Oracle® Communications Session Monitor

Security Guide

Release 5.2
F88050-01
January 2024

ORACLE

Oracle Communications Session Monitor Security Guide, Release 5.2

F88050-01

Contents

About this Guide

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

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

Documentation Set

> **Note:**
>
> Visit the Session Monitor Documentation page on docs.oracle.com for the latest version of user documentation.

Table 1 Documentation Suite for Session Monitor Release 5.2

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.
Fraud Monitor User Guide	Contains information for installing and configuring Fraud Monitor to monitor calls and detect fraud.
Installation Guide	Contains information for installing Session Monitor.
Mediation Engine Connector User Guide	Contains information for configuring and using the Mediation Engine Connector.
Operations Monitor User Guide	Contains information for monitoring and troubleshooting IMS, VoLTE, and NGN networks using the Operations Monitor.
Release Notes	Contains information about the Session Monitor Release 5.2 release, including new features.
Security Guide	Contains information for securely configuring Session Monitor.
Upgrade Guide	Contains information for upgrading Session Monitor.

Revision History

This section provides a revision history for this document.

Date	Description
January 2024	Initial release.

1

Session Monitor Security Overview

This chapter provides an overview of Oracle Communications Session Monitor security.

Basic Security Considerations

The following principles are fundamental to using any application securely:

- **Keep software up to date.** This includes the latest product release and any patches that apply to it.
- **Limit privileges as much as possible.** Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- **Monitor system activity.** Establish who should access which system components, and how often, and monitor those components.
- **Install software securely.** For example, use firewalls, secure protocols using TLS (SSL), and secure passwords. See " Performing a Secure Session Monitor Installation ".
- **Learn about and use the Session Monitor security features.** See " Implementing Session Monitor Security ".
- **Use secure development practices.** For example, take advantage of existing database security functionality instead of creating your own application security. See " Security Considerations for Developers ".
- **Keep up to date on security information.** Oracle regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible. See the "Critical Patch Updates and Security Alerts" Web site:

  `http://www.oracle.com/technetwork/topics/security/alerts-086861.html`

Understanding the Session Monitor Environment

When planning your Session Monitor implementation, consider the following:

- **Which resources need to be protected?**
  - You must protect customer data.
  - You must protect internal data, such as proprietary source code.
  - You must protect system components from being disabled by external attacks or intentional system overloads.
- **Who are you protecting data from?**

  For example, you need to protect your subscribers' data from other subscribers, but someone in your organization might need to access that data to manage it. You can analyze your workflows to determine who needs access to the data; for example, it is possible that a system administrator can manage your system components without needing to access the system data.

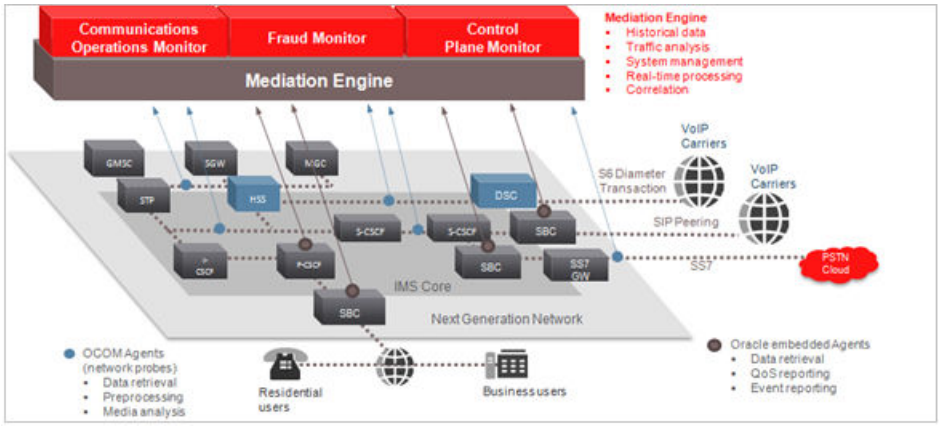
- **What will happen if protections on strategic resources fail?**

  In some cases, a fault in your security scheme is nothing more than an inconvenience. In other cases, a fault might cause great damage to you or your customers. Understanding the security ramifications of each resource will help you protect it properly.

Overview of Session Monitor Security

Figure 1-1 shows all the various components that comprise a Session Monitor system, including the components it connects to. Each installed or integrated component requires special steps and configurations to ensure system security.

