Oracle® Communications

Cloud Native Core Release Notes

Release 3.25.1.100.0
G23953-12
April 2026

Oracle Communications Cloud Native Core Release Notes, Release 3.25.1.100.0

G23953-12

Copyright © 2019, 2026, 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, software documentation, data (as defined in the Federal Acquisition Regulation), 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," "commercial computer software documentation," or "limited rights data" 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®, Java, MySQL, and NetSuite 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

Copyright © 2019, 2026, Oracle and/or its affiliates.

4 Resolved and Known Bugs

Copyright © 2019, 2026, Oracle and/or its affiliates.

Copyright © 2019, 2026, Oracle and/or its affiliates.

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:

- 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**.
- For Hardware, Networking and Solaris Operating System Support, select **3**.

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.

Copyright © 2019, 2026, Oracle and/or its affiliates.

What's New In This Guide

Release 3.25.1.100.0 - G23953-12, April 2026

BSF 25.1.101 Release
Updated the following sections with the details of BSF release 25.1.101:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- 3GPP Compatibility Matrix
- BSF Security Certification Declaration
- BSF Resolved Bugs

Release 3.25.1.100.0 - G23953-10, August 2025

cnDBTier 25.1.103 Release
Updated the following sections with the details of cnDBTier release 25.1.102:

- Media Pack
- Compatibility Matrix
- cnDBTier Resolved Bugs

SEPP 25.1.102 Release

Updated the following sections with the details of SEPP release 25.1.102:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- SEPP Security Certification Declaration
- SEPP Resolved Bugs

Release 3.25.1.100.0 - G23953-08, July 2025

cnDBTier 25.1.102 Release

Updated the following sections with the details of cnDBTier release 25.1.102:

- Media Pack
- Compatibility Matrix
- cnDBTier Resolved Bugs

SEPP ATS 25.1.102 Release

Updated the following section with the details of SEPP ATS release 25.1.102:

- SEPP Resolved Bugs
- Media Pack

Release 3.25.1.100.0 - G23953-06, June 2025

CNE 25.1.101 Release

Copyright © 2019, 2026, Oracle and/or its affiliates.

Updated the following sections with the details of CNE release 25.1.101:

- Cloud Native Environment (CNE)
- Media Pack
- Compatibility Matrix
- CNE Resolved Bugs
- CNE Known Bugs

OSO 25.1.103 Release

Updated the following sections with the details of OSO release 25.1.103:

- OSO
- Media Pack
- Compatibility Matrix
- OSO Resolved Bugs

SEPP 25.1.101 Release

Updated the following sections with the details of SEPP release 25.1.101:

- Security Edge Protection Proxy (SEPP)
- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- SEPP Security Certification Declaration
- SEPP Resolved Bugs

Release 3.25.1.100.0 - G23953-05, June 2025

OSO 25.1.102 Release

Updated the following sections with the details of OSO release 25.1.102:

- Operations Services Overlay (OSO)
- Media Pack
- Compatibility Matrix
- OSO Resolved Bugs

CNC Console 25.1.100 Release

Updated the Media Pack details as upgrade from release 23.4.x is also supported.

Release 3.25.1.100.0 - G23953-04, May 2025

OSO 25.1.101 Release

Updated the following sections with the details of OSO release 25.1.101:

- Operations Services Overlay (OSO)
- Media Pack
- Compatibility Matrix
- OSO Resolved Bugs

Copyright © 2019, 2026, Oracle and/or its affiliates.

CNC Console 25.1.100 Release

Updated the Media Pack details as upgrade from release 23.4.x is also supported.

Release 3.25.1.100.0 - G23953-03, May 2025

cnDBTier 25.1.101 Release

Updated the following sections with the details of cnDBTier release 25.1.101:

- Media Pack
- Compatibility Matrix
- cnDBTier Resolved Bugs
- cnDBTier Known Bugs

Release 3.25.1.100.0 - G23953-02, May 2025

Added a table in the following sections to list the license names for feature mapping:

- Binding Support Function (BSF)
- Cloud Native Environment (CNE)
- Cloud Native Core cnDBTier
- Cloud Native Configuration Console (CNC Console)
- Oracle Communications Cloud Native Core, Certificate Management (OCCM)
- Network Repository Function (NRF)
- Network Slice Selection Function (NSSF)
- Service Communication Proxy (SCP)
- Security Edge Protection Proxy (SEPP)
- Unified Data Repository (UDR)

Release 3.25.1.100.0 - G23953-01, April 2025

General Updates:

Added the following sections in Media and Documentation:

- Added the Generic Open Source Software Compatibility on Any Platform section to provide information about the open source software compatibility with CNC NFs.
- Added a table that lists the upgrade sequence for Cloud Native Core releases in the Media Pack section.
- Added a table that lists the CNE upgrade sequence in the Media Pack section.

BSF 25.1.100 Release

Updated the following sections with the details of BSF release 25.1.100:

- Binding Support Function (BSF)
- Media Pack
- Compatibility Matrix
- 3GPP Compatibility Matrix
- Common Microservices Load Lineup

Copyright © 2019, 2026, Oracle and/or its affiliates.

- BSF Security Certification Declaration
- BSF Resolved Bugs

cnDBTier 25.1.100 Release

Updated the following sections with the details of cnDBTier release 25.1.100:

- Cloud Native Core cnDBTier
- Media Pack
- Compatibility Matrix
- cnDBTier Resolved Bugs
- cnDBTier Known Bugs

CNC Console 25.1.100 Release

Updated the following sections with the details of CNC Console release 25.1.100:

- Cloud Native Configuration Console (CNC Console)
- Media Pack
- Compatibility Matrix
- 3GPP Compatibility Matrix
- Common Microservices Load Lineup
- CNC Console Security Certification Declaration
- CNC Console Resolved Bugs

CNE 25.1.100 Release

Updated the following sections with the details of CNE release 25.1.100:

- Cloud Native Environment (CNE)
- Media Pack
- Compatibility Matrix
- CNE Resolved Bugs
- CNE Known Bugs

NRF 25.1.100 Release

Updated the following sections with the details of NRF release 25.1.100:

- Network Repository Function (NRF)
- Media Pack
- Compatibility Matrix
- 3GPP Compatibility Matrix
- Common Microservices Load Lineup
- NRF Security Certification Declaration
- NRF Resolved Bugs
- NRF Known Bugs

NSSF 25.1.100 Release

Updated the following sections with the details of NSSF release 25.1.100:

Copyright © 2019, 2026, Oracle and/or its affiliates.

- Network Slice Selection Function (NSSF)
- Media Pack
- Compatibility Matrix
- 3GPP Compatibility Matrix
- Common Microservices Load Lineup
- NSSF Security Certification Declaration
- NSSF Resolved Bugs
- NSSF Known Bugs

OCCM 25.1.100 Release

Updated the following sections with the details of OCCM release 25.1.100:

- Oracle Communications Cloud Native Core, Certificate Management (OCCM)
- Media Pack
- Compatibility Matrix
- 3GPP Compatibility Matrix
- Common Microservices Load Lineup
- OCCM Security Certification Declaration
- OCCM Resolved Bugs
- OCCM Known Bugs

SCP 25.1.100 Release

Updated the following sections with the details of SCP release 25.1.100:

- Service Communication Proxy (SCP)
- Media Pack
- Compatibility Matrix
- 3GPP Compatibility Matrix
- Common Microservices Load Lineup
- SCP Security Certification Declaration
- SCP Resolved Bugs
- SCP Known Bugs

SEPP 25.1.100 Release

Updated the following sections with the details of SEPP release 25.1.100:

- Security Edge Protection Proxy (SEPP)
- Media Pack
- Compatibility Matrix
- 3GPP Compatibility Matrix
- Common Microservices Load Lineup
- SEPP Security Certification Declaration
- SEPP Resolved Bugs

Copyright © 2019, 2026, Oracle and/or its affiliates.

- SEPP Known Bugs

UDR 25.1.100 Release

Updated the following sections with the details of UDR release 25.1.100:

- Unified Data Repository (UDR)
- Media Pack
- Compatibility Matrix
- 3GPP Compatibility Matrix
- Common Microservices Load Lineup
- UDR Security Certification Declaration
- UDR Resolved Bugs
- UDR Known Bugs

Common Services Resolved Bugs

- Egress Gateway Resolved Bugs
- Ingress Gateway Resolved Bugs
- Alternate Route Service Resolved Bugs
- Helm Test Resolved Bugs
- Mediation Resolved Bugs

Common Services Known Bugs

- Egress Gateway Known Bugs
- Ingress Gateway Known Bugs

Copyright © 2019, 2026, Oracle and/or its affiliates.

1

Introduction

This document provides information about new features and enhancements to the existing features for Oracle Communications Cloud Native Core network functions.

It also includes details related to media pack, common services, security certification declaration, and documentation pack. The details of the fixes are included in the Resolved Bug List section. For issues that are not yet addressed, see the Customer Known Bug List.

For information on how to access key Oracle sites and services, see My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

2
Feature Descriptions

This chapter provides a summary of new features and updates to the existing features for network functions released in Cloud Native Core release 3.25.1.1xx.0.

> **Note**
>
> CCNC-XXXX is an internal identification number of the feature.

Automated Testing Suite (ATS) Framework

Release 25.1.100

There are no new features or feature enhancements in this release.

Binding Support Function (BSF)

Release 25.1.101

There are no new features or feature enhancements in this release.

Release 25.1.100

Oracle Communications Cloud Native Core, Binding Support Function (BSF) 25.1.100 includes the following enhancements:

- **Stale Binding Detection Audit, Report, and Recover**: Service disruptions caused by network storms, system overload, database latency, or other factors can interrupt signaling between the Policy and BSF, impacting session binding. BSF provides a mechanism to revalidate the binding information of a PDU session, and recover stale bindings, ensuring session integrity. For more information, see "*Stale Binding Detection Audit, Report, and Recover*" section in "*Oracle Communications Cloud Native Core, Binding Support Function User Guide*".
- **Stale Binding Manual Detection Tool**: Service disruptions caused by network storms, system overload, database latency, or other factors can interrupt signaling between Policy and BSF, impacting session binding. Currently, when binding is lost and Policy sessions are in a hung state, there is no way of knowing which sessions were lost or never received the binding. As a result, no action can be taken to solve this issue. The Binding Detection Tool addresses this by allowing manual queries of sessions created within a specific time frame in both Policy and BSF. For more information, see *Oracle Communications Cloud Native Core, Binding Detection Tool User Guide*.
- **Enhancements in menu.json for cnDBTier GRR Configuration**: The BSF CNC Console GUI supports integration of read-only Georeplicaiton Recovery (GRR) cnDBTier APIs. With this, users can have specific information on cnDBTier statuses on the CNC Console. For more information, see the "*Support for cnDBTier APIs in CNC Console*" section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- **Performance enhancement to achieve 54K TPS**: In this release, BSF can achieve 54K TPS through performance optimizations. For more information, see the "*BSF Benchmark Testing*" section in *Oracle Communications Cloud Native Core, Binding Support Function Benchmarking Guide*.
- **Traffic Segregation**: BSF supports end-to-end traffic segregation based on traffic types. This ensures that critical networks are not cross-connected or share the same routes, thereby preventing network congestion. For more information, see the "*Traffic Segregation*" section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.

The following table lists the license names for feature mapping. For additional licensing information, see *Oracle Communications Cloud Native Core Licensing Information User Manual*.

Table 2-1 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Binding Support Function - 25K Active Subscribers Perpetual	CCNC-8864	Stale Binding Detection Audit, Report, and Recover
Oracle Communications Cloud Native Core, Binding Support Function - 25K Active Subscribers Perpetual	CCNC-8840	SMPCF and BSF Stale Binding Manual Detection Tool
Oracle Communications Cloud Native Core, Binding Support Function - 25K Active Subscribers Perpetual	CCNC-5795	Enhancements in menu.json for cnDBTier GRR Configuration
Oracle Communications Cloud Native Core, Binding Support Function - 25K Active Subscribers Perpetual	CCNC-7763	Compatibility with two Webscale versions per release
Oracle Communications Cloud Native Core, Binding Support Function - 25K Active Subscribers Perpetual	CCNC-4504	Performance enhancement to achieve 54K TPS
Oracle Communications Cloud Native Core, Advance Cloud Native Environment - 25K Active Subscribers perpetual	CCNC-4443	Traffic Segregation

Cloud Native Environment (CNE)

Release 25.1.101

Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) 25.1.101 includes the following enhancement:

Support for Multus Thick Plugin for CNE deployments: With this feature, Multus Thick Plugin is installed whenever a new version of CNE is installed with CNLB enabled option. It is highly recommended to use Multus Thick Plugin based release for CNLB based CNE deployments. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide.*

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> - Only CNE Releases 24.3.3 and above support Multus Thick Plugin based CNE deployments.
> - CNE 24.2.x releases do not support Multus Thick Plugin and are not recommended for CNLB deployments.

Release 25.1.100

Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) 25.1.100 includes the following enhancements:

- **Support for BareMetal CNE Deployment with Bare Minimum Servers (3 Worker Nodes)**: With this feature, CNE allows you to set up a BareMetal deployment with a minimal resources of three worker nodes. This setup is ideal for testing and getting started with CNE. For more information about installing and upgrading CNE with bare minimum servers, see the "*Installing CNE using Bare Minimum Servers*" and "*Upgrading BareMetal CNE Deployed using Bare Minimum Servers*" sections respectively in *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
- **Hardware Agnostic Deployment Model for BareMetal CNE**: Currently, CNE validates and supports BareMetal deployments on HP Gen10 and Oracle X8-2 servers only. With this release, CNE supports installing BareMetal CNE on any servers, thereby allowing the users to choose their servers based on their requirement. For more information about the prerequisites and updated procedure to install BareMetal CNE on other servers, see the "*BareMetal Installation*" section in *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
- **Heterogenous Hardware Support for BareMetal CNE Deployment**: Currently, BareMetal deployments support homogeneous hardware make, type, and version for worker nodes in a cluster. This means, all the worker nodes in a cluster must have the same type of hardware server, type, and version (for example, HP Gen 10 server with similar CPU, cores, RAM, and storage). With this feature, CNE supports heterogeneous hardware, wherein worker nodes in a cluster can have different server, type, and version. This provides more flexibility and options to manage hardware failure, expand existing deployment cluster, and tackle hardware End Of Life (EOL) and availability. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide* and *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
- **Generic ToR Switch Configuration for BareMetal CNE**: With this feature, CNE facilitates you to set up your BareMetal cluster using any ToR switch, by providing generic specifications, prerequisites, and configuration templates. For more information about configuring the ToR switches, see the "*Configuring Top of Rack Switches*" section in *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
- **Traffic Segregation**: With this enhancement, CNE provides an option to use Cloud Native Load Balancer (CNLB) without internal traffic segregation. This means CNLB can be configured to have a single interface to handle only external traffic. For more information about CNLB configuration, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
- **New Versions of Common Services**: The following common services are upgraded in this release:

Copyright © 2019, 2026, Oracle and/or its affiliates.

- Helm - 3.16.2
- Kubernetes - 1.31.1
- Calico - 3.28.0
- Istio - 1.23.0

To get the complete list of third-party services and their versions, refer to the `dependencies_25.1.100.tgz` file provided as part of the software delivery package.

> **Note**
>
> CNE constitutes a number of third-party services. For information about these third-party services, refer to the documents of the respective third-party services.

The following table lists the license names for feature mapping. For additional licensing information, see *Oracle Communications Cloud Native Core Licensing Information User Manual*.

Table 2-2 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Cloud Native Environment - per 25K Subscribers Perpetual	CCNC-6155	Support for BareMetal CNE Deployment with Bare Minimum Servers (3 Worker Nodes)
Oracle Communications Cloud Native Core, Cloud Native Environment - per 25K Subscribers Perpetual	CCNC-7674	Hardware Agnostic Deployment Model for BareMetal CNE
Oracle Communications Cloud Native Core, Cloud Native Environment - per 25K Subscribers Perpetual	CCNC-8297	Heterogenous Hardware Support for BareMetal CNE Deployment
Oracle Communications Cloud Native Core, Cloud Native Environment - per 25K Subscribers Perpetual	CCNC-7672	Generic ToR Switch Configuration for BareMetal CNE
Oracle Communications Cloud Native Core, Advanced Cloud Native Environment - 25K Active Subscribers Perpetual	CCNC-8079	Traffic Segregation
Oracle Communications Cloud Native Core, Advanced Cloud Native Environment - 25K Active Subscribers Perpetual	CCNC-1192	Multiple Network Interface per POD Support

Operations Services Overlay (OSO)

Release 25.1.103

Oracle Communications Cloud Native Core, Operations Services Overlay (OSO) 25.1.103 includes the following enhancements:

- **Support for new versions**:
  - `25_1_common_oso:25.1.103`

Copyright © 2019, 2026, Oracle and/or its affiliates.

- 25_1_oso_snapshot:25.1.103

For more information, see *Oracle Communications Cloud Native Core, Operations Services Overlay Installation and Upgrade Guide.*

Release 25.1.102

Oracle Communications Cloud Native Core, Operations Services Overlay (OSO) 25.1.102 includes the following enhancements:
Support for new versions:

- 25_1_common_oso:25.1.102
- 25_1_oso_snapshot:25.1.102

For more information, see *Oracle Communications Operations Services Overlay Installation and Upgrade Guide*.

Release 25.1.101

Oracle Communications Cloud Native Core, Operations Services Overlay (OSO) 25.1.101 includes the following enhancements:
Support for new versions:

- 25_1_common_oso:25.1.101
- 25_1_oso_snapshot:25.1.101

For more information, see *Oracle Communications Operations Services Overlay Installation and Upgrade Guide*.

Release 25.1.100

Oracle Communications Cloud Native Core, Operations Services Overlay (OSO) 25.1.100 includes the following enhancements:

- **Support for Time Series Database (TSDB) Snapshot**: Prometheus uses Time Series Database (TSDB) to store the collected metrics. With this feature, OSO allows the users to capture a snapshot at a specific point of time of the Prometheus data store without shutting down or disrupting the Prometheus instance. It is useful for taking backups, recovery, or even debugging purposes.

  For more information, see the "*Support for Time Series Database (TSDB) Snapshot*" section in *Oracle Communications Operations Services Overlay User Guide*.

  For more information about the procedure to take TSDB snapshots, see the "*Creating Backup of Prometheus Time Series Database (TSDB) Using Snapshot Utility*" section in *Oracle Communications Operations Services Overlay Installation and Upgrade Guide*.
- **Support for new versions**:
  - 25_1_common_pod is replaced with 25_1_common_oso.
  - 25_1_oso_snapshot:25.1.100

  For more information, see *Oracle Communications Operations Services Overlay Installation and Upgrade Guide.*

Cloud Native Core cnDBTier

Release 25.1.103

There are no new features or feature enhancements in this release.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Release 25.1.102

There are no new features or feature enhancements in this release.

Release 25.1.101

There are no new features or feature enhancements in this release.

Release 25.1.100

Oracle Communications Cloud Native Core, cnDBTier (cnDBTier) 25.1.100 includes the following enhancements:

- **Enhanced Georeplication Recovery using Parallel Backup Transfer and Restore**: The backup transfer and restore mechanism used during a georeplication recovery involved additional data compression at the data node and serial backup transfer to the remote sites. This impacted the performance of georeplication recovery. With this feature, cnDBTier implements the following enhancements in backup transfer and restore thereby improving the performance and efficiency of georeplication recovery:
  - Avoids additional backup compression.
  - Supports parallel backup transfer from healthy cluster to georeplication recovery cluster.
  - Restores data node backups in parallel, as and when the backups are transferred from the healthy cluster to the georeplication recovery cluster.

  For more information, see *Oracle Communications Cloud Native Core, cnDBTier User Guide* and *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide.*
- **Support for TLS**: With this enhancement, cnDBTier supports TLS for application SQL pods to establish secure connection for communication with Network Functions (NFs). When the TLS feature is enabled, cnDBTier performs or supports the following operations during communication with NFs:
  - The application SQL pod uses the certificates provided or configured to establish an encrypted connection for communication with NFs. This encrypted connection remains throughout the life cycle of the connection between NF and cnDBTier.
  - The system reestablishes the TLS connection between NFs and cnDBTier after a georeplication recovery. That is, when a georeplication recovery completes successfully, the system reestablishes the encrypted connection between the NFs and cnDBTier. This ensures that cnDBTier continues supporting TLS connection after a georeplication recovery.

  For more information, see *Oracle Communications Cloud Native Core, cnDBTier User Guide* and *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide.*
- **Monitoring Cluster Events to Determine Data Loss in Clusters**: Network issues in the user environment led to cluster disconnections, which in turn resulted in the loss of cluster data. However, users were unable to monitor and identify the loss of data occurred due to network issues. With this feature, cnDBTier provides the following REST APIs to monitor cnDBTier cluster events to determine any data loss:
  - http://<base-uri>/db-tier/reset/parameter/cluster_restart_disconnect
  - http://<base-uri>/db-tier/reset/cluster/{cluster-name}/parameter/cluster_restart_disconnect

Copyright © 2019, 2026, Oracle and/or its affiliates.

  - http://<base-uri>/db-tier/cluster/status
  - http://<base-uri>/db-tier/cluster/status/events/{numberOfLastEvents}
  - http://<base-uri>/db-tier/all/cluster/status/
  - http://<base-uri>/db-tier/all/cluster/status/events/{numberOfLastEvents}

  For more information about these APIs, see *Oracle Communications Cloud Native Core, cnDBTier User Guide.*

- **Storing NDB Logs in PVC**: cnDBTier stores all NDB pod (ndbmgmd, ndbmysqld, ndbappmysqld) logs in PVC. These logs remain persistent even when the pods restart and they can be used to debug any data node related issues. However, ndbmtd logs were not stored in PVC. With this feature, cnDBTier stored ndbmtd logs in PVC, such that the logs remain available even after the pod is deleted. This feature is enabled in cnDBTier by default and doesn't require any configuration. For more information, see the "*Storing NDB Logs in PVC*" section in *Oracle Communications Cloud Native Core, cnDBTier User Guide.*
- **cnDBTier Automated Backup**: MySQL doesn't allow schema change in a cluster when a backup is in progress. However, users were unable to check the ongoing backup processes in the cluster and schedule their upgrades for schema changes. With this release, cnDBTier provides the http://<base-uri>/db-tier/status/cluster/local/backup REST API to fetch the details of the data node backups that are in progress in the NDB cluster. For more information about this API, see the "*cnDBTier Backup APIs*" section in *Oracle Communications Cloud Native Core, cnDBTier User Guide.*
- **cnDBTier Scaling**: With this release, cnDBTier automates the vertical scaling of PVCs using the `dbtscale_vertical_pvc script`. This simplifies the vertical scaling process and reduces human errors that may occur while performing the manual procedure. For more information about performing the vertical scaling using the `dbtscale_vertical_pvc` script, see the "*cnDBTier Scaling*" section in *Oracle Communications Cloud Native Core, cnDBTier User Guide.*
- **Support for New Versions of Software**: cnDBTier has updated the version of Oracle MySQL Cluster Database to 8.4.3 in this release.

> **Note**
>
> In `db-monitor-svc` script, the PVC and JVM-related metrics are disabled by default. This is due to PVC and JVM metrics fetch-time exceeding the Prometheus metrics fetch-timeout. This impacts the metrics fetch cycle.
>
> The following PVC metrics are disabled:
>
> - *db_tier_pvc_read_write_speed*
> - *db_tier_pvc_is_accesible*
> - *db_tier_pvc_failure_count*
>
> The following JVM metrics are disabled:
>
> - *jvm_max_memory*
> - *jvm_free_memory*
> - *jvm_total_memory*

The following table lists the license names for feature mapping. For additional licensing information, see *Oracle Communications Cloud Native Core Licensing Information User Manual*.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 2-3 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Network Slice Selection Function- 25K Active Subscribers Perpetual	CCNC-8876	Enhanced Georeplication Recovery using Parallel Backup Transfer and Restore
Oracle Communications Cloud Native Core, Network Slice Selection Function- 25K Active Subscribers Perpetual	CCNC-5332	Support for TLS
Oracle Communications Cloud Native Core, Policy and Charging Rules Function - 25K Subscribers Perpetual	CCNC-9356	Compatibility with two Webscale versions per release

Cloud Native Configuration Console (CNC Console)

Release 25.1.100

Oracle Communications Cloud Native Configuration Console (CNC Console) 25.1.100 includes the following enhancements:

- **Multiple Admin Support for CNCC IAM Deployments**: As CNC Console evolved from a simple interface for managing a single network function (NF) instance with one admin account to supporting multi-cluster deployments catering to multiple NF Instances including access management to observability applications, there was a need to have support for multiple admin users for managing the users across multiple customer operations teams. As part of this feature, CNC Console IAM is enhanced to support creation and management of multiple admin users in IAM using both internal and external IDPs (SAML and LDAP). For all the admin accounts managed in CNC Console, all the existing measurements, alarms, and logging mechanisms would be applicable to all admin users similar to the existing core users.

  There are default password policies defined for CNCC IAM users in the default realm. These policies are disabled by default and can be enabled, if needed.During the deployment, a default admin user is created. To create multiple CNCC IAM admin users, refer to the "*Post Installation steps*" section in *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide* and *Oracle Communications Cloud Native Configuration Console User Guide*.

The following table lists the license names for feature mapping. For additional licensing information, see *Oracle Communications Cloud Native Core Licensing Information User Manual*.

Table 2-4 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Cloud Native Environment - per 25K Subscribers Perpetual	CCNC-9858	Multiple Admin support for CNCC IAM deployments

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 2-4 (Cont.) License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Cloud Native Environment - per 25K Subscribers Perpetual	CCNC-8525	IAM Backend Upliftment

Oracle Communications Cloud Native Core, Certificate Management (OCCM)

Release 25.1.100

Oracle Communications Cloud Native Core, Certificate Management (OCCM) 25.1.100 includes the following enhancements:

- **Support to Increase the Certificate Management Capacity**: OCCM is designed to manage certificates for multiple NFs. This feature increases the maximum number of supported certificates (both OCCM and NF certificates) to 200. For more information about certificate management, see the "*Managing Certificates*" section in *Oracle Communications Cloud Native Core, Certificate Management User Guide*. For more information, see "*OCCM Configuration Maximum Limits", see the "OCCM Deployment Models*" section in *Oracle Communications Cloud Native Core, Certificate Management Installation, Upgrade, and Fault Recovery Guide*.
- **Expired Certificate Handling**: This feature enables OCCM to raise alert and stop the retry of CMP (Certificate Management Protocol) Identity (OCCM) certificate renewal. For the expired End Entity (NF) certificates, if OCCM is configured to sign the Certificate Management Protocol Version 2 (CMPv2) Key Update Request (KUR) using the certificate and key that is being renewed, then OCCM raises an alert indicating the expiry of the certificate and stop the retry of NF certificate renewal. For more information, see "*Expired Certificate Handling*" section in *Oracle Communications Cloud Native Core, Certificate Management Troubleshooting Guide*.
- **Bulk Migration of Certificates:** With this feature, you can update the issuer configuration and endpoint by updating fields such as the server URL, recipient Distinguished Name (DN), and issuer DN. This update is performed by migrating the certificates in bulk from the current issuer to a newly created issuer with the required configuration. For more information, see "*Bulk Migration of Certificates*" section in *Oracle Communications Cloud Native Core, Certificate Management User Guide*.

The following table lists the license names for feature mapping. For additional licensing information, see *Oracle Communications Cloud Native Core Licensing Information User Manual*.

Table 2-5 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Certificate Management - 25K Active Subscribers	CCNC-8810	Support to Increase the Certificate Management Capacity

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 2-5 (Cont.) License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Certificate Management - 25K Active Subscribers	CCNC-8808	Expired Certificate Handling
Oracle Communications Cloud Native Core, Certificate Management - 25K Active Subscribers	CCNC-6075	Bulk Migration of Certificates

Network Repository Function (NRF)

Release 25.1.204

Oracle Communications Cloud Native Core, Network Repository Function (NRF) 25.1.204 includes the following enhancements:

No new features or feature enhancements have been introduced in this release.

Release 25.1.203

Oracle Communications Cloud Native Core, Network Repository Function (NRF) 25.1.203 includes the following enhancements:

No new features or feature enhancements have been introduced in this release.

Release 25.1.202

Oracle Communications Cloud Native Core, Network Repository Function (NRF) 25.1.202 includes the following enhancements:

- **Egress Gateway Pod Protection Using Rate Limiting**: This feature applies a rate limiting mechanism to Egress Gateway pods, allowing them to process a predefined number of requests. When the request rate exceeds the configured threshold, the pods protect themselves by either rejecting additional requests with a custom error code or allowing them, based on the configuration.
  For more information about this feature, see the "Egress Gateway Pod Protection Using Rate Limiting" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **Support for 106K Ingress TPS with 91.2K SLF TPS in Growth Mode**: NRF supports processing up to 106K Transactions Per Second (TPS) in a growth environment configured with two sets, with each set accommodating upto 53K Ingress TPS and 45.6K SLF TPS utilization for enabling greater performance and scalability.
  For more information, see the "Benchmark Testing" section in *Oracle Communications Cloud Native Core, Network Repository Function Benchmarking Guide*.
- **NF Profile Count Enhancements**: NRF supports a maximum of 600 NF Profiles in a growth environment configured with two sets, with each set accommodating up to 300 NF Profiles. This enhancement improves scalability and capacity for large-scale network deployments.
  For more information, see the "NRF Supported Services" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*. For more information on NF Profiles supported per set in a Growth environment with two sets, see

Copyright © 2019, 2026, Oracle and/or its affiliates.

the section "Benchmark Testing" in *Oracle Communications Cloud Native Core, Network Repository Function Benchmarking Guide*.

- **Support for ASM 1.21.6**: NRF supports the Aspen Service Mesh (ASM) 1.21.6 version on Kubernetes 1.27 version from this release.
  For more information, see the "Configuring NRF to Support ASM" section in *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.

The following table lists the license names for feature mapping. For additional licensing information, see *Oracle Communications Cloud Native Core Licensing Information User Manual*.

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Network Repository Function - 25K Active Subscribers Perpetual	CCNC-10061	Support for ASM 1.21.x
Oracle Communications Cloud Native Core, Network Repository Function - 25K Active Subscribers Perpetual	CCNC-10371	Egress Gateway Pod Protection Using Rate Limiting
Oracle Communications Cloud Native Core, Network Repository Function - 25K Active Subscribers Perpetual	CCNC-11110	NF Profile Count Enhancements
Oracle Communications Cloud Native Core, Network Repository Function - 25K Active Subscribers Perpetual	CCNC-10184	Support for 106K Ingress TPS with 91.2K SLF TPS in Growth Mode

Release 25.1.200

Oracle Communications Cloud Native Core, Network Repository Function (NRF) 25.1.200 includes the following enhancements:

- **Ingress Gateway Pod Protection Using Rate Limiting**: This feature applies a rate limiting mechanism to Ingress Gateway pods, allowing them to process a predefined number of requests. When the request rate exceeds the configured threshold, the pods protect themselves by either rejecting additional requests with a custom error code or allowing them, based on the configuration.
  For more information about this feature, see the "Ingress Gateway Pod Protection Using Rate Limiting" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **Writing Messages of the Same Transaction in the Same Kafka Partition:** This feature ensures that NRF copies request and response messages of the same transaction to the same Kafka partition when sending messages to Data Director. This reduces latency in processing transaction data. The feature uses the *correlation-id* (a unique identifier) as the message key to correlate messages for a transaction.

  For more information about this feature, see the "NRF Message Feed" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **NRF Message Feed Enhancements**: The following additional message attributes are included in the metadata list, along with existing attributes:
  - source-ip
  - destination-ip
  - source-port
  - pod-instance-id

Copyright © 2019, 2026, Oracle and/or its affiliates.

  - destination-port

  For more information about this feature, see the "NRF Message Feed" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.

