Oracle® Communications

Cloud Native Core Release Notes

Release 3.25.2.100.0
G42905-03
November 2025

Oracle Communications Cloud Native Core Release Notes, Release 3.25.2.100.0

G42905-03

Contents

Preface

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

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.

What's New In This Guide

Release 3.25.2.100.0 - G42905-03, November 2025

- Updated the compatibility details of CNC Console, cnDBTier, and SCP release 25.2.100 in the Compatibility Matrix section.
- Added UDR in the upgrade path note in the Media Pack section.

Release 3.25.2.100.0 - G42905-02, November 2025

BSF 25.2.100 Release

Updated the Compatibility Matrix section with the details of BSF release 25.2.100.
Policy 25.2.100 Release

Updated the Compatibility Matrix section with the details of Policy release 25.2.100.

Release 3.25.2.100.0 - G42905-01, November 2025

General Updates:

Updated the Generic Open Source Software Compatibility on Any Platform section to provide information about the open source software compatibility with CNC NFs for 3.25.2.1xx.0 release.

BSF 25.2.100 Release

Updated the following sections with the details of BSF release 25.2.100:

- Binding Support Function (BSF)
- Media Pack
- Compatibility Matrix
- 3GPP Compatibility Matrix
- Common Microservices Load Lineup
- BSF Security Certification Declaration
- BSF Resolved Bugs
- BSF Known Bugs

cnDBTier 25.2.100 Release

Updated the following sections with the details of cnDBTier release 25.2.100:

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

Console 25.2.100 Release

Updated the following sections with the details of Console release 25.2.100:

- Cloud Native Configuration Console (CNC Console)

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- CNC Console Security Certification Declaration
- CNC Console Resolved Bugs
- CNC Console Known Bugs

OCCM 25.2.100 Release

Updated the following sections with the details of OCCM release 25.2.100:

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

OSO 25.2.100 Release

Updated the following sections with the details of OSO release 25.2.100:

- Operations Services Overlay (OSO)
- Media Pack
- OSO Resolved Bugs
- OSO Known Bugs

Policy 25.2.100 Release

Updated the following sections with the details of Policy release 25.2.100:

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

SCP 25.2.100 Release

Updated the following sections with the details of SCP release 25.2.100:

- 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 25.2.100 Release

Updated the following sections with the details of SEPP release 25.2.100:

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

UDR 25.2.100 Release

Updated the following sections with the details of UDR release 25.2.100:

- 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

- ATS Resolved Bugs
- Alternate Route Service Resolved Bugs
- Common Configuration Service Resolved Bugs
- Egress Gateway Resolved Bugs
- Ingress Gateway Resolved Bugs

Common Services Known Bugs

- Egress Gateway Known Bugs
- Ingress Gateway Known Bugs

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.

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 3.25.2.1xx.0.

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

2.1 Automated Testing Suite (ATS) Framework

Release 25.2.100

Oracle Communications Cloud Native Core, Automated Testing Suite (ATS) Framework 25.2.100 includes the following enhancements:

- **ATS API**: This enhancement enables ATS to use tags and stages in the requests. For more information, see the "Starting Jobs" section in *Oracle Communications Cloud Native Core Automated Testing Suite Guide*.
- **Parallel Test Execution**: This enhancement enables ATS to run test cases of both new features and regression pipelines. For more information, see the "Merged Execution" section in *Oracle Communications Cloud Native Core Automated Testing Suite Guide*.

2.2 Binding Support Function (BSF)

Release 25.2.100

Oracle Communications Cloud Native Core, Binding Support Function (BSF) 25.2.100 includes the following enhancements:

- **TLS 1.3 Support for Kubernetes API**: BSF can be deployed in a Kubernetes cluster that supports TLS 1.3. For more information, see the "Installing BSF" section in *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.
- **Support for Grafana 7.5.x**: BSF supports Grafana version 7.5.x. For more information, see the "Software Requirements" section in *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.
- **Disabling Audit on Controlled Shutdown**: The controlled shutdown feature is enhanced with impact of disabling audit service during controlled shutdown. For more information see "Controlled Shutdown of an Instance" section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.
- **Rx enhancement to add custom AVP for direct lookup of N7 session**: BSF supports to optimize the N7 session lookup for AAR-I messages in Rx call flows. BSF stores the cookie received in the binding registration request from Policy. Whenever BSF receives a AAR-I from an AF, it searches for the PCF identity of the Rx session and the cookie stored in the database. If the details are present, BSF shares it with Policy in a cookie along with

the AAR-I request. For more information, see "Support for Optimizing N7 Session Lookup for AAR messages in Rx Call Flows" section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.

- **Burst rate limit modification and customization for WARN logs for All BSF services**: In order to control the volume of logs, BSF allows to add a burst filter for logging against logs for all the microservices. The Burst filter provides a mechanism to control the rate at which LogEvents are processed by silently discarding events after the maximum limit has been reached. It enables to control the frequency and volume of warning messages generated. This ensures that excessive logging does not overwhelm the system or obscure critical information. For more information, see "Logging Support for Error Response" 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-9144	Support for TLS 1.3 on Internal API Communication
Oracle Communications Cloud Native Core, Binding Support Function - 25K Active Subscribers Perpetual	CCNC-10672	Support for Grafana 7.5.x

2.3 Cloud Native Core cnDBTier

Release 25.2.100

Oracle Communications Cloud Native Core, cnDBTier (cnDBTier) 25.2.100 includes the following enhancements:

- **Application Service Mesh (ASM) for External Communication**: This feature enables secure external communication through ASM (Application Service Mesh) by selectively applying Istio sidecar injection only to pods where external communication is involved. By selectively enforcing ASM policies, cnDBTier ensures the security and compliance of its external interfaces, while preserving high performance and simplifying manageability within the cnDBTier ecosystem.

  For more information, see the "Application Service Mesh (ASM) for External Communication" section in *Oracle Communications Cloud Native Core, cnDBTier User Guide*.

- **Support for Automated Certificate Lifecycle Management**: This feature enables automated TLS certificate lifecycle management for HTTPS, MySQL replication SQL pods and MySQL application SQL pods within the cnDBTier environment, ensuring secure and uninterrupted communication during certificate updates.

  For more information on the Backup Status API, see the "Support for Automated Certificate Lifecycle Management" section in *Oracle Communications Cloud Native Core, cnDBTier User Guide*.

- **Support for Grafana 7.5.x and 9.5.x**: This feature supports Grafana versions 7.5.x along with 9.5.x. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide.*

- **New Real Time Replication Status REST APIs Across All Sites** : This feature enhancement provides the following new real time cnDBTier Replication Status APIs across all sites.
  - http://*base-uri*/db-tier/replication/status/realtime)
  - http://*base-uri*/db-tier/replication/status/realtime/sitename/{siteName})
  - http://*base-uri*/db-tier/replication/status/realtime/sitename/{siteName}/remotesitename/{remoteSiteName}
  - http://*base-uri*/db-tier/replication/status/realtime/sitename/{siteName}/remotesitename/{remoteSiteName}/replgrourpid/{replGrourpId}

  For more information on the Replication Status REST APIs, see the "cnDBTier APIs" section in *Oracle Communications Cloud Native Core, cnDBTier 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 2-2 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Certificate Management - 25K Active Subscribers	CCNC-8162	Application Service Mesh (ASM) for External Communication
Oracle Communications Cloud Native Core, Certificate Management - 25K Active Subscribers	CCNC-8478	Support for Automated Certificate Lifecycle Management
Oracle Communications Cloud Native Core, Unified Data Repository - 25K Active Subscribers Perpetual	CCNC-10676	Support for Grafana 7.5.x and 9.5.x

2.4 Cloud Native Configuration Console (CNC Console)

Release 25.2.100

Oracle Communications Cloud Native Configuration Console (CNC Console) 25.2.100 includes the following enhancements:

- **Multiple Cluster Support for ASM Deployments**: Console multiple cluster support for ASM deployments has now been enabled. The procedure to migrate from a single cluster, single instance deployment to a multiple cluster, multiple instance deployment has been documented. CNC Console ASM Helm charts have been included as part of the package. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*.
- **TLS 1.3 Support for Kubernetes API** : CNC Console can be deployed in a Kubernetes cluster that supports TLS 1.3. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*.
- **CNC Console Installation and Upgrade Enhancements**: CNC Console has introduced new Helm configuration options to enhance the installation and upgrade process. In cnDBTier georeplicated environment, all database schema creation now occurs upfront at the initial site, ensuring smoother replication and minimizing errors related to schema synchronization during deployment and upgrades. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*.

