Oracle® Communications Session Monitor

Security Guide

Release 3.3.92

E74348-01

June 2016

ORACLE®

Oracle Communications Session Monitor Security Guide, Release 3.3.92

E74348-01

Contents

A Secure Deployment Checklist

Preface

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

Audience

This guide is intended for systems administrators, network administrators, and network operations team who installs and administers Session Monitor.

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
E74348-01	June 2016	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.

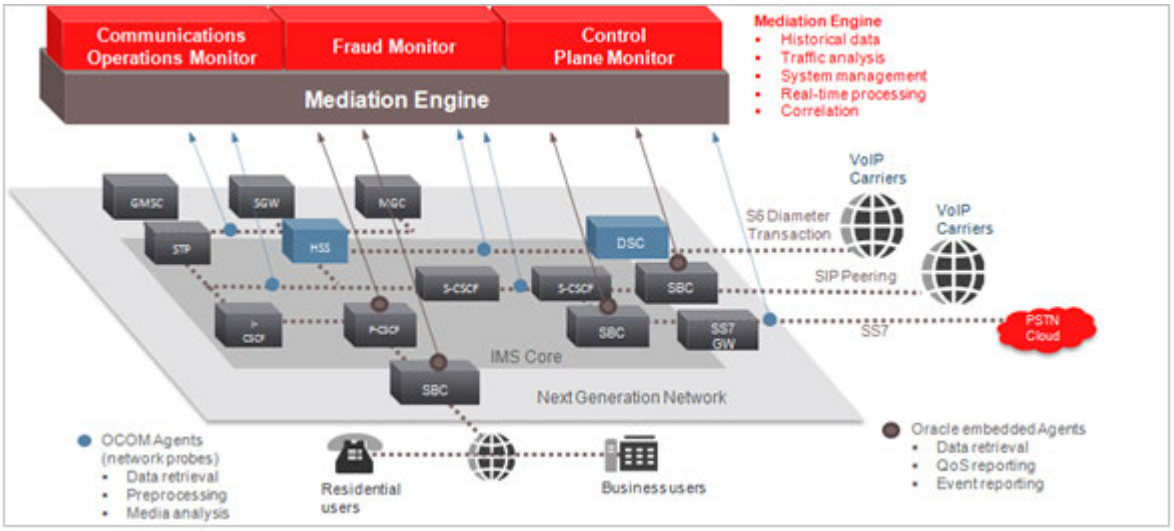
- **What will happen if protections on strategic resources fail?**

  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.

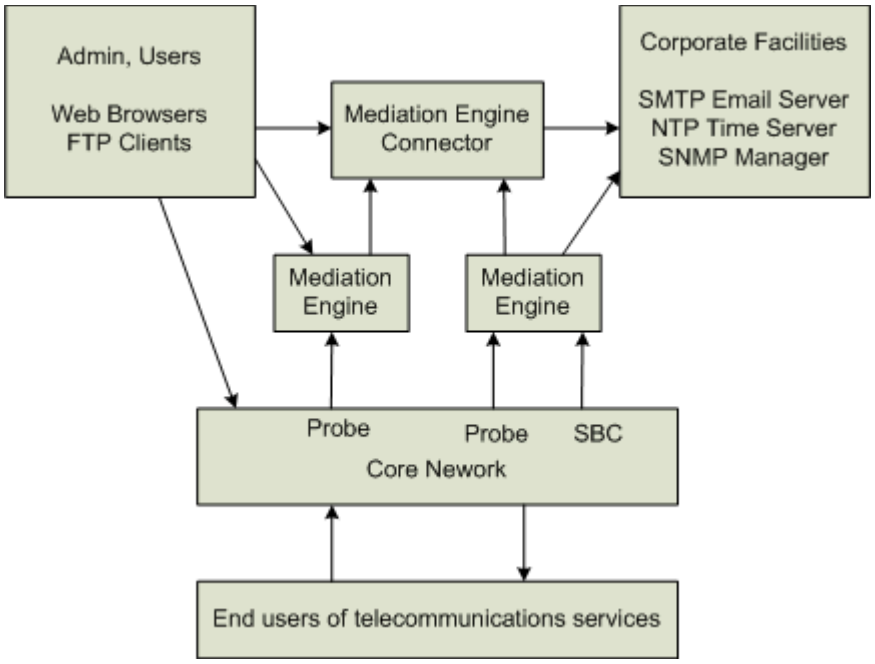
Figure 1–1 Session Monitor System Components



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.

