voice part of the network traffic, as opposed to the signaling (meta) part.

### VLAN

VLAN (Virtual Local Area Network) is a technique to separate a network into distinct, isolated broadcast domains. See https://en.wikipedia.org/wiki/Virtual_LAN.