- **Aligning MaxSurge and MaxUnavailable Parameter Values**: CNC Console has standardized the values of the `maxSurge` and `maxUnavailable` parameters in the CNC Console Helm charts to control deployment behavior for various CNC Console microservices. This configuration optimizes resource usage by ensuring that no extra pods are created during updates, as additional resources do not contribute to service continuity. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*
- **Support for Grafana 7.5.x**: CNC Console supports Grafana version 7.5.x. For more information, see *Oracle Communications Cloud Native Configuration Console 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 2-3 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Cloud Native Environment - per 25K Subscribers Perpetual	CCNC-9541	Multiple Cluster Support for ASM Deployments
Oracle Communications Cloud Native Core, Cloud Native Environment - per 25K Subscribers Perpetual	CCNC-9157	TLS 1.3 Support for Kubernetes API
Oracle Communications Cloud Native Core, Cloud Native Environment - per 25K Subscribers Perpetual	CCNC-11774	CNC Console Installation and Upgrade Enhancements
Oracle Communications Cloud Native Core, Cloud Native Environment - per 25K Subscribers Perpetual	CCNC-6007	Aligning MaxSurge and MaxUnavailable Parameter Values
Oracle Communications Cloud Native Core, Cloud Native Environment - per 25K Subscribers Perpetual	CCNC-10670	Support for Grafana 7.5.x

2.5 Cloud Native Environment (CNE)

Release 25.2.100

Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) 25.2.100 includes the following enhancements:

- **Secure DNS Zone Customization through CNLB**: This feature enhances the security and scalability of DNS requests by routing traffic based on domain zones, such as OAM or Signaling. It isolates DNS traffic and forwards requests through Cloud Native Load Balancers (CNLB) to external DNS servers, which are managed by the customers. For more information, see the "Secure DNS Zone Customization through CNLB" section in *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide*.
- **Support for Grafana 7.5.x and 9.5.x**: This feature supports Grafana versions 7.5.x along with 9.5.x. For more information, see the "Frequently Used Common Services" section in *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
- **Provision to Add Authentication to Container Registry**: This feature supports CNE container registry on Bastion hosts to add an authentication. Users will be able to provide username and password at the time of installation of CNE. Values are configured in the

secrets.ini file which contains the sensitive information. Once this feature is enabled user can login with the credentials to perform actions like upload images (this is done automatically for CNE provisioned users). This feature is optional, and will only work when username and password are provided in secrets.ini.
For more information, see the following sections in *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.

- Updating `cluster.tfvars` for CNLB
- Updating `cluster.tfvars` for MetalLB
- Environmental Variables

- **CNE support for CNLB nodes (OpenStack platform only)**: This feature is applicable to CNLB only and can only be used when CNE is installed with the cnlb_node_label option enabled. With this feature, users will be able to provision special type of Kubernetes nodes "cnlb_nodes". Only these nodes will be configured to run CNLB app pods. This feature is available on OpenStack platform only.
  For more information, see "Limited Kubernetes Cluster Nodes for CNLB" section in *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide*.
- **New Versions of Common Services**: The following common services are upgraded in this release:
  - Helm - 3.18.2
  - Kubernetes - 1.33.1
  - containerd - 1.7.16
  - Calico - 3.29.3
  - MetalLB - 0.14.4
  - Prometheus - 3.4.1
  - OCI Grafana - 7.5.17
  - Jaeger - 1.69.0
  - Istio - 1.24.0
  - Kyverno - 1.13.4
  - cert-manager - 1.12.4

  To get the complete list of third-party services and their versions, refer to the `dependencies_25.2.100.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.

2.6 Oracle Communications Cloud Native Core, Certificate Management (OCCM)

Release 25.2.100

Oracle Communications Cloud Native Core, Certificate Management (OCCM) 25.1.200 includes the following enhancement:

- **Certificate Screen Enhancement to Filter Certificates by Namespace Name**: OCCM has introduced the ability to filter available certificates by the name of the namespace on the Certificates GUI. This value is taken from the namespace selected in the certificate output field. For more information, see "Managing Certificates" in *Oracle Communications Cloud Native Core Certificate Management User Guide.*
- **Certificate Screen Enhancement to show Issuers in a Dropdown**: OCCM has enhanced the certificates GUI to include a dropdown for the issuer field in certificate configuration. This enables users to select from a list of issuers instead of manually entering an issuer name. For more information, see "Managing Certificates" in *Oracle Communications Cloud Native Core Certificate Management User Guide.*
- **Issuer and Certificate Screen Enhancement to show Namespaces in a Dropdown**: OCCM has enhanced the issuers and certificates GUIs to include a dropdown for the namespace field in certificate configurations. This enables users to select from a list of namespaces instead of manually entering the namespace name. For more information, see "Managing Issuers" and "Managing Certificates" in *Oracle Communications Cloud Native Core Certificate Management User Guide.*
- **Support for Grafana 7.5.x**: OCCM now supports Grafana 7.5.x. For more information, see the "Additional Software Requirements" section in *Oracle Communications Cloud Native Core Certificate Management 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 2-4 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Certificate Management - 25K Active Subscribers	CCNC-9611	Certificate Screen Enhancement to Filter Certificates by Namespace Name
Oracle Communications Cloud Native Core, Certificate Management - 25K Active Subscribers	CCNC-9609	Certificate Screen Enhancement to show Issuers in a Dropdown
Oracle Communications Cloud Native Core, Certificate Management - 25K Active Subscribers	CCNC-11042	Issuer and Certificate Screen Enhancement to show Namespaces in a Dropdown
Oracle Communications Cloud Native Core, Certificate Management - 25K Active Subscribers	CCNC-10678	Support for Grafana 7.5.x

2.7 Operations Services Overlay (OSO)

Release 25.2.100

Oracle Communications Cloud Native Core, Operations Services Overlay (OSO) 25.2.100 includes the following enhancement:

Support for new versions:

- Updated the version of oso_snapshot as 25.2.100.
- Added the oso_alert_config version as 25.2.100.
  For more information, see *Oracle Communications Cloud Native Core, Operations Services Overlay Installation and Upgrade Guide*.