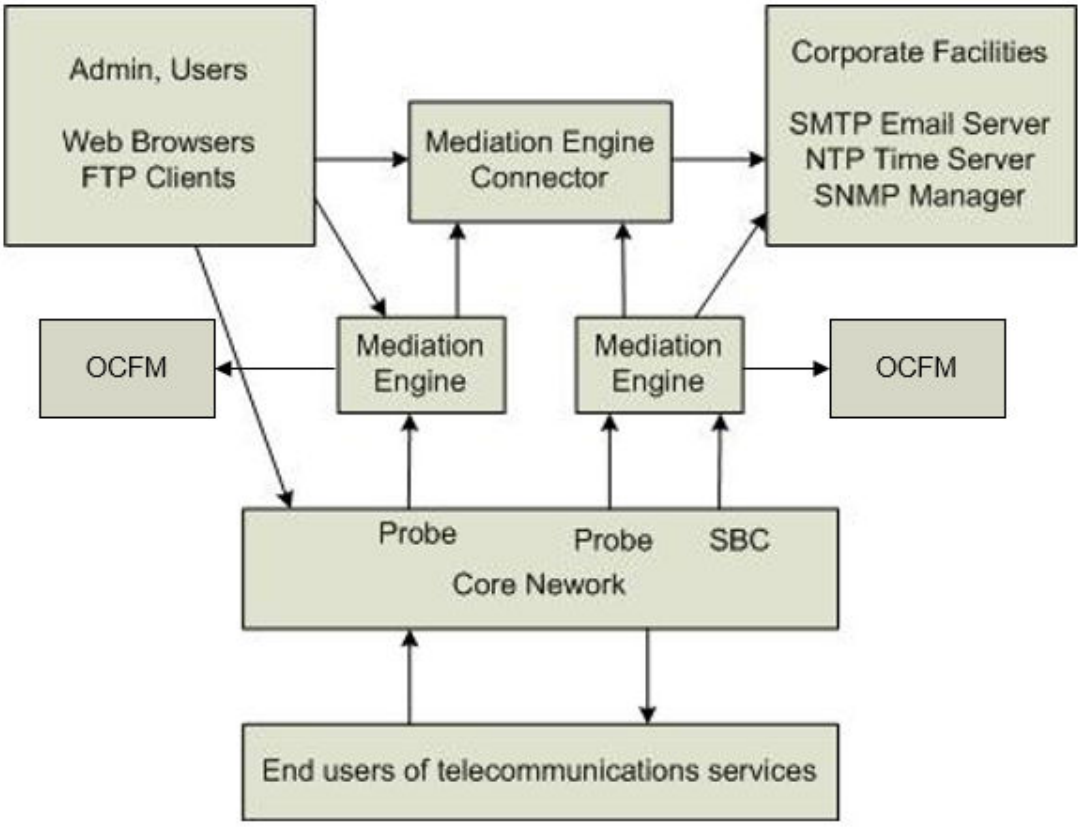
Figure 1-1 Session Monitor System Components



Recommended Deployment Configurations

Figure 1-2 shows a typical Session Monitor system deployment.

Figure 1-2 Typical Session Monitor System



Operating System Security

By default, shell access is disabled. 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 case.

Network Security

Session Monitor uses the following protocols to communicate with various components on specific ports:

UDP:

- Port 68: Used by the DHCP client.
- Port 123: Used by the NTP client.

- (Optional) Port 161: Used by the SNMP agent.
- (Optional) Port 162 outbound: Used for SNMP traps.
- (Optional) Port 5090: Used for Voice Quality from SIP phones on Mediation Engines.

TCP:

- TCP port range 1024-65536: Used for connection from the Mediation Engines to the probes.
- TCP port 443: Used for HTTPS connection from the Aggregation Engines to the Mediation Engines.
- TCP port range 1024-65536: Used for connection from the Aggregation Engines to the Mediation Engines.
- TCP port 4740: Used for IPFix over TLS.
- (Optional) TCP port 4739: Used for IPFix from Oracle Communications Session Border Controller on Mediation Engines.
- (Optional) TCP port 21: Used by the FTP and FTPS servers.

Probes:

Passively receives all telephony-related traffic.

Protocols that are marked optional are disabled by default. For information about how to enable these protocols, see *Operations Monitor User's Guide*.

Restrict access to Session Monitor machines by closing the unused ports. Session Monitor machines are typically connected to several networks; therefore, restrictions may vary for each machine.

Ensure that Session Monitor machines are not accessible from the Internet or have access to the Internet.

However, if the UCaaS CCaaS extension is enabled, then the Mediation Engine requires access to Internet.