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 (see Figure 1–3).

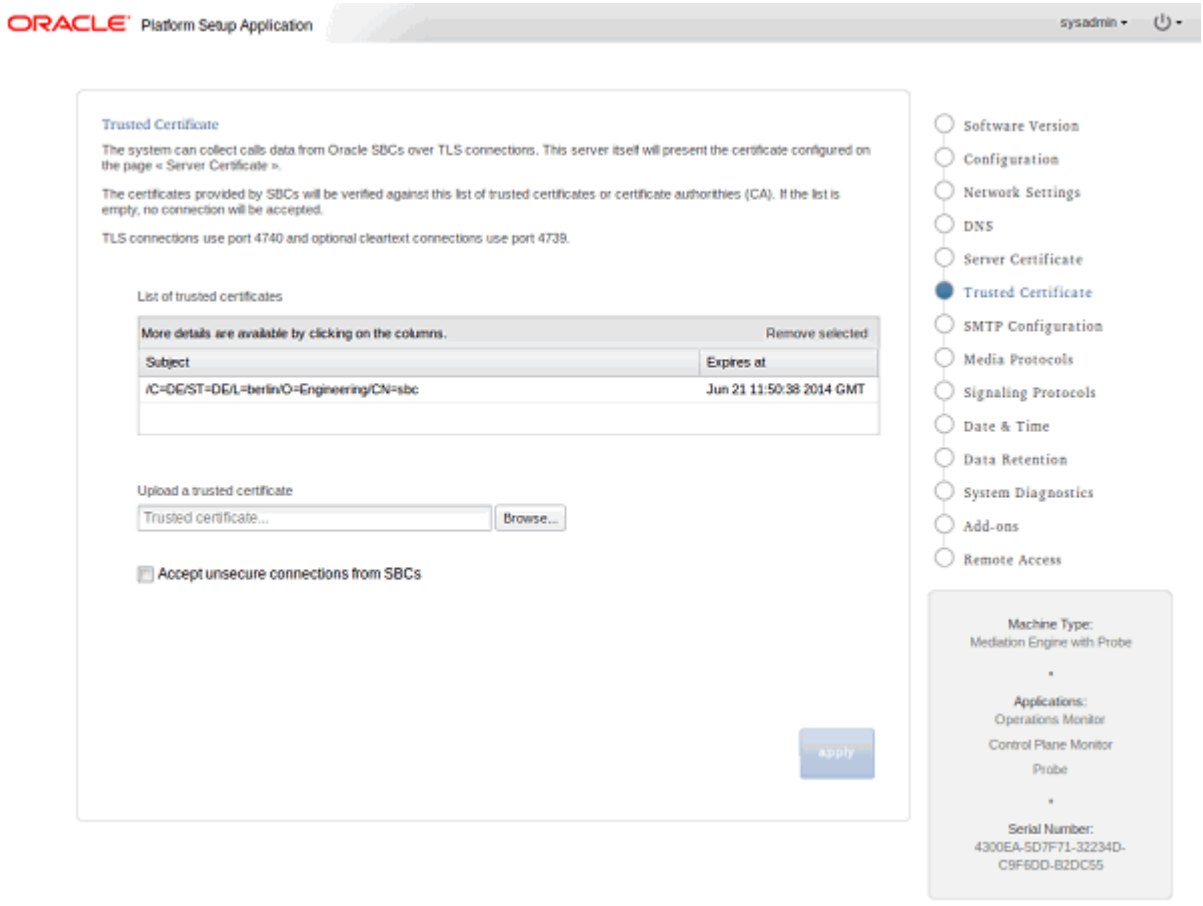
Alternatively, you can upload the CA that is used to sign session border controller's certificates. The certificate format is X.509 / PEM (X.509 extensions are not supported). Only the validity of the signatures are verified.

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 SBCs**; 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 1–3 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

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 email 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.