2.8 Policy

Release 25.2.100

Oracle Communications Cloud Native Core, Converged Policy 25.2.100 includes the following enhancements:

- **Integration for Traffic Prioritization for NRF-Client and Egress Gateway on Policy**: This feature provides the configurations to enable or disable both Traffic Prioritization for Egress-gateway and NRF-Client in Policy to support pod protection by throttling inbound requests if they are above configured rate. For more information, see the "NRF Client Configuration" section in *Oracle Communications Cloud Native Core, Policy Installation, Upgrade, and Fault Recovery Guide*.
- **TLS 1.3 Support for Kubernetes API**: Policy can be deployed in a Kubernetes cluster that supports TLS 1.3. For more information, see the "Installing Policy" section in *Oracle Communications Cloud Native Core, Policy Installation, Upgrade, and Fault Recovery Guide*.
- **Support for Grafana 7.5.x**: Policy supports Grafana version 7.5.x. For more information, see the "Software Requirements" section in *Oracle Communications Cloud Native Core, Policy Installation, Upgrade, and Fault Recovery Guide*.
- **Support for Immediate Report Handling**: Immediate Report Handling sends urgent notifications directly to the subscribed system as soon as a relevant change is detected. There is no need to wait for next polling cycle or batch update. This ensures the PCF receives up-to-date information in real-time, improving network efficiency and user experience. For more information see "Support for Immediate Report Handling for AM-Data and UE-Policy-Set on N36 Interface" section in *Oracle Communications Cloud Native Core, Policy User Guide*.
- **Conflict Resolution for URSP Rules N1N2 transfer to UE**: The feature integrates a conflict resolution mechanism into the Policy Control Function (PCF) to analyze and rectify UPSI/URSP rule conflicts in UE Policy actions obtained from PRE during policy evaluation. This process, guided by the selected conflict resolution strategy, ensures consistent policy actions and addresses discrepancies at the evaluation stage. For more information see "Conflict Resolution for URSP Rules N1N2 transfer to UE" section in *Oracle Communications Cloud Native Core, Policy User Guide*.
- **Disabling Audit on Controlled Shutdown**: The controlled shutdown feature is enhanced with impact of disabling audit service during controlled shutdown. For more information see "Controlled Shutdown of an Instance" section in *Oracle Communications Cloud Native Core, Policy User Guide*.
- **Enhancements to PRE metrics**: Policy is enhanced with addition of "occnp_policy_project_state_change_total" and "occnp_policy_project_current_state" PRE metrics. For more information see "PRE Metrics" section in *Oracle Communications Cloud Native Core, Policy User Guide*.
- **maxSurge and maxUnavailable Configuration in all Policy Services**: Policy allows to optimize management of Pods using `maxSurge` and `maxUnavailable` parameters under the rollingUpdate and pdb categories in `custom-values.yaml` file. For more information see the "Support for Optimized POD Management Using maxSurge and maxUnavailable During Policy Upgrade" section in *Oracle Communications Cloud Native Core, Policy User Guide*.
- **Optimizing N7 Session Lookup for AAR messages in Rx Call flow**: Policy supports to optimize the N7 session lookup for AAR-I messages in Rx call flows. Whenever SM service receives a Create request for an Rx session over N7 interface, if this feature is

enabled, during binding registration, SM service sends the session details such as `SmPolicyAssociationId` and `contextOwner (PCF-SM)` in a cookie `ocnf-service-cookie` to BSF. BSF stores the details sent in the cookie in BSF Management service database. Whenever Policy receives AAR-I request from BSF, the AAR-I request from BSF includes a `OCNF-SERVICE-COOKIE` Custom AVP that contains the Rx session details such as session owner and the session identifier such as `SmPolicyAssociationId` (Primary Key). If the cookie-owner is `PCF-SM`, Diameter Gateway skips calling the Binding service for primary key lookup. It processes the details in `OCNF-SERVICE-COOKIE` Custom AVP and decides whether to route the request to PCRF Core or for Diameter Connector. For more information, see "Optimizing N7 Session Lookup for AAR-I Messages in Rx Call Flows" section in *Oracle Communications Cloud Native Core, Policy User Guide*.

- **Enhanced logging (at WARN level) for microservices involved in PCRF & Diameter call flows**: Policy generates enhanced logging for error responses during SM/Rx call flows at their default log level. It provides sufficient visibility into issues within or across the external facing interfaces. The current default log level for Policy microservices is WARN. For more information, see "Logging Support for Error Response" section in *Oracle Communications Cloud Native Core, Policy User Guide*.
- **Burst rate limit modification and customization for WARN logs for all Policy microservices**: In order to control the volume of logs, Policy allows to add a burst filter for logging against logs for all the microservices. The Burst filter provides a mechanism to control the rate at which LogEvents are processed by silently discarding events after the maximum limit has been reached. It enables to control the frequency and volume of warning messages generated. This ensures that excessive logging does not overwhelm the system or obscure critical information. For more information, see "Logging Support for Error Response" section in *Oracle Communications Cloud Native Core, Policy User Guide*.
- **Stale Session Enhancement - replace PUT with GET UDR**: Policy supports to configure whether to use PUT or GET operation during subscription revalidation with UDR. For more information, see "Handling Stale Data in PDS" section in *Oracle Communications Cloud Native Core, Policy User Guide*.
- **Enhance support for Policy Authorization Service - Sponsored Data Connectivity (Chargeable Party)-Create Subscription for Usage Report**: The Sponsored Data Connectivity (SDC) defines standard method for Application Function (AF) to provide usage threshold information and requests usage report for sponsored data used by the subscriber. PCF allocates usage monitoring keys, grants SMF usage threshold, and delivers them to AF usage report received from SMF when the threshold is reached or the session is terminated. PCF supports SDC when the AF or Network Exposure Function (NEF) provides this support through the Policy Authorization Service. It allows subscriber application traffic to be sponsored by an application service provider. For more information see "Support for Sponsored Data Connectivity When AF/NEF Provides the Support Over Policy Authorization Service" section in *Oracle Communications Cloud Native Core, Policy User Guide*.
- **Supports Traffic Detection on SMF-N7 and TDF using Sd Interface**: PCF supports the Sd interface on Session Management Function (SMF)-N7 that enables it to communicate with the Traffic Detection Function (TDF). This interface allows PCF to provide Application Detection and Control (ADC) rules for traffic detection and enforcement at the TDF through Solicited Application Reporting. For more information, see the "Supports Traffic Detection on SMF-N7 and TDF using Sd Interface" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **CnPCF-3GPP-USER-LOC-INFO: NCGI Format Compliancy with 3GPP Rel18**: Policy supports customizing the encoding of NR Cell Global Identity (NCGI/NR CGI) in 3GPP-User-Location-Info AVP in for Diameter Rx-RAR and Rx-STA messages, when 3GPP-User-Location-Info AVP is sent with Geographic Location Type value 5GS TAI and NCGI.

For more information see "Support for Encoding of NCGI in 3GPP-User-Location-Info" section in *Oracle Communications Cloud Native Core, Policy 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, Policy Control Function - 25K Active Subscribers Perpetual	CCNC-10660	Support for Grafana 7.5.x
Oracle Communications Cloud Native Core, Policy Control Function - 25K Active Subscribers Perpetual	CCNC-10101	Stale Session Enhancement - replace PUT with GET UDR
Oracle Communications Cloud Native Core, Policy and Charging Rules Function - per 25K Subscribers Perpetual	CCNC-10091	CnPCF-3GPP-USER-LOC-INFO: NCGI Format Compliancy with 3GPP Rel18
Oracle Communications Cloud Native Core, Policy Control Function - 25K Active Subscribers Perpetual	CCNC-9942	Enhanced logging (at WARN level) for microservices involved in PCRF & Diameter call flows
Oracle Communications Cloud Native Core, Policy Control Function - 25K Active Subscribers Perpetual	CCNC-9813	Support for Immediate Report Handling
Oracle Communications Cloud Native Core, Policy and Charging Rules Function - per 25K Subscribers Perpetual	CCNC-9142	TLS 1.3 Support for Kubernetes API
Oracle Communications Cloud Native Core, Policy Control Function - 25K Active Subscribers Perpetual	CCNC-9118	Enhance support for Policy Authorization Service - Sponsored Data Connectivity (Chargeable Party)-Create Subscription for Usage Report
Oracle Communications Cloud Native Core, Policy Control Function - 25K Active Subscribers Perpetual	CCNC-9110	Integration for Traffic Prioritization for NRF-Client and Egress Gateway on Policy
Oracle Communications Cloud Native Core, Policy Control Function - 25K Active Subscribers Perpetual	CCNC-5728	Conflict Resolution for URSP Rules N1N2 transfer to UE
Oracle Communications Cloud Native Core, Policy and Charging Rules Function - per 25K Subscribers Perpetual	CCNC-9852	Supports Traffic Detection on SMF-N7 and TDF using Sd Interface