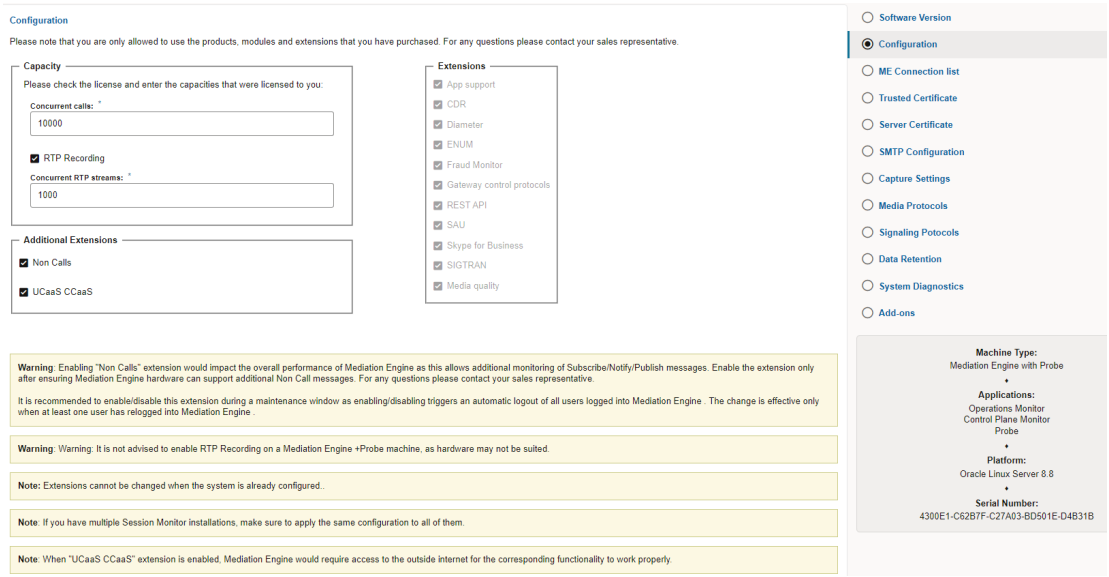
UCaaS CCaaS Connectivity

After the **UCaaS CCaaS** extension is enabled from the Platform Setup Applicationpage, the Mediation Engine requires access to the Internet, specifically to call Microsoft Graph REST APIs (https://graph.microsoft.com).

Ensure that the external Internet connectivity is enabled on Mediation Engine in such a case. The internet connectivity can either be directly enabled on Mediation Engine or it can be enabled using a proxy. For more information, see the Operations Monitor User Guide.

> **Note:**
>
> Operations Monitor creates only HTTPS connections to the call Microsoft Graph REST APIs.

Figure 1-3 Configuration



Connecting Oracle Communications Session Border Controllers to Mediation Engines

Connections from Oracle Communications Session Border Controllers to the Mediation Engine machines are encrypted. These encrypted (secure) connections use TLS on port 4740. The secure connections between the Mediation Engines and the session border controllers are established using SSL Certificates.

For a stand-alone system, you can register the certificates in Platform Setup Application on the Server Certificate page by downloading the Session Monitor certificate to the session border controller and uploading the session border controller certificate to the Session Monitor machine on the Trusted Certificate page.

If you manage certificates within a Public Key Infrastructure (PKI), you can download the Session Monitor certificates and have them signed by your Certificate Authority (CA). When you have the trusted CA certificate, upload the CA certificate to each Session Monitor machine.

Registering Certificates on the Session Border Controller

To register the certificates on the Oracle Communications Session Border Controller, go to the My Oracle Support Web site and follow the instructions in the Oracle Note at `https://support.oracle.com/epmos/faces/DocContentDisplay?id=1679579.1` to do the following:

- Configure the connection to Session Monitor
- Create a certificate for the session border controller.
- Register the certificate of Session Monitor, which can be downloaded from Platform Setup Application on the Server Certificate page. Alternatively, you can register the CA used to sign it.
- Enable TLS

Registering Certificates in Platform Setup Application

To register the certificates in Platform Setup Application, on the Trusted Certificate page in the **Upload a trusted certificate** section, upload the certificates of the session border controllers. The certificates will then appear under **List of trusted certificates** section.

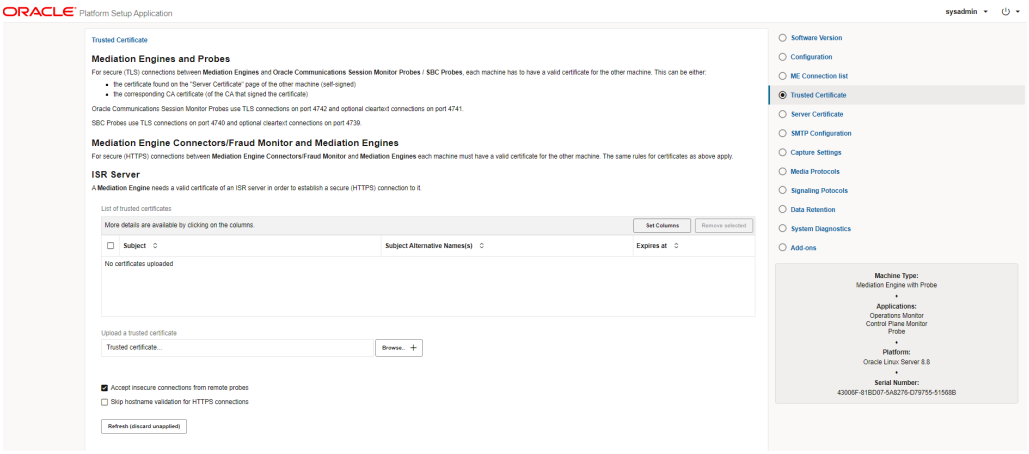
Alternatively, you can upload the CA that is used to sign session border controller's certificates. The certificate format is X.509 / PEM (X.509 extensions are not supported). Only the validity of the signatures are verified.

Unencrypted connections are not allowed by default, unless the system has been upgraded from an earlier release that did not support encrypted connections.

To use unencrypted connections (for example, in a testing environment), select **Accept unsecure connections from Session Border Controllers**; then disable the TLS option in the session border controller. The unencrypted connections use port 4739.