- **NF Profile Size Limit**: This feature allows to specify the maximum limit of the NF Profile size that can be registered with NRF. The NF Profile size is evaluated during the `NfRegister` or `NfUpdate` service operation, and if the profile size is within the configured maximum limit, the service operation is allowed. If the profile size breaches the configured thresholds, the service operation gets rejected.
  For more information about this feature, see the "NF Profile Size Limit" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide.*
- **Pod Level Traffic Rejections (Overload Control Enhancements)**: With this enhancement, NRF rejects the incoming requests at pod level for percentage-based overload control by removing the dependency on cache-based coordination across pods. When the overload control level is breached, the number of requests to be rejected is calculated based on the requests received at each Ingress Gateway pod. This ensures a more accurate and consistent request rejection even in scenarios with low Transactions Per Second (TPS) and uneven traffic distribution.

  For more information about this feature, see the "Pod Level Traffic Rejections" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide.*
- **Support for cnDBTier Backup Status APIs in CNC Console**: With this enhancement, cnDBTier backup status APIs are integrated into the CNC Console. Users can view cnDBTier backup status APIs, such as the current timestamp, backup in progress, and next scheduled backup on CNC Console.
  For more information, see the "Support for cnDBTier APIs in CNC Console" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.

The following table lists the license names for feature mapping. For additional licensing information, see *Oracle Communications Cloud Native Core Licensing Information User Manual*.

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Network Repository Function - 25K Active Subscribers Perpetual	CCNC-5363	NRF Message Feed Enhancements
Oracle Communications Cloud Native Core, Network Repository Function - 25K Active Subscribers Perpetual	CCNC-6080	Writing Messages of the Same Transaction in the Same Kafka Partition
Oracle Communications Cloud Native Core, Network Repository Function - 25K Active Subscribers Perpetual	CCNC-9424	Ingress Gateway Pod Protection Using Rate Limiting

Network Slice Selection Function (NSSF)

Release 25.1.100

Oracle Communications Cloud Native Core, Network Slice Selection Function (NSSF) 25.1.100 includes the following enhancements:

- **DNS SRV-Based Selection of NRF in NSSF:** The DNS SRV-based selection feature enhances the Network Slice Selection Function (NSSF) by introducing dynamic Network Repository Function (NRF) selection through DNS SRV records. This update improves network resilience by allowing NSSF to dynamically switch to alternate NRFs in case of primary NRF failures, ensuring continuous service availability. For more information, see

Copyright © 2019, 2026, Oracle and/or its affiliates.

the "*DNS SRV-Based Selection of NRF in NSSF*" section in *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide*.

- **Deleting All Slices in a TAI Using PATCH Remove Operation:** This feature enhances NSSF by enabling more flexible management of network slices in 5G networks. It allows the AMF to delete all slices for specific Tracking Areas (TAIs), TAILists, or TAIRanges using the PATCH operation. For more information, see the "*Deleting All Slices in a TAI Using PATCH Remove Operation*" section in *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide.*
- **Improved Error Response when All Slices are Removed:** NSSF now provides clearer responses, such as returning 204 No Content when all slices in an area are removed, while still allowing slices to be re-added through PATCH or PUT operations. This enhancement improves granularity, efficiency, and control for slice management while aligning with 3GPP standards. For more information, see the "*Deleting All Slices in a TAI Using PATCH Remove Operation*" section in *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide.*

The following table lists the license names for feature mapping. For additional licensing information, see *Oracle Communications Cloud Native Core Licensing Information User Manual*.

Table 2-6 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Network Slice Selection Function - 25K Active Subscribers Perpetual	CCNC-4529	DNS SRV-Based Selection of NRF in NSSF
Oracle Communications Cloud Native Core, Network Slice Selection Function - 25K Active Subscribers Perpetual	CCNC-9140	Deleting All Slices in a TAI Using PATCH Remove Operation
Oracle Communications Cloud Native Core, Network Slice Selection Function - 25K Active Subscribers Perpetual	CCNC-8381	Improved Error Response when All Slices are Removed
Oracle Communications Cloud Native Core, Network Slice Selection Function - 25K Active Subscribers Perpetual	CCNC-9228 CCNC-5077	Compatibility with two Webscale versions per release

Service Communication Proxy (SCP)

Release 25.2.102

There are no new features or enhancements in this release.

Release 25.2.101

There are no new features or enhancements in this release.

Release 25.2.100

Oracle Communications Cloud Native Core, Service Communication Proxy (SCP) 25.2.100 includes the following enhancements:

Copyright © 2019, 2026, Oracle and/or its affiliates.

- **LCM Automation**: The Lifecycle Management (LCM) Automation feature optimizes deployment and upgrade processes of SCP by automating service account creation. This enhancement allows you to automatically create user-defined service accounts without any manual intervention. For more information, see the "LCM Automation" section in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **TLS 1.3 Support for Kubernetes API**: SCP can be deployed in a Kubernetes cluster that supports TLS 1.3. For more information, see the "TLS 1.3 Support for Kubernetes API" section in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Support for Grafana 7.5.x**: SCP supports Grafana 7.5.x. For more information, see the "Software Requirements" section in *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.
- **Support for Sender NF Type based Routing Option Selection**: SCP enhances its routing options configuration to configure `senderNFType` so that routing options selection criteria can also consider sender NF Type for selecting a routing option. In addition, SCP enhances its logic to identify notification sender to consider sender NF type in routing options selection criteria. For more information, see the "Support for Sender NF Type based Routing Option Selection" section in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Support for 1200 NF Profiles**: SCP is enhanced to support 1200 NF profiles with a single Notification pod instance. For more information, see "SCP Services", "Upgrade", and "ASM Sidecar" sections in *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.

The following table lists the license names for feature mapping. For additional licensing information, see *Oracle Communications Cloud Native Core Licensing Information User Manual*.

Table 2-7 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Cloud Native Environment - per 25K Subscribers Perpetual	CCNC-10664	Support for Grafana 7.5.x
Oracle Communications Cloud Native Core, Service Communication Proxy - 25K Active Subscribers Perpetual	CCNC-9147	TLS 1.3 Support for Kubernetes API
Oracle Communications Cloud Native Core, Automated Lifecycle Management - 25K Active Subscribers	CCNC-8293	LCM Automation
Oracle Communications Cloud Native Core, Advanced Routing – 25K Active Subscribers Perpetual	CCNC-4404 and CCNC-5933	Routing Options Enhancement for Notification Messages
Oracle Communications Cloud Native Core, Service Communication Proxy - 25K Active Subscribers Perpetual	CCNC-11246	Support for 1200 NF Profiles

Security Edge Protection Proxy (SEPP)

Release 25.2.100

Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP) 25.2.100 includes the following enhancements:

Copyright © 2019, 2026, Oracle and/or its affiliates.

- **NRF Selection Mechanisms Using nrf client:** This feature allows the SEPP to dynamically select NRF instances based on real-time availability and site redundancy through DNS SRV configurations. In addition to the static configurations by operators, the SEPP can now resolve NRFs using DNS SRV based Fully Qualified Domain Names (FQDNs). The SEPP is configured with a primary NRF and multiple fallback NRFs, which take over if the primary NRF becomes unreachable.
  The nrf client uses the Alternate Route Service, which helps the SEPP find and select different Network Repository Functions (NRFs) by using DNS SRV-based lookups. This service allows the SEPP to translate Fully Qualified Domain Names (FQDNs) or virtual FQDNs into alternate NRF addresses. This setup enables the SEPP to prioritize and adjust connections to different NRFs based on specific service needs. For more information, see the "NRF Selection Mechanisms Using nrf client" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide* and "Customizable Parameters" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*.
- **Integrating SEPP with 5G Network Intelligence Fabric (5G NIF):** To route traffic to a Network Function, SEPP has traditionally relied on configurations or destination headers found in incoming SBI requests. For integration with the customized 5G Network Intelligence Fabric (5GNIF), SEPP must now discover this custom NF through the NRF, which holds this information. Once discovered, SEPP uses all existing routing mechanisms (such as alternate routing) to direct traffic to the identified 5GNIF instance. Additionally, SEPP is required to send copies of error messages, triggered by countermeasures or failed checks, to the 5GNIF for analytic purposes. For more information, see the "Integrating SEPP with 5G Network Intelligence Fabric (5G NIF)" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide* and the "Customizable Parameters" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*.
- **TLS 1.3 Support for Kubernetes API**: SEPP can be deployed in a Kubernetes cluster that supports TLS 1.3. For more information, see the "TLSv1.3 Support for Kubernetes API Server Communication" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*.
- **Support for Grafana 7.5.x**: SEPP supports Grafana 7.5.x. For more information, see the "*Software Requirements*" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*.

The following table lists the license names for feature mapping. For additional licensing information, see *Oracle Communications Cloud Native Core Licensing Information User Manual*.

Table 2-8 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Advanced Routing – 25K Active Subscribers Perpetual	CCNC-8037	Integrating SEPP with 5G Network Intelligence Fabric (5G NIF)
Oracle Communications Cloud Native Core, Security Edge Protection Proxy - 25K Active Subscribers Perpetual	CCNC-10188	NRF Selection Mechanisms Using nrf client
Oracle Communications Cloud Native Core, Security Edge Protection Proxy - 25K Active Subscribers Perpetual	CCNC-9149	TLS 1.3 Support for Kubernetes API Server Communication
Oracle Communications Cloud Native Core, Security Edge Protection Proxy - 25K Active Subscribers Perpetual	CCNC-10674	Support for Grafana 7.5.x

Copyright © 2019, 2026, Oracle and/or its affiliates.

Unified Data Repository (UDR)

Release 25.1.202

There are no new features or enhancements made in this release.

Release 25.1.201

There are no new features or enhancements made in this release.

Release 25.1.200

Oracle Communications Cloud Native Core, Unified Data Repository (UDR) 25.1.200 includes the following enhancements:

- **Lifecycle Management (LCM) Based Automation**: This feature optimizes the deployment or upgrade steps. This is achieved by automating service account creation that enables you to create user-defined service account automatically without performing any manual steps. For more information, see the "Lifecycle Management (LCM) Based Automation" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide* and *Oracle Communications Cloud Native Core, Provisioning Gateway Installation Guide*.
- **Support for Export of Policy Data in Comma Separated Value (CSV) Format**: This feature enables the Subscriber Export Tool to export the 5G and 4G subscriber policy data, which includes the profile data and policy data (*am-data, sm-data, and ue-policy-set*) in CSV file format from cnUDR. The converted subscriber data in CSV file format is used by the Subscriber Bulk Import Tool to import the subscriber data along with its policy data on an another instance of cnUDR. For more information, see the "Support for Export of Policy Data in Comma Separated Value (CSV) Format" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.
- **Support for Dual Stack**: With this feature, cnUDR and Provisioning Gateway can be deployed on a dual stack Kubernetes infrastructure. Using the dual stack mechanism, cnUDR and Provisioning Gateway establish and accept connections within pods and services in a Kubernetes cluster using IPv4 or IPv6. For more information, see the "Support for Dual Stack" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide* and *Oracle Communications Cloud Native Core, Provisioning Gateway Installation Guide*.
- **Support for cnDBTier Backup Status APIs in CNC Console**: With this enhancement, UDR can view the cnDBTier backup status, such as the current timestamp, backup in progress, and next scheduled backup using CNC Console. For more information, see the "cnDBTier Backup Status" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.
- **Ingress Gateway Pod Protection Using Rate Limiting**: With this feature, rate limiting mechanism is applied for Ingress Gateway pods. This mechanism allows pods to process a predefined number of requests. When the request rate exceeds the threshold, the pods take action to protect themselves. Depending on the configuration, the pods either reject the additional requests with a custom error code or allows the request. For more information, see the "Ingress Gateway Pod Protection Using Rate Limiting" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.
- **Support for ASM 1.21.6:** UDR 25.1.200 supports Aspen Service Mesh (ASM) 1.21.6 version on Kubernetes 1.27 version from this release. For more information, see the "Configuring UDR to Support Aspen Service Mesh" section in *Oracle Communications*

Copyright © 2019, 2026, Oracle and/or its affiliates.

Cloud Native Core, Unified Data Repository Installation, Upgrade, and Fault Recovery Guide.

The following table lists the license names for feature mapping. For additional licensing information, see *Oracle Communications Cloud Native Core Licensing Information User Manual*.

Table 2-9 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Subscriber Location Function - 25K Active Subscribers Perpetual	CCNC-10117	SLF capacity growth on 23.4.1 (Signalling TPS = 50K ; Provisioning TPS = 1.2K , Sub Cap: 64M)
Oracle Communications Cloud Native Core, Advance Networking - 25K Active Subscribers	CCNC-9467	Support for Dual Stack
Oracle Communications Cloud Native Core, Automated Lifecycle Management - 25K Active Subscribers	CCNC-9151	Lifecycle Management (LCM) Based Automation
Oracle Communications Cloud Native Core, Subscriber Location Function - 25K Active Subscribers Perpetual	CCNC-9133	Support for ASM 1.21.6
Oracle Communications Cloud Native Core, Automated Lifecycle Management - 25K Active Subscribers	CCNC-9094	Lifecycle Management (LCM) Based Automation
Oracle Communications Cloud Native Core, Unified Data Repository - 25K Active Subscribers Perpetual	CCNC-5480	Support for Export of Policy Data in Comma Separated Value (CSV) Format
Oracle Communications Cloud Native Core, Unified Data Repository - 25K Active Subscribers	-	Ingress Gateway Pod Protection Using Rate Limiting

Copyright © 2019, 2026, Oracle and/or its affiliates.

3
Media and Documentation

Media Pack

This section lists the media package for Oracle Communications Cloud Native Core 3.25.1.1xx.0. To download the media package, see MOS.

To learn how to access and download the media package from MOS, see Accessing NF Documents on MOS.

> **Note**
>
> The information provided in this section 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 Oracle Communications Cloud Native Core 3.25.1.1xx.0

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Binding Support Function (BSF)	25.1.101	25.1.100	BSF 25.1.101 supports fresh installation and upgrade from 25.1.100, 24.3.x, and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Binding Support Function (BSF)	25.1.100	25.1.100	BSF 25.1.100 supports fresh installation and upgrade from 24.3.x, 24.2.x, and 23.4.6. For more information, see *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.25.1.1xx.0

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Configuration Console (CNC Console)	25.1.100	NA	CNC Console 25.1.100 supports fresh installation and upgrade from 24.3.x, 24.2.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide.* **Note**: CNC Console supports N-2 NF versions during upgrade window. For example, CNC Console 25.1.100 supports SCP 25.1.100, 24.3.x, and 24.2.x. Any newly added features in Console which have NF dependency in latest release may not be available in previous release. Any newly added features in Console which have NF dependency in latest release may not be available in previous release.
Oracle Communications Cloud Native Core, cnDBTier (cnDBTier)	25.1.103	NA	cnDBTier 25.1.103 supports fresh installation and upgrade from 24.3.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, cnDBTier (cnDBTier)	25.1.102	NA	cnDBTier 25.1.102 supports fresh installation and upgrade from 24.3.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, cnDBTier (cnDBTier)	25.1.101	NA	cnDBTier 25.1.101 supports fresh installation and upgrade from 24.3.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, cnDBTier (cnDBTier)	25.1.100	NA	cnDBTier 25.1.100 supports fresh installation and upgrade from 24.3.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.25.1.1xx.0

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Cloud Native Environment (CNE)	25.1.101	NA	CNE 25.1.101 supports fresh installation and upgrade from 24.3.x and 25.1.100. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Cloud Native Environment (CNE)	25.1.100	NA	CNE 25.1.100 supports fresh installation and upgrade from 24.3.x. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Certificate Management (OCCM)	25.1.100	NA	OCCM 25.1.100 supports fresh installation and upgrade from 24.3.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Certificate Management Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Network Repository Function (NRF)	25.1.100	25.1.100	NRF 25.1.100 supports fresh installation and upgrade from 24.3.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Slice Selection Function (NSSF)	25.1.100	25.1.100	NSSF 25.1.100 supports fresh installation and upgrade from 24.3.x. For more information, see *Oracle Communications Cloud Native Core, Network Slice Selection Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Operations Services Overlay (OSO)	25.1.103	NA	OSO 25.1.103 supports fresh installation and upgrade from 24.3.x and 25.1.1xx. For more information, see *Oracle Communications Cloud Native Core, Operations Services Overlay Installation and Upgrade Guide*.
Oracle Communications Operations Services Overlay (OSO)	25.1.102	NA	OSO 25.1.102 supports fresh installation and upgrade from 24.3.x and 25.1.1xx. For more information, see *Oracle Communications Cloud Native Core, Operations Services Overlay Installation and Upgrade Guide.*

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.25.1.1xx.0

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Operations Services Overlay (OSO)	25.1.101	NA	OSO 25.1.101 supports fresh installation and upgrade from 24.3.x and 25.1.100. For more information, see *Oracle Communications Cloud Native Core, Operations Services Overlay Installation and Upgrade Guide.*
Oracle Communications Operations Services Overlay (OSO)	25.1.100	NA	OSO 25.1.100 supports fresh installation and upgrade from 24.3.x. For more information, see *Oracle Communications Operations Services Overlay Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core, Service Communications Proxy (SCP)	25.1.100	25.1.100	SCP 25.1.100 supports fresh installation and upgrade from 24.3.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	25.1.102	25.1.102	SEPP 25.1.102 supports fresh installation and upgrade from 25.1.1xx, 24.3.x, and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	25.1.101	25.1.102	SEPP 25.1.101 supports fresh installation and upgrade from 25.1.100, 24.3.x, and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	25.1.101	25.1.101	SEPP 25.1.101 supports fresh installation and upgrade from 25.1.100, 24.3.x, and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	25.1.100	25.1.100	SEPP 25.1.100 supports fresh installation and upgrade from 24.3.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide.*

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.25.1.1xx.0

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Unified Data Repository (UDR)	25.1.100	25.1.100	UDR 25.1.100 supports fresh installation and upgrade from 24.3.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Unified Data Repository Installation, Upgrade, and Fault Recovery Guide*.

Cloud Native Core Upgrade

To ensure a smooth and supported upgrade process, follow the upgrade sequence outlined in the table below. Product does not recommend skipping intermediate versions unless explicitly showed:

Figure 3-1 Cloud Native Core Upgrade

Source Releases	Target Releases								
	24.3. x	25.1.1xx	25.1.2xx	25.2.1xx	25.2.2xx	26.1.1xx	26.1.2xx	26.2.1xx	26.2.2xx
24.2. x	Y	Y	NS*	NS	NS	NS	NS	NS	NS
24.3. x	NA	Y	Y	NS	NS	NS	NS	NS	NS
25.1.1xx	NA	NA	Y	NS	NS	NS	NS	NS	NS
25.1.2xx	NA	NA	NA	Y	Y	NS	NS	NS	NS
25.2.1xx	NA	NA	NA	NA	Y	NS	NS	NS	NS
25.2.2xx	NA	NA	NA	NA	NA	Y	Y	NS	NS
26.1.1xx	NA	NA	NA	NA	NA	NA	Y	NS	NS
26.1.2xx	NA	NA	NA	NA	NA	NA	NA	Y	Y
26.2.1xx	NA	NA	NA	NA	NA	NA	NA	NA	Y
26.2.2xx	NA	NA	NA	NA	NA	NA	NA	NA	NA

CNE Upgrade

To ensure a smooth and supported upgrade process, follow the upgrade sequence outlined in the following table:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 3-2 CNE Upgrade

Source Releases	Target Releases								
	24.3. x	25.1.1xx	25.1.2xx	25.2.1xx	25.2.2xx	26.1.1xx	26.1.2xx	26.2.1xx	26.2.2xx
24.2. x	Y	NS	NS	NS	NS	NS	NS	NS	NS
24.3. x	NA	Y	NS	NS	NS	NS	NS	NS	NS
25.1.1xx	NA	NA	Y	NS	NS	NS	NS	NS	NS
25.1.2xx	NA	NA	NA	Y	NS	NS	NS	NS	NS
25.2.1xx	NA	NA	NA	NA	Y	NS	NS	NS	NS
25.2.2xx	NA	NA	NA	NA	NA	Y	NS	NS	NS
26.1.1xx	NA	NA	NA	NA	NA	NA	Y	NS	NS
26.1.2xx	NA	NA	NA	NA	NA	NA	NA	Y	NS
26.2.1xx	NA	NA	NA	NA	NA	NA	NA	NA	Y
26.2.2xx	NA	NA	NA	NA	NA	NA	NA	NA	NA

Compatibility Matrix

The following table lists the compatibility matrix for each network function:

> **Note**
>
> - For seamless integration and optimal performance of CNC NFs on third party platform, the third party platform needs to be compatible with the specified Kubernetes version.

Table 3-2 Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
BSF	25.1.101	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	1.14.6	• 1.31.x • 1.30.x • 1.29.x	25.1.1xx	25.1.1xx	NA	NA
BSF	25.1.100	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	1.14.6	• 1.31.x • 1.30.x • 1.29.x	25.1.1xx	25.1.1xx	25.1.1xx	NA

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
CNC Console	25.1.100	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	• 1.14.6 • 1.11.8 • 1.9.8	• 1.31.x • 1.30.x • 1.29.x	NA	25.1.1xx	25.1.1xx	24.3.x
cnDBTier	25.1.103	• 25.1.1xx • 24.3.x • 24.2.x	NA	NA	NA	• 1.31.x • 1.30.x • 1.29.x	NA	NA	NA	NA
cnDBTier	25.1.102	• 25.1.1xx • 24.3.x • 24.2.x	NA	NA	NA	• 1.31.x • 1.30.x • 1.29.x	NA	NA	NA	NA
cnDBTier	25.1.101	• 25.1.1xx • 24.3.x • 24.2.x	NA	NA	NA	• 1.31.x • 1.30.x • 1.29.x	NA	NA	NA	NA
cnDBTier	25.1.100	• 25.1.1xx • 24.3.x • 24.2.x	NA	NA	NA	• 1.31.x • 1.30.x • 1.29.x	NA	NA	NA	NA
CNE	25.1.100	NA	NA	NA	NA	1.31.x	NA	NA	NA	NA
CNE	25.1.100	NA	NA	NA	NA	1.31.x	NA	NA	NA	NA
NRF	25.1.100	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	1.14.6	• 1.31.x • 1.30.x • 1.29.x	25.1.1xx	25.1.1xx	25.1.1xx	24.3.x

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
NSSF	25.1.100	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	• 1.14.6 • 1.11.8	• 1.31.x • 1.30.x • 1.29.x	25.1.1xx	NA	NA	NA
OCCM	25.1.100	• 25.1.1xx • 24.3.x • 24.2.x	NA	NA	NA	• 1.30.x • 1.29.x • 1.28.x	23.4.x	NA	NA	NA
OSO	25.1.103	NA	NA	NA	NA	• 1.31.x • 1.30.x • 1.29.x	NA	NA	NA	NA
OSO	25.1.102	NA	NA	NA	NA	• 1.31.x • 1.30.x • 1.29.x	NA	NA	NA	NA
OSO	25.1.101	NA	NA	NA	NA	• 1.31.x • 1.30.x • 1.29.x	NA	NA	NA	NA
OSO	25.1.100	NA	NA	NA	NA	• 1.31.x • 1.30.x • 1.29.x	NA	NA	NA	NA
SCP	25.1.100	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	• 1.14.6 • 1.11.8	• 1.31.x • 1.30.x • 1.29.x	25.1.1xx	25.1.1xx	25.1.1xx	24.3.x

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
SEPP	25.1.102	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	25.1.1xx	1.14.6	• 1.31.x • 1.30.x • 1.29.x	25.1.1xx	NA	25.1.1xx	24.3.x
SEPP	25.1.101	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	25.1.1xx	1.14.6	• 1.31.x • 1.30.x • 1.29.x	25.1.1xx	NA	25.1.1xx	24.3.x
SEPP	25.1.100	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	25.1.1xx	1.14.6	• 1.31.x • 1.30.x • 1.29.x	25.1.1xx	NA	25.1.1xx	24.3.x
UDR	25.1.100	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	• 1.1.4.6 • 1.11.8	• 1.31.x • 1.30.x • 1.29.x	25.1.1xx	NA	25.1.1xx	NA

3GPP Compatibility Matrix

The following table lists the 3GPP compatibility matrix for each network function:

Table 3-3 3GPP Compatibility Matrix

CNC NF	NF Version	3GPP
BSF	25.1.101	• 3GPP TS 23.501 v17.7.0 • 3GPP TS 23.502 v17.7 • 3GPP TS 23.503 V17.7 • 3GPP TS 29.500 v17.7.0 • 3GPP TS 29.504 v17.7 • 3GPP TS 29.510 V17.7 • 3GPP TS 29.514 v17.7.0 • 3GPP TS 29.521 V17.7.0 • 3GPP TS 29.214 V17.7.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-3 (Cont.) 3GPP Compatibility Matrix

CNC NF	NF Version	3GPP
BSF	25.1.100	• 3GPP TS 23.501 v17.7.0 • 3GPP TS 23.502 v17.7 • 3GPP TS 23.503 V17.7 • 3GPP TS 29.500 v17.7.0 • 3GPP TS 29.510 v17.7 • 3GPP TS 29.513 V17.7 • 3GPP TS 29.521 v17.7.0 • 3GPP TS 33.501 V17.7.0
CNC Console	25.1.100	NA
cnDBTier	25.1.1xx	NA
cnDBTier	25.1.100	NA
CNE	25.1.1xx	NA
NSSF	25.1.100	• 3GPP TS 29.531 v15.5.0 • 3GPP TS 29.531 v16.5.0 • 3GPP TS 29.531 v16.8.0 • 3GPP TS 29.501 v16.10.0 • 3GPP TS 29.502 v16.10.0
OCCM	25.1.100	• 3GPP TS 33.310-h30 • 3GPP TR 33.876 v.0.3.0
OSO	25.1.1xx	NA
SCP	25.1.100	3GPP TS 29.500 v17.12.0
SEPP	25.1.1xx	• 3GPP TS 23.501 v17.6.0 • 3GPP TS 23.502 v17.6.0 • 3GPP TS 29.500 v17.8.0 • 3GPP TS 29.501 v17.7.0 • 3GPP TS 29.573 v17.6.0 • 3GPP TS 29.510 v17.7.0 • 3GPP TS 33.501 v17.7.0 • 3GPP TS 33.117 v17.1.0 • 3GPP TS 33.210 v17.1.0
UDR	25.1.100	• 3GPP TS 29.505 v15.4.0 • 3GPP TS 29.504 v16.2.0 • 3GPP TS 29.519 v16.2.0 • 3GPP TS 29.511 v17.2.0

> **Note**
>
> Refer to the Compliance Matrix spreadsheet for details on NFs' compliance with each 3GPP version mentioned in this table.

Common Microservices Load Lineup

This section provides information about common microservices and ATS for the specific NF versions in Oracle Communications Cloud Native Core Release 3.25.1xx.0.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-4 Common Microservices Load Lineup for Network Functions

CNC NF	NF Version	Alternate Route Svc	App-Info	ASM Configuration	ATS Framework	Config-Server	Debug-tool	Egress Gateway	Ingress Gateway	Helm Test	Mediation	NRF-Client	Perf-Info
BSF	25.1.101	25.102	25.1.104	25.1.101	25.1.100	25.1.104	25.1.101	25.1.102	25.1.102	25.1.101	NA	25.1.102	25.1.104
BSF	25.1.100	25.1.102	25.1.102	25.1.100	25.1.102	25.1.102	25.1.101	25.1.102	25.1.102	25.1.101	NA	25.1.102	25.1.102
CNC Console	25.1.100	NA	NA	NA	NA	NA	25.1.101	NA	25.1.101	25.1.101	NA	NA	NA
OCCM	25.1.100	NA	NA	NA	NA	NA	25.1.101	NA	NA	25.1.101	NA	NA	NA
NRF	25.1.100	25.1.103	25.1.101	25.1.100	25.1.100	NA	25.1.101	25.1.103	25.1.103	25.1.101	NA	NA	25.1.101
NSSF	25.1.100	25.1.102	25.1.101	25.1.100	25.1.102	25.1.101	25.1.101	25.1.102	25.1.102	25.1.101	NA	25.1.102	25.1.101
SCP	25.1.100	NA	NA	25.1.100	25.1.102	NA	25.1.101	NA	NA	25.1.101	25.1.103	NA	NA
SEPP	25.1.102	25.1.103	25.1.101	25.1.100	25.1.102	25.1.101	25.1.101	25.1.103	25.1.103	25.1.102	25.1.103	25.1.102	25.1.101
SEPP	25.1.101	25.1.103	25.1.101	25.1.100	25.1.102	25.1.101	25.1.101	25.1.103	25.1.103	25.1.102	25.1.103	25.1.102	25.1.101
SEPP	25.1.100	25.1.103	25.1.101	25.1.100	25.1.102	25.1.101	25.1.101	25.1.103	25.1.103	25.1.102	25.1.103	25.1.102	25.1.101
UDR	25.1.100	25.1.102	25.1.101	25.1.100	25.1.102	25.1.101	25.1.101	25.1.102	25.1.102	25.1.102	NA	25.1.102	25.1.101

Generic Open Source Software Compatibility on Any Platform

The following table offers a comprehensive list of software necessary for the proper functioning of an NF during deployment. However, this table is indicative, and the software used may vary based on the customer's specific requirements and solution.