2.9 Service Communication Proxy (SCP)

Release 25.2.100

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

- **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*.
- **Routing Options Enhancement for Notification Messages**: SCP enhances its routing options REST API configuration to configure `senderNFtype` so that routing options selection criteria can also consider sender NF Type for selecting a routing option. SCP enhances its logic to identify notification sender, which can be considered in routing options selection criteria for selecting a routing option for notification. For more information, see the "Routing Options Enhancement for Notification Messages" 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 2-6 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

2.10 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:

- **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 2-7 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

2.11 Unified Data Repository (UDR)

Release 25.2.100

Oracle Communications Cloud Native Core, Unified Data Repository (UDR) 25.2.100 includes the following enhancements:

- **Support for EIR International Mobile Equipment Identity Software Version (IMEISV) Fallback**: The IMEISV Fallback feature enables the EIR to use the International Mobile Equipment Identity (IMEI) for validation and authorization purposes when the IMEISV is not provisioned for a device in the database. This feature ensures continuity of service, improving reliability, and user experience. For more information, see the "Support for EIR International Mobile Equipment Identity Software Version (IMEISV) Fallback" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.
- **Diameter Gateway Enhancement**: This feature improves Diameter Gateway protocol message handling and enables seamless interoperability between 4G and 5G networks. This enhancement includes optimized message routing and improved message delivery across multiple sites. The following Diameter Gateway enhancements are introduced:
  - Support for Outgoing Messages through Diameter Signaling Router (DSR) or Proxy in SH interface: The Diameter Gateway now supports outgoing messages, such as Push Notification Request (PNR) when a DSR or proxy is present between the Policy and Charging Rules Function (PCRF) peer and cnUDR.
  - Support for Push Notification Request (PNR) Message Routing in Multiple Site Deployments: This enhancement enables PNR message routing in multiple site deployments when the direct connection to the peer is unavailable. For example, if the connection between Site 1 and the PCRF peer is unavailable, the message is automatically routed using Site 2. This functionality is now implemented in cnUDR to prevent message loss and ensure reliable communication across distributed environment.
    For more information, see the "Diameter Gateway Enhancement" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.
- **TLS 1.3 Support for Kubernetes API**: UDR 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, Unified Data Repository User Guide*.
- **Support for Grafana 7.5.x Version**: UDR supports Grafana 7.5.x version. For more information, see the "Software Requirements" section in *Oracle Communications 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 2-8 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Subscriber Location Function - 25K Active Subscribers Perpetual	CCNC-10666	Support for Grafana 7.5.x Version
Oracle Communications Cloud Native Core, 5G Equipment Identity Register - 25K Active Subscribers Perpetual	CCNC-10323	Support for EIR International Mobile Equipment Identity Software Version (IMEISV) Fallback

Table 2-8 (Cont.) License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Subscriber Location Function - 25K Active Subscribers Perpetual	CCNC-9995	SLF Security Type-B Audit Compliance
Oracle Communications Cloud Native Core, Subscriber Location Function - 25K Active Subscribers Perpetual	CCNC-9511	SLF Capacity and Performance validation for EOY25 forecast - 64M Sub with 67K TPS per segment (3 sites)
Oracle Communications Cloud Native Core, Subscriber Location Function - 25K Active Subscribers Perpetual	CCNC-9161	TLSv1.3 Support for Kubernetes API Server Communication
Oracle Communications Cloud Native Core, Unified Data Repository - 25K Active Subscribers Perpetual	CCNC-8432	Diameter Gateway Enhancement

3 Media and Documentation

3.1 Media Pack

This section lists the media package for Oracle Communications Cloud Native Core 3.25.2.1xx.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 3.25.2.1xx.0

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Binding Support Function (BSF)	25.2.100	25.2.100	BSF 25.2.100 supports fresh installation and upgrade from 25.1.2xx. For more information, see *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Configuration Console (CNC Console)	25.2.100	NA	CNC Console 25.2.100 supports fresh installation and upgrade from 25.1.2xx and 25.1.1xx. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Certificate Management (OCCM)	25.2.100	NA	OCCM 25.2.100 supports fresh installation and upgrade from 25.1.2xx and 25.1.1xx. For more information, see *Oracle Communications Cloud Native Core, Certificate Management Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Operations Services Overlay (OSO)	25.2.100	NA	OSO 25.2.100 supports fresh installation and upgrade from 25.1.2xx. For more information, see *Oracle Communications Cloud Native Core, Operations Services Overlay Installation and Upgrade Guide*.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.25.2.1xx.0

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, cnDBTier (cnDBTier)	25.2.100	NA	cnDBTier 25.2.100 supports fresh installation and upgrade from 25.1.2xx and 25.1.1xx. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Converged Policy (Policy)	25.2.100	25.2.100	Policy 25.2.100 supports fresh installation and upgrade from 25.1.2xx. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Service Communications Proxy (SCP)	25.2.100	25.2.100	SCP 25.2.100 supports fresh installation and upgrade from 25.1.2xx and 25.1.1xx. 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)	25.2.100	25.2.100	SEPP 25.2.100 supports fresh installation and upgrade from 25.1.2xx and 25.1.1xx. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Unified Data Repository (UDR)	25.2.100	25.2.100	UDR 25.2.100 supports fresh installation and upgrade from 25.1.2xx and 25.1.1xx. 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

Legends: NS: Not Supported, NA: Not Applicable, Y: Yes, upgrade supported

> **Note**
>
> - ***** Policy, CNCC, UDR, SLF, and cnDBTier supports upgrade from **24.2.x** to **25.1.2xx** (this exception applies only to upgrade from 24.2.x to 25.1.2xx).
> - ****** SCP, SEPP, UDR, SLF, CNCC, and cnDBTier supports upgrade from **25.1.1xx** to **25.2.1xx**.
>
> For more information about the upgrade, see *Oracle Communications Cloud Native Core Solution Upgrade Guide*.

CNE Upgrade

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

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

For more information about the upgrade, see *Oracle Communications Cloud Native Core Solution Upgrade Guide*.