Using unencrypted connections are not recommended in production environments.

Figure 1-4 Trusted Certificate Page



Email Security

Session Monitor uses email to send notifications and alerts. To send emails, Session Monitor needs access to an SMTP server. You configure the SMTP server details in Platform Setup Application on the SMTP Configuration page. Session Monitor supports TLS connections to the SMTP server.

If the SMTP server requires authentication, you will need to create an email account for Session Monitor. Ensure that the email account has only those privileges necessary for sending notification emails.

2

Session Monitor Secure Configuration

This document covers the necessary configuration of the Oracle Communications Operations Monitor system and of its environment to ensure secure operations. To follow these recommendations, you need access to Platform Setup Application (PSA) and to all the installed products, their manual, and possibly the administration tools for your networks.

Administrative Password

PSA must be protected by a password of your choice on all Operations Monitor machines. All the session products come with an administrator account to access their respective interface. To restrict access to these products, connect to their interface, and change the administrator account password on each. For administrator user credentials, contact your Oracle Sales Representative.

User Accounts

Operations Monitor features fine-grained multi-user capabilities which allows the administrator to create restricted accounts for day-to-day usage. Referring to each product manual, create one account for each person who uses the product, and set their permissions to allow their necessary tasks. You need to set a temporary password and communicate it with the end users, who should then change it. It is possible to force a user to do so by expiring its password. It is recommended to enforce a strict passwords policy by enabling the features and regularly expire passwords.

Encryption and Certificates

Each Operations Monitor server uses a unique certificate to guarantee its authenticity and protect users data. The certificates are initially self-signed, and a warning will be shown to users on their first access. To improve security of the connection and suppress these warnings, it is recommended that you sign the server certificate using your organization's Public Key Infrastructure (PKI). Follow the steps on the Server Certificate screen, and consult with your network administrator to sign the certificates of each Operations Monitor server. Plain HTTP access is not allowed.

Connections with Oracle Session Border Controller

In Operations Monitor connections from Oracle Session Border Controllers to Operations Monitor machines are encrypted. These connections use TLS on port 4740. Unsecured connections are not allowed by default, unless the system has been upgraded from an earlier release that did not support it. Authentication is achieved by means of certificates. In a standalone scenario, you can register the SBC certificate in Platform Setup Application as a trusted certificate, and register Operations Monitor certificate in the Session Border Controller. If you prefer to manage certificates within a PKI, you can instead sign these certificates, and register the trusted Certificate Authority (CA) in each machine.

On the Session Border Controller

Follow instructions in the Oracle Support note to:

- Configure the connection to Operations Monitor
- Create a certificate for the Session Border Controller
- Register the certificate of Operations Monitor, which can be downloaded from Platform Setup Application on the panel Server Certificate. Alternatively, register the CA used to sign it.
- Enable TLS

In Platform Setup Application

In Platform Setup Application, go to the panel, **Trusted Certificates**. Use the form to upload the certificate(s) of the SBC(s), which then appear in the list of trusted certificates. Alternatively, upload the CA that is used to sign Session Border Controller certificates. The certificate format is X.509 / PEM. X.509 extensions are not supported, only the validity of signatures is verified.

Unsecure Option

If you do not wish to use encrypted connections, for instance for testing, you can allow unsecure connections from Session Border Controllers on the **Trusted Certificate** panel. You can then disable the TLS option in the Session Border Controller. These connections will use port 4739. However, this setup is not recommended in production.

Connection between Mediation Engine and Mediation Engine Connector

The Mediation Engine Connector machines can access the Mediation Engine machines using HTTPS. Make sure that the URLs specified in the Aggregation Engine to reach the Mediation Engine machines start with https://.

Email Notifications

Session Monitor products can send notification emails. For this, it require access to an SMTP server, configurable with PSA. If the server requires authentication, an account needs to be created for Oracle Communications Operations Monitor. This account should not grant any other privileges that the product does not require. Session Monitor also supports TLS connections to the SMTP server.

Connections with ISR

Connection with ISR is performed using HTTPS protocol. Operations Monitor interacts with the external system and the complete security feature depends on both parties configurations. Hence, it is recommended to use FACE server hostname only with HTTPS protocol scheme.

Connection with Fraud Monitor

Connections from Operations Monitor to the Fraud Monitorare encrypted. These encrypted (secure) connections use TLS on port 12000 on Fraud Monitor. The secure connections between the Operations Monitor and the Fraud Monitor are established using SSL Certificates.

The connection between Mediation Engine and Fraud Monitor is secured for which the certificates need to be exchanged. See Connection with Fraud Monitor related to Fraud Monitor Configuration to download certificate.