> **Note**
>
> The Software Requirement column in the following table indicates one of the following:
>
> - Mandatory: Absolutely essential; the software cannot function without it.
> - Recommended: Suggested for optimal performance or best practices but not strictly necessary.
> - Conditional: Required only under specific conditions or configurations.
> - Optional: Not essential; can be included based on specific use cases or preferences.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-5 Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.1xx	NF 24.3.x	NF 24.2.x					
Kubernetes	1.31	1.30	1.29.1	Mandatory	Orchestration	Container Orchestration	Mandatory	Kubernetes orchestrates scalable, automated NF deployments for high availability and efficient resource utilization. **Impact**: Preinstallation is required. Without orchestration capabilities, deploying and managing network functions (NFs) can become complex, leading to inefficient resource utilization and potential downtime.
Helm	3.16.2	3.15.2	3.13.2	Mandatory	Management	Kubernetes Package Management	Mandatory	Helm, a package manager, simplifies deploying and managing NFs on Kubernetes with reusable, versioned charts for easy automation and scaling. **Impact**: Preinstallation is required. Not using this capability may result in error-prone and time-consuming management of NF versions and configurations, impacting deployment consistency.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-5 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.1xx	NF 24.3.x	NF 24.2.x					
Podman		4.9.4		Recommended	Runtime	Containerized NF Image Management	Mandatory	Podman manages and runs containerized NFs without requiring a daemon, offering flexibility and compatibility with Kubernetes. **Impact**: Preinstallation is required. Podman is a part of Oracle Linux. Without efficient container management, the development and deployment of NFs could become cumbersome, impacting agility.
containerd	1.7.22	1.7.16	1.7.13	Recommended	Runtime	Container Runtime	Mandatory	Containerd manages container lifecycles for running NFs efficiently in Kubernetes. **Impact**: A lack of a reliable container runtime could lead to performance issues and instability in NF operations.
Velero	1.13.2	1.12.0	1.12.0	Recommended	Backup	Backup and Disaster Recovery for Kubernetes	Optional	Velero backs up and restores Kubernetes clusters for 5G NFs, ensuring data protection and disaster recovery. **Impact**: Without backup and recovery capabilities, customers would risk data loss and extended downtime, requiring a full cluster reinstall in case of failure or upgrade.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-5 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.1xx	NF 24.3.x	NF 24.2.x					
Kyverno	1.12.5	1.12.5	1.9	Recommended	Security	Kubernetes Policy Management	Mandatory	Kyverno is a Kubernetes policy engine that allows to manage and enforce policies for resource configurations within a Kubernetes cluster. **Impact**: Failing to implement policy enforcement could lead to misconfigurations, resulting in security risks and instability in NF operations, affecting reliability.
MetalLB	0.14.4	0.14.4	0.14.4	Recommended	Networking	Load Balancer for Kubernetes	Mandatory	MetalLB provides load balancing and external IP management for 5G NFs in Kubernetes environments. **Impact**: MetalLB is used as LB solution in CNE. LB is mandatory for the solution to work. Without load balancing, traffic distribution among NFs may be inefficient, leading to potential bottlenecks and service degradation.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-5 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.1xx	NF 24.3.x	NF 24.2.x					
HAProxy		3.0.2		Recommended	Networking	Load Balancer / Reverse Proxy	Mandatory	HAProxy provides load balancing and high availability for 5G NFs, ensuring efficient traffic distribution and reliability. **Impact**: HAProxy is used as LB solution in CNE. LB is mandatory for the solution to work. Absense of effective traffic management could result in poor service distribution, impacting NF performance and leading to service interruptions.
CoreDNS	1.11.1	1.11.1	1.10.1	Recommended	Networking	Service Discovery for Kubernetes	Mandatory	CoreDNS is the DNS server in Kubernetes, which provides DNS resolution services within the cluster. **Impact**: DNS is an essential part of deployment. Without proper service discovery, NFs would struggle to communicate with each other, leading to connectivity issues and operational failures.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-5 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.1xx	NF 24.3.x	NF 24.2.x					
Multus	3.8	3.8.0	3.8.0	Recommended	Networking	Networking for Kubernetes traffic segregation	Conditional	Multus enables multiple network interfaces in Kubernetes pods, allowing custom configurations and isolated paths for advanced use cases such as NF deployments, ultimately supporting traffic segregation. **Impact**: Without this capability, connecting NFs to multiple networks could be limited, impacting network performance and isolation.
Fluentd	1.17.1	1.16.2	1.16.2	Recommended	Logging	Logging Agent	Mandatory	Fluentd is an open-source data collector that streamlines data collection and consumption, allowing for improved data utilization and comprehension. **Impact**: Not utilizing centralized logging can hinder the ability to track NF activity and troubleshoot issues effectively, complicating maintenance and support.
OpenSearch	2.11.0	2.11.0	2.11.0	Recommended	Logging	Search/ Analytics / Logging	Mandatory	OpenSearch provides scalable search and analytics for 5G NFs, enabling efficient data exploration and visualization. Lack of a robust analytics solution could lead to challenges in identifying performance issues and optimizing NF operations, affecting overall service quality.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-5 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.1xx	NF 24.3.x	NF 24.2.x					
OpenSearch Dashboard	2.11.0	2.11.0	2.11.0	Recommended	Logging	Dashboard/ Visualization for OpenSearch	Mandatory	OpenSearch Dashboard visualizes and analyzes data for 5G NFs, offering interactive insights and custom reporting. **Impact**: Without visualization capabilities, understanding NF performance metrics and trends would be difficult, limiting informed decision-making.
AlertManager	0.27.0	0.27.0	0.27.0	Recommended	Alerting	Alerting (Integration with Prometheus)	Mandatory	Alertmanager is a component that works in conjunction with Prometheus to manage and dispatch alerts. It handles the routing and notification of alerts to various receivers. **Impact**: Not implementing alerting mechanisms can lead to delayed responses to critical issues, potentially resulting in service outages or degraded performance.
prometheus-kube-state-metric	2.13.0	2.13.0	2.10.1	Recommended	Monitoring	Kubernetes Metrics (for Prometheus)	Mandatory	Kube-state-metrics is a service that generates metrics about the state of various resources in a Kubernetes cluster. It's commonly used for monitoring and alerting purposes. **Impact**: Without these metrics, monitoring the health and performance of NFs could be challenging, making it harder to proactively address issues.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-5 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.1xx	NF 24.3.x	NF 24.2.x					
Prometheus Operator	0.76.0	0.76.0	0.72.0	Recommended	Monitoring	Prometheus Instance Management in Kubernetes	Conditional	The Prometheus Operator is used for managing Prometheus monitoring systems in Kubernetes. Prometheus Operator simplifies the configuration and management of Prometheus instances. **Impact**: Not using this operator could complicate the setup and management of monitoring solutions, increasing the risk of missed performance insights.
prometheus-node-exporter	1.8.2	1.8.2	1.7.0	Recommended	Monitoring	Node-Level Metrics for Prometheus	Mandatory	Node Exporter is a Prometheus exporter for collecting hardware and OS-level metrics from Linux hosts. **Impact**: Without node-level metrics, visibility into infrastructure performance would be limited, complicating the identification of resource bottlenecks.
Prometheus	2.52	2.52	2.51.1	Mandatory	Monitoring	Metrics/ Monitoring System	Mandatory	Prometheus is a popular open-source monitoring and alerting toolkit. It collects and stores metrics from various sources and allows for alerting and querying. **Impact**: Not employing this monitoring solution could result in a lack of visibility into NF performance, making it difficult to troubleshoot issues and optimize resource usage.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-5 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.1xx	NF 24.3.x	NF 24.2.x					
Grafana	9.5.3	9.5.3	9.5.3	Recommended	Visualization	Monitoring/ Visualization Tool	Mandatory	Grafana is a popular open-source platform for monitoring and observability. It provides a user-friendly interface for creating and viewing dashboards based on various data sources. **Impact**: Without visualization tools, interpreting complex metrics and gaining insights into NF performance would be cumbersome, hindering effective management.
Calico	3.28.1	3.27.3	3.26.4	Recommended	Networking	Networking/ Network Security for Kubernetes	Mandatory	Calico provides networking and security for NFs in Kubernetes with scalable, policy-driven connectivity. **Impact**: CNI is mandatory for the functioning of 5G NFs. Without CNI and proper plugin, the network could face security vulnerabilities and inadequate traffic management, impacting the reliability of NF communications
metrics-server	0.7.2	0.7.1	0.6.1	Recommended	Monitoring	Resource Metrics for Kubernetes	Mandatory	Metrics server is used in Kubernetes for collecting resource usage data from pods and nodes. **Impact**: Without resource metrics, auto-scaling and resource optimization would be limited, potentially leading to resource contention or underutilization.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-5 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.1xx	NF 24.3.x	NF 24.2.x					
snmp-notifier	1.5.0	1.4.0	1.4.0	Recommended	Notification	SNMP Notification Service	Mandatory	snmp-notifier sends SNMP alerts for 5G NFs, providing real-time notifications for network events. **Impact**: Without SNMP notifications, proactive monitoring of NF health and performance could be compromised, delaying response to critical issues.
Jaeger	1.60.0	1.60.0	1.52.0	Recommended	Tracing	Distributed Tracing	Mandatory	Jaeger provides distributed tracing for 5G NFs, enabling performance monitoring and troubleshooting across microservices. **Impact**: Not utilizing distributed tracing may hinder the ability to diagnose performance bottlenecks, making it challenging to optimize NF interactions and user experience.
CSI	NA	NA	NA	Mandatory	Storage	Distributed, Orchestrated, and Block Storage	Mandatory	Provides scalable object, block, and file storage, with orchestration capabilities and block storage provisioning for persistent storage in Kubernetes. **Impact**: CSI is mandatory for the functioning of 5G NFs. Without CSI, managing storage could lead to data loss, inefficiencies, and challenges in scaling storage systems effectively.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-5 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.1xx	NF 24.3.x	NF 24.2.x					
ceph	18.2.1	18.2.1		Recommended	Storage	Distributed Storage	Mandatory	The ceph storage system offers scalable object, block, and file storage. It is used in bm CNE solution. **Impact**: Ceph is used in bm OCCNE solution. CSI is mandatory for the solution to work. Not using this distributed storage system would complicate data management, leading to potential data loss and challenges in handling large data volumes effectively.
rook	1.15.2	1.13.3	1.13.3	Recommended	Storage	Storage Orchestration	Mandatory	Rook is the Ceph orchestrator for Kubernetes that provides storage solutions. It is used in bm CNE solution. **Impact**: CSI is mandatory for the solution to work. Not utilizing Rook could increase the complexity of deploying and managing Ceph, making it difficult to scale storage solutions in a Kubernetes environment.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-5 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.1xx	NF 24.3.x	NF 24.2.x					
cinder-csi-plugin	1.31.1	1.30.0	1.29.0	Recommended	Storage	Block Storage Plugin	Mandatory	Cinder CSI (Container Storage Interface) plugin is for provisioning and managing block storage in Kubernetes. It is often used in OpenStack environments to provide persistent storage for containerized applications. **Impact**: Cinder CSI Plugin is used in OpenStack vCNE solution. Without this integration, provisioning block storage for NFs could be manual and inefficient, complicating storage management.

Security Certification Declaration

This section lists the security tests and the corresponding dates of compliance for each network function:

BSF Security Certification Declaration

Release 25.1.101

Table 3-6 BSF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	March 16th, 2026	No unmitigated critical or high findings

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-6 (Cont.) BSF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Feb 17th, 2026	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	March 25th, 2026	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	March 30th, 2026	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Release 25.1.100

Table 3-7 BSF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Apr 1, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Feb 18, 2025	No unmitigated critical or high findings

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-7 (Cont.) BSF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Apr 1, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Apr 7, 2025	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

CNC Console Security Certification Declaration

Release 25.1.100

Table 3-8 CNC Console Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Mar 25, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Apr 2, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Apr 2, 2025	No unmitigated critical or high finding

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-8 (Cont.) CNC Console Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Apr 2, 2025	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

OCCM Security Certification Declaration

Release 25.1.100

Table 3-9 OCCM Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Apr 2, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Apr 2, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Apr 2, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Apr 2, 2025	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Copyright © 2019, 2026, Oracle and/or its affiliates.

NRF Security Certification Declaration

Release 25.1.204

Table 3-10 NRF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Mar 5, 2026	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Mar 5, 2026	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Mar 5, 2026	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Mar 5, 2026	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Release 25.1.203

Table 3-11 NRF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Oct 22, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Oct 22, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Oct 22, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Oct 22, 2025	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Release 25.1.202

Table 3-12 NRF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Sep 25, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Sep 25, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Sep 25, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Sep 25, 2025	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Release 25.1.200

Table 3-13 NRF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Jul 09, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Jul 09, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Jul 09, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Jul 09, 2025	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Copyright © 2019, 2026, Oracle and/or its affiliates.

NSSF Security Certification Declaration

Release 25.1.100

Table 3-14 NSSF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Feb 27, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Feb 27, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Feb 27, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Feb 27, 2025	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

SCP Security Certification Declaration

Release 25.2.102

Table 3-15 SCP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	November 7, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	November 7, 2025	No unmitigated critical or high findings

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-15 (Cont.) SCP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	November 7, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	November 7, 2025	No findings

Release 25.2.101

Table 3-16 SCP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	November 7, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	November 7, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	November 7, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	November 7, 2025	No findings

Release 25.2.100

Table 3-17 SCP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	November 5, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	November 5, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	November 5, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	November 5, 2025	No findings

Overall Summary: No critical or severity 1 security issues were found or pending during internal security testing.

Copyright © 2019, 2026, Oracle and/or its affiliates.

SEPP Security Certification Declaration

Release 25.2.100

Table 3-18 SEPP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	October 27, 2025	No unmitigated critical or high findings. Scan done through Fortify.
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	October 27, 2025	No unmitigated critical, high, medium, and low findings. Scan done through RestFuzz.
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	October 27, 2025	No unmitigated critical or high findings. Scan done through Blackduck.
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	October 27, 2025	No issues found. Scan done through McAfee.

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

UDR Security Certification Declaration

Release 25.2.100

Table 3-19 UDR Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	November 10, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	November 10, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	November 10, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	November 10, 2025	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Documentation Pack

All documents for Oracle Communications Cloud Native Core (CNC) 3.25.2.1xx.0 are available for download on SecureSites and MOS.

To learn how to access and download the documents from SecureSites, see Oracle users or Non-Oracle users.

To learn how to access and download the documentation pack from MOS, see Accessing NF Documents on MOS.

The NWDAF documentation is available on Oracle Help Center (OHC).

Copyright © 2019, 2026, Oracle and/or its affiliates.

4
Resolved and Known Bugs

This chapter lists the resolved and known bugs for Oracle Communications Cloud Native Core release 3.25.1.1xx.0.

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

Service requests for supported Oracle programs may be submitted by you online through Oracle's web-based customer support systems or by telephone. The service request severity level is selected by you and Oracle and should be based on the severity definitions specified below.

Severity 1

Your production use of the supported programs is stopped or so severely impacted that you cannot reasonably continue work. You experience a complete loss of service. The operation is mission critical to the business and the situation is an emergency. A Severity 1 service request has one or more of the following characteristics:

- Data corrupted.
- A critical documented function is not available.
- System hangs indefinitely, causing unacceptable or indefinite delays for resources or response.
- System crashes, and crashes repeatedly after restart attempts.

Reasonable efforts will be made to respond to Severity 1 service requests within one hour. For response efforts associated with Oracle Communications Network Software Premier Support and Oracle Communications Network Software Support & Sustaining Support, please see the Oracle Communications Network Premier & Sustaining Support and Oracle Communications Network Software Support & Sustaining Support sections above.

Except as otherwise specified, Oracle provides 24 hour support for Severity 1 service requests for supported programs (OSS will work 24x7 until the issue is resolved) when you remain actively engaged with OSS working toward resolution of your Severity 1 service request. You must provide OSS with a contact during this 24x7 period, either on site or by phone, to assist with data gathering, testing, and applying fixes. You are requested to propose this severity classification with great care, so that valid Severity 1 situations obtain the necessary resource allocation from Oracle.

Severity 2

You experience a severe loss of service. Important features are unavailable with no acceptable workaround; however, operations can continue in a restricted fashion.

Severity 3

You experience a minor loss of service. The impact is an inconvenience, which may require a workaround to restore functionality.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Severity 4

You request information, an enhancement, or documentation clarification regarding your software but there is no impact on the operation of the software. You experience no loss of service. The result does not impede the operation of a system.

Resolved Bug List

The following Resolved Bugs tables list the bugs that are resolved in Oracle Communications Cloud Native Core Release 3.25.1.1xx.0.

BSF Resolved Bugs

Release 25.1.101

Table 4-1 BSF 25.1.101 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39114782	BSF was not rerouting traffic causing increased Diameter error rates.	BSF-Site1 was connected to three PCF sites (PCF-Site1, PCF-Site2, PCF-Site3). PCF-Site1 is primary site. Because of planned/ unplanned maintenance activities, it was moved to controlled shutdown followed by scaling down all the Diameter Gateway pods, or the Diameter Gateway pods were scaled down without complete shutdown. After this controlled shutdown, BSF-Site1 wasn't able to route Rx AAR-I messages to new alternate PCF sites, whereas AAR-Us/STRs were routed to alternate sites.	2	25.1.100

BSF ATS 25.1.101 Resolved Bugs

There are no ATS resolved issues for BSF 25.1.101.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Release 25.1.100

Table 4-2 BSF 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37291979	Post BSF upgrade Over load congestion	Multiple *3004 Diameter Too Busy* error messages were causing overload congestion alarm. **Doc Impact**: There is no doc impact.	1	23.4.4
37773183	No health request going out from egress GW to scp as expected	There were no health requests going out from Egress Gateway to SCP. **Doc Impact**: There is no doc impact.	2	23.4.4
37155277	Duplicate bindng makes AAR fails with 5012 DIAMETER_UNABLE_TO_COMPLY	Authorization Authentication Request (AAR) failed with *5012 DIAMETER_UNABLE_TO_COMPLY* error message due to duplicate binding. **Doc Impact**: There is no doc impact.	3	24.2.0
37444668	BSF generating SYSTEM_OPERATIONAL_STATE_NORMAL alert	If the system was running in normal state, then `SYSTEM_OPERATIONAL_STATE_NORMAL` alert was getting triggered but it was not getting cleared. **Doc Impact**: There is no doc impact.	3	24.2.1
37508079	BSF REST API incorrect path for Controlled Shutdown	The REST API for controlled shutdown had incorrect path. **Doc Impact**: Updated the REST API path for controlled shutdown. For more information, see "Controlled Shutwown at Ingress and Diameter Gateway" section in *Oracle Communications Cloud Native Core, Binding Support Function REST Specification Guide*.	4	24.2.1

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> Resolved bugs from 24.2.2 have been forward ported to Release 25.1.100.

Table 4-3 BSF ATS 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37312003	Perfinfo_Overload_Manager scenario is failing	The `Perfinfo_Overload_Manager` scenario was failing.	3	24.2.1
37313029	Unexpected ServiceAccount Creation of ATS	There was an unexpected global keyword added in the ATS Helm charts as part of ATS base image integration. As a result, Helm charts were not able to find the custom service account name set in `custom_values.yaml` file.	3	24.3.0

CNC Console Resolved Bugs

Release 25.1.100

Table 4-4 CNC Console 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37486049	Route Path exceeding length for GW metrics	The length for `Route_path` in CNC Console metrics exceeded the limit, which caused the OSO prom-svr to fail after the CNC Console upgrade. **Doc Impact**: There is no doc impact.	2	24.2.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-4 (Cont.) CNC Console 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37496319	Improvements in CNCC upgrade/ rollback procedure	The CNC Console upgrade and rollback procedure needed updates to improve clarity and ensure a better understanding of the process. **Doc Impact**: Updated the procedure in *M-CNCC IAM DB Rollback or Restore* section of *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide.*	2	25.1.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-4 (Cont.) CNC Console 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37486298	CNCC 24.2.1 Installation guide documentation queries	• The cnDBTier note has to be updated to set "ndb_allow_copying_alter_table" to ON during Console deployment. • CNC Console Alert configuration in Prometheus section in *Oracle Communications Cloud Native Configuration Console User Guide* had to be updated to include a note about updating the alert rules file to change the default namespace to the Console deployed namespace. **Doc Impact**: Updated the note about the `ndb_allow_copying_alter_table` parameter in *Configuring Database* section of *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*.	3	24.2.1

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-4 (Cont.) CNC Console 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37468422	CNCC 24.3.0 Metric not displayed for one of the A-CNCC Query due to duplicate RefId	The CNC Console metric dashboard file had a duplicate Reference ID. The dashboard file has to be updated to remove the duplicate Referece ID, making each entry unique. **Doc Impact**: There is no doc impact.	3	24.3.0
37465056	CNCC 24.1.0 CnccIamIngressGatewayServiceDown alert active in aCore deployment	When deploying CNC Console as an aCore only, the `CnccIamIngressGatewayServiceDown` alert was always triggered due to the absence of the IAM pod. **Doc Impact**: Updated the note about the `occncc_agent_alertrules_.yaml` file and e `occncc_manager_alertrules_.yaml` file in *CNC Console Alerts* section of Oracle Communications Cloud Native Configuration Console User Guide.	3	24.1.0
37596832	Wrong MIB file not corresponding SNMP-Notifier sent info in the alert trap towards SNMP server	The wrong MIB file, which did not correspond to the SNMP-Notifier, was sent in the alert trap towards the SNMP server. **Doc Impact**: There is no doc impact.	3	24.2.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-4 (Cont.) CNC Console 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37649019	Avoid printing payload in security logs if its gets too large	Large response payloads were printed in security logs and stored in memory which could have caused OOM (Out of Memory) issues during high loads. **Doc Impact**: There is no doc impact.	3	25.1.100
37316800	CNCC 23.4.1 Helm Chart does not pass Helm Strict linting	The Helm chart did not pass Helm strict linting. The customer ran YAML lint on the Console Helm charts and reported multiple "duplication of key" errors. **Doc Impact**: There is no doc impact.	4	23.4.1
37306647	Upgrading CNCC documentation makes no mention of uploading target version images	The "Upgrading CNC Console" section of the *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide* had to be updated to include the step for uploading the target version images. **Doc Impact**: Updated the procedure in *Upgrading CNC Console* section of *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*.	4	24.3.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> Resolved bugs from 24.3.0 have been forward ported to Release 25.1.100.

cnDBTier Resolved Bugs

Release 25.1.103

Table 4-5 cnDBTier 25.1.103 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38220013	dbtrecover script is affecting db-monitor-svc	A deadlock occurred in the db-monitor-svc during SQL pod restart that caused connection assignment failure, as the monitoring service was unable to assign connections correctly. **Doc Impact**: There is no doc impact.	2	25.1.100
38224168	Update georeplication recovery procedure to remove duplicate steps	Updated the georeplication recovery procedure to remove the duplicated steps. **Doc Impact**: Removed the steps that mention about the creation of NFs during georeplication failure recovery. For more information see the *Restoring Georeplication (GR) Failure* section in Oracle Communications Cloud Native Core cnDBTier Installation, Upgrade, and Fault Recovery Guide.	2	25.1.102

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-5 (Cont.) cnDBTier 25.1.103 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38200832	Schema change distribution is slowing down replication causing data discrepancy across 2 sites	In a multi-site Policy Control Function (PCF) setup, where site 1 (policy1) was completed a PCF application upgrade that included a schema upgrade, and site 2 (policy3) had fallen behind in replication, resulting in data discrepancies. **Doc Impact**: There is no doc impact.	2	25.1.200
37942052	Replication for Site2 and Site3 went down temporarily during the upgrade of CNDB Site1	When ndbmysql-2 and ndbmysqld-3 pods restarted at the same time during an upgrade in a NDB (MySQL Cluster) setup, it lead to data inconsistency. **Doc Impact**: There is no doc impact.	2	24.2.5
37978500	Incorrect key file for table 'SmPolicyAssociation'; try to repair it	The Incorrect key file for table error was encountered for specific tables like Smservice and common configuration tables. It is recommended to always reopen the table with the missing index. **Doc Impact**: There is no doc impact.	2	23.4.6

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-5 (Cont.) cnDBTier 25.1.103 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37668951	The information_schema and table schema is seen to be inconsistent when policy upgrade was performed	During the 2-site policy upgrade, there was an issue with the schema inconsistency, specifically related to the addition of a new column mode and an index in the table occnp_policyds.pds subscriber. **Doc Impact**: There is no doc impact.	2	25.1.200
38245044	Documentation should mention which site to be sourced in dbtremovesite	Updated the cnDBTier documentation for `dbtremovesite` to specify which site should be used as the source. **Doc impact**: Updated the "Removing cnDBTier Cluster" section to specify which site should be used as the source when using dbtremovesite script. For more information, see Oracle Communication Cloud Native Core, cnDBTier User Guide.	4	25.1.200

Note

Resolved bugs from 23.4.7, 24.2.4, and 24.3.1 have been forward ported to release 25.1.103.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Release 25.1.102

Table 4-6 cnDBTier 25.1.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38065663	Table entry mismatch over a 2-site 6-channel ASM setup having pod/ container pre-fix	In a two site, six-channel ASM setup, having pod/ container prefix, the multi channel sqllist was not empty and `ignoredb` and `dodb` databases were updated wrongly in the `my.cnf` file. There was a mismatch in tables & entries across the sites. **Doc Impact**: There is no doc impact.	2	25.1.200
38088870	Georeplication was halted in 25.1.200 with 3 channel, replication, Shutdown task and checksum validation tasks were getting halted occasionally	In a three channel replication setup, during the georeplication process the shutdown task threads were occasionally getting stuck in the `db-replication-svc` service. **Doc Impact**: There is no doc impact.	2	25.1.200
37842445	dbtreplmgr script unable to stop replica on HTTPS and TLS enabled setup	In a 4-site, HTTPS and TLS enabled, backup encryption and password encryption enabled setup, when the `dbtreplmgr` script was run to gracefully stop the replication, the replication did not stop and exited with an error. This was due to the hardcoded HTTP parameter in the script. **Doc Impact**: There is no doc impact.	2	24.2.5

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-6 (Cont.) cnDBTier 25.1.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38197150	Horizontal data pod scaling failed using dbtscale_ndbmtd_pods script and exited with 'Create Nodegroup FAILED" error	In a four site, ASM enabled, backup encrypted and password encrypted setup, the horizontal data pod scaling failed while using the dbtscale_ndbmtd_pods script and exited with 'Create Nodegroup FAILED" error. Users must wait for the new ndbmtd pods to start and assigned with the "no nodegroup" state before creating the node groups. **Doc Impact**: There is no doc impact.	2	25.1.102
38197150	Retry repartitioning of the tables if any data node is down or backup is in progress	While scaling the ndbmtd pods, repartitioning of the tables was unsuccessful. The `dbt_reorg_table_partition` script must be rerun until the tables are repartitioned successfully if any data node is down or backup is in progress. **Doc Impact**: There is no doc impact.	2	25.1.102

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-6 (Cont.) cnDBTier 25.1.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37911174	Doc Changes: Stopping cnDBTier Georeplication Between Sites caused replication outage between all sites	While performing the steps given in the cnDBTier User Guide to stop the cnDBTier while performing georeplication between the sites, was causing replication outage. **Doc Impact**: The "Starting or Stopping cnDBTier Georeplication Service" section was updated to include the following step: • Run the following command to stop the replication service switchover in cnDBTier with respect to siteName: `$ curl -X PUT http://$IP:$PORT/ocdbtier/georeplication/switchover/stop/sitename/{siteName}` For example, run the following command to stop the replication service switchover in cnDBTier with	2	24.2.2

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-6 (Cont.) cnDBTier 25.1.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release

		respect to cluster1:
		
		`$ curl -X PUT http://$IP:$PORT/ocdbtier/georeplication/switchover/stop/sitename/cluster1`
		
		Sample output:
		
		`{`
		
		`"replicationSwitchOver":"stop" }`
		
		For more information about how to start or stop cnDBTier Georeplication service, see *Oracle Communications Cloud Native Core cnDBTier Installation, Upgrade, and Fault Recovery Guide.*		

38204318	Site removal script dbtremovesite is failing with error of script version mismatch on CNDB v25.1.102	While running the `dbtremovesite` site removal script, the script was failing due to the version mismatch. **Doc impact**: There is no doc impact.	2	25.1.102

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-6 (Cont.) cnDBTier 25.1.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38161643	cnDBTier upgrade from 23.4.7 to 25.1.101 failed	cnDBTier upgrade from version 23.4.7 to version 25.1.101 (which was having Webscale version 1.3) was failing because the `kubectl exec` commands did not explicitly specify the container name in Pre/Post upgrade scripts. **Doc Impact**: There is no doc impact.	3	25.1.100
37952176	The metric `db_tier_ndb_backup_in_progress` temporarily shows a value of 1 when a data pod is deleted, even though no backup is actually running on the system	Even though no backup was running on the cnDBTier setup, when a data pod was deleted, the metric `db_tier_ndb_backup_in_progress` temporarily reports a value of 1. **Doc Impact**: There is no doc impact.	3	25.1.100
38077565	Single Stack IPv6 upgrade from 25.1.101 to 25.1.200 pre-upgrade-hooks logs report IPv6 not enabled. Setting LOOPBACK_IP to '127.0.0.1'	In a four site, single-channel cnDBTier setup with IPv6 enabled, when upgrading cnDBTier 25.1.101 to 25.1.200, the pre-upgrade hook incorrectly reported "IPv6 not enabled". **Doc Impact**: There is no doc impact.	3	25.1.200

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-6 (Cont.) cnDBTier 25.1.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37943375	The `dbtscale_vertical_pvc` script doesn't throw any error when wrong charts are provided to the script	The `dbtscale_vertical_pvc` script did not throw an error when wrong charts are provided to the script. The `dbtscale_vertical_pvc` script did not validate the chart version. **Doc Impact**: There is no doc impact.	3	25.1.200
38077638	Helm upgrade from 25.1.101 to 25.1.200 reporting TDE secret changed though it was not altered	While upgrading the helm version from 25.1.101 to 25.1.200, in a four site, single-channel, IPv6 enabled setup, the post-upgrade hooks log reported that TDE secret was changed though it was not altered, however `EncryptedFileSystem` was updated in the values.yaml file that resulted in `ndbmtd` pods to restart with `--initial` option. **Doc Impact**: Added the EncryptedFileSystem flag in the "Rolling Back cnDBTier" section in *Oracle Communication Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*	3	25.1.200

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-6 (Cont.) cnDBTier 25.1.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38144181	Add the additional replication error numbers, 1091 and 1826 to the list of replication errors and remove the error number 1094 from the list	Added the following new error numbers to the list of replication errors: • 1091 (Can't DROP – column/key doesn't exist) • 1826 (Duplicate foreign key constraint name) Removed the error "1094 - Unknown command" from the list. **Doc Impact**: There is no doc impact.	3	23.4.2
38151238	Observed "ERROR 1296: Got error 4009 'Cluster Failure'" during GRR	In a four site, 3-channel, backup encryption enabled cnDBTier setup, during georeplication recovery process the "Cluster Failure" error was observed. This error occurred while running the `dbtrecover` script during the MONITOR_PARALLEL_BACKUP_TRANSFER and MONITOR_PARALLEL_BACKUP_RESTORE phases. **Doc Impact**: There is no doc impact.	4	25.1.200

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-6 (Cont.) cnDBTier 25.1.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37980727	Clarification Required for modifying the https/tls secrets	The section "Certificates to Establish TLS Between Georeplication Sites" in cnDBTier Installation Guide for updating the secrets, did not specify to "Patch" the secret instead of recreating it when the certificate expires or when there is a change in the root CA. The cnDBTier User Guide was updated to add a step to modify SSL/TLS Certificates using the Patch Command Instead of deleting. **Doc Impact**: Updated the section "Certificates to Establish TLS Between Georeplication Sites" to patch the secrets instead of recreating them while establishing TLS between georeplication sites in *Oracle Communication Cloud Native Core, cnDBTier User Guide*.	4	24.2.1

Note

Resolved bugs from 23.4.7, 24.2.4, and 24.3.1 have been forward ported to release 25.1.102.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Release 25.1.101

Table 4-7 cnDBTier 25.1.101 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37807135	`dbtscale_ndbmtd_pods` was not working in release 24.2.5	`dbtscale_ndbmtd_pods` was failing in single-site setup of 24.2.5 as the labels were not present in stateful sets (STS). **Doc Impact**: There is no doc impact.	2	24.2.5
37753846	Vertical scaling of PVC failed while using `dbtscale_vertical_pvc` script	During vertical scaling of Persistent Volume Claim (PVC), the `dbtscale_vertical_pvc` script was failing, because *DBTIER_RELEASE_NAME* was not configured. **Doc Impact**: There is no doc impact.	3	24.2.4
37839960	The `cmp` command was not found in container for which `ndbmtd` pods always perform restart with `--initial` flag	Even when MySQL NDB parameters were not changed, `ndbmtd` pods were restarting with `--initial` flag, because of which the time taken to restart the data nodes had increased. **Doc Impact**: There is no doc impact.	3	25.1.100
37855078	Geo Redundancy Replication was not working in IPv6-enabled cnDBTier deployment	During database replication service deployment, when IPv6 address is configured in the `remotesiteip` configuration, Georedundant Replication (GRR) was not working. **Doc Impact**: There is no doc impact.	3	25.1.100
37789389	`dbtscale_vertical_pvc` script did not work if `ndbdisksize` was in decimal format	`dbtscale_vertical_pvc` script was failing, if `ndbdisksize` value was in decimal format. **Doc Impact**: There is no doc impact.	3	25.1.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-7 (Cont.) cnDBTier 25.1.101 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37909755	Documentation required proper release number to be updated for TDE handling with `--initial` flag	In the "Rolling Back cnDBTier" section, the existing NDB parameters list did not provide the TDE parameter that is required to restart the `ndbmtd` pods with `--initial` flag. **Doc Impact**: There is no doc impact.	3	25.1.100

> **Note**
>
> Resolved bugs from 23.4.7, 24.2.4, and 24.3.1 have been forward ported to release 25.1.101.