3.2 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*	25.2.100	• 25.2.1xx • 25.1.2xx	• 25.2.1xx • 25.1.2xx	• 25.2.1xx • 25.1.2xx	• 1.21.6 • 1.14.6 • 1.11.8	• 1.33.x • 1.32.x	25.2.1xx	NA	NA	NA
CNC Console*	25.2.100	• 25.2.1xx • 25.1.2xx • 25.1.1xx	• 25.2.1xx • 25.1.2xx • 25.1.1xx	• 25.2.1xx • 25.1.2xx • 25.1.1xx	• 1.21.6 • 1.14.6 • 1.11.8	• 1.33.x • 1.32.x • 1.31.x	NA	25.2.1xx	25.2.1xx	25.1.2xx
cnDBTier*	25.2.100	• 25.2.1xx • 25.1.2xx • 25.1.1xx	NA	• 25.2.1xx • 25.1.2xx • 25.1.1xx	• 1.21.6 • 1.14.6 • 1.11.8	• 1.33.x • 1.32.x • 1.31.x	NA	NA	NA	NA
CNE	25.2.100	NA	NA	NA	NA	1.33.x	NA	NA	NA	NA
OCCM	25.2.100	• 25.2.1xx • 25.1.2xx	NA	NA	NA	• 1.33.x • 1.32.x	25.2.1xx	NA	NA	NA

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
OSO*	25.2.100	NA	NA	NA	• 1.21.6 • 1.14.6 • 1.11.8	• 1.32.x • 1.31.x • 1.30.x	NA	NA	NA	NA
Policy*	25.2.100	• 25.2.1xx • 25.1.2xx	• 25.2.1xx • 25.1.2xx	• 25.2.1xx • 25.1.2xx	• 1.21.6 • 1.14.6 • 1.11.8	• 1.33.x • 1.32.x	25.2.1xx	NA	NA	NA
SCP*	25.2.100	• 25.2.1xx • 25.1.2xx • 25.1.1xx	• 25.2.1xx • 25.1.2xx • 25.1.1xx	• 25.2.1xx • 25.1.2xx • 25.1.1xx	• 1.21.6 • 1.14.6 • 1.11.8	• 1.33.x • 1.32.x • 1.31.x	25.2.1xx	25.2.1xx	25.2.1xx	25.1.2xx
SEPP*	25.2.100	• 25.2.1xx • 25.1.2xx • 25.1.1xx	• 25.2.1xx • 25.1.2xx • 25.1.1xx	• 25.2.1xx • 25.1.2xx • 25.1.1xx	• 1.21.6 • 1.14.6 • 1.11.8	• 1.33.x • 1.32.x • 1.31.x	25.2.1xx	25.2.1xx	25.2.1xx	25.1.2xx
UDR*	25.2.100	• 25.2.1xx • 25.1.2xx • 25.1.1xx	• 25.2.1xx • 25.1.2xx • 25.1.1xx	• 25.2.1xx • 25.1.2xx • 25.1.1xx	• 1.21.6 • 1.14.6 • 1.11.8	• 1.33.x • 1.32.x • 1.31.x	25.2.1xx	NA	25.2.1xx	NA

> **Note**
>
> *: Kubernetes 1.20.x and 1.25.x versions are only supported for ASM based deployment.

3.3 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	25.2.1xx	• 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	25.2.1xx	NA
cnDBTier	25.2.1xx	NA
OCCM	25.2.1xx	• 3GPP TS 33.310-h30 • 3GPP TR 33.876 v.0.3.0
OSO	25.2.1xx	NA
Policy	25.2.1xx	• 3GPP TS 33.501 v17.7.0 • 3GPP TS 29.500v16.9.0 • 3GPP TS 23.501v16.9.0 • 3GPP TS 23.502v16.9.0 • 3GPP TS 23.503v16.9.0 • 3GPP TS 29.504v16.9.0 • 3GPP TS 29.507v16.9.0 • 3GPP TS 29.510v16.9.0 • 3GPP TS 29.512v16.14 • 3GPP TS 29.513v16.9.0 • 3GPP TS 29.514v16.14.0 • 3GPP TS 29.214v16.5.0 • 3GPP TS 29.518v16.13.0 • 3GPP TS 29.519v16.8 • 3GPP TS 29.520v16.8 • 3GPP TS 29.521v16.8.0 • 3GPP TS 29.525v16.9.0 • 3GPP TS 29.594v16.7 • 3GPP TS 23.203 v16.2.0 • 3GPP TS 29.212 V16.3.0 • 3GPP TS 29.213v16.3 • 3GPP TS 29.214 v16.2.0 • 3GPP TS 29.219 v16.0.0 • 3GPP TS 29.335v16.0
SCP	25.2.1xx	3GPP TS 29.500 v17.12.0

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

CNC NF	NF Version	3GPP
SEPP	25.2.1xx	• 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	25.2.1xx	• 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.

3.4 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 3.25.2.1xx.0.

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	25.2.100	25.2.104	25.2.103	25.2.100	25.2.101	25.2.103	25.2.102	25.2.104	25.2.104	25.2.102	NA	25.2.102	25.2.103
CNC Console	25.2.100	NA	NA	NA	NA	NA	25.2.102	NA	25.2.104	25.2.102	NA	NA	NA
OCCM	25.2.100	NA	NA	NA	NA	NA	25.2.101	NA	NA	25.2.101	NA	NA	NA
Policy	25.2.100	25.2.104	25.2.103	25.2.100	25.2.101	25.2.103	25.2.102	25.2.104	25.2.104	25.2.102	NA	25.2.102	25.2.103
SCP	25.2.100	NA	NA	25.2.100	25.2.101	NA	25.2.102	NA	NA	25.2.102	25.1.101	NA	NA
SEPP	25.2.100	25.2.104	25.2.102	25.2.100	25.2.101	25.2.102	25.2.102	25.2.104	25.2.104	25.2.102	25.1.108	25.2.102	25.2.102
UDR	25.2.100	25.2.104	25.2.102	25.2.100	25.2.101	25.2.102	25.2.102	25.2.104	25.2.104	25.2.102	NA	25.2.102	25.2.102

3.5 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.

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 25.2.1xx	NF 25.1.2xx	NF 25.1.1xx					
Kubernetes	1.33.1	1.32.0	1.31.0	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.

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 25.2.1xx	NF 25.1.2xx	NF 25.1.1xx					
Helm	3.18.0	3.17.1	3.16.2	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.
Podman	4.9.4	4.9.4	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	2.0.5	1.7.24	1.7.22	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.

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 25.2.1xx	NF 25.1.2xx	NF 25.1.1xx					
Velero	1.13.2	1.13.2	1.13.2	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.
Kyverno	1.13.4	1.13.4	1.12.5	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.

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 25.2.1xx	NF 25.1.2xx	NF 25.1.1xx					
CoreDNS	1.12.0	1.11.3	1.11.1	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.
Multus	v4.2.1-thick	4.1.3	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 network segregation. **Impact**: Without this capability, connecting NFs to multiple networks could be limited, impacting network performance and isolation.
Fluentd	1.17.1	1.17.1	1.17.1	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.

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 25.2.1xx	NF 25.1.2xx	NF 25.1.1xx					
OpenSearch	2.19.1	2.15.0	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.
OpenSearch Dashboard	2.19.1	2.15.0	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	0.28.0	0.28.0	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.

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 25.2.1xx	NF 25.1.2xx	NF 25.1.1xx					
prometheus-kube-state-metric	2.16.0	2.15.0	2.13.0	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.
Prometheus Operator	0.83.0	0.80.1	0.76.0	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	1.9.1	1.8.2	1.8.2	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.

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 25.2.1xx	NF 25.1.2xx	NF 25.1.1xx					
Prometheus	3.4.1	3.2.0	2.52	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.
Grafana	7.5.17	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	3.29.3	3.29.1	3.28.1	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

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 25.2.1xx	NF 25.1.2xx	NF 25.1.1xx					
metrics-server	0.7.2	0.7.2	0.7.2	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.
snmp-notifier	2.0.0	1.6.1	1.5.0	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	1.690	1.65.0	1.60.0	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.
rook	1.16.7	1.16.6	1.15.2	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.

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 25.2.1xx	NF 25.1.2xx	NF 25.1.1xx					
cinder-csi-plugin	1.32.0	1.32.0	1.31.1	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.

3.6 Redhat Openshift Compliance Matrix

The following table lists the planned Redhat Openshift compliance matrix for each network function.

