Oracle® Intelligent Communication Orchestration Network
Security Guide

Release 25.1.0

G42305-01

ORACLE®

Oracle Intelligent Communication Orchestration Network Security Guide, Release 25.1.0

G42305-01

Contents

1   Security and Privacy

1

Security and Privacy

Security is the top priority for the Oracle® Intelligent Communication Orchestration Network from design to implementation following Oracle's Oracle Software Security Assurance (OSSA) requirements. Oracle provides this guide to ensure you that the Oracle® Intelligent Communication Orchestration Network is configured securely and its features are delivered securely.

Topics:

- [About Oracle® Intelligent Communication Orchestration Network](#)
- [Security Recommendations](#)
- [Privacy Policy](#)
- [Security Operations](#)
- [Access Your Information](#)

About Oracle® Intelligent Communication Orchestration Network

The Oracle® Intelligent Communication Orchestration Network enables Enterprises and Managed Service Providers to connect Unified Communications (UC) and Contact Centers (CC) because the service supports connecting to both on-premises and SaaS-based UC and CC solutions. The Oracle® Intelligent Communication Orchestration Network focuses on bringing voice communications services together in one place to relieve you from managing Carrier Service compatibility issues.

Security Recommendations

Oracle builds security into the Oracle® Intelligent Communication Orchestration Network with the following recommendations for you to note.

- The Oracle® Intelligent Communication Orchestration Network User Interface allows only TLS1.2 connections. Ensure that only secured ciphers are allowed from your browsers: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 and TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256.
- The Oracle® Intelligent Communication Orchestration Network server certificate is signed by Oracle's Digit CERT Certificate Authorities. Ensure that your browsers trust Oracle Certificate Authorities: **Digicert SHA2 Secure Server CA2 (Signing CA)** and **Digicert Global ROOT CA (root CA)**.
- For Session Border Controller interfaces that interconnect with Oracle® Intelligent Communication Orchestration Network service points by way of TLS, ensure to add Oracle Root CA to its trusted certificate list. The root CA "Digicert Global Root G2" can be downloaded from https://knowledge.digicert.com/general-information/digicert-trusted-root-authority-certificates.
- Account management: Oracle recommends that you add accounts on a minimum privileges needed basis, where more permissions can be added as needed. When an account is no longer needed, suspend and remove it as soon as possible.

Security Operations

All Oracle® Intelligent Communication Orchestration Network communications are secured (TLS1.2+ with secured ciphers). Data at rest (customer configuration and operation data) is protected with secured ciphers and key lengths.

Oracle also monitors the Oracle® Intelligent Communication Orchestration Network with a secure SIEM program for real time threat detection. All Oracle® Intelligent Communication Orchestration Network deployments and environments are scanned and monitored for any threat intrusion and supply chain risks.

Privacy Policy

The Oracle® Intelligent Communication Orchestration Network collects and uses your information to administer, support, improve, and obtain feedback on our services, to detect and prevent faults, breaches of our network security, the law, or our contractual terms. Oracle will not sell or rent your personal data to others outside Oracle® Intelligent Communication Orchestration Network , except where the law permits or unless you specifically agree.

Information collected by Oracle® Intelligent Communication Orchestration Network may be transferred and disclosed to any of the following parties:

- Companies related to Oracle

- Lawyers, auditors, or advisers to Oracle

- Agents acting on behalf of Oracle

- Oracle business partners

- Agents, affiliates, contractors, and third-party service providers who provide administrative, telecommunications, computer, payment, and other services to Oracle in relation to Oracle's business operations

- Any persons and corporate entities to whom Oracle is obliged to disclose under the requirements of law relating to Oracle or any of its affiliates or partners

- Governmental and judicial bodies and regulators

Access Your Information

You can request access to your personal data information retained by Oracle, make corrections to it, ask us more generally about the kind of personal data we hold, and what our policies and practices are in relation to the information.