Table 4-8 cnDBTier 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37468403	Cluster Failure observed in PCF microservices	Schema synchronization issue in MySQL caused cluster failures in PCF microservices. **Doc Impact**: There is no doc impact.	1	23.4.4
37177542	Correct the value of binlogpurgetimer	The default value of binlogpurgetimer was incorrect in the `custom_values.yaml` file. **Doc Impact**: There is no doc impact.	2	24.3.0
37191116	PCF DBTIER 24.2.1 Install - Error with template	Helm chart template issues caused cnDBTier installation to fail on Helm 3.6.x. **Doc Impact**: There is no doc impact.	2	24.2.1
37217585	Incorrect key file for table errors following DBTier GRR	The dbtrecover script did not have an option to restart the SQL pods after performing a georeplication recovery. **Doc Impact**: There is no doc impact.	2	23.4.4

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-8 (Cont.) cnDBTier 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36615339	cndb ndbmtd-3 pod for site1 and site2 are going into crashloopback after rollback form 24.3.0rc2 to 24.1.1	ndbmtd pods went into the *crashloopback* state after a rollback. **Doc Impact**: There is no doc impact.	2	24.1.0
37077361	Issue being observed in monitoring metrics on 24.3.0; ASM disabled; network policy enabled	DB monitor service had issues with monitoring and fetcing metrics. The following optimizations were performed to resolve this issue: • Thread Pool Management is optimized to resolve issues with metric fetching. • Metric fetching is optimized to prevent multiple database calls for simultaneous requests. **Doc Impact**: There is no doc impact.	2	24.3.0
37214770	Standby replication channel went into FAILED state and didn't recover after restarting one management Dell switch	When adding a site, the system did not insert all records to the DBTIER_INITIAL_BINLOG_POSITION table after scaling ndbmysqld pods. **Doc Impact**: There is no doc impact.	2	23.3.1
37019697	Unable to run recovery using dbtrecover script on a setup deployed with pod and container prefix	Georeplication recovery using `dbtrecover` script did not work on setups that were deployed with pod and container prefix. **Doc Impact**: There is no doc impact.	2	24.3.0
37173763	dbtrecover not marking all down sites as FAILED	The `dbtrecover` script didn't update the status of all failed sites as FAILED. **Doc Impact**: There is no doc impact.	2	24.3.0
37163647	SR recovery issues	Issues were observed during system file maintenance and recovery. **Doc Impact**: There is no doc impact.	2	24.2.1

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-8 (Cont.) cnDBTier 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37294880	dbtrecover script requires hardening to prevent it from using another version's dbtrecover library files	The `dbtrecover` script used dbtrecover library files from other cnDBTier versions. **Doc Impact**: There is no doc impact.	3	23.4.5
36613148	Avoid using occne-cndbtier pattern suggestion for DBTIER namespace examples due to OCCNE log ingestion filters	cnDBTier documents didn't clarify that the occne-cndbtier namespace name used in the documents is a sample namespace name and users must configure the name according to their environment. **Doc Impact**: Notes are added to *Oracle Communications Cloud Native Core, cnDBTier User Guide* and *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide* to state that the namespace names used in the documents are samples and they must be replaced with the actual namespace name. For more information about the notes, see *Oracle Communications Cloud Native Core, cnDBTier User Guide* and *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.	3	23.3.1
37101586	Procedure to update vertical scaling for mgm pod should be documented	*Oracle Communications Cloud Native Core, cnDBTier User Guide* didn't include the procedure to scale the management pods vertically. **Doc Impact**: The procedure to vertically scale the management pods is added to *Oracle Communications Cloud Native Core, cnDBTier User Guide*. For more information about this procedure, see *Oracle Communication, Cloud Native Core, cnDBTier User Guide*.	3	24.2.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-8 (Cont.) cnDBTier 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37175416	Missing Alerts for NDBAPPMYSQLD or NDBMYSQLD	*Oracle Communications Cloud Native Core, cnDBTier User Guide* did not state that `HIGH_CPU` alerts are specific to data nodes. **Doc Impact**: `HIGH_CPU` alert description in the user guide is updated to include this detail. For more information on this alert, see *Oracle Communications Cloud Native Core, cnDBTier User Guide*.	3	23.4.4
37271956	JVM Matrics glitch in Between Execution for Certain Duration	Database monitor service was unable to fetch JVM metrics intermittently. **Doc Impact**: There is no doc impact.	3	24.3.0
37270980	pvc monitor metrics missed on EIR setup	PVC metrics were not supported in cnDBTier 25.1.100, however cnDBTier did not have an option to disable PVC metrics. **Doc Impact**: There is no doc impact.	3	24.3.0
37359397	occndbtier-24.3.0 db-monitor-svc is reporting multiple error logs with Non GR site	Database monitor service reported multiple error logs when there were no ndbmysqld pods in the cluster. **Doc Impact**: There is no doc impact.	3	24.3.0
37091194	DBTier 24.2.1 RestFuzz scan results flagged 500 (1) Response codes	cnDBTier RestFuzz scan displayed 500 error code for the get@/db-tier/purge/epoch/serverids/{serverIds} API. **Doc Impact**: There is no doc impact.	3	24.2.1
37202609	During DBTier upgrade from 24.2.1 to 24.3.0-rc.2 patching of statefulset.apps/ndbappmysqld is skipped due to kyverno validation failed and later not retried from post-upgrade job	cnDBTier did not retry the updateStrategy patch failures during cnDBTier upgrade. **Doc Impact**: There is no doc impact.	3	24.3.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-8 (Cont.) cnDBTier 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37242453	DR failing at state VALIDATERESOURCES and logs do display the reason to the failure	Replication service logs did not capture information about georeplication recovery failures that occurred during the DR_STATE_VALIDATE_RESOURCES state. **Doc Impact**: There is no doc impact.	3	24.3.0
37253044	CNDB OSO Alert file is not appling in OSO 24.3.0 due to the improper structure of the MYSQL_NDB_CLUSTER_DISCONNECT Alert summary and description	cnDBTier OSO alert file was not compatible with OSO due to discrepancies in the `MYSQL_NDB_CLUSTER_DISCONNECT` alert summary and description. **Doc Impact**: There is no doc impact.	3	24.3.0
37273003	Missing metric data on policy SM setup	Metric data were missed intermittently in Policy cnDBTier setup. **Doc Impact**: There is no doc impact.	3	24.3.0
37272556	Error "Removed Meter" observed in db-monitor-svc pod logs of 24.3.0.0.0-rc.8 during EIR traffic run	Meters were not added back after they were removed from the DB monitor service, which was the expected behavious. **Doc Impact**: There is no doc impact.	3	24.3.0
37277299	lost Metrics data/information due to frequent prometheus calls	Metric data was lost due to frequent Prometheous calls. To resolve this issue, the metrics fetching logic in the DB monitor service is optiomized to prevent multiple database calls. **Doc Impact**: There is no doc impact.	3	24.3.0
37281889	The MIB format of dbTier is not compatible with OCCNE MIB definition.	The Management Information Base (MIB) format of cnDBTier was not compatible with the MIB definition in CNE. **Doc Impact**: There is no doc impact.	3	24.3.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-8 (Cont.) cnDBTier 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37078075	cnDBtier "Thread pool did not stop" errors log message	cnDBTier logs had the following unnecessary error message which had to be removed: "Thread pool did not stop". **Doc Impact**: There is no doc impact.	3	22.4.2
37058248	DB Tier metrics are missing for some times from the db-monitor-svc	cnDBTier metrics were missing from the DB monitor service as the system was unable to fetch the metrics from the database. **Doc Impact**: There is no doc impact.	3	24.2.0
37106462	DR not failing at VALIDATERESOURCES when bad site has insufficient CPU	Georeplication recovery did not fail during the VALIDATERESOURCES stage when the failed site did not have sufficient CPU resource. **Doc Impact**: There is no doc impact.	3	24.3.0
37143214	All states of DR not displayed when DR triggered via dbtrecover	cnDBTier didn't display all states of georeplication recovery when the georeplication recovery was triggered using the dbtrecover script. **Doc Impact**: There is no doc impact.	3	24.3.0
37288140	DBTier image versions not updated properly in umbrella values.yaml file for 24.2.2 and 24.3.0 DBTier charts	cnDBTier image versions were incorrect in the `custom_values.yaml` file. **Doc Impact**: There is no doc impact.	3	24.3.0
37278381	DR is stuck and continuously retrying backup due to space issue in ndbmtd backup pvc	Fault recovery got stuck and the system tried to take backup continuously even when there was no space available in the ndbmtd backup PVC. **Doc Impact**: There is no doc impact.	3	24.3.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-8 (Cont.) cnDBTier 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37352523	Cndb tier 23.4 Helm chart does not pass Helm Strict Linting	Duplicate labels were generated for ndbmysqldsvc. As a result, users were unable to deploy cnDBTier Helm charts. **Doc Impact**: There is no doc impact.	3	23.4.4
36142511	Heartbeat status returns 502 error code when accessed via CNDB sub-menu GUI and REST API for NRF	cnDBTier heart beat status API returned "502 Bad Gateway" response code in the ASM environment. **Doc Impact**: There is no doc impact.	3	23.4.0
37404406	DBTier 24.2.1 helm rollback from TLS to non-TLS same version not dropping TLS	Rollback from a TLS enabled version to a non-TLS version failed as the documentation procedure was not followed correctly. **Doc Impact**: There is no doc impact.	3	24.2.1
37365660	cnDBtier 24.2.2 restore database from backup is not restoring the data completely	The `cndbtier_restore.sh` script did not restore the data completely. **Doc Impact**: There is no doc impact.	3	24.2.2
37601066	cnDBTier:24.2.x:snmp MIB Complain from SNMP server	cnDBTier Simple Network Management Protocol (SNMP) MIB file did not support appending .1 in the OID value. **Doc Impact**: There is no doc impact.	3	24.2.0
37663827	cnDbTier 23.4.7 remote server private keys _permission issue	Permission issues were observed in the remote servers when private keys were set with the permission value of 600. **Doc Impact**: There is no doc impact.	3	23.4.6
37649201	Upgrade failed with error serviceaccount "mysql-cluster-upgrade-serviceaccount" not found	cnDBTier upgrade failed with the 'serviceaccount "mysql-cluster-upgrade-serviceaccount" not found' error, even though the service account existed. **Doc Impact**: There is no doc impact.	3	24.2.2

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-8 (Cont.) cnDBTier 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37270980	PVC monitor metrics missed on EIR setup	cnDBTier did not fetch the metrics continuously when running the traffic on the EIR setup. Instead, there was a break or the metric was omitted on Prometheus. **Doc Impact**: There is no doc impact.	3	24.3.0
37049002	Document cache/realtime time api details in DBtier user guide	cnDBTier API documentation didn't state whether the APIs provides real time or cached data. **Doc Impact**: There is no doc impact.	4	23.4.6
37196445	Documentation error in vertical scaling of ndbmgmd procedure	The procedure to scale ndbmgmd pods vertically was incorrect in the user guide. **Doc Impact**: There is no doc impact.	4	24.3.0
37252269	DR error log not clear for VALIDATERESOURCE state	Fault recovery error log did not provide clear information about the VALIDATERESOURCE state. **Doc Impact**: There is no doc impact.	4	24.3.0
37275946	Hikari connection pool warn message observed in db-monitor-svc logs	Hikari connection pool warning messages were observed in DB monitor service and DB replication service. **Doc Impact**: There is no doc impact.	4	24.3.0
37272259	mysql-cluster-replication-svc logs continuous print of "SSLEngineImpl.java:825| Closing outbound of SSLEngine"	Duplicate SSL messages were observed in replication service logs. **Doc Impact**: There is no doc impact.	4	24.3.0
37144276	DBTier 24.2.1 Network policies - Incorrect pod selector for ndbmysqld	Incorrect pod selector was observed for ndbmysqld pods when network policy was enabled. **Doc Impact**: There is no doc impact.	4	24.2.1

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-8 (Cont.) cnDBTier 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37401291	DBTier User Guide Needs update for BACKUP_SIZE_GROWTH alarm from 23.1.0	The backup size limit after which the `BACKUP_SIZE_GROWTH` alert is triggered was incorrectly mentioned as 5% instead of 20% in the *Oracle Communications Cloud Native Core, cnDBTier User Guide*. **Doc Impact**: There is no doc impact.	4	23.1.0
37550094	In Installation Guide at traffic Segregation with CNLB, mention to change siteport 80 to 8080	CNLB traffic segregation documentation did not contain information about the site port numbers. **Doc Impact**: There is no doc impact.	4	24.3.0

> **Note**
>
> Resolved bugs from 23.4.7, 24.2.4, and 24.3.1 have been forward ported to release 25.1.100.

CNE Resolved Bugs

Release 25.1.101

Table 4-9 CNE 25.1.101 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37854450	CNE Version 25.1.100 fails when issued 'kubectl delete pod' command	While deleting a pod, when 'kubectl delete pod' command was issued, CNE installation failed intermittently. This was caused by the delay in Kyverno API response. **Doc Impact**: There is no doc impact.	2	25.1.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-9 (Cont.) CNE 25.1.101 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37869655	CNE Version 25.1.100 fails when issued 'kubectl delete pod' command	In some environments, while trying to delete a pod, deletion command failed due to the delay in the Kyverno API response. **Doc Impact**: There is no doc impact.	2	25.1.100
37799030	CNE installation fails due to missing Velero images	CNE installation failed due to missing Velero build from the source images. **Doc Impact**: There is no doc impact.	3	25.1.100
37842711	CNE installation fails in OL9	In the latest Oracle Linux 9 release, partitions were created differently. However, CNE `cloud_growpart` tasks required specific configuration. This resulted in bastions not having enough space to handle all their dependencies and configuration files leading to CNE installation failure. **Doc Impact**: There is no doc impact.	4	25.1.100

Release 25.1.100

Table 4-10 CNE 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37161841	OCCNE 23.4.1 (LBVM patch 23.4.6) : Security groups are removed from the ports during switchover.	The Load Balancer Controller (`lb-controller`) failed to perform a LBVM switchover when OpenStack compute node hosting the ACTIVE LBVM was shut down. **Doc Impact**: There is no doc impact.	3	• 23.4.1 • 24.3.0 • 24.1.1

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-10 (Cont.) CNE 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36874451	CNE 24.1.0 (Vmware) - OCCNE lb-controller pods stops processing service events or producing logs	The Load Balancer Controller (`lb-controller`) pod was stuck and did not function after getting an exception in the logs. **Doc Impact**: There is no doc impact.	3	24.1.0
37239612	24.2.1 VMware missing egress NAT rules on LBVM	Load Balancer Controller (`lb-controller`) did not install SNAT rules for egress communication. **Doc Impact**: There is no doc impact.	3	24.2.1
37040679	vCNE opnstack upgrade failure with Local DNS enabled due to missing auto plugin config	Upgrade from 23.4.4 failed at the Common Service Upgrade stage due to loss of communication between the cluster and the OpenStack Cloud. This issue was traced back to the Local DNS, which was responsible for OpenStack FQDN resolution. **Doc Impact**: There is no doc impact.	3	24.1.1
37213561	Alerting rules deleted after CNE upgrade	The alerting rules were deleted from NFs after a CNE upgrade. **Doc Impact**: There is no doc impact.	3	24.2.0
37176194	CNE 24.1.1 - Bastion recovery appears to have reset local repo secret, leading to certificate issues	After performing the recovery procedure, Kubernetes reported errors while creating or restarting pods. **Doc Impact**: There is no doc impact.	3	24.1.1

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-10 (Cont.) CNE 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36946610	Repeated OPENSEARCH_DOWN alarms in Prometheus.	`OPENSEARCH_DOWN` alert was triggered with critical severity even when the shards health was yellow (moderate) due to the alert expression. **Doc Impact**: There is no doc impact.	3	23.4.4

> **Note**
>
> Resolved bugs from 24.2.4 and 24.3.2 have been forward ported to Release 25.1.100.

OSO Resolved Bugs

Release 25.1.103

Table 4-11 OSO 25.1.103 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38062402	VNFD has bug double quotes are not correctly defined.	VNFD files had issues. The double quotes were not correctly defined in the files. **Doc Impact**: There is no doc impact.	3	25.1.101
38058360	serverFiles parameter is missing OSO PROM YAML file	The `serverFiles` attribute was missing in `ocoso_csar_25_1_103_0_0_0_prom_custom_values.yaml` file for OSO prometheus. This attribute is used to onboard targets for scraping in prometheus configuration. **Doc Impact**: There is no doc impact.	3	25.1.101

Release 25.1.102

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-12 OSO 25.1.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38028960	unknown field "minReadySeconds" install failure in alert manager	Customer used Webscale 1.3 as an underlying platform, which had Kubernetes v1.20. It is required that all Oracle software should be compatible with Webscale 1.3. **Doc Impact**: There is no document impact.	3	25.1.101
37978275	VNFD was expected to reflect two VNF components but only references a single deployment Helm chart	VNFD files in CSAR package were referenced to a single deployment Helm chart instead of two VNF components for Prometheus and Alertmanager charts. **Doc Impact**: Added the following charts and files in the CSAR package: • `prom_deployment_chart` • `alm_deployment_chart` • `prom_values.yaml` • `alm_values.yaml` For more information, see *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.	3	25.1.100

Release 25.101

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-13 OSO 25.1.101 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37978275	VNFD was expected to reflect two VNF components but only references a single deployment Helm chart	VNFD files in CSAR package were referenced to a single deployment Helm chart instead of two VNF components for Prometheus and Alertmanager charts. **Doc Impact**: Added the following charts and files in the CSAR package: • `prom_deployment_chart` • `alm_deployment_chart` • `prom_values.yaml` • `alm_values.yaml` For more information, see *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.	3	25.1.100

Release 25.1.100

There are no resolved bugs in this release.

Copyright © 2019, 2026, Oracle and/or its affiliates.

NRF Resolved Bugs

Release 25.1.204

Table 4-14 NRF 25.1.204 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38990515	Auditor microservice: `observedGeneration` in the JSON string is not defined in the `V1PodStatus`	The NRF Auditor microservice logged errors when parsing the `observedGeneration` field in the pod status JSON, which is not defined in the Kubernetes `V1PodStatus` schema. This occurred on clusters where there were Kubernetes version discrepancies between CNE and NRF. All pods remained operational despite these log errors. **Doc Impact:** Updated the supported CNE and Kubernetes versions. For more information, see "CNE Requirement" and "Software Requirements" section in *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.	3	25.1.203

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-14 (Cont.) NRF 25.1.204 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38771967	SMF Discovery Request With preferred-tai Answered With preferredTaiMatchInd:false Despite All Match	NRF returned `preferredTaiMatchInd:false` in response to SMF discovery requests containing a matching `preferred-tai`, due to the filter being incorrectly applied only to `SmfInfo` and not to `SmfInfoList`. The logic now assesses both fields, ensuring the flag is correctly set to true if any matched entries are found in the `SmfInfoList`. **Doc Impact**: There is no doc impact.	3	25.1.202

Release 25.1.203

Table 4-15 NRF 25.1.203 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37604778	TLS1.3 Handshake is failing between NRF and SCP	NRF TLS1.3 Handshake failed if the client (SCP) sent session resumption during handshake. **Doc Impact:** There is no doc impact.	3	24.2.3

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-15 (Cont.) NRF 25.1.203 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38179022	Outgoing signalling messages from NRF-egressgateway getting failed while using IPv6 address in SLFHost Configuration	When destination host address is configured as IPv6Address, outgoing signalling messages are failing on Egress Gateway. This is because NRF backend microservices is sending IPv6Address without square brackets. This is applicable to NRF to SLF, NRF to NRF forwarding, NRF Growth and NFStatusNotify use-cases. Before Fix: Host Address configured as IPv6 value signalling message will fail for the use-cases defined. After Fix : Signalling messages will be delivered to IPv6 based host configured for the use-cases defined. **Doc Impact**: There is no doc impact.	3	25.1.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Release 25.1.202

Table 4-16 NRF 25.1.202 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38336947	Unable to configure SLF Options due to missing or null values for `maxSlfAttemptsUpperLimit` and `maxSlfAttemptsLowerLimit`	While configuring the SLF Options, the NRF returned a failure. This occurred when the values for `maxSlfAttemptsUpperLimit` and `maxSlfAttemptsLowerLimit` were set to null. **Doc Impact:** There is no doc impact.	1	24.2.4
38476808	NRF: NF Profile Update with Large SNSSAI is not generating Notifications for Remote Growth Set Subscriptions	When an NFProfile update included a large number of SNSSAIs or other attributes, the NF Subscription microservice to Cache Data microservice query failed due to a header size error. As a result, the NF Subscription microservice reverted to a local database lookup and generated notifications only for local NRF set subscriptions. Consequently, notifications for remote NRF segment subscriptions were not generated for these profile update. **Doc Impact**: There is no doc impact.	2	25.1.201

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-16 (Cont.) NRF 25.1.202 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38373486	NRF growth connectivity broke between set-1 and set-2 in performance setup	With larger payload sizes, NRF Ingress Gateway microservice sends backpressure signal to the upstream, which resulted in latency at Ingress Gateway microservice, even though the backend latency is below 100ms, which caused the original request to timeout and fail. Increased the value of `maxInMemorySize` parameter to fix the issue. **Doc Impact:** For more information, see "Configuring NRF" section in *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.	2	25.1.200

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-16 (Cont.) NRF 25.1.202 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38415299	SLF based discovery requests failing with cause "Internal Server Error"	SLF retries were not handled correctly when error responses were received without a body, resulting in excessive SLF retry attempts. Specifically, upon receiving an SLF response with a `502` status code and no body, the system continued to retry without adhering to an upper limit across the configured hosts. **Doc Impact:** There is no doc impact.	3	25.1.200
38432201	REST API nrf-state-data subscription-details response includes nfProfileDataCount instead of subscriptionDataCount	NRF state data API response contained an incorrect attribute name `nfProfileDataCount` instead of `subscriptionDataCount` for subscription-details response. **Doc Impact:** There is no doc impact.	3	24.2.4

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-16 (Cont.) NRF 25.1.202 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38444392	NRF is returning 200 OK response with empty nfInstances list when SLF and Forwarding are enabled and the discovery request gets forwarded.	When the SLF was not reachable from NRF and both SLF and forwarding features were enabled, NRF1 forwarded the request to NRF2. After forwarding, NRF2 returned a response to NRF1. Regardless of the status of NRF2's response, NRF1 always returned a 200 OK response with an empty `nfInstances` list in the NFDiscover service operation response. As a result, NRF did not send NF profiles in the `200 OK` response, regardless of the actual response status from the forwarded NRF. **Doc Impact:** There is no doc impact.	3	25.1.200

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-16 (Cont.) NRF 25.1.202 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38370654	ERR_UNKNOWN_HOST is mentioned twice in custom yaml under errorCodeProfiles	The `ERR_UNKNOWN_HOST` key was present twice in the `errorCodeProfiles` section of the NRF custom values YAML. This caused NRF to select the wrong value for `ERR_UNKNOWN_HOST`, resulting in incorrect responses and subsequent FT failures. The duplicate entry was removed from `errorCodeProfiles`, ensuring that NRF used only the correct entry for the `ERR_UNKNOWN_HOST` key. **Doc Impact:** There is no doc impact.	3	25.1.201
38103938	log4j2_events_total metric is not getting pegged	The `log4j2_events_total` metric was not being updated in any of the NRF microservices except for NRF Configuration microservice. Consequently, the metric appeared in Prometheus, but its value remained at zero. This led to reduced observability due to a misleading count of log events, showing zero log events even when log events were being emitted. **Doc Impact:** There is no doc impact.	4	25.1.200

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-16 (Cont.) NRF 25.1.202 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36570522	NRF performance - Intermittent failures observed in NFdiscovery operation with Error code 500	Intermittent failures were observed in the NFDiscovery operation, which impacted NRF performance. **Doc Impact:** There is no doc impact.	3	24.1.0
38462967	NRF performs additional reroutes in forwarding and SLF scenarios	NRF performed additional reroutes in discovery forwarding and SLF scenarios when it received error responses without a body. When the NRF discovery service received such responses to forwarding requests, it did not handle them correctly, resulting in the reroute logic being triggered regardless of the `maximumHopCount` configuration. In these error scenarios—such as when the target NRF was unreachable or misconfigured and an error response without a body was received—excessive reroutes and failures occurred. This increased both latency and the number of failures, leading to higher outbound load and potential NF overload. **Doc Impact:** There is no doc impact.	3	25.1.200

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-16 (Cont.) NRF 25.1.202 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38102687	During IGW and Registration service connectivity break, NRF is going to L2 overload state causing 25% discovery traffic failure	In NRF 25.1.200, when connectivity between the Ingress Gateway microservice and Registration microservice was disrupted, NRF entered the L2 overload state, resulting in a 25% failure rate for discovery traffic. SLF retries were not calculated correctly when error responses were received without a body, leading to an excessive number of retries. Specifically, when a 502 error response without a body was received, retries continued across all configured SLF hosts without checking the upper limit. Once all hosts were exhausted, NRF returned a 500 error to the consumer NF. **Doc Impact:** There is no doc impact.	3	25.1.200

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-17 NRF ATS 25.1.202 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38191585	OSO pods running out of memory	During ATS runs, OSO pods encountered out-of-memory (OOM) errors. This was caused by a rapid increase in metrics cardinality, as new nfinstanceId values were continuously generated during each ATS run, leading to excessive memory consumption.	3	24.2.4
38350539	New feature 'SystemOptions52_HBTimerEnhancement_ErrornessInput.feature' is not being executed	The new feature `SystemOptions52_HBTimerEnhancement_ErrornessInput.feature` was not executed individually. The root cause was that the feature file tag did not match the name of the file, preventing the individual execution of this test case	3	25.1.200

Copyright © 2019, 2026, Oracle and/or its affiliates.

Release 25.1.200

Table 4-18 NRF 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37839300	Secondary NRF(e1e2) sending 500 internal server errors towards SMSF when primary NRF w2 is taken OOR	When an NF switched from one NRF to another NRF, and if the NF Profile did not contain the `fqdn` attribute, the NRF processed the NF Profile successfully and saved it in the database. However, before generating the response, the NRF pegged the metric `ocnrf_nf_switch_over_total`, which indicated that the NF had switched over from one NRF to another. This metric had the dimension `NfFqdn`, which corresponded to the `fqdn` in the profile. Since the attribute was not present in the profile, the metric threw an exception and resulted in a Failure Response being generated. **Doc Impact:** There is no doc impact.	1	24.2.3

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-18 (Cont.) NRF 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37912207	Feature Discovery Parameter Value Based Skip SLF Lookup backward compatible	Discovery queries using attributes other than `dnn` were not supported in `valueBasedSkipSlfLookupParams`. When the value-based Skip SLF feature was enabled, using query attributes other than `dnn` led to backward compatibility issues. Support was added to fall back to the older Skip SLF lookup mechanism when the value-based Skip SLF feature was enabled and the query attribute was not `dnn`. **Doc Impact:** There is no doc impact.	2	25.1.100
37912978	SLFOptions configuration not working after upgrade	The `SLFOptions` configuration did not work after the upgrade. The issue was caused by the upgrade logic related to the `SLFOptions` configuration. **Doc Impact:** There is no doc impact.	2	25.1.100
37788289	Discovery query results in Empty Profile when discovery query is forwarded due to AMF profile is Suspended and Empty response received from Forwarded NRF.	During NF profile processing, if a NF profile did not match the `guami` query parameter, NRF did not process the suspended profiles when the EmptyList feature was enabled for AMF. **Doc Impact:** There is no doc impact.	3	24.2.4

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-18 (Cont.) NRF 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37784967	discovery response contains Profile having load value(30) greater then DiscoveryResultLoadThreshold (20)	If the `NFService` load was not present, the `NFProfile` load was not used to perform validation for the `DiscoveryResultLoadThreshold` feature. **Doc Impact**: There is no doc impact.	3	24.2.4
37704295	Discovery requests with preferred-locality return otherLocalityInd attribute as "false" despite non-matched localities.	Discovery requests from consumer NFs that included the `preferred-locality` parameter were returning the `otherLocalityInd` attribute as **"false"**, even when there were non-matching localities among the returned `NFProfiles`. The values of `otherLocalityInd` and `preferredLocalityMatchInd` were set based on both the preferred locations configured in the NRF and the locality attribute present in the discovery query. The values of `otherLocalityInd` and `preferredLocalityMatchInd` were set based **only** on the locality attribute in the discovery query. **Doc Impact:** There is no doc impact.	3	23.4.5

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-18 (Cont.) NRF 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37135700	Delay Nnrf Services - Small Load Condition	NRF did not send `SETTINGS_MAX_CONCURRENT_STREAMS` in the HTTP/2 settings frame. As a result, the client considered the maximum number of concurrent streams to be 1, which caused requests to be queued and eventually time out. Consumers were not able to create concurrent streams to send traffic. NRF sent the `SETTINGS_MAX_CONCURRENT_STREAMS` based on the Helm configuration `serverDefaultSettingsMaxConcurrentStream`, which was set to 1000 by default in version 25.1.200. **Doc Impact:** There is no doc impact.	3	23.4.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-18 (Cont.) NRF 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36989541	The Number of concurrent HTTP2 streams is not limited	NRF did not send `SETTINGS_MAX_CONCURRENT_STREAMS` in the HTTP2 settings frame. Due to this, the client considered the concurrent stream as 1, which causes requests to be queued and times out. **Doc Impact:** This behavior is controlled by the `ingressgateway.serverDefaultSettingsMaxConcurrentStream` parameter. For more information, see "Ingress Gateway Microservice Parameters" in *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide.*	3	23.4.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-18 (Cont.) NRF 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37187942	Incorrect Discovery Response when EmptyList and Forwarding feature enabled together for feature	When the emptyList and forwarding features were enabled, and NRF had profiles matching the target-nf-type in the REGISTERED and SUSPENDED states—but with only the SUSPENDED profiles matching the discovery query—these profiles were not considered while sending the discovery response. Due to this issue, even when there were profiles matching the discovery query in the SUSPENDED state and the emptyList feature was enabled, NRF sent back an empty discovery response. This scenario needed to be handled to send the matching SUSPENDED profiles as part of the emptyList response. **Doc Impact:** There is no doc impact.	3	24.3.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-18 (Cont.) NRF 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38026282	Response code from NRF is coming 400, instead of 500 when the backend services is down.	By default, NRF sent the incorrect error code 400 when the backend service was not available. The error code value was changed to 500 for *Unknown Host Exception* cases in the deployment YAML. Please find the updated configuration below: *name: ERR_UNKNOWN_HOST* *errorCode: 500* *errorCause: "Unknown Host Exception at IGW"* *errorTitle: "Unknown Host Exception"* *errorDescription: "Unknown Host Exception"* **Doc Impact**: There is no doc impact.	3	25..1.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-18 (Cont.) NRF 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37760760	Incorrect ingress gateway port number was whitelisted in NRF network policy's allow-ingress-sbi section for https connections	An incorrect Ingress Gateway port number had been whitelisted in the NRF network policy's `allow-ingress-sbi` section for HTTPS connections. As a result, the NRF network policies did not function as expected, since HTTPS requests to the Ingress Gateway were blocked due to the incorrect port configuration. The NRF network policy custom values YAML was subsequently updated with the correct Ingress Gateway port number for HTTPS connections. The ports should have the values "8081" and "8443". **Doc Impact**: There is no doc impact.	3	24.2.3
35675295	NRF- Missing mandatory "iat claim" parameter validation is not happening in CCA header for feature - CCA Header Validation	NRF was not validating missing mandatory "iat claim" parameter in CCA header. **Doc Impact**: There is no doc impact.	3	23.2.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-18 (Cont.) NRF 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37797310	NFRegistration logs some attributes are showing wrong data	The ThreadContext was not properly cleared after each request. In certain error scenarios, particularly when Input/Output errors occurred while reading the input message the controller method was never reached. As a result, values like nfInstanceID, requestUrl, and so on, were retained from previous requests due to context leakage. **Doc Impact**: There is no doc impact.	4	24.2.4
37417637	Disable/Hide CCA Header Validation Flag (which is not applicable for NRF use case) from NRF CNCC GUI	The "**enabled**" field under CCA Header screen in CNC Console GUI was editable (reason: the "readonly" flag for fields is configured to false by default). The "**enabled**" field flag is read-only now. **Doc Impact**: There is no doc impact.	4	24.2.2