Table 3-6 Redhat Openshift Compliance Matrix

CNC NF Release	Webscale	RedHat Openshift	Kubernetes	Helm	F5 ASM	F5 SPK
cnDBTier 25.2.100	1.3.x	4.7.x	1.20.x	3.12.3	1.11.8	NA
	1.5.x	4.12.x	1.25.x	3.12.3	1.14.6	1.7.11
OSO 25.2.100	1.3.x	4.7.x	1.20.x	3.12.3	1.11.8	NA
	1.5.x	4.12.x	1.25.x	3.12.3	1.14.6	1.7.11
Policy 25.2.100	1.3.x	4.7.x	1.20.x	3.12.3	1.11.8	NA
	1.5.x	4.12.x	1.25.x	3.12.3	1.14.6	1.7.11
BSF 25.2.100	1.3.x	4.7.x	1.20.x	3.12.3	1.11.8	NA
	1.5.x	4.12.x	1.25.x	3.12.3	1.14.6	1.7.11
OCCM 25.2.100	1.3.x	4.7.x	1.20.x	3.12.3	1.11.8	NA
	1.5.x	4.12.x	1.25.x	3.12.3	1.14.6	1.7.11
SCP 25.2.100	1.3.x	4.7.x	1.20.x	3.12.3	1.11.8	NA
	1.5.x	4.12.x	1.25.x	3.12.3	1.14.6	1.7.11
CNCC 25.2.100	1.3.x	4.7.x	1.20.x	3.12.3	1.11.8	NA
	1.5.x	4.12.x	1.25.x	3.12.3	1.14.6	1.7.11
SEPP 25.2.100	1.3.x	4.7.x	1.20.x	3.12.3	1.11.8	NA
	1.5.x	4.12.x	1.25.x	3.12.3	1.14.6	1.7.11
UDR 25.2.100	1.3.x	4.7.x	1.20.x	3.12.3	1.11.8	NA

Table 3-6 (Cont.) Redhat Openshift Compliance Matrix

CNC NF Release	Webscale	RedHat Openshift	Kubernetes	Helm	F5 ASM	F5 SPK
	1.5.x	4.12.x	1.25.x	3.12.3	1.14.6	1.7.11

3.7 Security Certification Declaration

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

3.7.1 BSF Security Certification Declaration

Release 25.2.100

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	Oct 14, 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 16, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Oct 10, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Oct 10, 2025	No findings

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

3.7.2 cnDBTier Security Certification Declaration

Release 25.2.100

Table 3-8 cnDBTier Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	October 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	October 7, 2025	No unmitigated critical or high findings

Table 3-8 (Cont.) cnDBTier Security Certification Declaration

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

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

3.7.3 CNC Console Security Certification Declaration

Release 25.2.100

Table 3-9 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	Oct 30, 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 24, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Oct 30, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Oct 30, 2025	No findings

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

3.7.4 OCCM Security Certification Declaration

Release 25.2.100

Table 3-10 OCCM Security Certification Declaration

Compliance Test Description	Test Completion	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Sep 29, 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 29, 2025	No unmitigated critical or high findings

Table 3-10 (Cont.) OCCM Security Certification Declaration

Compliance Test Description	Test Completion	Summary
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Sep 29, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Sep 29, 2025	No findings

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

3.7.5 Policy Security Certification Declaration

Release 25.2.100

Table 3-11 Policy Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Oct 14, 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 15, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Oct 13, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Oct 10, 2025	No findings

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

3.7.6 SCP Security Certification Declaration

Release 25.2.100

Table 3-12 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

Table 3-12 (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 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.

3.7.7 SEPP Security Certification Declaration

Release 25.2.100

Table 3-13 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.

3.7.8 UDR Security Certification Declaration

Release 25.2.100

Table 3-14 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

Table 3-14 (Cont.) UDR Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
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.

3.8 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).

4 Resolved and Known Bugs

This chapter lists the resolved and known bugs for Oracle Communications Cloud Native Core release 3.25.2.1xx.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.

4.1 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.

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.

4.2 Resolved Bug List

The following Resolved Bugs tables list the bugs that are resolved in Oracle Communications Cloud Native Core Release 3.25.2.1xx.0.

4.2.1 BSF Resolved Bugs

Release 25.2.100

Table 4-1 BSF 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38281129	Unable to Edit Load Shedding Profiles After BSF Upgrade and Rollback (Error Code: 1009)	After upgrading BSF from 25.1.100 to 25.1.200, two newly added Load Shedding Profiles-LSP-overload and LSP-congestion could no longer be edited using the UI. This behavior persists even after migrating the congestion profiles and rolling back to BSF 25.1.100. When attempting to edit, the Error Code: 1009 is displayed. **Doc Impact:** There is no doc impact.	2	25.1.200
38209382	BSF-ATS 25.1.200 New-feature | "BSFStaleBinding_Deletion_Logging_Enhancement" failing	While executing the new feature BSFStaleBinding_Deletion_Logging_Enhancement, it was observed that the “Stale_Binding_Deletion_PCF_Response_404_Management_Audit_Logs_Enabled”and “Stale_Binding_Deletion_PCF_Response_404_Management_Audit_Logs_Disabled” scenarios were failing frequently with the error message. **Doc Impact:** There is no doc impact.	3	25.1.200

Table 4-1 (Cont.) BSF 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38263288	BSF - Reconnection attempt from DSR to BSF does not happen when DPR with BUSY cause	When a controlled shutdown was triggered, BSF sent Diameter Disconnect Peer Requests (DPR) to all connected peers. The DPR included a Disconnect-Cause AVP set to "BUSY". RFC 6733 specifies that peers receiving a "BUSY" disconnect cause should not attempt automatic reconnection. Consequently, DSR(adjacent nodes) links must be reset manually to restore connectivity. **Doc Impact:** There is no doc impact.	3	24.2.2
38533717	BSF 25.1.100: AUDIT_NOT_RUNNING alert is firing even when audit service is active	The AUDIT_NOT_RUNNING alert was being triggered in BSF 25.1.100 even though the audit queue is active and an on-demand audit completes successfully. The alert continued to trigger despite the audit pods processing data normally. **Doc Impact:** There is no doc impact.	3	25.1.100
38043770	BSF ocbsf-custom-values yaml does not expose containerPortNames	BSF custom values 25.1.100 YAML did not expose containerPortName used to provision the backendPortName in the CNLB annotations. **Doc Impact:** There is no doc impact.	4	25.1.100

4.2.2 cnDBTier Resolved Bugs

Release 25.2.100

Table 4-2 cnDBTier 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38236749	Disaster Recovery (DR) getting stuck for fatal scenario on prefix-enabled 4-site single channel IPv6 setup	While restoring ndb database, binlogs were not cleaned. The command `DELETE FROM replication_info.DBTIER_INITIAL_BINLOG_POSTION` was missing in the Restore procedure. **Doc impact**: Updated the sample output to include `DELETE FROM replication_info.DBTIER_INITIAL_BINLOG_POSTION` command in the "Downloading the Latest DB Backup Before Restoration" section in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide.*	2	25.1.200
37864092	dbtscale_ndbmtd_pods script exited with 'Create Nodegroup FAILED' for wrong nodegroup	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. 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	24.2.5
38204318	Site removal script dbtremovesite is failing with error of script version mismatch on CNDB	While running the `dbtremovesite` site removal script, the script was failing due to the version mismatch. The cnDBTier library version was updated per the script version. **Doc impact:** There is no doc impact.	2	25.1.102
38204306	dbtremovesite script exits with ERROR - DBTIER_SCRIPT_VERSION (<25.1.100>) does not match DBTIER_LIBRARY_VERSION(<25.1.200>)	Version of the `dbtremovesite` script did not match with the cnDBTier library version which resulted in an error. The cnDBTier library version was updated per the script version. **Doc impact**: There is no doc impact.	2	25.1.201

