Oracle® Communications Session Monitor

Security Guide

Release 4.0

E89197-01

November 2017

ORACLE®

Oracle Communications Session Monitor Security Guide, Release 4.0

E89197-01

Contents

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 install and administer 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
E89197-01	November 2017	Initial release.

1

Session Monitor Secure Configuration

This document covers the necessary configuration of the Oracle Communications Operations Monitor (OCOM) 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 OCOM 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

OCOM 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 OCOM 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 OCOM server. Plain HTTP access is not allowed.

Connections with Oracle SBCs

In OCOM connections from Oracle SBCs to ME machines are encrypted. These connections use TLS on port 4740. Unsecure 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 stand- alone scenario, you can

register the SBC certificate in Platform Setup Application as a trusted certificate, and register OCOM certificate in the SBC. 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 SBC

Follow instructions in the Oracle Support note to:

- Configure the connection to OCOM
- Create a certificate for the SBC
- Register the certificate of OCOM, which can be downloaded from PSA on the panel Server Certificate. Alternatively, register the CA used to sign it.
- Enable TLS

In PSA

In PSA, 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 SBCs 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 SBCs on the **Trusted Certificate** panel. You can then disable the TLS option in the SBC. These connections will use port 4739. However, this setup is not recommended in production.

Connection between ME and MEC

The MEC machines can access the ME machines using HTTPS. Make sure that the urls entered in the AE to reach the ME machines start with https://.

Email Notifications

OCSM 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 OCOM. This account should not grant any other privileges that the product does not require. OCSM also supports TLS connections to the SMTP server.

Connections with ISR

Connection with ISR is performed using HTTP protocol. OCOM 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.