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-18 (Cont.) NRF 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36707560	NRF Rest API "ALL_NF_TYPE" coming back even after deleting in the Discovery Validity Period table	The NRF REST API "ALL_NF_TYPE" reappeared even after it was deleted from the Discovery Validity Period table. On the CNC Console GUI, users observed that in **EDIT** mode, the **SAVE** operation was successful when **DELETE** was attempted to clear the list. However, after saving, the deleted row reappeared, resulting in no effective change. **Doc Impact**: There is no doc impact.	4	24.1.0
35672666	NRF- Incorrect "detail" value in CCA Header Response when missing mandatory "exp/aud claim" for feature - CCA Header Validation	NRF was sending an incorrect message in the `detail` attribute of the `ProblemDetails` field during CCA. **Doc Impact**: There is no doc impact.	4	23.2.0

Note

Resolved bugs from 24.2.4 have been forward ported to Release 25.1.200.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-19 NRF ATS 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37826579	NRF ATS installation is failing on clusters which do not have ASM installed.	NRF ATS installation failed on clusters which do not have ASM installed. The VirtualService resource did not have a flag to enable or disable its creation with respect to the ASM deployment. In clusters where ASM was not installed, the `VirtualService` CRD was not present, caused the ATS installation to fail. The `istio-vs.yaml` was placed under a flag to disable its creation in non-ASM deployments.	2	25.1.100

NSSF Resolved Bugs

Release 25.1.100

Table 4-20 NSSF 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37315559	Can the commonCfgServer configuration be removed from the NSSF CV file?	This issue was related to the presence of a redundant configuration section in the NSSF CV file across multiple microservices. Although the comments in the yaml file indicated that this section should not be modified, the support requested its removal from the default `ocnssf_custom_values.yaml` file for future releases. **Doc Impact**: There is no doc impact.	3	24.2.1

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-20 (Cont.) NSSF 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37223591	Questions - NSSF 24.1.1	There were queries about NSSF's deregistration behavior under various failure scenarios. The support team requested clarification on handling service failures, including Ingress Gateways, Database status, and NS Subscription or NRF Discovery replicas. **Doc Impact**: There is no doc impact.	3	24.1.1
36817980	NSSF is sending Tacrangelist in response for NSAvailability procedure but not created in DB (Auth & Rule table) for NSAvailability procedure.	This issue was related to the NSSF sending a `TacRangeList` in the response for the NSAvailability procedure, even though it was not created in the database. The missing entry caused inconsistencies between the response and stored data. The issue was investigated, and the necessary database updates were implemented to ensure consistency. **Doc Impact**: There is no doc impact.	3	24.2.0
37281954	NSSF is not sending notification request retry with max count configured as httpMaxRetries towards AMF for the error response, flag is enabled.	NSSF was not retrying notifications to the AMF as per the configured httpMaxRetries value. The root cause was incorrect mapping of the Helm parameter in the deployment YAML, preventing changes from taking effect. **Doc Impact**: There is no doc impact.	3	24.3.0
37372023	NSSF ATS 24.3.0: ATS installation failed with PV Enabled for VolumeName.	NSSF ATS 24.3.0 installation failed with Persistent Volume enabled due to a volume name validation issue in the Helm charts. The issue was caused by improper handling of PV configurations. The Helm charts were updated to resolve the problem. **Doc Impact**: There is no doc impact.	3	24.3.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-20 (Cont.) NSSF 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37225956	User guide needs to be updated with NRF client nfProfileList param details.	The NSSF documents were updated to include details about the NRF client `nfProfileList` parameters. **Doc Impact**: Updated *Network Slice Selection Function Installation, Upgrade, and Fault Recovery Guide* and *Oracle Communications Cloud Native Core, Network Slice Selection Function REST Specification Guide* to document the details of Helm and REST API parameters for `nfProfileList`.	3	24.2.1
36817926	Tailist info is not coming in Availability put response while entry has been created in DB in Auth and Rule table for Availability put procedure for white-listed AMF.	The TAI list information was missing in the Availability PUT response, even though an entry had been created in the database (Auth & Rule table) for an allowed AMF. **Doc Impact**: There is no doc impact.	3	24.2.0
37278862	NSSF is not sending notification retry towards AMF when response for first notification was 404 "subscriber not found" and feature flag is false.	NSSF was not retrying the notification to AMF after receiving a 404 "Subscriber Not Found" response when the feature flag was false, aligning with the behavior mentioned in the *Network Slice Selection Function User Guide*. **Doc Impact**: There is no doc impact.	3	24.3.0
37636625	NSSF:24.3.0: Inconsistencies seen when defining NSS rule with tac.	In NSSF 24.3.0, inconsistencies were observed when defining NSS rules with TAC, as the TAC values were not reflected in responses despite being present in the database. However, when using tacRange, no such issue was found. **Doc Impact**: There is no doc impact.	3	24.3.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-20 (Cont.) NSSF 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37717280	NSSF OcnssfOcpmConfigServiceDown Alert - Incorrect Expression.	`OcnssfOcpmConfigServiceDown` alert expression incorrectly used the container dimension in the sum by() function, whereas this metric did not have container as a label. Instead, `app_kubernetes_io_name` should have been used, aligning with other service-down alerts. **Doc Impact**: There is no doc impact.	3	24.2.1
36889943	Traffic moves from site2 to site1, we are getting 404 error code for ns-availability scenarios.	The issue was occurring when traffic was moving from site 2 to site 1 in network slice availability scenarios, resulting in 404 error code. The deployment involved three geographical sites, each handling 3.5K traffic. Despite the replication channel being active, network slice availability data was not synchronizing across all sites as expected, causing request failures. **Doc Impact**: There is no doc impact.	3	24.2.0
37740191	NSSF ATS 25.1.00.rc3, "DNSSRV" feature is randomly failing during ATS run.	DNSSRV feature was failing randomly due to an inconsistency in the `nrfclient_nrf_operative_status` metric validation. The expected count for the service was 1, but the actual count was 0, leading to validation failure. **Doc Impact**: There is no doc impact.	3	24.2.1

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-20 (Cont.) NSSF 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37651423	Subscribe Service Operation error pointing to missing supportedFeatures.	The Network Slice Selection Function was responding with a 400 "BAD_REQUEST" error during the Subscribe Service Operation for the `nnssf-nssaiavailability` service in the customer environment. The error was being caused by a missing supportedFeatures attribute, leading to a NullPointerException during subscription data parsing. According to 3GPP TS 29531, supportedFeatures is a conditional attribute required if any optional features are supported. The error occurred only when duplicate nssai_subscriptions were present in the Database. **Doc Impact**: There is no doc impact.	3	24.3.0
37323951	Prometheus URL comment should be mentioned overload and LCI/OCI feature in NSSF CV file.	The comment for the Prometheus URL in the `ocnssf_custom_values.yaml` file only mentioned its necessity for the Load Control Indicator/Overload Control Indicator feature. However, the URL was also mandatory for the overload feature. Without the correct Prometheus URL, the overload feature was not functioning as expected. **Doc Impact**: There is no doc impact.	4	24.3.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-20 (Cont.) NSSF 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37101322	Ephemeral storage of the NSSF deployment is displayed in NSSF Custom Yaml, however it is not displayed when describing the deployment.	The ephemeral storage configuration was present in the `ocnssf_custom_values.yaml` and Helm values but was not reflected when describing the deployment. This was due to missing parameters (logStorage, crictlStorage, and ephemeralStorageLimit) in the custom values file. Without these parameters, the default value was set to 0, disabling ephemeral storage. **Doc Impact**: There is no doc impact.	4	24.3.0
37037110	OCNSSF: averageCpuUtil Parameter missing from Custom Yaml.	The `averageCpuUtil` parameter was missing from the `ocnssf_custom_values.yaml` file, leading to failures in updating the Horizontal Pod Autoscaler (HPA) limits. **Doc Impact**: The details of averageCpuUtil parameter were also updated in the "Customizing NSSF" chapter of the *Network Slice Selection Function Installation, Upgrade, and Fault Recovery Guide.*	4	24.2.0
37270555	Incorrect NF name (NRF instead of NSSF) specified in custom yaml.	Incorrect Network Function name ("NRF" instead of "NSSF") was specified in the `ocnssf_custom_values.yaml` file. This mislabeling appeared in the HTTPS/2.0 configuration comments for the Ingress Gateway. **Doc Impact**: There is no doc impact.	4	24.3.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-20 (Cont.) NSSF 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37277288	Statistics name need to be correct in user guide 24.3.0.	The metric name in the Cloud Native Core, Network Slice Selection Function User Guide was incorrectly documented as `ocnssf_nssaiavailability_notification_delete_on_subscription_not_found` instead of `ocnssf_nssaiavailability_notification_delete_on_subscription_not_found_total`, as seen in Grafana. **Doc Impact**: The name of the metric was updated in the *Network Slice Selection Function User Guide* in the relevent sections.	4	24.3.0
37308075	Counter description needs to be documented.	The description for the `Subscription_removed` dimension was missing in the *Network Slice Selection Function User Guide*. **Doc Impact**: The description for the `Subscription_removed` dimension was added in the *Network Slice Selection Function User Guide.*	4	24.3.0

OCCM Resolved Bugs

Release 25.1.100

Table 4-21 OCCM 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37779808	Incorrect alert expression in alert OccmMemoryUsageMinorThreshold	An alert was raised due to incorrect alert expression.	3	24.2.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-21 (Cont.) OCCM 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37436671	OCCM 24.3 user guide errors for occm_cert_request_status_total metric and OID 1.3.6.1.4.1.323.5.3.54.1.2.7012	The OID number for `occm_cert_request_status_total` metric was incorrect in the *Oracle Communications Cloud Native Core, Certificate Management User Guide*.	4	24.3.0

> **Note**
>
> Resolved bugs from 24.3.0 have been forward ported to Release 25.1.100.

SCP Resolved Bugs

Release 25.1.203

Table 4-22 SCP 25.1.203 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39072215	High CPU Utilization Observed on Load Manager reached upto 98% at 1200 NF Profiles (730K MPS)	While the traffic was run at 730K MPS with 1200 NF profiles and sent 80 to 100 notifications per second for at least 12 hours, Load Manager CPU utilization reached 98% and the load-manager microservice logged an error continuously. **Doc Impact**: There is no doc impact.	2	25.1.200
38895958	SCP forwarding single header even when multiple headers are present with same header name	SCP consolidated two 3gpp-sbi-binding headers sent by SMSF down to one header when AMF received the request. **Doc Impact**: There is no doc impact.	2	25.1.200
38666287	ArrayIndexOutOfBound Exception observed in traffic run	After enabling Model D and Mediation, SCP-Worker continuously logged TLS, Jetty, and Micronaut exceptions. **Doc Impact**: There is no doc impact.	3	25.1.200

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-22 (Cont.) SCP 25.1.203 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38676349	Page not found exception observed in configuration pod	After upgrading SCP from 25.1.100 to 25.2.100, scrolling errors were logged every 12 to 14 minutes for the occ1-mudflap-ocscp-scpc-configuration-7d98dddc59-qlrkv pod when the log level was set to INFO. **Doc Impact**: There is no doc impact.	3	25.1.200
38736605	Worker not sending any response back to consumer if no foreign SCP is found service foreign producer.	SCP-Worker did not send any response back to the consumer NF when no foreign SCP was found for the foreign producer. **Doc Impact**: There is no doc impact.	3	25.1.200
38711265	Not able to do any configuration changes in CNCC SCP GUI	When cnDBTier, CNC Console, and SCP were deployed in an IPv6 only environment, the CNC Console displayed only SCP information, and configuration changes could not be made. **Doc Impact**: There is no doc impact.	3	25.1.201
38896281	Unable to route when port definition is missing from NFServices in NF Profile using only FQDN	When an NF profile contained only an FQDN with no IP address or port, SCP did not route traffic correctly over TLS with the HTTPS scheme. **Doc Impact**: There is no doc impact.	3	24.2.6
38923076	SCP creates routing rules for NRF with incorrect FQDN format where MNC has 2 digits	In the R16 release, SCP routing rule configuration incorrectly generated a two-digit MNC in the FQDN for a PLMN ID, instead of using the required three-digit format for the 5G domain. **Doc Impact**: There is no doc impact.	3	24.2.6
38943409	SCP tampering with HTTP2 body in message feed	SCP sent a modified message body to Data Director instead of the exact body that it received, which caused the Content-Length value to not match the actual body length. **Doc Impact**: There is no doc impact.	3	25.1.200
39008940	TTMELAB STAGE-3 | SCP0015 WS1.5 Regression fail during nightly runs	Multiple SCP ATS test cases failed over the last few days, and the NF pod logs were not available at the time of failure. **Doc Impact**: There is no doc impact.	3	25.1.200

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-22 (Cont.) SCP 25.1.203 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38972143	SCP does not get registered with NRF (java.lang.IllegalArgumentException in Subscription pod))	Although all pods were running, and SCP received notifications from NRF, SCP was not registered with NRF. **Doc Impact**: There is no doc impact.	3	25.1.202
38751557	Every SCP Audit, picks up NRF profile for de-register event and SCP's self profile as change event to have trigger towards notification, which later gets ignored at notification	During each SCP audit, the audit process selected an NRF profile for a de-registration event and SCP's self profile for a change event, which triggered notifications that were later ignored. **Doc Impact**: There is no doc impact.	4	25.1.200
38746228	OpenAPI file is not generated correctly in SCP package	The configuration pod generated an OpenAPI file (OCSCP-Configuration-OpenAPI.json) during the CICD process, but the file was empty because the output path was not enabled. **Doc Impact**: There is no doc impact.	4	25.1.200

> **Note**
>
> Resolved bugs from 24.2.4, 24.3.0, and 25.1.100 have been forward ported to Release 25.1.203.

Table 4-23 SCP ATS 25.1.203 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38702138	ATS Framework fails to handle uri formation with bracket for ipv6 of worker pod IP	After deploying SCP, ATS, cnDBTier, and CNC Console on an IPv6 environment, two test cases failed with a parse error while fetching metrics from the Prometheus. **Doc Impact**: There is no doc impact.	3	25.1.201

Copyright © 2019, 2026, Oracle and/or its affiliates.

Release 25.1.202

Table 4-24 SCP 25.1.202 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38692824	SCP used to accept a non standard health request for a success response, path validation of health request was not proper	In earlier releases of SCP, the response was the default response for the OPTIONS method (200 OK default response even if the path URI does not match is not through SCP application logic). It was the underlying Spring Boot behavior to respond with 200 OK as the default response. In the later release, there is a strict match for the path irrespective of the method. This difference is part of SCP's transition from Spring Boot to Micronaut. **Doc Impact**: There is no doc impact.	2	25.1.100
38552864	Mediation updates on discovery headers is not considered in the SbiDiscovery request creation	SCP did not consider the newly added or updated 3gpp-Sbi-Discovery-preferred-locality header from the mediation service when sending requests to NRF. **Doc Impact**: There is no doc impact.	2	25.1.200
38152282	SCP continues to use old certificates even after patching secrets with new certificates	SCP continued to use old certificates even after patching secrets with new certificates. SslProviderObject had previously been available in Reactor Netty to handle H2, TCP, and NONE configurations, but Micronaut Netty did not offer a direct alternative. **Doc Impact**: There is no doc impact.	3	25.1.200
38552625	Check applied certificate before primary certificate reload on SSL config details SSE for 25.1.2x-patch	When an SSL configuration details SSE was received, the system reloaded the primary server certificate, which was incorrect. It should have first checked the applied certificate and reloaded the same certificate. **Doc Impact**: There is no doc impact.	3	25.2.100
38552644	Fix TLS certificate reload issues for 25.1.200	When the primary server certificate had expired and the scp-worker pod was restarted, it continued to use the expired primary server certificate.	3	25.1.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-24 (Cont.) SCP 25.1.202 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38553536	ocscp_worker_egress_res_total Metric not getting pegged	The ocscp_worker_egress_res_total metric was not updated for responses from SCP. **Doc Impact**: There is no doc impact.	3	25.1.200
38553016	SCP generated timestamp sent to kafka without padding for nanoseconds	SCP was sending messages to Kafka with timestamps that lacked proper padding for nanoseconds, resulting in Kafka interpreting the sequence of messages incorrectly. **Doc Impact**: There is no doc impact.	3	24.2.5
38552977	DNSSRV based alternate routing not working for static configuration	DNS SRV-based alternate routing did not work for static configuration when the apiRoot header was present. **Doc Impact**: There is no doc impact.	3	25.2.100
38471728	Accept header added by SCP if it´s not in the original request	SCP added the header Accept: application/json to an outbound request when the original request from the NF Consumer did not include an Accept header, and the NF Producer rejected the request because it only supported Accept: application/problem+json or no Accept header. In earlier releases, SCP did not add an Accept header when the original request did not have. **Doc Impact**: There is no doc impact.	3	25.1.201
38553599	Pseudo header values are not being taken in request Ingress mediation trigger point	The Pseudo header values were not considered in the request ingress mediation trigger point rules. The acceptance criteria required that pseudo header values were considered in these rules when present. **Doc Impact**: There is no doc impact.	3	25.2.100
38543550	SCP rejecting profiles due to canaryReleaseConfigName	SCP rejected profiles when an incorrect canaryReleaseConfigName was configured. **Doc Impact**: There is no doc impact.	3	25.1.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-24 (Cont.) SCP 25.1.202 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38552843	SCP Errors generated during the upgrade from 25.1.100 to 25.1.200 are not captured in the ocscp_metric_scp_generated_response_total metrics	During the upgrade from SCP 25.1.100 to 25.1.200, SCP errors were not recorded in the ocscp_metric_scp_generated_response_total metric. **Doc Impact**: There is no doc impact.	3	25.1.200
38552894	Rate Limit Service Initialization Flag Correction	In rare scenarios, the `BucketProxy` variable was not initialized with appropriate value when an SCP-worker pod comes up, causing ingress rate limiting rules to fail and returning an internal server error to the consumer NF. **Doc Impact**: There is no doc impact.	3	24.2.5
38553620	DD client stub running with debug logs enabled	The DDClient stub was configured with DEBUG as the default log level instead of INFO. **Doc Impact**: There is no doc impact.	4	25.1.200

> **Note**
>
> Resolved bugs from 24.2.4, 24.3.0, and 25.1.100 have been forward ported to Release 25.1.202.

Table 4-25 SCP ATS 25.1.202 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38553659	Timeout for request to promethues is missing in ATS	The Prometheus client did not consider request timeouts, and when Prometheus did not respond, ATS remained stuck indefinitely. With timeouts configured for Prometheus requests, ATS did not remain stuck. **Doc Impact**: There is no doc impact.	4	25.1.200

Copyright © 2019, 2026, Oracle and/or its affiliates.

Release 25.1.201

Table 4-26 SCP 25.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38284085	SCP 25.1.200 Notification throwing NF_RULE_PROCESSOR_FAILURE for all NFs except UDR	While testing SCP 25.1.200, it was observed that routing rules for four test UDR profiles were processed and updated successfully. However, all other NF profiles were rejected, resulting in the following exception: "message":"Category: NF_RULE_PROCESSOR_FAILURE, Event: RULE_PROCESSOR_MISCELLANEOUS, EventId: OSCP-NTF-RULPRC-EV001" **Doc Impact**: There is no doc impact.	2	25.1.200
38206028	Error while trying to Upgrade SCP from 25.1.100 to 25.1.200 and on fresh install of 25.1.200	The following error was observed while upgrading SCP from 25.1.100 to 25.1.200: INSTALLATION FAILED: YAML parse error on ocscp/charts/scpc-configuration/templates/configuration.yaml: error converting helm.go:84: [debug] error converting YAML to JSON: yaml: line 19: did not find expected key YAML parse error on ocscp/charts/scpc-configuration/templates/configuration.yaml **Doc Impact**: There is no doc impact.	3	25.1.200
38318190	SCP 25.1.200 ModelD AUSF discovery failure: getAusfInfo() is null	During service discovery of the nausf-auth service for NRF, the AUSF profile was sent by NRF in the response. However, SCP encountered a 500 error because the Ausfinfo header was missing from the response. **Doc Impact**: There is no doc impact.	3	25.1.200

> **Note**
>
> Resolved bugs from 24.2.4, 24.3.0, and 25.1.100 have been forward ported to Release 25.1.201.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-27 SCP ATS 25.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38328447	Metric "ocscp_metric_nf_lci_tx_total" at times does not get validated if scp is not enabled to decode consumer on the basis of XFCC header and response from producer having LCI gets conveyed to Consumer NF	The ocscp_metric_nf_lci_tx_total metric was not consistently validated when SCP was not enabled to decode the consumer based on the XFCC header. As a result, responses from the producer NF containing LCI were incorrectly conveyed to the consumer NF. **Doc Impact**: There is no doc impact.	3	25.2.100

Release 25.1.200

Table 4-28 SCP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37838652	SCP unable to send requests when maxStreamId is reached on a connection	SCP was unable to send requests when the stream ID reached its maximum value. **Doc Impact**: There is no doc impact.	2	25.1.100
37942341	SCP is erroneously routing inter-SCP traffic to other SCP instances within the same region.	SCP generated inter-SCP routing rules for instances that were located within the same region. **Doc Impact**: There is no doc impact.	2	25.1.100
38120012	SCP internal traffic sent to OCNADD despite fix for BUG 37226666 delivered in 24.2.2	The internal traffic from SCP 24.2.4 was incorrectly routed to OCNADD, even though a fix for this issue was provided in SCP 24.2.2. **Doc Impact**: There is no doc impact.	3	24.2.2
38012554	SCP/ ATS_25.1.100_Full_Regression_Failure_0252925	In SCP-ATS 25.1.100, a complete regression test failed with error codes. **Doc Impact**: There is no doc impact.	3	25.1.100
37931177	Notifications {"title":"Loop Detected","status":508" }	In SCP 25.1.100, notifications with the title "Loop Detected" and status code 508 were incorrectly generated. **Doc Impact**: There is no doc impact.	3	25.1.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-28 (Cont.) SCP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37859976	SCP is showing 504 errors for peer SCPs in the egress response metrics which excludes ocscp-initiated messages	SCP generated 504 errors when the peer SCP was unreachable and the destination route was exhausted. **Doc Impact**: There is no doc impact.	3	25.1.100
37843293	SCPMediationConnectivityFailure alerts are active even the connectivity is fine toward mediation	SCPMediationConnectivityFailure alerts were previously active despite confirmed connectivity toward Mediation. **Doc Impact**: There is no doc impact.	3	24.2.2
37840642	'DBOperation Failed: Failed to get ServiceEntry' exception was observed on the notification pod within the SCP	During a traffic run at the rate of 730K MPS with 700 NF profiles, a 'DBOperation failed to get service entry' exception occurred on the SCP. The setup included 7 SCP triplets in each region. **Doc Impact**: There is no doc impact.	3	25.1.100
37840553	A warning concerning an 'empty version map' was observed while running traffic at a rate of 730K MPS using a 700 NF profile.	While running traffic at a rate of 730K MPS using 700 NF profiles, a warning about an "empty version map" was observed. **Doc Impact**: There is no doc impact.	3	25.1.100
37815522	SCP Provides Grafana wrong Metric in Prometheus CPU utilization and Prometheus memory utilization	SCP provided incorrect metrics to Grafana for Prometheus CPU utilization and Prometheus memory utilization. **Doc Impact**: There is no doc impact.	3	24.2.2
37775369	SCPProducerNfSetUnhealthy Alert not getting raised	The `SCPProducerNfSetUnhealthy` alert was not raised. **Doc Impact**: There is no doc impact.	3	25.1.100
37746963	SCP Worker pod generating high Kube API traffic	In SCP 24.2.2, the SCP-Worker pod generated high Kubernetes API traffic. **Doc Impact**: There is no doc impact.	3	24.2.2

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-28 (Cont.) SCP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37721950	Getting IP instead of FQDN in peerscpfqdn dimension of SCPUnhealthyPeerSCPDetected Alert	The `peerscpfqdn` dimension of the `SCPUnhealthyPeerSCPDetected` alert displayed an IP address instead of FQDN. **Doc Impact**: There is no doc impact.	3	25.1.100
37721565	If SCP received request message with 3gpp-Sbi-Client-Credentials header with x5u - X.509 URL, then SCP should passthrough without CCA validation and should not reject the request message.	When SCP received a request message containing the 3gpp-Sbi-Client-Credentials header with an x5u (X.509 URL), it incorrectly rejected the message instead of bypassing CCA validation and processing the request. **Doc Impact**: There is no doc impact.	3	25.1.100
37713112	LCI and OCI not having validation for timestamp header causing nullPointerException leading to failure in responding to the consumer	LCI and OCI lacked validation for the timestamp header, which resulted in `NullPointerException`. This issue caused failures in responding to consumer NFs. **Doc Impact**: There is no doc impact.	3	25.1.100
37700589	SCP Notification pod restarted while sending invalid notification requests at a higher rate around 2K TPS	The SCP-Notification pod restarted when sending invalid notification requests at a high rate, approximately 2K TPS. **Doc Impact**: There is no doc impact.	3	25.1.100
37693288	SCP does not make NF rule profile for the de-registered NF on Last NF De-registration	SCP did not make NF rule profile for the de-registered NF on the last NF de-registration. **Doc Impact**: There is no doc impact.	3	24.3.0
37657153	Configuration pod crash was noticed on SCP when traffic was flowing at 730K MPS (signaling) and 1K TPS (control plane) GET requests to retrieve the ingress rate limit configuration	The configuration pod restarted in SCP when handling traffic at 730K MPS (signaling) and 1K TPS (control plane). This occurred during GET requests to retrieve the ingress rate limit configuration. **Doc Impact**: There is no doc impact.	3	25.1.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-28 (Cont.) SCP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37640874	SCP Metrics and dimensioning questions	Discrepancies related to metric dimensions and descriptions were observed in SCP 24.3.0. **Doc impact**: Updated the descriptions of the `ocscp_nf_end_point` dimension and the `ocscp_nrf_notifications_requests_nf_total` metric in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	3	24.3.0
37640288	SCP Possibility to create subscriptions using the fqdn for TLS purpose	In the SCP implementation with NRF using TLS, notifications were not being received. This issue occurred because subscriptions were created using the IP address instead of the Fully Qualified Domain Name (FQDN), which was required by the NRF verification process. **Doc Impact**: There is no doc impact.	3	24.2.2
37634513	DiscardWithErrorRspCount parameter needs to be corrected in worker logs.	The `DiscardWithErrorRspCount` parameter in worker logs was incorrectly recorded. **Doc Impact**: There is no doc impact.	3	25.1.100
37632229	SBI Message Priority Rest API does not allow nftype as query parameter & PUT operation on existing rule is not allowed for change in scope of method array list	The SBI Message Priority REST API did not support `nftype` as a query parameter. Additionally, the PUT operation on an existing rule was not permitted when attempted to modify the scope of the method array list. **Doc Impact**: There is no doc impact.	3	25.1.100
37565543	SCP Alert triggered SCPEgressTrafficRoutedWithoutRateLimitTreatment without ERL enabled	In SCP 24.2.1, an alert for SCPEgressTrafficRoutedWithoutRateLimitTreatment was triggered, even though Egress Rate Limiting was not enabled. **Doc Impact**: There is no doc impact.	3	24.2.1

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-28 (Cont.) SCP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37439576	API Missing Validation for Mandatory Parameter: "enabled"	When a PUT request was made to the scp-features REST API, SCP did not return an error if the mandatory "enabled" parameter was missing. **Doc Impact**: There is no doc impact.	3	25.1.100
37428245	scp does not show profile details for NF-TYPE= SCP under edit profile option	When editing a profile for NF-TYPE=SCP, SCP did not display the profile details. **Doc Impact**: There is no doc impact.	3	25.1.100
37428201	scp returns misleading error when editing static nrf profiles	When editing static NRF profiles, SCP returned a misleading error message. **Doc Impact**: There is no doc impact.	3	25.1.100
37426620	SCP scp-subscription pod is generating WARN messages with "{Response is Successful but NO BODY found}"	In SCP 24.2.1, the SCP-Subscription pod generated WARN messages {Response is Successful but NO BODY found}". **Doc Impact**: There is no doc impact.	3	24.2.1
37407917	"Max Retry Attempts field" is saved as zero value in Routing options of Mediation tab.	When saving routing options in the Mediation tab, the "Max Retry Attempts" field was stored as a zero value, even if a different value was entered. **Doc Impact**: There is no doc impact.	3	25.1.100
36173358	SCP Unable to forward notification requests when request is received with FQDN at profile level and DNS is not configured to resolve the FQDN.	When a notification request was received with a Fully Qualified Domain Name (FQDN) at the profile level and the DNS was not configured to resolve the FQDN, SCP was unable to forward the request. **Doc Impact**: There is no doc impact.	3	23.3.0
38157537	SCP notification pod in CrashLoopBackOff state after OCCNE upgrade from 24.2.3 to 24.2.6	After upgrading CNE from 24.2.3 to 24.2.6, SCP-Notification pod entered a CrashLoopBackOff state, despite functioning correctly before the upgrade. **Doc Impact**: There is no doc impact.	3	24.2.3

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-28 (Cont.) SCP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38157409	SCP Worker pod continuous restarts due to Traffic Feed stackTrace java.lang.StringIndexOutOfBoundsException: begin 7, end 4	The SCP-Worker pod continuously restarted due to a Traffic Feed stack trace error, specifically a `java.lang.StringIndexOutOfBoundsException` with begin index 7 and end index 4. **Doc Impact**: There is no doc impact.	3	24.2.3
38143198	SCP not allowing to edit NRF record in NRF SRV configuration	SCP did not allow to edit NRF record in the NRF SRV configuration. **Doc Impact**: There is no doc impact.	3	25.1.100
38116473	Enhancement in metric ocscp_metric_scp_generated_response_total to get pegged for timeout and connection error from mediation ms.	The `ocscp_metric_scp_generated_response_total` metric did not accurately reflect timeout and connection errors from the mediation service, leading to incomplete data representation. **Doc Impact**: There is no doc impact.	3	24.2.0
38111599	Envoy filter configuration section needs to be corrected in 25.1.200 user guide of SCP	In the 25.1.200 *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*, `name` and `type` fields were incorrectly documented for ASM configuration to allow the XFCC header. **Doc impact**: Updated the `name` and `type` fields for ASM configuration to allow the XFCC header in the "Deployment Configurations" section in *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.	3	25.1.100
38109905	ATS scenario is failing because duplicate registration observed on setnrfl1.nrfset.5gc.mnc012.mcc345 nrf post migration	Duplicate registrations were observed on the NRF setnrfl1.nrfset.5gc.mnc012.mcc345 after migration, causing the ATS scenario to fail. **Doc Impact**: There is no doc impact.	3	25.1.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-28 (Cont.) SCP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38073526	OCI threshold API returns error despite putting correct data.	The OCI threshold API returned an error when provided with accurate data, preventing successful threshold configuration. **Doc Impact**: There is no doc impact.	3	25.1.100
38034923	SCP User guide discrepancies	The metrics with dimension `ocscp_nf_service_name` were not updated to use `ocscp_nf_service_type` in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*. **Doc impact**: Replaced the dimension `ocscp_nf_service_name` with `ocscp_nf_service_type` in the "Metrics" section in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	3	24.3.0
38030151	NrfBootStrapInfo: Heartbeat request is happening with old replaced nrf	SCP sent heartbeat requests using an outdated NRF instance that was replaced. **Doc Impact**: There is no doc impact.	3	25.1.100
38025580	NrfBootStrapInfo: Audit is happening with the old replaced nrf	During the audit process, SCP referenced outdated NRF information was previously replaced. **Doc Impact**: There is no doc impact.	3	25.1.100
37987680	On Dual stack setup, service entry for foreign SCP profile is getting created with ipv4 only.	In a dual stack setup, the service entry for a foreign SCP profile was incorrectly created using only IPv4, despite SCP's capability to support both IPv4 and IPv6. **Doc Impact**: There is no doc impact.	3	25.1.100
37954103	SCP not able to register mate SCP profile if capacity is not present in profile	SCP failed to register a secondary profile when the associated primary profile lacked the required capacity. **Doc Impact**: There is no doc impact.	3	25.1.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-28 (Cont.) SCP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37511517	During SCP overload scenario(200%), Request and Response processing time for SCP exceeded 2 seconds	While performing upgrade and rollback operations between SCP 23.4.x and 24.2.x, the request and response processing time exceeded the expected limit of 10 seconds. **Doc Impact**: There is no doc impact.	3	24.2.3
37779596	Error Message summary needs to be corrected in CNCC for NF Service Config Set	The Error Message summary required correction on the CNC Console for NF Service Config Set. **Doc impact**: There is no doc impact.	4	25.1.100
37779565	ocscp_notification_nf_profile_rejected_total metrics pegged with internal error in case of received invalid notification with mandatory parameter missing in request	The `ocscp_notification_nf_profile_rejected_total` metric remained pegged with an internal error when an invalid notification was received with a mandatory parameter missing in the request. **Doc Impact**: There is no doc impact.	4	25.1.100
37697207	Api root header with ipv6 without square bracket and no port gives 500.	When an API root header contained an IPv6 address without square brackets and no specified port, it returned response 500. **Doc Impact**: There is no doc impact.	4	25.1.100
37690826	Exceptions list is not updating properly under nextHopSEPP when one exception is passing the list	When one exception was passing through the list, the exceptions list under nextHopSEPP was not updated. **Doc Impact**: There is no doc impact.	4	25.1.100
37659775	clarification for Side Car Proxy Server Header	The following sidecar proxy server header behavior was observed: "SCP responds to client with “503” and "envoy" as server header". **Doc impact**: Added the "Understanding sideCarProxyServerHeader and sideCarProxyStatusCode Configurations" subsection in *Oracle Communications Cloud Native Core, Service Communication Proxy REST Specification Guide*.	4	23.4.3