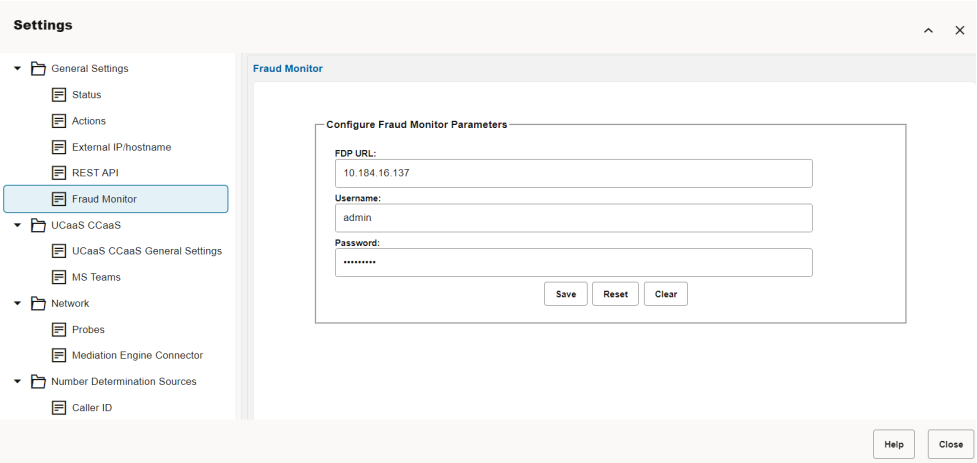
- Ensure that Fraud Monitor certificate has been downloaded from Fraud Monitor PSA Server Certificate page. The certificate can either be a self-signed certificate or CA certificate.
- In Mediation Engine PSA, navigate to **Trusted Certificates**, upload the certificate downloaded from Fraud Monitor PSA Server Certificate page.
- In Mediation Engine PSA, navigate to **Server Certificate**, download the Server Certificate.
- In Fraud Monitor PSA, navigate to **Trusted Certificate,** upload the certificate downloaded from Mediation Engine PSA Server Certificate page.

> **Note:**
>
> The supported format of the server certificate is PEM.

- After the successful certificate exchange configure the Fraud Monitor URL at **admin >Setting >General Settings >Fraud Monitor**.

> **Note:**
>
> The user name and Password must be same as the Fraud Monitor Username and Password used to log in to the Fraud Monitor.

Figure 2-1 Fraud Monitor configuration Page



- The Operations Monitor initiates secured (TLS) connection to Fraud Monitor, if Fraud Detection is enabled from the below path **admin >Settings >System Settings >Enable call Events publisher**

3
Fraud Monitor Secure Configuration

This chapter covers the necessary configuration of the Fraud Monitor system and of its environment to ensure secure operations. To follow these recommendations, you need access to Platform Setup Application (PSA) and to all the installed products, their manual, and possibly the administration tools for your networks.

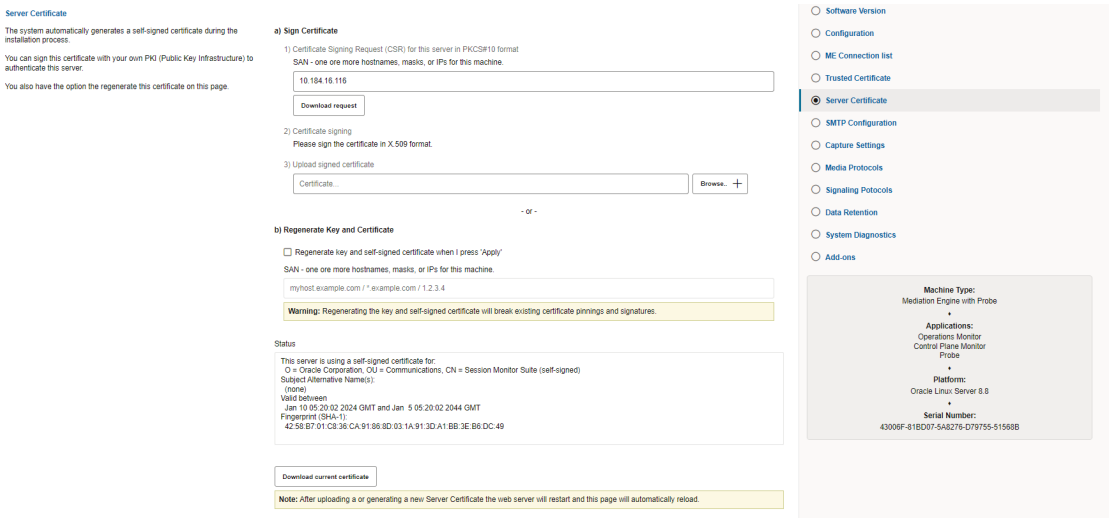
In Platform Setup Application

The Platform Setup Application guides you through the configuration steps to get the Fraud Monitor running. It includes configuring the machine type, Trusted Certificate, Server Certificate and SMTP settings.

In Mediation Engine Platform Setup Application, go to the panel, **Server Certificate** and click the **Download Current Certificate**.

Perform same steps on the Fraud Monitor Platform Setup Application Server Certificate page to download current certificate.