Table 4-2 (Cont.) cnDBTier 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38224168	Document update required for georeplication procedure from 25.1.200 procedure	Added a procedure that explains georeplication recovery steps in cnDBTier Installation Guide. **Doc impact**: Added the "Restoring Georeplication (GR) Failure" section in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.	2	25.1.102
38224230	Document update required for georeplication procedure from 25.1.200 procedure	Added a procedure that explains georeplication recovery steps in cnDBTier Installation Guide. **Doc impact**: Added "Restoring Georeplication (GR) Failure" section in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.	2	25.1.200
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
37668951	information_schema and table schema is seen to be inconsistent when policy upgrade was performed	After a policy upgrade, the metadata in information_schema did not reflect the actual table schema. **Doc impact**: There is no doc impact.	2	25.1.200
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

Table 4-2 (Cont.) cnDBTier 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37975847	All data nodes experienced a simultaneous restart following the cnDBTier upgrade	A simultaneous restart of all data nodes (that is, all ndbmtd pods) following a cnDBTier upgrade was observed. **Doc impact**: There is no doc impact.	2	25.1.200
38278713	Document update required "DB Tier Stop Replica API" in User Guide	cnDBTier User Guide did not provide a reference in the "DBTier Stop Replica API" section to the procedure that explained the steps to gracefully start and stop georeplication between sites. **Doc impact** Added a reference to the "Stopping cnDBTier Georeplication Between Sites" section in the "DBTier Stop Replica API" section in *Oracle Communications Cloud Native Core, cnDBTier User Guide*.	2	25.1.201
38266388	Update DBTier User Guide for Vertical Scaling of db-replication-svc CPU and RAM	After upgrading the sites the CPU and RAM values in the YAML files for db-replication-svc, the repl-grp1 pods did not restart, and the updated resource values were not applied. The values in georeplication recovery resources in the yaml file were updated and performed vertical scaling which was successful. **Doc impact**: Updated the yaml values for GRR using the db-replication-svc service. For more information, see the "Vertical Scaling of db-replication-svc Pods" section in *Oracle Communications Cloud Native Core, cnDBTier User Guide*	2	25.1.200
38220013	dbtrecover Script is affecting db-monitor-svc	A deadlock occurred in the db-monitor-svc during SQL pod restarts that caused connection assignment failure, as the monitoring service was unable to assign connections correctly. **Doc impact**: There is no doc impact.	3	25.1.100

Table 4-2 (Cont.) cnDBTier 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37859265	dbtscale_ndbmtd_pods disrupted by ndbmtd pod restart	When dbtscale_ndbmtd_pods are run to scale data nodes (ndbmtd pods) on site1 from 8 to 14. The script was due to a ndbmtd pod restart during the scale operation is disrupted. **Doc impact**: There is no doc impact.	3	25.1.100
37859029	dbtscale_ndbmtd_pods failed when ndb backup triggered while scaling in progress	While scaling ndbmtd pods using the dbtscale_ndbmtd_pods script, the pods were scaled up, and REORGANIZE PARTITION had started. However, the script terminated with an error. **Doc impact**: There is no doc impact.	2	24.2.5
38458488	RCKL SM-PCF West 001 GRR Failed	Enhance backup status handling by validating NDB backup completion and error states. **Doc impact**: There is no doc impact.	2	23.4.6
38204318	Site removal script dbtremovesite is failing with error of script version mismatch on CNDB v25.1.102	Encountered issues running the dbtremovesite script on version 25.1.102. Initially, there was a "Permission denied" error, which was resolved by setting the executable permission on the script. However, the script then failed due to a version mismatch. To resolve, ensure the script uses the correct version value. **Doc Impact**: There is no doc impact.	2	25.1.102
38129271	Upgrade from 23.4.0 to 25.1.100 broke replication between sites	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	23.4.6

Table 4-2 (Cont.) cnDBTier 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38144181	Add additional replication errors(1091, 1826) in the replication skip error section and remove 1094 replication erro from 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	23.4.6
37942052	dbtscale_ndbmtd_pods not working when release name contains prefix	When a single-site setup was deployed with a prefix used in the release name, and when the `dbtscale_ndbmtd_pods` script was run on this setup, the script was failing with the following error: "Error: UPGRADE FAILED: "mysql-cluster" has no deployed releases". This was because DBTIER_RELEASE_NAME was not set. **Doc impact**: There is no doc impact.	3	25.1.200
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. 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.	3	25.1.100
38288330	db-monitor-svc requests Backup Transfer Status Before Transfer Starts	Georeplication recovery (non-fatal) was implemented using dbtrecover on a 2-site Georeplication (GR) setup with multi-channel replication with the following condition: • site 1 = Good site • site 2 = Site being recovered Errors were observed in the backup-mgr-svc pod on site-1 and no GRR related logs were printed in the backup-mgr-svc logs. **Doc Impact**: There is no doc impact.	3	25.1.200

Table 4-2 (Cont.) cnDBTier 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38304684	Georeplication recovery failed with 6 channel replication channel over SM setup	Georeplication recovery was failing because the required Persistent Volume Claims (PVC) size for the replication service was not configured rightly. **Doc Impact**: There is no doc impact.	3	25.1.201
38314302	Document steps to create service account manually in case Helm MOP is enabled and individual flag are set as false with user defined name	cnDBTier documentation did not provide steps to create service account, roles, and role binding manually if user does not want automated service account creation. **Doc Impact**: Updated the steps to create the Namespace in the "Verifying and Creating Namespace" section. For more information, see *Oracle Communications Cloud Native Core cnDBTier Installation, Upgrade, and Fault Recovery Guide*	2	25.1.201
38278476	Documentation for serviceAccounts/create flag is not clear when it is set as true	cnDBTier documentation did not provide comprehensive and clear documentation of RBAC configuration parameters. **Doc Impact**: Added a table "autoCreateResources Configurations" that provides autoCreateResources parameter configurations in different scenarios in the "LCM Based Automation" section in *Oracle Communications Cloud Native Core, cnDBTier User Guide*	3	25.1.200
38148329	Documentation error in "Remove cnDBTier Geo-Redundant Site" procedure	In the 'Removing cnDBTier cluster1' section, the reference log mentioned is for site1 removal instead of site4 which is incorrect. **Doc Impact**: Updated the "Removing cnDBTier cluster1" section in *Oracle Communications Cloud Native Core, cnDBTier User Guide* to mention the correct site name.	3	25.1.200

Table 4-2 (Cont.) cnDBTier 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38130703	db-monitor-svc logging ERRORs: "[DbtierRetrieveBackupTransferMetrics] No Backups Transfers Started to provide the Backup Status Metrics"	In a 2-site, 6-channel setup with 10 million entries, after changing the root, occne, and occnerepluser passwords using the dbtpasswd script, the db-monitor-svc is reporting an ERROR message that is not actually indicative of an error condition. **Doc Impact**: There is no doc impact.	3	25.1.200
38161643	cnDBTier upgrade from 23.4.7 to 25.1.101 is failed	The upgrade of cnDBTier from 23.4.7 to 25.1.101 failed in the ME lab environment running webscale 1.3 due to a missing 'mysql' executable, preventing the pre-upgrade hook from completing. However, the upgrade was successful in environments using webscale 1.5. **Doc Impact**: There is no doc impact.	3	25.1.100
38331530	Some of the cnDBTier metrics are not pegging after rollback of DBTier from 25.2.100-rc.1 to 25.1.200	Some cnDBTier metrics do not update after rolling back from 25.2.100-rc.1 to 25.1.200 as TCP connections in the db monitor service remain stuck in CLOSE_WAIT state. **Doc Impact**: There is no doc impact.	3	25.1.200
38346857	PCF-DBTIER-ndbmysqld Pods Stuck after Upgrade||24.2.6	After upgrading to 24.2.6, PCF-DBTIER-ndbmysqld pods may become stuck due to NULL values in the stop_replication_mysqlds column. **Doc Impact**: There is no doc impact.	3	24.2.6
38245044	Documentation should mention which site to be sourced in `dbtremovesite`	cnDBTier documentation did not provide details on which site must be used as the source when using the `dbtremovesite` script. **Doc Impact**: Updated the "Removing cnDBTier Cluster" section to specify which site must 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