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-28 (Cont.) SCP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37648525	Then Vender Specific Error ID for error resulted because of ConnectionFailed due to jetty client and ConnectionTimeout at SCP are same	A Vendor Specific Error ID was triggered due to a connection failure between Jetty client and SCP. The failure was caused by a connection timeout, and the error IDs for both the Jetty client and SCP were identical. **Doc impact**: Updated the Error ID OSCP-WRK-ROUTE-E002 in "Table 3-6 SCP-Worker Microservice Error IDs" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	4	25.1.100
37615522	Two subscription requests are sent for UDM, with TSI as NRF for UDM and LOCAL for the other NFs, in the upgrade setup from 24.3.0 to 25.1.100	During an upgrade from SCP 24.3.0 to 25.1.100, two subscription requests were sent to the UDM. One request used TSI as the NRF for the UDM, while the other used LOCAL for the remaining NFs. **Doc Impact**: There is no doc impact.	4	25.1.100
37585269	Error Message needs to be corrected on the Console GUI while configuring Consumer Info configuration	An incorrect error message appeared on the CNC Console when configuring Consumer Info configuration. **Doc Impact**: There is no doc impact.	4	25.1.100
37505826	SCP CNCC, NF Discovery Response Cache Configuration Rule screen should a have visible column for added Exclude Discovery Query Parameters	On the CNC Console, the NF Discovery Response Cache Configuration Rule section did not have a column to view added Exclude Discovery Query parameters. **Doc Impact**: There is no doc impact.	4	25.1.100
37407899	SCP returns incorrect error while modifying NRF Profile on SCP	When modifying an NRF profile on SCP, an incorrect error message was returned. **Doc Impact**: There is no doc impact.	4	25.1.100
37309676	dnnList missing from pcfInfo in PCF profile on CNCC GUI	In SCP 24.2.1, the `dnnList` field was missing from the `pcfInfo` section in the PCF profile when viewed on the CNC Console. **Doc Impact**: There is no doc impact.	4	25.1.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-28 (Cont.) SCP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37273615	SCP returns 500 internal error in case of action parameter missing from approuting options REST API request	When the action parameter was missing from the approuting options REST API request, SCP returned a 500 internal error. **Doc Impact**: There is no doc impact.	4	25.1.100
37043138	Getting ocscp_nf_setid as UNKNOWN instead of nf_setid of PCF in the metric ocscp_metric_http_rx_res_total	The `ocscp_metric_http_rx_res_total` metric displayed `ocscp_nf_setid` as UNKNOWN instead of the expected `nf_setid` of PCF. **Doc Impact**: There is no doc impact.	4	24.3.0
36714066	SCP OCI Recovery Validity Period Description in Console UI needs to be updated.	The description for SCP OCI Recovery Validity Period on the CNC Console required an update. **Doc Impact**: There is no doc impact.	4	24.2.0
38043000	Service Group Configuration for CHF	In SCP 24.3.0, the service group configuration for CHF was found to be incorrect. **Doc impact**: Removed the "Configuring Service Groups Parameters" section from *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	4	24.3.0
37304141	nsiList values showing as NULL on CNCC GUI despite being set in SCP	The `nsiList` values appeared as NULL on the CNC Console, even though they were correctly set in SCP. **Doc Impact**: There is no doc impact.	4	25.1.100
37976004	SCP ATS Overall Results Report Misspells Feature as Featue	In SCP-ATS 25.1.100, the Overall Results Report incorrectly spelled "Feature" as "Featue." **Doc Impact**: There is no doc impact.	4	25.1.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-28 (Cont.) SCP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37966147	http and https port default needs to be updated in SCP installation guide	*Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide* contained incorrect default port information for HTTP and HTTPS. **Doc impact**: Updated the port numbers of `scpProfileInfo.scpInfo.scpPorts.https` and `scpProfileInfo.scpInfo.scpPorts.http` Helm parameters in the "Global Parameters" section of *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.	4	25.1.100
37869819	Put request for NFServiceConfig doesn't trigger reconfiguration for old NFType/NFService	A PUT request for NFServiceConfig failed to trigger reconfiguration when the request involved an older NFType or NFService. **Doc Impact**: There is no doc impact.	4	25.1.100
37930930	SCP User Guide - Table A-1 HTTP Status Code Supported on SBI	The HTTP status codes supported on the SBI interface were not correctly updated in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*. **Doc impact**: Updated the "Table A-2 Additional Status Codes Applicable for Reroute Condition List (reRouteConditionList) " with correct HTTP status codes in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	4	25.1.100

> **Note**
>
> Resolved bugs from 24.2.4 and 24.3.0 have been forward ported to Release 25.1.200.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-29 SCP ATS 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38128249	SCP0015 WS1.5 failed SCP_Subscription_SubscriptionWithNRFforNfTypeUDM_P0 - 062725	The test case failed while validating the nrf_subscription_delete request. **Doc Impact**: There is no doc impact.	3	25.1.100
38128999	SCP0015 WS1.5 failed SCP_EgressRateLimitingRelease16_AUSF_P0 - 062725	The scenario scenario-1_RateLimitingEgressAlternateRouteReverseLookup failed due to the metric metricfAUSF3 returning a value of 601 instead of 600. All the configurations were correct, but the test case failed due to the metric count exceeding the expected value. **Doc Impact**: There is no doc impact.	3	25.1.100

SEPP Resolved Bugs

Release 25.2.100

Table 4-30 SEPP 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38245287	Getting NPE intermittently in pn32f logs with Cat3 time check at 1K TPS	A Null Pointer Exception (NPE) occurred in the pn32f logs when the Cat3 time check feature was enabled. This issue was specific to deployments with a single pod using default resources, under a traffic load of 1,000 transactions per second (TPS). The NPE caused service degradation, leading to requests being rejected with a 500 error. **Doc Impact**: There is no doc impact.	2	25.1.200

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-30 (Cont.) SEPP 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38292305	Observing failures during SEPP perf run with updated payloads and URIs	During performance testing, payloads and URIs were updated to include unique IMSIs and additional body information. Traffic was generated at 5,000 messages per second (MPS) across the route cNF → cSEPP → pSEPP → pNF. After starting the test run, traffic degradation was observed within a few minutes. The issue occurred with SEPP features enabled, where every message contained a unique IMSI. The degradation worsened over time. **Doc Impact**: There is no doc impact.	2	25.1.200
38360262	Multipart Message boundary req header format causing 500 internal error in pn32-f	The pn32f microservice was rejecting multipart messages when the boundary value in the request header was formatted in a specific way. This issue prevented the microservice from processing such messages correctly. **Doc Impact**: There is no doc impact.	2	25.1.201

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-30 (Cont.) SEPP 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38477659	Replica count discrepancy observed in SEPP deployment after installation with the default YAML.	After installing SEPP using the default yaml file, a discrepancy was observed in the replica counts of certain pods. According to both the default yaml configuration and the SEPP Installation Guide, the following components were expected to have 2 replicas: • ocsepp-appinfo • ocsepp-nf-mediation • ocsepp-ocpm-config • ocsepp-sepp-nrf-client-nfdiscovery • ocsepp-sepp-nrf-client-nfmanagement However, post-deployment, these components were running with only 1 replica each. **Doc Impact:** Updated the default value of `nrfclient.nrf-client.nrf-client-nfmanagement.enablePDBSupport` parameter from false to true in the 'nrf client' section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide.*	2	25.1.200
38462361	Coherence profile need to be changed in SEPP Yaml	During a SEPP performance run, the Coherence profile in the SEPP yaml configuration was updated to improve performance. Initially, the Coherence profile was set to use 2 CPU and 2 Gi of memory. After the change, the profile was updated to use 4 CPU and 4 Gi of memory. **Doc Impact:** Updated the 'Resource Requirement' section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide.*	3	25.1.200

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-30 (Cont.) SEPP 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38423604	SEPP-NRF client integration Feature Helm Config parameters has not clarified the min and max values in the User and Installation Guide.	The default values for `nrfRetryConfig` and `healthCheckConfig` in the Helm configuration were updated. These changes are necessary to ensure accurate and up-to-date information in the SEPP Installation document. **Doc Impact:** Updated the Configurable Parameters section and updated the default values for `nrfRetryConfig` and `healthCheckConfig` in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide.*	3	25.1.200
38354072	OCC desires guidance for SEPP configuration for dual stack when using standard static address configuration parameters.	Static IPs were not functioning correctly with dual stack when using the standard static address configuration parameters. The issue was resolved by disabling the static IP setting and applying the `metallb.universe.tf/loadBalancerIPs` annotation to the service. **Doc Impact:** Updated the Dual Stack section of *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*.	3	25.1.201
38245043	Getting error in pn32f logs when cat3 time check is enabled	When the cat3 time check was enabled, an error occurred in the pn32f logs. This error was continuously logged each time a user authentication request was sent, leading to performance degradation. **Doc Impact**: There is no doc impact.	3	25.1.200

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-30 (Cont.) SEPP 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38198230	3gpp-Sbi-Max-Rsp-Time set as 8000 for nrf requests	The HTTP custom header "3gpp-Sbi-Max-Rsp-Time" was set to 8 seconds for NRF NIF discovery requests by the SEPP. However, the SEPP services did not wait for the full 8 seconds for the NRF response. This resulted in errors and the following exception being generated: *"3gpp-Sbi-Max-Rsp-Time"* **Doc Impact**: There is no doc impact.	3	25.1.200
37482876	SEPP-PERF: 429 error code is being returned despite 428 being configured for rate limiting at SEPP_25.1.0-rc1	When the global rate limiting feature was enabled, the system incorrectly returned a 429 error code instead of the expected 428 error code as configured in the rate-limiting policies at SEPP. The correct behavior should be to return the 428 error code as per the configured policies. **Doc Impact**: There is no doc impact.	3	25.1.100
38064564	Incorrect Log Level Shown for ocsepp-plmn-ingress-gateway Microservice in CNCC_25.1.200 – Shows WARN or INFO Instead of ERROR Configured Log Level a	The ocsepp-plmn-ingress-gateway microservice incorrectly displayed logs at WARN or INFO levels, despite being configured for ERROR level logging. **Doc Impact**: There is no doc impact.	3	25.1.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-30 (Cont.) SEPP 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38199334	"requestPath" dimension is empty in SEPP CAT1 Feature Alerts(Warn,Minor,Major,Critical) in both CSEPP and PSEPP .	In the Cat-1 Service API Query Parameter Validation feature, the alerts `seppN32fSrvcApiQryPrmValFailAltWarn`, `seppN32fSrvcApiQryPrmValFailAltMinor`, `seppN32fSrvcApiQryPrmValFailAltMajor`, and `seppN32fSrvcApiQryPrmValFailAltCritical` displayed an empty {{requestPath}} dimension across all alert levels. This issue was observed in both CSEPP and PSEPP deployments. **Doc Impact**: There is no doc impact.	3	25.1.200
38120235	PLMN-IGW pods restart observed due to 137 error code (oomkilled) during SEPP_25.1.200-rc.2 perf run while pSEPP site down and plmn-igw restart scenario's	During SEPP performance testing with fault insertion scenarios, PLMN-IGW pods on the PSEPP side restarted when PSEPP was restored after a complete scale-down. The restart was caused by error code 137 (OOMKilled), leading to temporary traffic disruption. **Doc Impact**: There is no doc impact.	3	25.1.200
38264214	SEPP Grafana dashboard provided with release has incorrect expression for CN32F Request-Response Latency Time	The KPI used to calculate CN32F Request-Response Latency Time in the Grafana dashboard was incorrect. **Doc Impact**: There is no doc impact.	3	25.1.100
38187439	response is not in json format when there is a timeout error	In timeout scenarios, the error response body was not in JSON format. **Doc Impact**: There is no doc impact.	3	25.1.200

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-30 (Cont.) SEPP 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37969620	Internal server error from SEPP when the payload is bigger than 262144 bytes	An internal server error occurs in SEPP when the payload exceeds 262,144 bytes. Any requests with a payload size larger than 262,144 bytes will not be routed through SEPP. **Doc Impact**: There is no doc impact.	3	25.1.100
38254800	SEPP-PERF: High Latency and Call Failures observed during SEPP_25.1.200-GA performance run at 40K MPS with feature enabled	During long-duration performance testing (10-hour and 72-hour runs) at 40,000 messages per second (MPS) on SEPP version 25.1.200, high latency was observed. The issue was reproducible when a 50ms server delay was introduced, suggesting a scalability or processing bottleneck when multiple SEPP features were enabled. Additionally, enabling the CAT-3 Previous Location Check feature increased latency by approximately 30ms across all call flows. **Doc Impact**: There is no doc impact.	3	25.1.200
38257593	pn32f memory usage keep on increasing at 550 TPS with cat3 time check enabled	When the Cat-3 Time check feature was enabled on the PSEPP, a memory leak was observed in certain scenarios. This issue caused the memory usage to increase continuously under a traffic load of 550 transactions per second (TPS), consisting of 500 successful and 50 failed transactions. The deployment was a single pod with default resource configurations. **Doc Impact**: There is no doc impact.	3	25.1.200

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-30 (Cont.) SEPP 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38245130	Getting "csepp-setSubscriber Id Value : null" error in the pn32f logs at 50 TPS with Cat3 time check	When the Cat-3 Time check feature was enabled, the pn32f logs displayed the error "csepp-setSubscriber Id Value : null" under a traffic load of 50 transactions per second (TPS). The deployment was a single pod with default resource configurations, and the cache refresh time was set to a low value of 10 milliseconds. This issue resulted in service degradation, with corresponding service requests being rejected with a 406 error code. Additionally, message drops were observed on SBI messages where the CAT-3 Time check feature was applied. **Doc Impact:** Updated the default value of `Cache Refresh Timer` parameter in Cat-3 Time LocationCheck for Roaming Subscribers section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy REST Specification Guide.*	3	25.1.200
38256559	service-api-allowed-list configuration output body is coming as "201 CREATED"	A PUT request to the service-api-allowed-list API on the SEPP Config service incorrectly returned a plain text response instead of a structured JSON message. The server responded with the literal string "201 CREATED," which does not conform to the expected JSON format. **Doc Impact:** Updated the return status of POST method of 'Security Countermeasure Service API Allowed List Name REST API' in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy REST Specification Guide.*	3	25.1.200

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-30 (Cont.) SEPP 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38391070	SEPP and SEPP ATS 25.1.201 Package Concern	A yaml safe load operation on the `Entry-Definitions` in the TOSCA metadata failed while processing a CSAR (Cloud Service Archive). The error occurred due to the presence of tab characters from line 42 to line 53 in the file `Definitions/ocats_ocsepp.yaml`. The yaml parser encountered an invalid token starting with a tab character, resulting in the following error: `ERROR: found character '\t' that cannot start any token in "Definitions/ocats_ocsepp.yaml", line 42, column 1` The issue was resolved by replacing the tab characters with the appropriate number of spaces, ensuring compliance with yaml formatting standards. **Doc Impact:** No doc impact.	3	25.1.201

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-30 (Cont.) SEPP 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38343926	SEPP 24.3.2 //25.1.200 does not honor NF profile capacity parameter set by user.	The NRF client did not honor the SEPP Profile capacity value specified by the user and instead defaulted to a value of 100. By default, the NFProfile was configured in Helm mode, causing the load and capacity variables to be retrieved from the perf-info service rather than directly from the NFProfile. As a result, the default value of 100 was propagated through the NFProfileUpdate and sent to the NRF. The code was updated to ensure the correct value was applied. **Doc Impact:** Updated the 'perf info' section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*.	3	24.3.2
38404940	Proactive status feature enabled but requests are no being sent.	The SEPP EGW was not sending out the Proactive Health check OPTIONS request, even though it was part of the RS Profile in the DB. When the proactive monitoring feature was enabled for a peer and the config-mgr-svc pod had been restarted, the parameters "healthApiPath" and "healthApiMethod" were removed from the peer configuration of the N32 Egress Gateway. **Doc Impact:** No doc impact.	3	25.1.200

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-30 (Cont.) SEPP 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38374106	Reroute to secondary Remote SEPP.	An update to the document was required to explain the secondary remote SEPP routing scenario in the User Guide, Section "Proactive Status Updates." **Doc Impact:** Updated the Detailed Description of the "Proactive Status Updates on SEPP" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*.	4	25.1.100
38196081	Section 6.1. of SEPP IUG needs to be updated.	After successfully uninstalling SEPP, the user received an incorrect message stating that certain resources were retained due to a resource policy. The message listed the following ConfigMaps: `egress-ratelimit-map` and `rss-ratelimit-map`. This step is no longer necessary and should be removed from the documentation. **Doc Impact:** Updated the Uninstalling SEPP Using Helm section to remove the step referencing the retention of ConfigMaps (egress-ratelimit-map and rss-ratelimit-map) after SEPP uninstallation in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*.	4	25.1.200

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-30 (Cont.) SEPP 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38015469	SEPP 25.1.100 Custom Values does not expose all containerPortNames	In the `ocsepp_custom_values_25.1.100.yaml` file, not all `containerPortNames` required for provisioning the `backendPortName` in the CNLB annotations were exposed. Specifically, the `con-port-http` parameter related to the configuration microservice was missing. As a result, the user had to manually add the parameter and port in the `ocsepp_custom_values_<version>.yaml` file to ensure proper functionality. **Doc Impact:** Updated the 'config-mgr-svc' section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*.	4	25.1.100
38186154	multipe DB related errors observed when SEPP is freshly installed	During SEPP installation, the config-mgr-svc pod logged incorrect errors indicating missing tables in the seppdb database. **Doc Impact**: There is no doc impact.	4	25.1.200
37834640	content-type http header is being sent in case TimeCheck is failed with 200 response code	When the Cat3 time check feature was enabled, and the error action code was configured as 200 for both failure and exception scenarios, the system incorrectly sent a `Content-Type` HTTP header in the response when the UDR was down. This header indicated that a response body was present, even though no body was actually included in the response. **Doc Impact**: There is no doc impact.	4	25.1.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-30 (Cont.) SEPP 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38290487	Troubleshooting Guide – SEPP Alerts inconsistencies	Several issues related to alerts were identified in the SEPP User Guide. These issues fall into the following categories: 1. **Alerts with Incorrect Resolution or Details Fields:** Some alerts contained inaccurate or incomplete information in the "Resolution" or "Details" fields, leading to potential confusion for users. 2. **Alerts Naming:** The naming conventions for certain alerts were inconsistent or unclear, making it difficult for users to understand the purpose or context of the alerts. 3. **OID Conflicts / Mismatches:** Object Identifiers (OIDs) associated with alerts were found to have conflicts or mismatches, causing issues in alert identification and handling. These inconsistencies and errors impacted the usability and reliability of the alert system as described in the user guide. **Doc Impact:** Updated the Alert expressions and resolutions of *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*.	4	25.1.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-30 (Cont.) SEPP 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38186154	Multipe DB related errors observed when SEPP is freshly installed	Upon SEPP installation, erroneous log entries indicating missing tables in the seppdb were detected within the config-mgr-svc pod. These error messages were logged and visible in the pod's output. **Doc Impact**: There is no doc impact.	4	25.1.200
38225384	SEPP 25.1.200 tagName in perf-info section of YAML file.	In the perf-info section of the SEPP CV yaml file, the comments preceding the `tagName` were limited to changes for CNE versions 1.8 and 1.9, which are no longer relevant. It was identified that a similar change is required for higher CNE versions, such as 23.3.4. Specifically, the value needs to be updated from the default namespace to kubernetes_namespace. **Doc Impact**: There is no doc impact.	4	25.1.200
38484307	Getting "Unable to parse to JSON" repetitive error in performance pod logs.	Repetitive "Unable to parse to JSON" errors were observed in the performance pod logs. The root cause was identified as an incorrect Prometheus URL specified in the CV file. The URL was set to `http://occne-kube-prom-stack-kube-prometheus.occne-infra:80`, which was not valid for the environment. **Doc Impact**: There is no doc impact.	4	25.1.200

Copyright © 2019, 2026, Oracle and/or its affiliates.

UDR Resolved Bugs

Release 25.1.202

Table 4-31 UDR 25.1.202 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38972130	Several pods do not get running in bmOCCNE 25.2.200	When deploying EIR on CNE, some pods did not start because of an undefined field in the pod status. The affected pods reported an application startup failure caused by an error creating the bean `additionalStartupChecks`. The log showed a `BeanCreationException` due to an undefined field, `observedGeneration`, in the JSON string for pod status. This field is not supported in the `V1PodStatus` properties, which caused the application to fail when starting the pods. **Doc Impact:** Updated the supported CNE and Kubernetes versions. For more information, see "CNE Requirement" and "Software Requirements" section in *Oracle Communications Cloud Native Core, Unified Data Repository Installation, Upgrade, and Fault Recovery Guide*.	3	25.1.201

Release 25.1.201

Table 4-32 UDR 25.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38157962	CnUDR is not generating PNR when multiple peer entry in ID1ODATA	cnUDR failed to generate a Push Notification Request (PNR) when multiple peer entries were present in ID1ODATA for a subscriber. **Doc Impact:** There is no doc impact.	2	24.2.5

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-32 (Cont.) UDR 25.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38317377	cnUDR fails to send POST Notify due to multiple subscription for PCF peers.	cnUDR failed to send POST Notify requests to Policy Control Function (PCF) due to multiple subscriptions for PCF peers during a provisioning update. **Doc Impact:** There is no doc impact.	2	24.2.6
38044356	SLF- SFTP is not working for a file transfer from export tool pod to provgw auditor pod .	Secure File Transfer Protocol (SFTP) failed to transfer files from the Subscriber Export Tool pod to the Provisioning Gateway auditor pod, preventing subscriber auditing. **Doc Impact:** There is no doc impact.	3	25.1.200
38245680	SLF-ATS 25.1.200: Fetch_log_upon_failure functionality not working	When the Fetch_log_upon_failure feature was enabled in SLF-ATS, it did not generate application logs, which caused test runs to fail even for features that passed. **Doc Impact:** There is no doc impact.	3	25.1.200
38344790	[5G_EIR 25.1.200] S13 interface error	The S13 interface returned DIAMETER_UNABLE_TO_COMPLY (5012) and other errors, such as DIAMETER_LOOP_DETECTED and DIAMETER_MISSING_AVP, because the International Mobile Equipment Identity (IMEI) length was invalid. **Doc Impact:** There is no doc impact.	3	25.1.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Release 25.1.200

Table 4-33 UDR 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37814291	UDR:How to specify resources for each container in Bulk-Import	During Subscriber Bulk Import Tool deployment, the users were unable to specify resources for individual containers in the configuration. Each container was deployed with the same CPU and memory resources (6 CPU and 7Gi memory), leading to excessive resource utilization when all containers were deployed. **Doc Impact:** Updated the total CPU and total Memory for the nudrbulkimport Microservice in the "Resource Requirements for UDR Tools" section in *Oracle Communications Cloud Native Core, Unified Data Repository Installation, Upgrade, and Fault Recovery Guide*.	3	24.2.0
37777519	SLF - Not able to change the loglevel for nrfClientManagement service	In the 25.1.100 release of SLF, users were unable to change the log level for the nrfClientManagement service from the CNC Console. When attempting to change the log level from WARN to DEBUG, an error occurred in the NrfClientManagement pod and the log level was not updated in the NrfClient pod. **Doc Impact:** There is no doc impact.	3	25.1.100
37590048	OCUDR:snmp MIB Complain from SNMP server	In the SLF, EIR, and UDR Management Information Base (MIB), users encountered an issue when loading them into an Simple Network Management Protocol (SNMP) server. The SSNMP notifier was appending a ".1" suffix to the SNMP trap, resulting in an error. **Doc Impact:** There is no doc impact.	3	24.2.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-33 (Cont.) UDR 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37501534	SLF_Controlled_shutdown not working after helm upgrade	In the 24.2.0 release of SLF, the Controlled Shutdown feature was not working as expected after a Helm upgrade. When attempting to apply a controlled shutdown from the CNC Console, SLF remained in the registered state and did not transition to the suspended state. Error messages were observed in the app Info logs, indicating an inability to get the operational state, and in the nudr-config logs, indicating an invalid URI sent from the client. **Doc Impact:** There is no doc impact.	3	24.2.0
37462379	NSSF - Customer facing ASM install issue	The user encountered a YAML parse error when attempting to install Aspen Service Mesh (ASM) using the provided charts. The error occurred due to a missing key in the envoy filter configuration of the service mesh resource yaml file. **Doc Impact:** There is no doc impact.	3	24.2.0
37785011	DIAMGW POD restart observed while running peformance for 10K SH & 17.2K N36 for 24 Hours with DB restart	In a performance test running for 24 hours with 10K SH and 17.2K N36, the diameter gateway pod was observed to restart multiple times. The restarts were caused by an Out of Memory (OOM) error, which resulted in the pod being terminated and restarted. **Doc Impact:** There is no doc impact.	3	25.1.100
37884685	Incorrect Metrics Mapping for diam_conn_local and diam_conn_network in UDR Namespace	The diam_conn_local and diam_conn_network were incorrectly mapped, leading to misinterpretation of system health and peer connectivity. **Doc Impact:** There is no doc impact.	3	24.2.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-33 (Cont.) UDR 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37955075	Missing excludeInboundPorts and excludeOutboundPorts in EGW and Alternate-Route	The excludeInboundPorts and excludeOutboundPorts annotations were missing in the Egress Gateway (EGW) and Alternate-Route sections in the custom value yaml file. **Doc Impact:** There is no doc impact.	3	25.1.100
37883833	SLF 25.1.100 Servicemesh - Envoy filter need to be updated	In release 25.1.100, Jetty HTTP/2 client connections would hang due to high stream IDs. This occurred in long-lived connections with a high volume of requests, causing outbound traffic to stop until the server-side Istio sidecar terminated the connection due to idle timeout. The issue was resolved by updating the Envoy filter. **Doc Impact:** There is no doc impact.	3	25.1.100
37915245	SLF 25.1.100 REST API Configuration for nfscoring is missing in guide	The REST API configuration details for *nfscoring* were missing from the UDR documentation. **Doc Impact:** Updated REST API configuration of `nfscoring` in the "Configuration APIs for Common Services" section in *Oracle Communications Cloud Native Core, Unified Data Repository REST Specification Guide*.	3	25.1.100
38022882	Ingress Gateway Provisioning Pods Restarting in UDR 24.2.4 Under Load	In UDR version 24.2.4, ingress gateway provisioning pods were observed to restart continuously under load during test validation. This issue occurred at approximately 50 transactions per second (TPS) and was accompanied by log entries indicating "Error occurred in Netty Inbound Handler for address." **Doc Impact:** There is no doc impact.	3	24.2.4

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-33 (Cont.) UDR 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37532285	Subscriber trace is missing for "400 Bad request " response of Duplicate POST Request	The subscriber trace was missing for a "*400 Bad Request*" response that occurred when a duplicate POST request was made. The issue occurred when the Allow Subscription Recreation feature was set to false. **Doc Impact:** There is no doc impact.	4	25.1.100

Common Services Resolved Bugs

ATS Resolved Bugs

Release 25.1.100

There are no resolved bugs in this release.

ASM Configuration Resolved Bugs

Release 25.2.100

There are no resolved bugs in this release.

Alternate Route Service Resolved Bugs

Table 4-34 Alternate Route Service 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36935315	Implement SA Guidelines for SecurityContext Configuration on GW	Some of the fields and SecurityContext configuration were not done for Gateway Services.	3	24.3.0
37039309	Tcpdump and Ping tools of debug tools is not working in egress gateway debug tools container	Tcpdump and Ping tools of debug tools did not work in Egress Gateway debug tools container.	3	24.3.0

Note

Resolved bugs from 24.3.x have been forward ported to Release 25.1.100.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Egress Gateway Resolved Bugs

Table 4-35 Egress Gateway 25.1.103 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37685576	Flooded with IRC Exception warn messages in EGW	Received the `IllegalReferenceCountException` warn messages in Egress Gateway after editing some values of traffic.sidecar.istio.io/excludeInboundPorts or traffic.sidecar.istio.io/excludeOutboundPorts in the Egress Gateway deployment and SVC.	2	24.2.11
37601685	High CPU when reset streams are triggered	Gateway Services experienced high CPU when reset streams were triggered.	2	24.2.12

Note

Resolved bugs from 24.2.x have been forward ported to Release 25.1.103.

Table 4-36 Egress Gateway 25.1.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37480520	After successful update of certificate in NRF k8S by OCCM by recreate process new certificate validity is not used in TLS handshake by NRF GW	After successful update of the certificate in NRF Kubernetes by OCCM (recreation process), the new certificate validity was not used in the TLS handshake by NRF Gateway Services.	2	25.1.100
37009578	SCP Monitoring not happening for subset of configured SCPs	SCP monitoring did not happen for the subset of configured SCPs.	2	23.4.4
37563087	Traffic routing done based on deleted peer/peerset and routes	Traffic routing was done based on the deleted peer or peerset and routes.	2	25.1.100

Note

Resolved bugs from 23.4.x have been forward ported to Release 25.1.102.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-37 Egress Gateway 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37319725	Update Notify sent towards SMF via EGW, fails at EGW due to NullPointerException followed by a timeout	The Update Notify sent towards SMF through Egress Gateway failed at Egress Gateway due to NullPointerException followed by a timeout.	2	25.1.100
37363928	Handshake failure when SEPP Egress gateway not initiating TLS connection	The handshake failure occurred when SEPP Egress Gateway did not initiate a TLS connection.	2	25.1.100
36935315	Implement SA Guidelines for SecurityContext Configuration on GW	Some of the fields and SecurityContext configuration were not done for Gateway Services.	3	24.3.0
36928822	No error codes observed in the Egress GW Grafana dashboard when FQDN is mis-configured	No error codes were observed in the Egress Gateway Grafana dashboard when FQDN was incorrectly configured.	2	23.4.4
37143723	If peer1 is used as a virtual host, which is not resolved, egress gateway is not routing the request to peer2 , which is host and port. Also, peer health status is empty	When peer 1 was used as a virtual host, which was not resolved, Egress Gateway did not route the request to peer 2, which was a host and port. Also, peer health status was empty.	3	24.2.4
37194307	Egress gateway drops all SEPP traffic after some time on dual stack setup	On a dual stack setup, SEPP traffic was processed, however, the SEPP traffic was blocked after some time due to IllegalStateException on n32-egress-gateway.	3	24.3.1

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-37 (Cont.) Egress Gateway 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37236640	Timeout exception occurred while sending notification request to Notification Server (25.1.0)	Timeout exception occurred while sending Notification requests to the Notification server.	2	23.2.12
36876832	100% CPU and traffic failures observed at EGW	100% CPU and traffic failures were observed at Egress Gateway.	2	23.4.7
36938693	EGW pods getting stuck and not processing any traffic (Policy 24.3.0)	Egress Gateway pods were stuck and could not process any traffic.	2	23.4.8
36950565	Body omitted from request while sending multipart messages	While enhancing SEPP to support multipart messages, it was observed that N32-EGW was sending empty body in the request, but it received the full payload from the CN32F service.	2	24.2.0
36666519	Producer/Consumer FQDN contain ":port" while messageCopy is enabled on GWs	FQDN of producer NF and consumer NF had ":port" while messageCopy was enabled on Gateway Services.	4	23.4.0
36987637	Egress gateway jetty client not able to handle HTTP2 zero size header table	Egress Gateway Jetty client was unable to handle the HTTP2 zero size header table.	2	24.1.5
35927069	Entry updated in DNS Server is not getting reflected while checking the healthStatus in Egress Gateway	The entry updated in DNS Server did not appear while checking the healthStatus in Egress Gateway.	3	23.3.3
36305260	Egress gateway is adding duplicate headers in response [Alternate routing use case}	Egress Gateway added multiple duplicate headers, x-reroute-attempt-count and x-retry-attempt-count, in responses.	3	24.1.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-37 (Cont.) Egress Gateway 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37039309	Tcpdump and Ping tools of debug tools is not working in egress gateway debug tools container	Tcpdump and Ping tools of debug tools did not work in Egress Gateway debug tools container.	3	24.3.0
37148443	Egress gateway not accepting IPv6 address in the configuration	In the Roaming partner profile, when IPv6 address was provided in the Remote SEPP IP address, Egress Gateway did not accept IPv6 address in the configuration.	3	24.3.1
37236640	Timeout exception occurred while sending notification request to Notification Server (25.1.0)	Timeout exception occurred while sending Notification requests to the Notification server.	2	23.2.12

Note

Resolved bugs from 24.1.x have been forward ported to Release 25.1.100.