Figure 3-1 Server Certificate

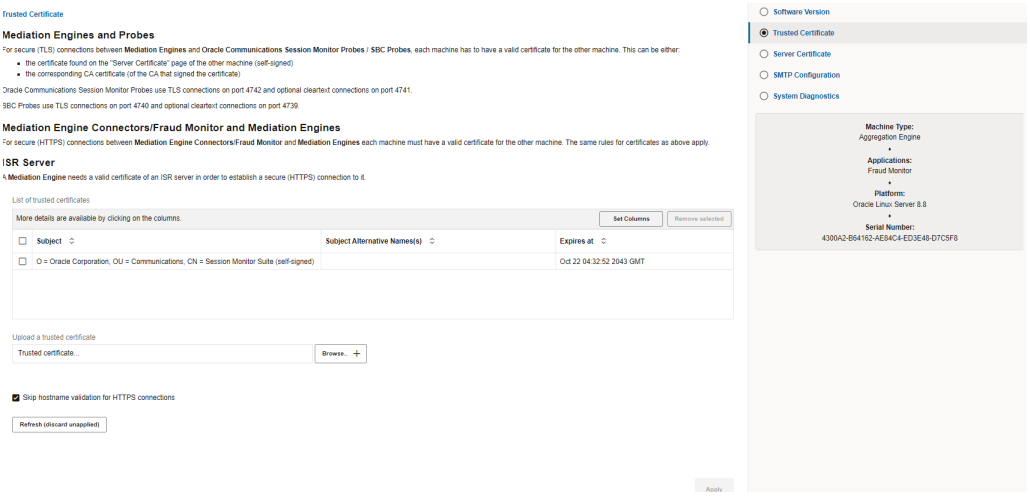


In Fraud Monitor Platform Setup Application, go to the panel, **Trusted Certificates**. Use the form to upload the certificate(s) of the Mediation Engine(s), which then appear in the list of trusted certificates. Alternatively, upload the CA that is used to sign Mediation Engine certificates. See the figure shown above.

Similarly in Mediation Engine Platform Setup Application, navigate to **Trusted Certificates** upload the certificate downloaded from Fraud Monitor Platform Setup Application Server Certificate page.

> **Note:**
>
> After the Mediation Engine-Fraud Monitor secure configuration, if the secure connection has any issues due to incorrect certificate exchange, invalid or missing certificate, it is recommended that you set the **Enable Call Events Publisher** setting to **False** under the Mediation Engine System Settings at the earliest.

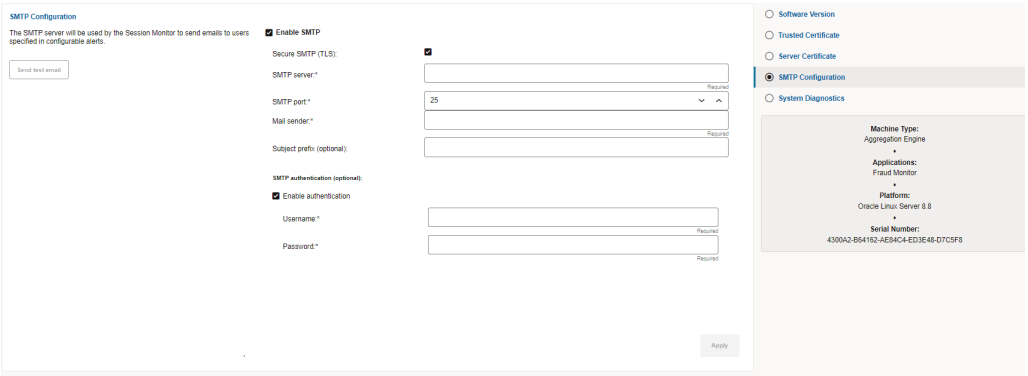
Figure 3-2 Mediation Engine and Probes



Email Notifications

Fraud Monitor products can send notification e-mails. For this, it require access to an SMTP server, configurable with Platform Setup Application. If the server requires authentication, an account needs to be created for Fraud Monitor. This account should not grant any other privileges that the product does not require. Fraud Monitor also supports TLS connections to the SMTP server.

Figure 3-3 SMTP Configuration



4

Performing a Secure Session Monitor Installation

This chapter presents planning information for your Oracle Communications Session Monitor installation.

For information about installing Session Monitor, see *Session Monitor Installation Guide*.

Pre-Installation Configuration

Perform the following pre-installation tasks:

- Ensure that the Session Monitor machine is reachable through the TCP port 443.
- If the E-mail SMTP server supports authentication, create an account dedicated to Session Monitor.
- Session Monitor acts as an SNMP device. Obtain the address and community string of the SNMP management system.

Installing Session Monitor Securely

Perform a custom installation to avoid installing options and products you do not need. If you perform a typical installation, remove or disable features that you do not need after the installation.

When installing Session Monitor, do the following:

- Change the password when prompted.
- On the Network Settings page, enable monitoring only on necessary interfaces.
- On the SMTP Page:
  - If your SMTP server supports TLS, make sure to enable TLS.
  - If your SMTP server supports authentication, make sure to enable authentication and to use an account dedicated to Session Monitor.
- On the Date & Time page, (if your organization runs an NTP server) make sure to provide the IP address of the local and redundant NTP servers.

Post-Installation Configuration

This section explains security configuration to complete after Session Monitor is installed.