Encryption and Certificates

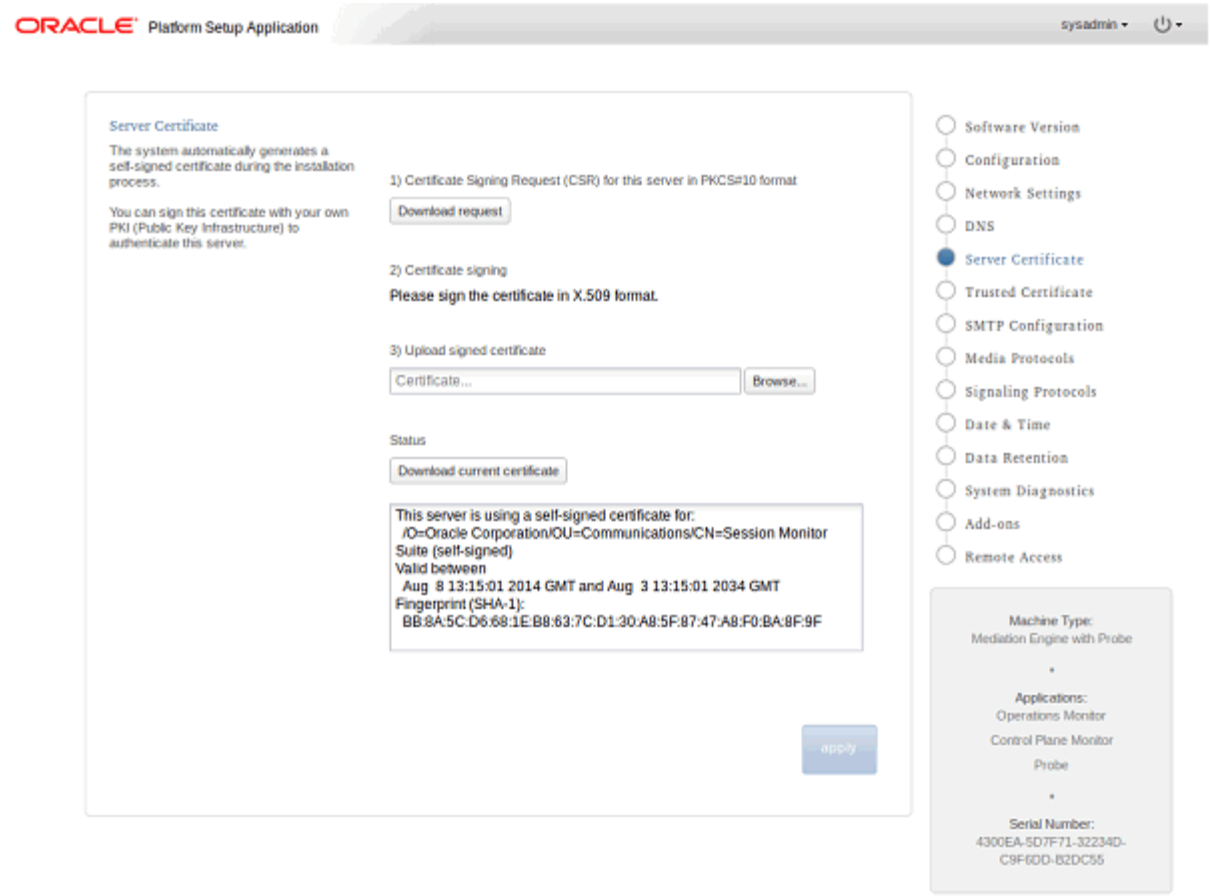
All Session Monitor interfaces can only be accessed through encrypted (secure) HTTPS connections. Each Session Monitor machine uses a unique certificate to establish secure connections and to guarantee its authenticity and protect users' data.

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.

Figure 2–1 shows the Server Certificate page in Platform Setup Application.

Figure 2–1 Server 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 entered in the Aggregation Engine to access the Mediation Engine machines start with **https://**.

See *Session Monitor Mediation Engine Connector User's Guide* for more information.

3

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.

4

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.

By default, Session Monitor REST APIs are not secured. When you use REST APIs to access Operations Monitor features, use your API key.

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.

See *Operations Monitor User's Guide* for more information about how to enable and generate your API Key.

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