Ingress Gateway Resolved Bugs

Table 4-38 Ingress Gateway 25.1.103 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37601685	High CPU when reset streams are triggered	Gateway Services experienced high CPU when reset streams were triggered.	2	24.2.12

Note

Resolved bugs from 24.2.x have been forward ported to Release 25.1.103.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-39 Ingress Gateway 25.1.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37744851	Installation is failing with POP25 validation failrure even though POP25 feature is disabled	The Ingress Gateway Helm installation failed with a POP25 validation failure.	3	25.1.101
37333191	oc_ingressgateway_http_responses_total metrics are not updated when call is rejected by ratelimiting	The `oc_ingressgateway_http_responses_total` metric was not updated when the call was rejected by rate limiting.	3	25.1.100
37365106	401 unauthorized metric not updated in "oc_ingressgateway_http_responses_total"	The oc_ingressgateway_http_responses_total metric was not updated when the call was rejected by rate limiting with ASM enabled.	3	25.1.100
37369197	Error reason for Pod protection by rate limiting is not updated for default error profile.	The error reason for the Pod Protection using Rate Limiting feature was not updated for the default error profile.	4	25.1.100
37403771	NRF upgrade failed with igw post upgrade hooks in error state	NRF upgrade failed with Ingress Gateway postupgrade hooks in the error state.	2	23.4.10
37417212	Rest Configuration is success for ERROR Profile which is not defined in values file	The REST configuration was successful for ERROR Profile which was not defined in the values file.	4	25.1.100
37416293	Fill rate is allowing decimal value during helm but same is rejecting in REST configuration	The Fill rate allowed the decimal value during the Helm configuration, however, the same was rejected in the REST configuration.	4	25.1.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-39 (Cont.) Ingress Gateway 25.1.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37359902	Success percentage drops to 47-52% during in-service upgrade/ rollback of IGW from 24.3.3 to 25.1.0 and vice-versa	Success percentage reduced to 47-52% during the in-service upgrade or rollback of Ingress gateway from 24.3.3 to 25.1.0 and conversely.	2	25.1.100
37480520	After successful update of certificate in NRF k8S by OCCM by recreate process new certificate validity is not used in TLS handshake by NRF GW	After successful update of the certificate in NRF Kubernetes by OCCM (recreation process), the new certificate validity was not used in the TLS handshake by NRF Gateway Services.	2	25.1.100
37563087	Traffic routing done based on deleted peer/peerset and routes	Traffic routing was done based on the deleted peer or peerset and routes.	2	25.1.100

Note

Resolved bugs from 23.4.x have been forward ported to Release 25.1.102.

Table 4-40 Ingress Gateway 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36935315	Implement SA Guidelines for SecurityContext Configuration on GW	Some of the fields and SecurityContext configuration were not done for Gateway Services.	3	24.3.0
36932086	mcore-ingress-gateway pod keeps increasing until the pod is restarted	The mcore-ingress-gateway pod continued to increase until the pod restarted.	2	23.4.4
36672146	3gpp-sbi-lci header is not included in response for signalling requests	The 3gpp-sbi-lci header was not included in the response for signaling requests.	3	24.2.1

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-40 (Cont.) Ingress Gateway 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36915822	IGW sends requests to NRF backend services when they are in NotReady (0/1) state	Ingress Gateway sent requests to NRF discovery service pods when the pods were in the NotReady(0/1) state.	3	23.4.3
37032005	IGW is timing out with 408 request intermittently	Ingress Gateway was timing out for certain messages, and in such cases, logs were observed in Ingress Gateway.	3	24.3.0
36882493	NullPointerException From IGW for GET pending-req-count	NullPointerException was observed in Ingress Gateway for the GET pending-req-count.	2	23.4.6
36950565	Body omitted from request while sending multipart messages	While enhancing SEPP to support multipart messages, it was observed that N32-EGW was sending empty body in the request, but it received the full payload from the CN32F service.	2	24.2.0
37039309	Tcpdump and Ping tools of debug tools is not working in egress gateway debug tools container	Tcpdump and Ping tools of debug tools did not work in Egress Gateway debug tools container.	3	24.3.0

Note

Resolved bugs from 23.4.x have been forward ported to Release 25.1.100.

Common Configuration Service Resolved Bugs

Release 25.1.100

There are no resolved bugs in this release.

Helm Test Resolved Bugs

Release 25.2.1xx

There are no resolved bugs in this release.

Copyright © 2019, 2026, Oracle and/or its affiliates.

App-Info Resolved Bugs

Release 25.2.1xx

There are no resolved bugs in this release.

Mediation Resolved Bugs

Release 25.2.100

There are no resolved bugs in this release.

NRF-Client Resolved Bugs

Table 4-41 NRF-Client 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36730314	[AM_UE Performance]upgrade fails from PCF 24.1.0_GA to 24.2.0_rc7 " Error creating bean with name 'hookService' defined in URL"	While upgrading NRF-client some how there are multiple records in the common config hook db, this generates issues while completing the hook process. Until now the workaround was to manually delete the duplicate records.	2	24.2.0
37746681	NRF-Client Sends continous PUT/ PATCH requests to NRF when UDR is in SUSPENDED state	When the NF changes from running to not running, NRF-client enters into an endless cycle of PUT and PATCH request part of the hearbeat process. This overloads with many requests.	2	25.1.100

Perf-Info Resolved Bugs

Release 25.2.1xx

There are no resolved bugs in this release.

Debug Tool Resolved Bugs

Release 25.2.1xx

There are no resolved bugs in this release.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Known Bug List

The following tables list the known bugs and associated Customer Impact statements.

BSF Known Bugs

Release 25.1.101

There are no known bugs in this release.

Release 25.1.100

There are no known bugs in this release. Known bugs from 24.3.0 have been forward ported to Release 25.1.100.

CNC Console Known Bugs

Release 25.1.100

There are no known bugs in this release.

Copyright © 2019, 2026, Oracle and/or its affiliates.

cnDBTier Known Bugs

Release 25.1.103

Table 4-42 cnDBTier 25.1.103 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38199454	DB Entries on Site-1 and Site-2 are not in sync after doing an in service upgrade from 24.2.6 to 25.1.200 on a 2 site GR setup	After performing an in-service upgrade from version 24.2.6 to 25.1.200 on a 2-site Geo-Replication (GR) setup, database entries between Site-1 and Site-2 are not in sync.	Replication delay is observed. **Workaround**: Perform the following steps: 1. Complete the DBTier software upgrade. All the DB Tier pods should be upgraded to the new DBTier version. 2. Perform rolling restart of ndbappmysqld and ndbmysqld stateful sets.	2	24.2.6

Copyright © 2019, 2026, Oracle and/or its affiliates.

Release 25.1.102

Table 4-43 cnDBTier 25.1.102 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38199454	DB Entries on Site-1 and Site-2 are not in sync after doing an in service upgrade from 24.2.6 to 25.1.200 on a 2 site GR setup	After performing an in-service upgrade from version 24.2.6 to 25.1.200 on a 2-site Geo-Replication (GR) setup, database entries between Site-1 and Site-2 are not in sync.	Replication delay is observed. **Workaround**: Perform the following steps: 1. Complete the DBTier software upgrade. All the DB Tier pods should be upgraded to the new DBTier version. 2. Perform rolling restart of ndbappmysqld and ndbmysqld stateful sets.	2	24.2.6
38220013	dbtrecover Script is affecting db-monitor-svc	After running georeplication recovery (GRR), the db-mon-svc service intermittently enters a deadlock state, leading to unresponsiveness of both its db-mon-svc REST API and metrics scraping. This condition persists until the service is restarted.	Intermittently after running GRR, db-mon-svc has deadlock threads. Db-mon-svc API and metric scraping are not working until it gets restarted. **Workaround**: Restart the DB Monitor service after georeplication recovery is completed	3	25.1.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Release 25.1.101

Table 4-44 cnDBTier 25.1.101 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37842445	`dbtreplmgr` script is unable to stop the replica on HTTPS and TLS-enabled setup on cnDBTier	`dbtreplmgr` script is unable to stop the replica on HTTPS and TLS-enabled setup.	`dbtreplmgr` script cannot be used when HTTPS is enabled to start and stop replication. **Workaround**: Perform the steps given in the "Starting or Stopping cnDBTier" section in *Oracle Communications Cloud Native Core, cnDBTier User Guide* to start and stop replication.	3	24.2.5

Release 25.1.100

Table 4-45 cnDBTier 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37839960	The ndbmtd pods restart with "initial" option, due to which the restart time of the pod increases	During a single or multisite deployment, when the cluster is upgraded with configuration changes, the ndbmtd pods restart with -- initial option. This is because the cmp command in the ol9 docker container is removed. This leads to the increased pod restart time.	The issue increases the upgrade time because the ndbmtd pods take more time to restart. **Workaround**: Perform upgrade or rollback of cnDBTier without service account instead of automated upgrade or rollback using the service account.	3	25.1.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

CNE Known Bugs

Release 25.1.101

Table 4-46 CNE 25.1.101 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36740199	bmCNE installation on X9-2 servers fail	Preboot execution environment Preboot execution environment (PXE) booting occurs when installing Oracle Linux 9 (OL9) based BareMetal CNE on X9-2 servers. The OL9.x ISO UEK kernel installation hangs on X9-2 server. When booted with OL9.x UEK ISO, the screen runs for a while and then hangs with the following message "Device doesn't have valid ME Interface".	BareMetal CNE installation on X9-2 servers fails. **Workaround**: Perform one of the following workarounds: • Use x8-2 servers. • Use CNE 23.3.1 or older version on X9-2 servers.	2	23.4.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Release 25.1.100

Table 4-47 CNE 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36740199	bmCNE installation on X9-2 servers fail	Preboot execution environment (PXE) booting occurs when installing Oracle Linux 9 (OL9) based BareMetal CNE on X9-2 servers. The OL9.x ISO UEK kernel installation hangs on X9-2 server. When booted with OL9.x UEK ISO, the screen runs for a while and then hangs with the following message "Device doesn't have valid ME Interface".	BareMetal CNE installation on X9-2 servers fails. **Workaround**: Perform one of the following workarounds: • Use x8-2 servers. • Use CNE 23.3.x or older version on X9-2 servers.	2	23.4.1

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-47 (Cont.) CNE 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37799030	OCCNE images_25.1.100.tar missing velero images	CNE 25.1.100 doesn't have the Velero images in the images tar file. This issue can lead to install and upgrade failures.	This issue can cause CNE 25.1.100 installation and upgrade failures. **Workaround**: Download Velero images from the internet. Additionally, perform the following steps after provisioning the registry with the necessary images while configuring the container image registry. For more information, see the "Configuring Container Image Registry" section (Step 1) in *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*. • Run the following commands to set a common environment: **Provision the registry with the**	2	25.1.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-47 (Cont.) CNE 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			necessary Velero images $ CENTRAL_REPO=<central-repo-name> $ CENTRAL_REPO_REGISTRY_PORT=<central-repo-registry-port> $ OCCNE_VERSION=<OCCNE version> $ OCCNE_CLUSTER=<cluster-name> $ OCCNE_vCNE=<openstack, oci,		

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-47 (Cont.) CNE 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			vmware, or do not define if Bare-Metal> $ if [-x "$(command -v podman)"]; then OCCNE_CONTAI		

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-47 (Cont.) CNE 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			NER_ENGINE= 'podman' else OCCNE_CONTAINER_ENGINE= 'docker' fi • Create a text file with Velero images: $ cat <<EOF >> velero		

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-47 (Cont.) CNE 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			_images.txt docker.io /velero/velero :v1.13.2 docker.io /velero/velero_plugin_for_aws :1.9.2 docker.io /velero/velero_plugi		

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-47 (Cont.) CNE 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			n_for_csi :0.7.1 EOF • Load Velero images on Central Repo Registry: $ for IMAGE in $(cat velero_images.txt); do TAGGED_IMAGE		

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-47 (Cont.) CNE 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			_NAME=$ {IMAGE / docker .io\ / velero \ // occne/ } $ {OCCNE _CONTA INER_E NGINE} image pull $ {IMAGE } $ {OCCNE _CONTA INER_E		

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-47 (Cont.) CNE 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			NGINE} image tag ${IMAGE} ${CENTRAL_REPO}:${CENTRAL_REPO_REGISTRY_PORT}/${TAGGED_IMAGE_NAME} ${OCCNE_CONTAINER_ENGINE} image push ${CENTRAL_REPO}:${CENTRAL_REPO_REGISTRY_PORT}/${TAGGED_IMAG		

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-47 (Cont.) CNE 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			E_NAME } $ {OCCNE _CONTA INER_E NGINE} image rm $ {IMAGE } $ {CENTR AL_REP O}:$ {CENTR AL_REP O_REGI STRY_P ORT}/$ {TAGGE D_IMAG E_NAME } done		

OSO Known Bugs

Release 25.1.103

There are no known bugs in this release.

Release 25.1.102

There are no known bugs in this release.

Release 25.1.101

There are no known bugs in this release.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Release 25.1.100

There are no known bugs in this release.

NRF Known Bugs

Release 25.1.204

Table 4-48 NRF 25.1.204 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
39050962	Incorrect discovery response w.r.t smf slice selection and incorrect value for preferredTaiMatchInd	While processing NFDiscover Service operation for SMF NF type with DNN and Preferred TAI, SMF profiles are returned in the NFDiscover response, partially matched with different `smfinfo` element in `smfInfoList` for `tai` and `dnn` attributes.	Consumer network functions will receive SMF profiles whose SMFInfoList includes SMFInfo entries that partially match the TAI and DNN attributes. **Workaround**: There is no workaround.	3	25.1.203

Release 25.1.203

NRF 25.1.203 is a Critical Patch Update. Critical Patch Updates provide security patches for supported Oracle on-premises products. They are available to customers with valid support contracts. For more information, see Critical Patch Updates, Security Alerts, and Bulletins.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-49 NRF 25.1.203 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38671036	Incorrect dimension name "SubscriptionIdType" for SLF Request/Response metric	The metrics `ocnrf_SLF_tx_requests_total` and `ocnrf_SLF_rx_responses_total` have an incorrect dimension `SubscriptionIdType` with values as SUPI and GPSI. The correct dimension name should be `SubscriberIdType`.	The metric is pegged with dimension as `SubscriptionIdType` as SUPI or GPSI can be misleading. But this does not have an impact on the KPIs. **Workaround**: There is no workaround.	3	25.1.202

Copyright © 2019, 2026, Oracle and/or its affiliates.

Release 25.1.202

Table 4-50 NRF 25.1.202 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38327826	NRF uses only own site data when GeoRedundancy feature is enabled.	When the `overrideReplicationCheck` Helm flag is set to true, NRF operates as a standalone site during the initial configuration of geoRedundancy or when sites are reconfigured. In this scenario, NRF assumes replication is up across all sites, regardless of their actual replication status. However, following a fresh installation, the mated sites may not yet be configured using `geoRedundancyOptions`, leading to inaccurate replication assumptions.	NRF sites will function as stand alone and will use only own site state data for service operations. **Workaround**: After updating the `geoRedundancyOptions` on the site, perform a rolling restart of the cache data service, discovery, registration, subscription, access token, artisan, auditor, and configuration pods. This ensures that the new configuration is properly loaded.	3	25.1.200

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-50 (Cont.) NRF 25.1.202 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38179022	Outgoing signalling messages from NRF-egressgateway getting failed while using IPv6 address in slfhost	Outgoing signaling messages fail when the destination host address is configured with an IPv6 value on the Egress Gateway microservice. This issue occurs because the NRF backend microservices send the IPv6 address without square brackets. The problem impacts the following use cases: NRF to SLF, NRF to NRF Forwarding, and NRF Growth.	Signaling messages fail when the host address is configured with an IPv6 value for the defined use cases. **Workaround**: There is no workaround.	3	25.1.200

Copyright © 2019, 2026, Oracle and/or its affiliates.

Release 25.1.200

Table 4-51 NRF 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38327826	Message copy feature: Access token request generated at EGW towards NRF not being sent to kafka properly	There is an issue with the access token request generated at the Egress Gateway. The response message received at the Egress Gateway from the access token microservice is being fed into Kafka, but the request message is not being sent to Kafka. Both the request and response messages need to be fed into the same Kafka partition for the same transaction.	The response message received at Egress Gateway from Access Token microservice is being fed into Kafka, while the request message is not being sent in Kafka. **Workaround**: There is no workaround.	3	25.1.200

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-51 (Cont.) NRF 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37412089	For NFSetId case-sensitive validation, registration request is getting accepted for NID having value not compliant to fixed length of 8 digit hexadecimal number as per 3GPP.	For NFSetId case-sensitive validation, registration request is getting accepted for NID having value not compliant to fixed length of 8 digit hexadecimal number as per 3GPP.	NRF will accept the NFRegister/ NFDiscover service operations request with non-compliant NFSetID containing NID digits. **Workaround:** NFs should use correct length of NID digits as per 3GPP for NFRegister/ NFDiscover service operations request.	3	23.4.6
37760595	Discovery query results in incorrect match with preferred-locality=US%2bEast	NRF is returning NFProfile ordered at first position with locality matching with space (that is, US East) while query contains + (that is, US+East).	NFProfiles in response may be ordered with space first then followed by other localities. **Workaround:** Locality attribute should not have space or plus as special characters. Or if query have %252B as encoded character then NFProfile with + will match that is, US+East.	3	24.2.4

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-51 (Cont.) NRF 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36366551	During NRF upgrade from 23.3.1 to 23.4.0 restart observed in NRF ingress-gateway with exit code 143 randomly	During NRF Upgrade from 23.3.1 to 23.4.0, sometime it is observed that NRF ingress-gateway pods restarts. The issue happens only when both the Primary and Secondary Coherence Leader pods gets upgraded at the same time during rolling Update.	This can happen randomly, but when happens, the pod comes up automatically after restart. No manual step is required to recover the pod. **Workaround:** The ingress-gateway section of the NRF custom values yaml, the *rollingUpgdate.maxUnavailable* and *rollingUpdate.maxSurge* needs to set to 5%. This will ensure only one Pod of ingress-gateway updates at a time. However, this will increase the overall upgrade time of all the ingress-gateway pods.	3	23.4.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-51 (Cont.) NRF 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37965223	Error Codes are not picked from errorCodeProfile configuration for Pod protection with rate limit	Error Codes are not picked from errorCodeProfile configuration for Pod protection with rate limit.	When Ingress Gateway rejects the requests, it takes the error code from Helm attribute errorCodeProfiles instead of REST. **Workaround:** Update the error code for *ERR_POD_PROTECTION_RATE_LIMIT* in the helm attribute *ingressgateway.errorCodeProfiles.*	3	25.1.200
37965589	The Ingress gateway pod restarted and went into crashloopbackoff when 10k traffic was sent to a single pod	The Ingress gateway pod restarted and went into crashloopbackoff when 10k traffic was sent to a single pod.	The ingress gateway Pod Protection using rate limiting feature was enabled. To simulate high burst of traffic, 10k TPS was sent to a single IGW pod. The Ingress Gateway pod restarted and the pod went into crashloopbackoff state. The issue is observed with ASM enabled. The side car container crashed due to OOM. **Workaround:** Traffic cannot reach to 10k.	3	25.1.200

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-51 (Cont.) NRF 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37604778	TLS1.3 Handshake is failing between NRF and SCP	TLS1.3 Handshake is failing between NRF and SCP as SCP was sending Session resumption extensions towards NRF (Ingress Gateway).	TLS v1.3 will not work if Client is sending session resumption extensions. **Workaround:** Client should not send Session Resumption extension.	3	24.2.3
38104210	NFUpdate - Partial update dnnUpfInfoList and dnnSmfInfoList are accepting string value instead of object	NFUpdate - Partial update dnnUpfInfoList and dnnSmfInfoList are accepting string value instead of object	*dnnUpfInfoList* and *dnnSmfInfoList* will have wrong information as per 3GPP. This is fault insertion case, when string values are used instead of the *DnnSmfInfoItem* and *DnnUpfInfoItem* object. **Workaround:** *dnnSmfInfoItem* and d*nnUpfInfoItem* attributes shall be used as per 3GPP during patch to avoid this issue.	3	25.1.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-51 (Cont.) NRF 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37412138	Error response generated by NRF needs to be corrected when registration request is sent with incorrect order for mcc and mnc	Error response generated by NRF needs to be corrected when registration request is sent with incorrect order for mcc and mnc.	No Impact on signaling message processing. Only error message details doesn't include correct error reason. **Workaround:** There is no workaround available.	4	23.4.6
38103938	log4j2_events_total metric is not getting pegged	*log4j2_events_total* metric is not getting pegged.	Metric for log4j is not pegged. **Workaround:** There is no workaround available.	4	25.1.200
38103958	Congestion Config CNC Console GUI screen not working correctly	Congestion Config CNC Console GUI screen not working correctly.	CNC Console GUI is not working for congestion config. **Workaround:** There is no workaround available.	4	25.1.200

Copyright © 2019, 2026, Oracle and/or its affiliates.

NSSF Known Bugs

Release 25.1.100

Table 4-52 NSSF 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37048499	GR replication is breaking post rollback to of CNDB 24.2.1-rc.4	The cnDBTier replication mechanism is experiencing performance degradation during rollbacks under high transaction volumes, leading to potential transaction ordering inconsistencies and constraint failures on the secondary site. Additionally, any binlog instruction failure is disrupting the replication channel. For the Network Service Selection Function (NSSF), the NsAvailability functionality is encountering a replication channel break when rolling back an upgrade from 24.2.x to 24.3.x if an availability delete and an availability update are occurring within a few seconds.	NSSF's Availability (NsAvailability) functionality may experience a replication channel break during the rollback of an upgrade from 24.2.x to 24.3.x if an availability delete and an availability update occur within a short time frame of a few seconds. **Workaround:** If the replication channel breaks, it can be recovered by following the replication channel recovery procedure outlined in the section 7.4.7.1 – Resolving Georeplication Failure Between cnDBTier Clusters in a Two-Site Replication in the *Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.	24.3.0	2

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-52 (Cont.) NSSF 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37776049	Dynamic log level updating Using CNCC for various micro services for NSSF. "LogDiscarding" Option is coming while fetching configured log level via REST but in CNCC while configured that option is not present	NsConfig Log level is not updated at runtime.	There is no impact on traffic; however, debugging becomes difficult if the NsConfig service log level needs to be changed at runtime. **Workaround:** Helm parameter can be used to change the log level of NsConfig. It can be modified as needed.	25.1.100	3
37773632	[10.5K TPS] when we are deleting all CNDB pods, ns-selection 2 pods have stuck in a 1/2 state.	When all pods of cnDBTier are deleted then NSSF NsSelection pods are getting stuck.	There is minimal impact on traffic when cnDBTier recovers. However, if all cnDBTier pods are deleted, NsSelection pods may not distribute traffic properly, leading to pods getting stuck. **Workaround:** Delete the stuck pods. Newly spawned pods will be able to take traffic.	25.1.100	3
37763453	Error code 500, instead 4XX, when NSSF receives duplicated incorrect Authorization	Ingress Gateway is not responding with error when Auth token is incorrect.	There is no traffic loss. **Workaround:** There is no workaround available.	24.3.0	3

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-52 (Cont.) NSSF 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37762864	[10.5K TPS] nrf-client discovery and management pod has restarted when all CNDB pod faults using chaos-mesh	When cnDBTier pod is forcefully kept in a stuck state, NRF-client pods enter a restart state.	There is no impact on traffic when the cnDBTier pods are recovered. **Workaround:** There is no workaround available.	25.1.100	3
37731732	Autopopulation with 3NRFs: Even though candidate AMF doesn't have same plmn as amfset it is storing in database and is getting resolved when amf resolution is called	NSSF is autopopulating AMF candidates from NRFs into the Database (DB) even when the candidate AMF does not belong to the same PLMN as the AMF set.	There is no traffic loss. **Workaround:** There is no workaround available.	25.1.100	3
37684563	[10.5K Traffic—without Replication Break] While 7K burst traffic to site1, NSSF reduced the success rate by 3.528% with 500 and 503 error code and then recovered it	Intermittent loss of traffic occurs when traffic is moved from one site to another.	Minimal traffic loss, with approximately 3.5% of traffic lost for a few seconds before recovering. **Workaround:** There is no workaround available.	25.1.100	3
37684124	[10.5K Traffic] while adding the empty frame in all requests, NSSF rejected the ns-selection traffic, dropping 0.045% with a 503 error code	Intermittent traffic loss occurs when traffic is moved from one site to another.	There is minimal traffic loss of approximately 3.5%, which occurs for a few seconds before the traffic recovers. **Workaround:** There is no workaround available.	25.1.100	3

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-52 (Cont.) NSSF 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37681032	NSSF 24.2.1: Missing Edit Option for nsconfig Logging Levels in CNCC GUI	When an empty packet is forcefully added to traffic (negative scenario), 0.045% of traffic is discarded with error code 503.	There is minimal traffic loss of 0.045%, occurring only in an error scenario. **Workaround:** There is no workaround available.	24.2.1	3
37639879	oauth failure is not coming in oc_ingressgateway_http_responses_total metrics	There is an Incorrect metric pegging for *oc_ingress_http_response_total* in the OAuth failure scenario.	There is no impact on the traffic. **Workaround:** There is no workaround available.	25.1.100	3
37623199	If an accept header is invalid, NSSF should not send a notification to AMF. it should send 4xx instead of 500 responses to the nsssai-auth PUT and DELETE configuration.	NSSF is performing database (DB) operations and triggering notifications to the AMF even when an invalid Accept header was present in nsssai-auth PUT and DELETE requests.	There is no impact on the traffic. **Workaround:** There is no workaround available.	25.1.100	3
37606284	With DNS SRV feature enabled for selection of NRF, NSSF fails to establish connection with NRF	When tested with three NRF instances configured across different sites, using geo-redundant ASM-based deployment, NSSF failed to establish a connection with the NRF when DNS SRV-based discovery was enabled.	There is no impact on the traffic. **Workaround:** There is no workaround available.	25.1.100	3

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-52 (Cont.) NSSF 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37591102	OCNSSF:24.2.x:snmp MIB Complain from SNMP server	SNMP traps are not being raised due to an issue with the MIB file.	There is no impact on the traffic. **Workaround:** Updated MIB file with scope set to shared.	24.2.0	3
37216832	[9K TPS Success] [1K TPS Slice not configured in DB] NSSF is sending the success responses for slice which has not configured in database and failure response of slice which has configured in database for pdu session establishment request.	In an error scenario test where 9,000 error messages are sent, NSSF is incorrectly responding with success for 0.4% of the messages.	There is minimal impact on the traffic. **Workaround:** There is no workaround available.	24.3.0	3
37184196	3-site GR setup ASM and Oauth Enabled : 10.5K TPS Traffic on SITE1 : during restoration of site (post Failover for 18 hours), new NsAvailability PUT is not syncing to site which is recovered	Intermittently, after replication recovery, data is not synchronized, leading to error responses for a limited duration.	There is minimal impact on the traffic. **Workaround:** There is no workaround available.	24.3.0	3
37136539	[dnsSrvEnabled: false] [peer Health monitoring: disabled] NSSF is not sending the notification towards peer2 host if peer1 is down	When DnsServices is disabled and static routes are used, notifications are not rerouted when the primary peer is down.	There is a loss of notification in a specific case when static routing is used. **Workaround:** Enable DnsServices and use virtual FQDNs.	24.2.1	3
37136248	If dnsSrvEnabled is set to false and peer1 is used as a virtual host, the egress gateway will not sending the notification to peer2 host and peer health status is empty	Health check status processing has an issue at the Egress Gateway, causing requests to be forwarded to an unhealthy peer.	There is no traffic loss, as the message is retried and eventually reaches the correct node. **Workaround:** There is no workaround available.	24.2.1	3

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-52 (Cont.) NSSF 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37099843	Upgrade 3 Site GR Setup, while upgrading NSSF and CNDB, we observed that the Ns-availability success rate dropped 0.07%, 0.77%, and 1.19%, respectively, for each site, and we got 500, 503, and 403, 408 error codes.	During an in-service upgrade, 0.25% to 1% of messages are being responded to with error codes.	During an upgrade, 0.25% to 1% of messages are lost. The impact is low as this occurs only during upgrade or rollback when pods are starting. After the upgrade, the behavior returns to normal. **Workaround:** There is no workaround available.	24.3.0	3
36734417	NSSF 2 Site GR :IN service solution Upgrade : 1.25K TPS : traffic loss of 0.259% and 0.027% at Site 1 and Site 2 during the NSSF upgrades, with latency of roughly 1.43 seconds and 886 ms.	During an in-service upgrade, 0.25% of messages are being responded to with error codes.	During an upgrade, 0.25% of messages are lost. The impact is low as this occurs only during upgrade or rollback when the pods are starting. **Workaround:** There is no workaround available.	24.2.0	3
36662054	NSSF-CNCC: Ingress pod: Discard Policy mapping configured without mandatory param	The CNCC GUI does not validate the Discard Policy mapping configuration.	There is no impact on the traffic. **Workaround:** The operator can configure the Discard Policy mapping with the correct value.	24.1.0	3

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-52 (Cont.) NSSF 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36552026	KeyId, certName, kSecretName, and certAlgorithm invalid values are not validating in the oauthvalidator configuration.	Invalid values for KeyId, certName, kSecretName, and certAlgorithm are not being validated in the OAuthValidator configuration.	There is no impact on the traffic. **Workaround:** While configuring the OAuthValidator, the operator must ensure proper values are used.	24.1.0	3
36285762	After restarting the NSselection pod, NSSF is transmitting an inaccurate NF Level value to ZERO percentage.	After restarting the NsSelection pod, NSSF is transmitting an inaccurate NF Level value.	There is no impact on the traffic. **Workaround:** NA	23.4.0	3
36265745	NSSF is only sending NF-Instanse/NF-Service load level information for multiple AMF Get Requests	When multiple AMF are sending requests to NsSelection microservice, then for some requests, only NF-Instance scope LCI headers are received or only NF-Service scope LCI headers are received.	There is no impact on the traffic. **Workaround:** There is no workaround available.	23.4.0	3
35971708	while pod protection is disabled, OcnssfIngressGatewayPodResourceStateMajor alert is not clear and resource metric is not updating to -1	When the Pod Protection feature is disabled, the previous alerts are not getting cleared.	There is no impact on the traffic. **Workaround:** There is no workaround available.	23.3.0	3
35922130	Key Validation is missing for Ingress Gateway pod protection parameter name configuration	The Ingress Gateway REST API configuration is missing validations for the POD Protection feature.	There is no impact, as the operator can configure correct values as mentioned in the guide. **Workaround:** Configure NSSF with the correct values as per the REST API guide.	23.3.0	3