Changing the Default Administrator Passwords

All Session Monitor products (Operations Monitor, Fraud Monitor, and Mediation Engine Connector) are installed with a default *admin* account. The admin account is used to access the product's Web interface. On first login, the administrator is prompted to choose a unique

password for the admin account. Fraud Monitor currently does not prompt to choose a password; the administrator should change the password manually.

You can also connect to each product's Web interface and change the admin account password at any time.

The Platform Setup Application is installed with a default *sysadmin* account. On each Session Monitor machine, log into the Platform Setup Application, and change the sysadmin account password.

Password Enhancements

Software release version 4.4 and later support complexity requirements for passwords. After upgrading to 4.4 or later, the system will accept old passwords but force users to reset their password to meet the complexity requirements.

Passwords must have the following characteristics:

- At least 8 characters
- At least one uppercase character
- At least one digit
- At least one special character

Encryption and Certificates

All Session Monitor interfaces can only be 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.

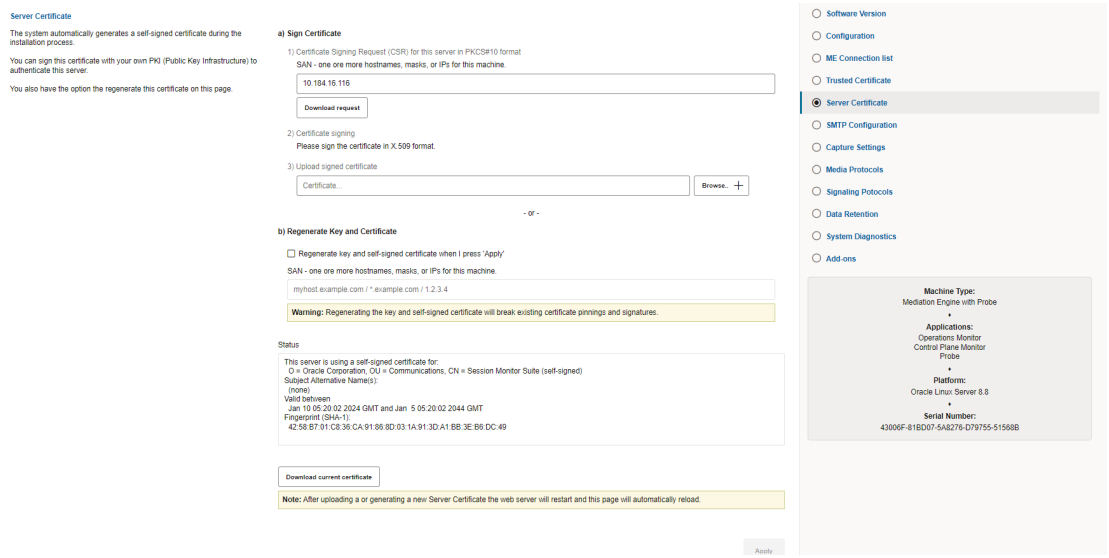
The certificates are automatically generated on the Session Monitor machines during the installation process. The certificates are initially self-signed, and when a user accesses the interface the first time, a **This Connection is Untrusted** warning message is shown. To improve security of the connections and to suppress the warning message, Oracle recommends that you sign the server certificate using your organization's Public Key Infrastructure (PKI).

Consult with your network administrator and follow the steps on the Server Certificate page in Platform Setup Application to sign the certificates of each Session Monitor machine.

Enable **Skip hostname validation for HTTPS connection** when using self-signed certificates that were generated during installation.

The figure shows the Server Certificate page in Platform Setup Application.

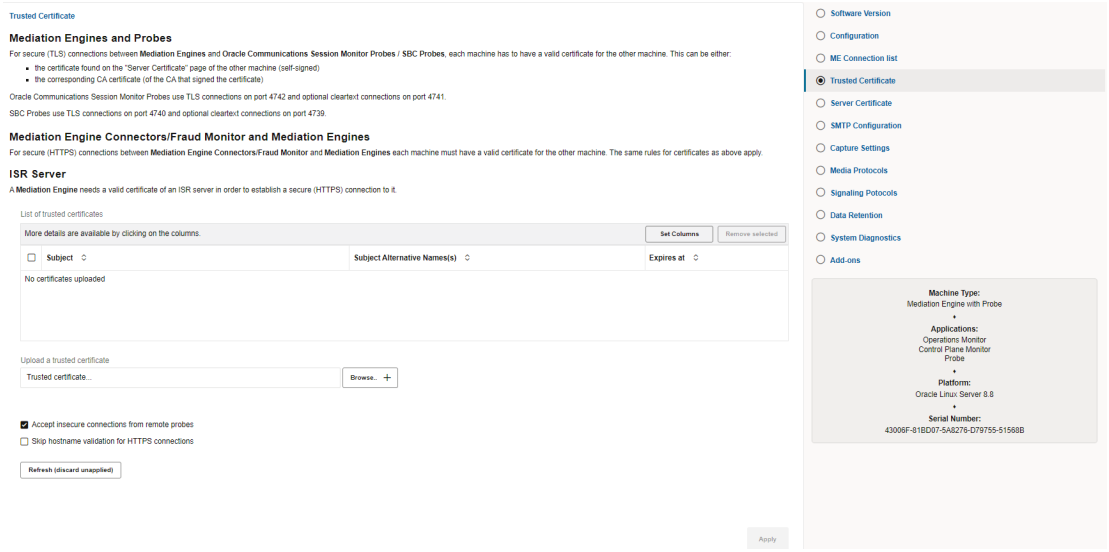
Figure 4-1 Server Certificate Page



The Status of the Server Certificate from Platform Setup Application, **Subject Alternative Name(s): (none)** indicates that SAN is not defined.

