Oracle® Communications Session Monitor

Security Guide

November 2017

E89197-01

Security Guide,

Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Security Guide

Secure Configuration

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

Administrative Password

Platform Setup Application should be protected by a password of your choice on all OCOM machines. Moreover all products come with an administrator (username is admin) account to access their respective interface. To restrict access to these products, connect to their interface, and change the admin account password on each.

User Accounts

OCOM features fine-grained multi-user capabilities which allows the administrator to create restricted accounts for day-to-day usage. Refering to each product manual, create one account for each person who will use the product, and set their permissions to allow their necessary tasks. You will 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 organisation's Public Key Infrastructure (PKI). Please 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 (Public Key Infrastructure), you can instead sign these certificates, and register the trusted CA (Certificate Authority) in each machine.

On the SBC

Follow instructions in this 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 Platform Setup Application on the panel Server Certificate . Alternatively, register the CA used to sign it
- Enable TLS

In PSA

In Platform Setup Application, go to the panel Trusted Certificates . Use the form to upload the certificate(s) of the SBC(s), which will 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 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. To do so they need access to an SMTP server, configurable with Platform Setup Application. 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 need. OCSM also supports TLS connections to the SMTP server.

Connections with ISR

Connection with ISR with perfomed using http protocol. Given the fact that OCOM will interact with external system, whole security picture depends on both parties configurations. It is high advisable to have FACE server hostname only with https protocol scheme.