

Oracle® Communications

Cloud Native Core Release Notice



Release 2.3.1
F35503-01
September 2020

ORACLE®

F35503-01

Copyright © 2020, 2019, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle 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

1	Introduction	
2	Feature Descriptions	
	Security Edge Proxy Protection (SEPP)	2-1
3	Media and Documentation	
	Media Pack	3-1
	Documentation Pack	3-1
4	Resolved and Known Bugs	
	Severity Definitions	4-1
	Resolved Bug List	4-2
	Customer Known Bug List	4-2

My Oracle Support

My Oracle Support (<https://support.oracle.com>) is your initial point of contact for all product support and training needs. A representative at Customer Access Support can assist you with My Oracle Support registration.

Call the Customer Access Support main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at <http://www.oracle.com/us/support/contact/index.html>. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select **2** for New Service Request.
2. Select **3** for Hardware, Networking and Solaris Operating System Support.
3. Select one of the following options:
 - For Technical issues such as creating a new Service Request (SR), select **1**.
 - For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

What's New In This Guide

This is the first publication of Cloud Native Core (CNC) Release Notes for Release 2.3.1.

1

Introduction

This Release Notice includes feature descriptions, and media and documentation pack contents. This document includes listings for both the resolved and known bugs for this release. Directions for accessing key Oracles sites and services are explained in [MOS](#). Release Notices are included in the documentation pack made available with every software release.

2

Feature Descriptions

This chapter provides a summary of each feature released in Cloud Native features release 2.3.1.

Security Edge Proxy Protection (SEPP)

Security Edge Proxy Protection (SEPP) 1.4.0 provides the following major feature in CNC 2.3.1 release.

- Support for N32 Interface with TLS protection mode
 - N32-C Interface support
 - N32-F Interface support
 - 3GPP-Target-SBI-API-Root header support
- API for Roaming Partner Profile Configuration
- NRF Registration Support
- Logging, Alerts and Metrics support: Metrics and Alerts support has been updated. For more information on the metric details, see Cloud Native Security Edge Proxy Protection (SEPP) User's Guide.

3

Media and Documentation

Oracle Communications software is available for electronic download on the Oracle Software Delivery Cloud (OSDC). Documentation is delivered electronically on the Oracle Help Center (OHC). Both the software Media Pack and Documentation Pack are listed in this chapter.

Media Pack

This section lists the media package for Cloud Native Core 2.3.1. For downloading the package, refer to [MOS](#).

Note:

This list is accurate at the time of release but is subject to change. See the Oracle software delivery website for the latest information.

Table 3-1 Media Pack Contents for Cloud Native Core 2.3.1

Description	Versions	ATS Test Cases Included	Upgrade	Compliance
Oracle Communications Cloud Native Core Security Edge Protection Policy (SEPP)	1.4.0	Yes	Supports fresh installation as well as upgrade from 1.3.0 to 1.4.0. For more information on installation or upgrading, see Oracle Communications Cloud Native Core Security Edge Protection Proxy (SEPP) Installation Guide.	Compatible with CNE 1.6.0

Documentation Pack

All documents are available for download from the [Oracle Help Center \(OHC\)](#) site.

4

Resolved and Known Bugs

This chapter lists the resolved and known bugs for Cloud Native Core release 2.3.1.

These lists are distributed to customers with a new software release at the time of General Availability (GA) and are updated for each maintenance release.

Severity Definitions

The problem report sections in this document refer to bug severity levels. Definitions of these levels can be found in the publication, *TL 9000 Quality Management System Measurement Handbook*.

Problem Report: A report from a customer or on behalf of the customer concerning a product or process defect requesting an investigation of the issue and a resolution to remove the cause. The report may be issued via any medium.

Problem reports are systemic deficiencies with hardware, software, documentation, delivery, billing, invoicing, servicing, or any other process involved with the acquisition, operation, or performance of a product. An incident reported simply to request help to bring back the service or functionality to normal without the intent to investigate and provide a resolution to the cause of the incident is not a problem report.

1. **Critical:** Conditions that severely affect the primary functionality of the product and because of the business impact to the customer requires non-stop immediate corrective action regardless of time of day, or day of the week as viewed by a customer on discussion with the organization such as:
 - Product inoperability (total or partial outage),
 - A reduction in the capacity capability, that is, traffic/data handling capability, such that expected loads cannot be handled,
 - Any loss of emergency capability (for example, emergency 911 calls), or
 - Safety hazard or risk of security breach.
2. **Major:** Product is usable, but a condition exists that seriously degrades the product operation, maintenance, or administration, etc., and requires attention during pre-defined standard hours to resolve the situation.
The urgency is less than in critical situations because of a less immediate or impending effect on product performance, customers, and the customer's operation and revenue such as:
 - Reduction in product's capacity (but still able to handle the expected load),
 - Any loss of administrative or maintenance visibility of the product and/or diagnostic capability,
 - Repeated degradation of an essential component or function, or
 - Degradation of the product's ability to provide any required notification of malfunction.

-
-
3. **Minor:** Other problems of a lesser severity than "critical" or "major" such as conditions that have little or no impairment on the function of the system.

The numbered severity levels in the tables below correspond to these definitions of 1-Critical, 2-Major, or 3-Minor.

Resolved Bug List

The following Resolved Bugs tables list the bugs that are resolved in Cloud Native Release 2.3.1.

Security Edge Protection Proxy (SEPP) 1.4.0 Resolved Bugs



Note:

Security Edge Protection Proxy (SEPP) 1.4.0 has no resolved bugs.

Customer Known Bug List

Customer Known Bugs tables list the known bugs and associated Customer Impact Statements. This information is provided for information purposes only.

Security Edge Protection Proxy (SEPP) 1.4.0 Customer Known Bugs



Note:

Security Edge Protection Proxy (SEPP) 1.4.0 has no customer known bugs.