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-52 (Cont.) NSSF 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35921656	NSSF should validate the integer pod protection parameter limit.	The REST API for configuring Pod Protection is missing validations.	The Pod Protection configuration is accepting invalid values. **Workaround:** The operator must ensure that the configured values should align with the guidelines provided in the documentation.	23.3.0	3
35888411	Wrong peer health status is coming "DNS SRV Based Selection of SCP in NSSF"	NSSF is not showing as unhealthy for a non-existent SCP. If peerConfiguration is set with the first peer as a non-existent SCP and the second peer as a virtual host, the peerHealth status incorrectly shows peer1 as healthy, despite it being non-existent.	There is no impact on the traffic. A non-responsive SCP is not considered for status. As a result, no status is displayed. **Workaround:** There is no workaround available.	23.3.0	3
35860137	In Policy Mapping Configuration in Ingress Gateway, For the samplingPeriod parameter, max value of parameter validation should be necessary.	Rest API for configuration of ocpolicymapping has missing validations.	There is no impact on the traffic. **Workaround:** The operator must ensure the configuration values should align with the guidelines provided in the documentation.	23.3.0	3
37622760	NSSF should send 415 responses to ns-selection and ns-availability requests if their content type is invalid.	NSSF responds with the 405 error instead of the 406 error when an invalid header value for Content-Type is provided.	There is no impact on the traffic. **Workaround:** NA	25.1.100	4

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-52 (Cont.) NSSF 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37617910	If ns-selection and ns-availability are invalid Accept Header, NSSF should not send 404 responses of UnSubscribe and subscription patch request. it should be 406 error code and "detail":"No acceptable".	NSSF responds with the 405 error instead of the 406 error when an invalid header value for Access-Type is provided.	There is no impact on the traffic. **Workaround:** There is no workaround available.	25.1.100	4
37612743	If URLs for ns-selection and ns-availability are invalid, NSSF should return a 400 error code and title with INVALID_URI.	NSSF responds with the 405 error instead of the 400 error when an invalid URI is provided.	There is no impact on the traffic. **Workaround:** There is no workaround available.	25.1.100	4
37606772	3-site GR setup ASM and Oauth Enabled: 15K TPS Traffic on SITE1 : we observed the 503 SERVICE_UNAVAILABLE error code	In an overload scenario, when 155% of traffic is sent, NSSF intermittently responds with the 503 error.	There is minimal impact on traffic in an overload scenario. **Workaround:** There is no workaround available.	25.1.100	4
37592343	Subscription Patch should be a part of Availability Sub Success (2xx) % panel in Grafana Dashboard	The Grafana dashboard does not include the subscription patch in the status of NsAvailability Pod state computation.	There is no impact on the traffic. **Workaround:** There is no workaround available.	25.1.100	4
36881883	In Grafana, Service Status Panel is showing more than 100% for Ns-Selection and Ns-Avaliability Data	The Grafana dashboard is showing more than 100% success, which is incorrect.	There is no impact on the traffic. **Workaround:** There is no workaround available.	24.2.0	4
36653494	If KID is missing in access token, NSSF should not send "Kid missing" instead of "kid configured does not match with the one present in the token"	The error response text is not in line with the expected format.	There is no impact on the traffic. **Workaround:** There is no workaround available.	24.1.0	4

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-52 (Cont.) NSSF 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35986423	Both Ingress Gateway pod protection and overload feature enabled, NSSF is not clearing the overload alerts when overload feature disabled in runtime.	Alerts for Overload Control are not getting cleared when the feature is disabled.	There is no impact on the traffic. **Workaround:** There is no workaround available.	23.3.0	4
35986361	NSSF will not modify the weight values in metrics simultaneously if the weight value changes. The weight metric has changed when any pod raises a new alarm.	NSSF, as part of pod protection, raises alerts when the pod is in a DOC (Dead or Clogged) condition. The issue is that once an alert is raised, it does not subside even after the condition is updated.	There is no impact on the traffic, as NSSF manages the condition. However, the alert subsides only when there is a change in state. **Workaround:** There is no workaround available.	23.3.0	4
35855377	The abatementValue less than onsetValue should be validated by NSSF in the Overload Level Threshold Configuration.	The Ingress Gateway REST API configuration is missing validations for the Overload feature.	There is no impact on the traffic, as the operator can configure the Overload feature with the correct values as mentioned in the REST API guide. **Workaround:** Configure the Overload feature with the correct values as per the REST API guide.	23.3.0	4

OCCM Known Bugs

Release 25.1.100

There are no known bugs in this release.

SCP Known Bugs

Release 25.2.102

There are no new known bugs in this release. Known bugs from 25.2.100 have been forward ported to release 25.2.102.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Release 25.2.101

There are no new known bugs in this release. Known bugs from 25.2.100 have been forward ported to release 25.2.101.

Release 25.2.100

Table 4-53 SCP 25.2.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38543852	Traffic dip observed during upgrade and rollback on SCP from 25.1.100 to 25.2.100	A decrease in traffic was observed during the upgrade and rollback of SCP from SCP 25.1.100 to SCP 25.2.100.	• During the upgrade from SCP 25.1.100, some requests may fail if they are directed to terminating scp-worker pods. Consumers NF should retry these failed requests or implement alternate routing. • The issue appears to be isolated to SCP 25.1.100 and does not impact SCP 25.2.100. **Workaround:** Consumer need to be configured to retry or alternate route the failed requests.	2	25.2.100
38619677	SCP 25.2.100 - Inconsistent Values for serviceIpFamilies in CV File vs. Installation Guide	The allowed values for the serviceIpFamilies section in the `custom_values.yaml` file are listed as "IPv4, IPv6 in array," but the draft *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide* specified different valid options in the "Global Parameters" section.	A minor comment correction in the `custom_values.yaml` file. It does not have any functional impact. **Workaround:** None	3	25.2.100
38071919	Port is not derived from NFProfileLevelAttrConfig in case of ModelD Notification and SCP does AR using hardcoded port 80	When a Model-D notification is received, the port is not correctly derived from NFProfileLevelAttrConfig, resulting in SCP using a hard-coded port 80 for alternate routing.	The default port 80 is used irrespective of scheme for notification routing. Also, the port and scheme for the profile level FQDN or IP are not considered. The impact is limited to routing of non-default notification messages as part of Model-D. **Workaround:** None	3	25.1.200

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-53 (Cont.) SCP 25.2.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38008367	Overlapping regex validation missing for apiSpecificResourceUri in routing config API	The routing configuration REST API allows overlapping regex patterns in the `apiSpecificResourceUri` field, leading to ambiguous routing when a request matches multiple patterns.	There is conflicting routing config set selection in case of overlapping regex in `apiSpecificResourceUri`. **Workaround:** Overlapping regex should not be configured.	3	25.1.100
37970295	Worker pod restart observed due to coherence timeout when single cache pod is used	When increasing the number of worker pods from 1 to 23 with only one cache pod in use, worker pods restart due to coherence timeout.	It does not have any impact as SCP redeployment is required to update `nfsetid` and not a recommended change. **Workaround:** None	3	25.1.200
37969345	topologysourceinfo REST API is not case sensitive for nfType	When updating the Topology Source of an NF Type from LOCAL to NRF using the PUT method, the REST API successfully processes the request without errors, but SCP triggers an on-demand audit with `nfType=udm`, resulting in empty NF responses.	The REST API with a case not matching the 3GPP specified NFType would result in an empty response. **Workaround:** Provide `NFType` as per the 3GPP standard.	3	23.4.0
37887650	Crash observed on SCP-Worker with traffic feed enabled with 2 trigger points when Traffic exceeds 7K req/sec	When traffic feed is enabled with two trigger points, the SCP-Worker crashes if traffic exceeds 7K requests per second.	The SCP-Worker pod restarts when the traffic feed requests are overloaded. **Workaround:** Traffic is redistributed to other pods.	3	25.1.200
37622431	Audit failures observed during overload situation when traffic is operating at maximum rated capacity and surpasses the pod limits by 50%.	When traffic is operating at maximum rated capacity and exceeds the pod limits by 50%, audit failures are observed while SCP is in the overload condition.	In overload conditions, SCP-Worker pod protection mechanism discards some of the internally generated NRF audit requests. **Workaround:** Audit is periodic in nature and eventually successful when the overload condition subsides.	3	25.1.100
37575057	Duplicate Routing when producer responses with location header in 3xx cases	SCP performs duplicate routing when the producer NF responds with the location header in 3xx cases.	SCP will send requests to producer NF again if the producer NF in redirect URL and alternate routing rules are the same. **Workaround:** None	3	25.1.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-53 (Cont.) SCP 25.2.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36757321	Observed 429's due to pod overload discards during upgrade from 24.1.0 to 24.2.0-rc.5	During an upgrade from SCP 24.1.0 to 24.2.0, five worker nodes consumed more than six vCPUs while handling 60K MPS, resulting in the generation of 429 errors.	Some discards might be observed during an upgrade in case of bursty traffic due to the SCP-Worker pod protection mechanism. **Workaround:** It is recommended to perform an upgrade during low traffic rate to avoid pod overload.	3	24.2.0
37995299	SCP not able to delete foreign SCP routing details post deregistration	When a foreign SCP profile is unregistered, SCP fails to remove the associated routing details for certain profiles.	Some foreign SCP routing rules are not cleared if nfsetId is updated. **Workaround:** None	3	25.1.200
37949191	ocscp_metric_nf_lci_tx_total metric is incrementing even when no LCI headers are received from peer NFs	The `ocscp_metric_nf_lci_tx_total` metric incorrectly increments even when no LCI headers are received from peer NFs.	It has a minor observability impact. **Workaround:** None	3	25.1.200
36600245	SCPIgnoreUnknownService Alerts is not getting raised for all the ignored services at SCP	The SCPIgnoreUnknownService alert is not raised for all ignored services, with only the first ignored service triggering an alert.	An alert will not be raised for the first occurrence of an unknown service. **Workaround:** The INFO alert is raised from the second occurrence onward with minimal impact.	3	24.2.0
37572287	Multiple worker pods restart observed in the event of cache pods get into a restart state when traffic is running at 730K MPS	Multiple scp-worker pods restart when scp-cache pods enter a restart state during traffic at 730 K MPS.	The issue occurs only when all scp-cache pods are forcefully shut down simultaneously during high-rate traffic. Graceful shutdown of scp-cache pods does not cause the issue, and there is no impact if at least one scp-cache pod is running. **Workaround:** It is not recommended to perform force shutdown of pods.	3	25.1.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-53 (Cont.) SCP 25.2.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37554502	SCP-worker pod restart with overload errors observed on newly spawned pods after 25% or 50% of the SCP-worker pods goes into a restart state	Newly spawned SCP-worker pods restart and show overload errors after 25% or 50% of the SCP-worker pods enter a restart state.	The SCP-Worker pod occasionally restarts due to a startup probe failure when it cannot retrieve configuration during startup. This issue occurs only during startup, so there is no functional impact because the pod has not started handling traffic. **Workaround:** Pod recovers after the restart when it is able to get configuration.	3	25.1.100
38444738	ocscp_nf_end_point value is not coming in ocscp_metric_5gsbi_rx_req_total	SCP does not identify notification requests with the callback header and XFCC header for partial matching against the callback header from the notification sender configuration in the routing option config.	The ocscp_nf_end_point dimension is not applicable for metric. There is no functional impact. **Workaround:** None	3	25.2.100
38523731	Configuration Pre install hooks stuck if "+" in DB password	The configuration preinstall hooks get stuck when attempting to establish a connection with the database if the database password is set to Password123+123+123.	Install or upgrade failure occurs if "+" is used in the DB password. **Workaround:** Do not use "+" in the DB password.	3	25.2.100
37886252	High memory consumption in OSO was observed during traffic runs at 730K MPS, primarily due to high-cardinality samples generated by SCP.	A high memory consumption in OSO is observed during the traffic run at 730K MPS, mainly due to high-cardinality samples generated by SCP.	Retrieving metrics from OSO is slow because of a large number of samples. **Workaround:** None	3	25.1.100
38317992	SCP worker pod throttles egress traffic when remote server does not send max concurrent stream	The SCP-worker pod throttles egress traffic when the remote server does not send the maximum concurrent stream value.	SCP configures maximum concurrent streams to 1 if no value is specified by producer NF, impacting concurrent requests on a connection. **Workaround:** Provide a maximum concurrent streams value from producer NF.	3	25.1.100
36926043	SCP shows unclear match header and body in mediation trigger points	In the Mediation Trigger Points feature, SCP displays unclear text instead of the expected match header and body information.	It does not have any functional impact. **Workaround:** None	4	24.2.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-53 (Cont.) SCP 25.2.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38079614	SCP All Services: Remove use of java.util.date and org.joda.time. Use java.time instead because of threadsafety and better method list..	SCP services relies on `java.util.date` and `org.joda.time` for date and time handling, which are not thread-safe and lack modern functionality.	It does not have any impact as it is a minor code enhancement. **Workaround:** None	4	25.1.200
38004328	Installation guide has incorrect definition of mediation_status parameter	The `mediation_status` parameter was incorrectly set to true in the `custom.values.yaml` file configuration. This configuration is intended for production use, which may lead to unintended behavior or errors when deployed.	The SCP NF profile that is getting registered with NRF can have the `mediation_status` attribute, which is not required. It has no functional impact. **Workaround:** This attribute can be commented in the SCP deployment file.	4	25.1.100
37543889	SubscriptionInfo is getting ignored in case if User comments out customInfo in NRF Details.	If the `customInfo` field is commented out in the NRF profile within the deployment `values.yaml` file and `subscriptionInfo` is set to true with a specified scheme, the code incorrectly ignores the provided scheme and instead extracts the scheme from `ScpInfo`.	This issue appears only if the customInfo section of NrfProfile is removed from the deployment file. **Workaround:** The `subscriptionInfo` parameter is documented in Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide should not be deleted.	4	25.1.100
38098107	SCP is Not considering Version and Trailer fields from Jetty response	SCP is not considering version and trailer fields from Jetty responses.	It does not have any impact as fields are not currently used. **Workaround:** None	4	25.1.200
38614032	Request to Clarify nativeEgressHttpsSupport Comment Line in SCP Custom Values yaml file	The comment lines for the `nativeEgressHttpsSupport` setting contains unclear use of the "PNF" acronym, and instances of "Producer NF" terminology are identified where "Server NF" is more appropriate.	It does not have any functional impact. Only a comment is changed in the deployment file. **Workaround:** None	4	25.2.100
38526996	Fix low severity code issue identified during 25.2.100 release Code Audit	The objective of this issue is to resolve all low-severity code issues found during the SCP 25.2.100 code audit.	A minor code enhancements with no functional impact. **Workaround:** None	4	25.2.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-53 (Cont.) SCP 25.2.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38471475	Problem Details update for notificationSender parameter in Routing Option Config API	The Routing Options Config API does not return the expected error messages when the mandatory `apiNameAxHeading` parameter is missing, invalid, or provided as an empty string in the PUT request.	It has incorrect problem details on incorrect the `notificationSender` parameter configuration with no functional impact. **Workaround:** None	4	25.2.100
38471270	SCP is sending 400 response code instead of 404 for OSCP-WRK-NFSEL-E001 Error ID	SCP returns a 400 error code with a specific response when NRF configuration table contained incorrect NRF set details.	The consumer NF receives incorrect error code when incorrect NRF set details are configured. **Workaround:** Configure correct NRF set details.	4	25.1.200

Copyright © 2019, 2026, Oracle and/or its affiliates.

SEPP Known Bugs

Release 25.2.100

Table 4-54 SEPP 25.2.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
38449487	Discrepancy in server header value in response to consumer and message copy to NIF	A discrepancy is observed in the server header in the response to the consumer and the message copy sent to NIF when the following conditions are met: • NIF is enabled • NIF error message copy is enabled • Topology Hiding is enabled (with default configuration) • The service request is rejected due to Topology Hiding/ Unhiding at pSEPP Server: SEPP-ocsepp-plmn-ingress-gateway.gg-gate-eta-asm-20301752-gate-sepp2 – This value is responded back to the consumer. "server":["SEPP-sepp2.inter.oracle.com"]} – This value is sent to NIF. Expected Value: The server header value sent to the consumer is incorrect. It should be:	The consumer receives the incorrect server header value. **Workaround:** None	3	25.2.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-54 (Cont.) SEPP 25.2.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
		SEPP-sepp2.inter.oracle.com			
38390393	"configMgrNoHealthyNIFAlert" does not get cleared if NIF feature is disabled	The "configMgrNoHealthyNIFAlert" remains uncleared even after the NIF feature is disabled. Steps: Enable the NIF feature. 1. Do not register NIF in NRF. 2. Wait for the alert "configMgrNoHealthyNIFAlert."Disable the NIF feature. The alert stays active even after disabling the NIF feature.	The customer continues to receive the NIF alert, despite having disabled the NIF feature. **Workaround:** None	3	25.2.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-54 (Cont.) SEPP 25.2.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
38278479	Getting "No https instances configured" intermittently in PLMN EGW logs	The "No https instances configured" error appears intermittently in the PLMN EGW logs. Steps to reproduce: 1. Register NIF in NRF. 2. Enable the NIF feature on SEPP. 3. Run a traffic mix at 1K. 4. The following error appears in the PLMN EGW logs: `{"instant":{"epochSecond":1754383985,"nanoOfSecond":471394161},"thread":"egw-app-thread8","level":"ERROR","loggerName":"ocpm.cne.gateway.exception.EgressGatewayExceptionHandler","message":"Exception occurred for routeId: nifPeer and destination: ocsepp.com:80. errorMessage: featureName='SbiRoutingFeature-seppDisabled', routeId='nifPeer', errorReason='No https instances configured', status='500 INTERNAL_SERVER_ERROR'`	Even though no HTTPS peer is configured, the EGW intermittently tries to route the message to an HTTPS peer. **Workaround:** None	3	25.2.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-54 (Cont.) SEPP 25.2.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
		errorCause: errorStackTrace: ocpm.cne.gateway.filters.sbi.util.SbiRoutingRulesEngine.seppDisabledProcessing(SbiRoutingRulesEngine.java:602),","endOfBatch":false,"loggerFqcn":"org.apache.logging.log4j.spi.AbstractLogger","threadId":137,"threadPriority":5,"messageTimestamp":"2025-08-05T08:53:05.471+0000","ocLogId":"${ctx:ocLogId}","xRequestId":"${ctx:xRequestId}","pod":"ocsepp-plmn-egress-gateway-5ffc6b84f8-6thtg","processId":"1","instanceType":"prod","egressTxId":"egress-tx-1644560773"}			
38257593	pn32f memory usage keep on increasing at 550 TPS with cat3 time check enabled	The memory usage on PN32F keeps increasing with 550 TPS when the Cat-3 Time Check feature is enabled.	Memory usage is constantly increasing. **Workaround:** Disable CAT-3Time Check feature is not in use.	3	25.1.200

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-54 (Cont.) SEPP 25.2.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
38188255	Different error codes (nif enabled and disabled) for timeout when there is a delay of 1000 ms at server	Different timeout error codes are received by the consumer when NIF is enabled and disabled. This behavior should be consistent. Scenario 1: • Server delay of 1000ms • NIF is enabled • Send service request: The following response is received by the consumer: 504 GATEWAY_TIMEOUT 1100 ms Scenario 2: • Server delay of 1000ms • NIF is disabled • Send service request: The following response is received by the consumer: `{"type":null,"title":"Request Timeout","status":408,"detail":"sepp2.inter.oracle.com: egressgateway: Request Timeout: OSEPP-EGW-E002","instance":null,"cause":"Request Timeout at EGW","invalidParams":null}`	The user sees different timeout errors when NIF is enabled. **Workaround:** None	3	25.2.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-54 (Cont.) SEPP 25.2.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
38374302	content-type should be updated for invalid value for /sepp-configuration/v1/nif/msg-copy/params	The Content-Type should be updated to reflect an invalid value for /sepp-configuration/v1/nif/msg-copy/params when: • A long string is supplied for apiName while updating NIF message copy parameters. • The response is 400. • The Content-Type is application/json instead of application/problem+json.	In case of an error, the user sees the Content-Type as application/json instead of application/problem+json. **Workaround:** None	4	25.2.100
37818065	Errors being reported in SEPP plmn egw pod logs intermittently	Intermittent errors are being observed in the PLMN EGW pods, even in the absence of traffic. The error message reads: 'Watcher exception due to: errorMessage: Resource version too old: 464623931 (current version: 554740871) errorCause: Resource version too old: 464623931 (current version: 55474087)" Base Bug on GW 38082705	Unnecessary log flooding observed on the plmn-egress-gateway pod. **Workaround:** None	4	25.1.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

SEPP 25.2.100 Gateway Known Bugs

Table 4-55 SEPP 25.2.100 Gateway Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
38115706	[SEPP-NRF] NRF-client jaeger traces are not getting linked to egress-gateway microservices on Jaeger	Autonomous and on-demand nrf-client requests are visible in the Jaeger traces, but they are not linked to the next microservice, i.e., plmn-egress-gateway in SEPP. The trace should include all spans across microservices that it spans, ensuring full trace visibility across the workflow.	Jaeger traces from nrf-client are not linked to parent spans, requiring the flow to be mapped manually. This disconnect disrupts the trace continuity across microservices. **Workaround:** None	3	25.1.100
35898970	DNS SRV Support-The time taken for cache update is not same TTL value defined in SRV record.	The time taken to update the cache does not align with the TTL defined in the SRV records. In some cases, the cache updates before the TTL expires, while in other instances, it updates after the TTL has passed. The expectation is the cache should update exactly as per the TTL. For example, if the TTL is set to 60 seconds, the cache should update once every 60 seconds, only after the TTL has expired.	If the priority or weight is changed, it may take longer than the TTL for the cache to update and for the changes to be reflected in the environment. **Workaround:** After updating the configuration, restart both the n32-egress-gateway and alternate-route-svc.	3	23.4.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-55 (Cont.) SEPP 25.2.100 Gateway Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
36263009	PerfInfo calculating ambiguous values for CPU usage when multiple services mapped to single pod	In the cgroup.json file, multiple services are mapped to a single endpoint, which leads to ambiguity in CPU usage calculations. This has impacted the overall load calculation.	The overall load calculation is inaccurate, which can lead to incorrect information about the system's load. **Workaround:** None	3	23.4.1
36614527	[SEPP-APIGW] Overload Control discard policies not working with REST API and CNCC	The default values for Overload Control discard policies cannot be edited or changed. When attempting to save the configuration, the following error is thrown: "ocpolicymapping does not contain this policy name." This same issue occurs when using the REST API as well.	Users will not be able to edit Overload Discard Policies through the CNC Console. **Workaround:** Helm configuration can be used to configure Overload Discard Policies, allowing users to manage these settings outside of the CNC Console.	3	24.2.0

UDR Known Bugs

Release 25.1.202

There are no new known bugs in this release. Known bugs from 25.1.200 have been forward ported to release 25.1.202.

Release 25.1.201

There are no new known bugs in this release. Known bugs from 25.1.200 have been forward ported to release 25.1.201.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Release 25.1.200

Table 4-56 UDR 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38011942	ocudr-custom-values-25.1.100.yaml (used for EIR and SLF) does not expose containerPortNames	The ocudr-custom-values-25.1.100.yaml file used for Equipment Identity Register (EIR) and Subscriber Location Function (SLF) does not expose containerPortNames that are required to provision the backendPortName in the Cloud Native Load Balancer (CNLB) annotations.	There is no impact. **Workaround:** You must change the port names from the internal charts.	3	25.1.100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-56 (Cont.) UDR 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release

38089584	PROVGW- We observed ERROR log related to alternate-route on PROVGW egress pod	While executing 50K lookups and 1.44K provisioning on the Subscribe Location Function (SLF) site1 through provisioning gateway, an error occurred when scaling the egress gateway from two to zero replicas for 15 minutes and then recovering it back to two replicas. The error is related to the alternate route and was consistently observed on the provgw egress.	There is no impact.
			Workaround:
			You must update the *egressgateway* section of the custom_values yaml file as follows:
			`sbiRouting:`
			`peerConfiguration:`
			`peerSetConfiguration:`
				3	25.1.200

Common Services Known Bugs

ATS Known Bugs

Release 25.1.100

There are no known bugs in this release.

ASM Configuration Known Bugs

Release 25.2.100

There are no known bugs in this release.

Alternate Route Service Known Bugs

Release 25.1.100

There are no known bugs in this release.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Egress Gateway Known Bugs

Table 4-57 Egress Gateway 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36730017	Register request towards alternate-route is giving incorrect response of 200	While performing the register request, Gateway Services received a 200 OK response, where the FQDN entry is not present in the DNS server.	While performing Alternate Route Services register request, success response is received when the FQDN entry is absent in the DNS server. **Workaround**: There is no workaround available.	4	24.1.0
35948415	The PUT API allows you to add cause values to the "sbiroutingerrorcriteriasets" in policy 23.2.2.	The PUT API allows you to add cause values to sbiroutingerrorcriteriasets in Policy 23.2.2. The following parameters are introduced in the Error cause-based re-try feature in 23.2.6 and 23.4.0 patch releases, however, these parameters could be configured in the previous releases: "cause": { "path": ".cause", "reason": ["UNSPECIFIED_MSG_FAILURE","SUBSCRIPTION_NOT_FOUND"],	Non-applicable configuration is getting allowed with PUT API operation. **Workaround**: There is no workaround available.	3	23.2.2

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-57 (Cont.) Egress Gateway 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37355062	occnp_oc_egressgateway_peer_health_status reports incorrect peer health from one pod	The `occnp_oc_egressgateway_peer_health_status` metric was getting pegged correctly on the Egress Gateway leader pod but was not getting updated on non-leader Egress Gateway pods, causing inconsistent status between a leader and a non-leader pod for the same peer.	When the metric was fetched from the non-leader pod, it was showing an incorrect status compared to the leader pod. **Workaround**: There is no workaround available.	3	23.4.3
37501092	Egress Gateway not retrying to sameNRF or Next NRF when "errorCodes: -1" for errorSetId: 5XX on retryErrorCodeSeriesForNex/SametNrf OauthClient configuration	Egress Gateway does not treat -1 as all errors codes correctly for 5XX errors as it does for 4XX errors. So, when you use -1 to cover all 5XX errors, it does not work as expected.	Any rule that depends on -1 to catch all 5XX errors may not work. **Workaround**: There is no workaround available.	3	24.2.5
37451580	Metric not getting pegged after health ping request is sent towards a peer	The required number of parameters to peg `oc_egressgateway_peer_health_ping_request_total` and `oc_egressgateway_peer_health_ping_response_total` metrics were inconsistent when vfqdn was present and vfqdn was absent.	The metric was showing inconsistent behavior while pegging. **Workaround**: There is no workaround available.	4	24.2.9

Copyright © 2019, 2026, Oracle and/or its affiliates.

Ingress Gateway Known Bugs

Table 4-58 Ingress Gateway 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36677373	NRF- Missing mandatory "iat claim" parameter validation is not happening in CCA header for feature - CCA Header Validation	As per the feature description, "iat" is a mandatory parameter in JWT claims. When CCA header request is sent without "iat" claim and "maxTokenAge": 0 is set in /nrf/nf-common-component/v1/igw/ccaheader. The missing mandatory parameter is not validated, and the CCA header request gets accepted by NRF.	Mandatory validation to be performed on parameter would be missed at Gateway Services and request would be processed. **Workaround**: There is no workaround available.	3	23.2.0
36464641	When feature Ingress Gateway POD Protection disabled at run time alerts are not getting cleared and metrics are getting pegged in NRF 23.4.0	When the Ingress Gateway Pod Protection feature is disabled at run time, alerts are not getting cleared and metrics are getting pegged in NRF 23.4.0.	Alerts are not getting cleared and metrics would be pegged even when feature is disabled during run time. **Workaround**: There is no workaround available.	3	23.4.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-58 (Cont.) Ingress Gateway 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35526243	Operational State change should be disallowed if the required pre-configurations are not present	Currently, the operational state at Ingress Gateway can be changed even if thecontrolledshutdownerrormapping and errorcodeprofiles are not present. Thisindicates that the required action of rejecting traffic will not occur. There must be a pre-check to check for these configurations before allowingthe state to be changed. If the pre-check fails, the operational state shouldnot be changed.	Request will be processed by Gateway Services when it is supposed to be rejected. **Workaround**: There is no workaround available.	3	23.2.0
34610831	IGW is accepting incorrect API names with out throwing any error	Ingress Gateway is accepting incorrect API names without displaying any error. If there is a typo in the configuration UDR, the command should get rejected. Otherwise, it gives the wrong impression that the configuration is correct but the desired behavior is not observed.	The non-existing resource name would be pretended to be successfully updated in REST configurations . **Workaround**: There is no workaround available.	3	22.2.4

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-58 (Cont.) Ingress Gateway 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37483564	NPE observed in IGW during traffic run	NPE is emitted by the PreGateway filter when trying to peg the response_processing_latency metric. The metric value is calculated when the response was received by the PostGateway filter and the time it took to reach the PreGateway filters. The PostGateway filter is supposed to add the ResponseReceivedTime attribute to the response. The PreGateway filter makes an assumption that ResponseReceivedTime is always present in the response. In case of discard due to overload control, the PostGateway filter is never invoked and ResponseReceivedTime is never added. The code to peg tries to get a ResponseReceivedTime attribute from the exchange, which is missing. This NPE is observed by Spring and pegged as http_server_requests_seconds_count.	NPE is emitted by the PreGateway filter when trying to peg the response_processing_latency metric. The exception was observed and handled by Spring Cloud Gateway. **Workaround**: There is no workaround available.	3	23.4.6

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-58 (Cont.) Ingress Gateway 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37506720	Overload Discard Percentage for NRF Microservices	Ingress Gateway handles both Access Token and Discovery traffic using a single microservice and a shared configuration. Due to significant differences in traffic volumes, this approach leads to suboptimal overload control behavior.	This unified handling of both Access Token and Discovery traffic causes performance degradation, especially under high Discovery load, potentially leading to unnecessary throttling or delayed responses for Access Token requests. **Workaround**: Perform local discard to remove excess requests locally without involving coherence or global coordination mechanisms.	2	24.2.11
35913189	Missing validation of the failureReqCountErrorCodeSeriesId mandatory parameter in the Ingress Gateway's Routes Configuration	As per NSSF_REST_Specification_Guide, Section 5.2.1.5, failureReqCountErrorCodeSeriesId is a mandatory parameter for Routes Configuration in Ingress Gateway. The request is rejected by Ingress Gateway when the failureReqCountErrorCodeSeriesId parameter is not present in the JSON payload.	Requests will be processed by considering the mandatory configuration from the existing deployment configuration when it is not configured through REST APIs. **Workaround**: There is no workaround available.	4	23.3.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Common Configuration Service Known Bugs

Release 25.1.100

There are no known bugs in this release.

Helm Test Known Bugs

Release 25.2.1xx

There are no known bugs in this release.

Mediation Known Bugs

Release 25.2.100

There are no known bugs in this release.

NRF-Client Known Bugs

Release 25.2.1xx

There are no known bugs in this release.

App-Info Known Bugs

Release 25.2.1xx

There are no known bugs in this release.

Perf-Info Known Bugs

Release 25.2.1xx

There are no known bugs in this release.

Debug Tool Known Bugs

Release 25.2.1xx

There are no known bugs in this release.

Copyright © 2019, 2026, Oracle and/or its affiliates.