On the Trusted Certificate page, the list of trusted certificates also displays the SAN for each certificate.

Figure 4-2 Trusted Certificate Page



Connection Between Mediation Engine and Aggregation Engine

The Aggregation Engine machines can only access the Mediation Engine machines using HTTPS. Make sure that the URLs specified in the Aggregation Engine to access the Mediation Engine machines start with **https://**.

For a successful secure connection between Mediation Engine and Mediation Engine Connector 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) or the corresponding CA certificate (of the CA that signed the certificate).

For more information, see *Session Monitor Mediation Engine Connector User's Guide*.

Connection Between Mediation Engine and Interactive Session Recorder

Mediation Engine requires a valid Interactive Session Recorder certificate to establish secure and validated connection. The supported certificate format is PEM.

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

5

Implementing Session Monitor Security

This chapter explains the security features of Oracle Communications Session Monitor.

Setting Up User Accounts

Session Monitor allows administrators to create end-user accounts for users to perform their day-to-day tasks. Secure user access by doing the following:

- Create a temporary password for the user account and require that the user change the password. It is possible to set the temporary password to expire and force a user to change the password.
- Set the user permissions to allow only the tasks the user can perform.

Oracle recommends enforcing strict passwords policy by enabling the features *Require complex passwords* and *Regularly expire passwords*.

Refer to *Operations Monitor User's Guide* and *Session Monitor Mediation Engine Connector User's Guide* to enable these features.

Configuring and Using Authentication

Authentication is the process of verifying a user's identity and determining whether the user has access to a system using credentials such as user name and password.

Session Monitor supports RADIUS authentication. When you enable RADIUS authentication, Session Monitor performs RADIUS authentication against a RADIUS server each time a user logs in.

When you configure RADIUS authentication, you must specify a shared secret that is shared by Session Monitor and the RADIUS server. The shared secret is used to validate that the RADIUS messages are sent between a RADIUS client and server that share the same secret.

See *Operations Monitor User's Guide* for more information about RADIUS authentication.

SSL Implementation

For all the following connections:

- Mediation Engine-Mediation Engine Connector
- Mediation Engine-Fraud Monitor
- Mediation Engine-Interactive Session Recorder
- Mediation Engine-Probe

Ensure that a proper SSL certificate validation is done.

There is also an option on **Trusted Certificates** page, if hostname should be validated.

> **Note:**
>
> On the **Trusted Certificate** page, enable the **Skip hostname validation for HTTPS connection** check-box when uploading the certificates that does not contain valid hostnames.

6

Security Considerations for Developers

This chapter provides information for developers about how to create secure applications for Oracle Communications Session Monitor and how to extend Session Monitor without compromising security.

> **Caution:**
>
> When creating your own applications, or using third-party applications, test your scripts in a test environment to ensure they are safe before uploading them to your production environment. Applications approved by Oracle are safe to use in your environments. However, non-approved applications could cause security and performance issues. Oracle is not responsible for any loss, costs, or damages incurred from using your own applications, or third-party applications.

Securing REST APIs

Using Session Monitor REST API, you can access most Operations Monitor features through HTTPS REST calls.

Session Monitor supports calling REST APIs using CA certificates.

Follow these guidelines to secure your API key:

- Store the API key on an external system which has restricted access.
- Perform only secured backups of the external system where the API key is stored.
- Do not pass the API key on the command line.
- Change the API key regularly.

For more information on how to enable and generate an API Key, and the use of certificates to call REST APIs, see the *Operations Monitor User's Guide* .

A

Secure Deployment Checklist

The following security checklist lists guidelines to help you secure Oracle Communications Session Monitor and its components.

Secure Deployment Checklist

- Install only the components you require.
- Enable only the extensions and features you require.
- Ensure that all default passwords have been changed.
- Enforce user passwords to expire upon creation.
- Enforce strong password management.
- Ensure that users store their password securely, or not at all.
- Ensure that users close all sessions and log out from the web browser after they are finished with their work.
- Grant only the necessary privileges to each user.
- Restrict network access by doing the following:
  - Use firewalls.
  - Ensure that the system is not reachable from the Internet.
  - Ensure that the system cannot reach the Internet nor resolve public DNS names.
  - Use network traffic encryption.
  - Never leave an unnecessary open ports in a firewall.
  - Harden the system by installing it in a secure location where it would be difficult for a hacker to access.

  > **Note:**
  >
  > If you have enabled the UCaaS CCaaS extension, access to the Internet is required.

- Apply all security patches and workarounds.
- Contact Oracle Security Products if you discover vulnerability in any Oracle product.