Table 4-2 (Cont.) cnDBTier 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38263193	cnDBTier 25.1.200 User Guide corrections requested for section 7.14 Support for Dual Stack	cnDBTier documentation had a broken link in the section "Support for a Dual Stack". **Doc Impact**: Corrected the broken link in the section "Support for Dual Stack" in *Oracle Communications Cloud Native Core, cnDBTier User Guide*.	4	25.1.200
38352838	GRR execution from CNCC GUI failed with 500	GRR using Console is supported only starting from release 24.2.x. **Doc Impact**: There is no doc impact.	4	25.1.100
38308023	DBTIER: Why are there steps to (re)create keys and secrets during DBTIER upgrade? a requirement?	The Upgrade section in cnDBTier documentation mentioned the step to recreate SSH keys and secrets. **Doc Impact**: Updated the documentation to remove the step that mentions creating SSH keys and secrets in the section "Upgrading cnDBTier Cluster" in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide.*	4	25.1.200

Note

Resolved bugs from 24.2.6, 25.1.103, and 25.1.201 have been forward ported to Release 25.2.100.

4.2.3 CNC Console Resolved Bugs

Release 25.2.100

Table 4-3 CNC Console 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38603006	CNCC 25.2.100: Remove namespace reference from CNCC OSO Alert file	All references to `k8s_namespace` and associated parameters have been removed from each alert expression in the OSO alert file. As a result, alerts are no longer parametrized by namespace, which may have broadened their scope depending on the remaining label filters. In addition, MemoryUsage alerts that relied on the `container_memory_usage_bytes` metric are removed because OSO does not have access to these KPIs. **Doc Impact:** Removed `k8s_namepsace` reference from alerts in the Console Alert chapter in *Oracle Communications Cloud Native Configuration Console User Guide*.	3	25.1.100
38381583	TTMELAB:CNDBTIER:25.1.101: Data mismatch between tables in Geo replicated sites	Information related to upgrade and rollback scenarios is needed. **Doc Impact:** Added upgrade and rollback scenarios in *Oracle Communications Cloud Native Core Solution Upgrade Guide* to describe different scenarios of georeplication sites.	3	25.1.100
38581566	CNCC Console deployment in a cnLB environment	The CNC Console documentation has been updated to describe Ingress and Egress network attachment annotations. Sample configurations have also been added to demonstrate their use. **Doc Impact**: Updated *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide* to reflect the above-mentioned changes.	4	25.1.200

> **Note**
>
> Resolved bugs from 25.1.201 have been forward ported to Release 25.2.100.

4.2.4 CNE Resolved Bugs

Release 25.2.100

There are no resolved bugs in this release.

4.2.5 OSO Resolved Bugs

Release 25.2.100

Table 4-4 OSO 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38058360	OSO 25.1.102 serverFiles parameter is missing OSO PROM YAML file	The `ServerFile` parameter was missing in the OSO custom values configuration file. As a result, Prometheus is unable to pick up metrics as expected and targets were showing down. The `ServerFile` parameter is added in the OSO custom values configuration file. **Doc impact**: There is no doc impact.	3	25.1.100

4.2.6 OCCM Resolved Bugs

Release 25.2.100

There are no resolved bugs in this release.

4.2.7 Policy Resolved Bugs

Table 4-5 Policy 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37718445	Intermittent error 3002(Timeout) is observed for CCA	Intermittent error 3002 (Timeout) was observed for CCA and RAA. **Doc Impact:** There is no doc impact.	2	23.4.5
37974232	SM-PCF 23.4.6 PCF taking time to process the Session Terminate Request	PCF was taking time to process the STR and responding sm update notify (remove all the pcc rules) after the session is terminated by SMF. **Doc Impact:** There is no doc impact.	2	23.4.6

Table 4-5 (Cont.) Policy 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38107532	Policy 24.2.4 Different handling of UNKNOWN_RULE_NAME	Difference in behavior is observed when handling the same CCR-I and CCR-U for UNKNOWN_RULE_NAME in CCR-U. **Doc Impact:** There is no doc impact.	2	24.2.4
38076342	AUDIT_NOT_RUNNING Critical Alarm raised in PCF	A critical alert, "AUDIT_NOT_RUNNING", was observed. **Doc Impact:** There is no doc impact.	2	24.2.3
37762722	When PCF is in complete shutdown state, audit notifications continues to sent out	When the PCF was in “complete shutdown” state, the Audit service generated the audit notifications. These Notifications were supposed to be rejected by the Gateway. However, they were not being rejected and sent out. **Doc Impact:** There is no doc impact.	3	23.2.0
37664840	Alerts or metrics for LDAP links down	The system did not generate any alert or expose metrics when the LDAP peer connection was lost. **Doc Impact:** There is no doc impact.	3	22.4.2
38324550	PRA test getting Exception as Object is not a function	It is observed that the CCR-I was getting success. However, CCR-U was getting an error as "TypeError: #<Object> is not a function" from the PRE. **Doc Impact:** There is no doc impact.	3	24.2.5
38079813	Multiple pods restarted for application ns which resulted into subscriber fallback	It was observed that the multiple pods were restarted for application namespace which resulted into subscriber fallback. **Doc Impact:** There is no doc impact.	3	23.4.9
37776221	Question about CNCP alerts	Existing alert expressions were incorrect and wasn't triggering alert even in actual high memory or CPU utilization. **Doc Impact:** There is no doc impact.	3	24.2.2

Table 4-5 (Cont.) Policy 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37833722	Diameter Gateway Metrics requires additional dimension for Identifying PCF and BSF identities	The Diameter Gateway metric on both PCF and BSF did not reflect- • PCF metric (occnp_diam_request_network_total) did not reflect which BSF the diameter request came from and for corresponding responses it did not reflect which BSF the response was sent to. • BSF metric (ocbsf_diam_request_network_total/ ocbsf_diam_response_network_total) did not reflect which PCF the request was sent by the BSF and similarly for response which PCF responded. **Doc Impact:** There is no doc impact.	3	24.2.4
38208003	cnPCRF //24.2.6 PCF is triggering dedicated bearer even after AAR is Rejected	It is observed that PCF was triggering Gx-RAR - dedicated bearer even PCF was rejecting the AAR message. **Doc Impact:** There is no doc impact.	3	24.2.6
38141617	Multiple features failing in Regression Pipeline	Following features were failing in individual as well as in full regression: • NRF_Autonomous_Registration_and_Error_Mapping_NF_Consumer • Discover_UDR_Using_GroupId_SM_AM_UE_ModelID • Policy_Integration_with_SCP • Policy_SCP-Health_API **Doc Impact:** There is no doc impact.	3	25.1.200
38191375	Rx-STA-5063 failures	Rx STA 5063 (Service_Not_Authorized) diameter error occurred. **Doc Impact:** There is no doc impact.	3	23.4.9
38186653	PCF-23.4.9: One of the Audit pod restart during Upgrade	The issue was observed in audit pod restart during PCF upgrade. There is only one audit pod restarted not the other one. **Doc Impact:** There is no doc impact.	3	23.4.9

Table 4-5 (Cont.) Policy 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38179661	One PCRF core pod is handling More Request during the Audit	During audit, only one of the PCRF core pod was handling more request, meanwhile the timeout(3002) error was observed. **Doc Impact:** There is no doc impact.	3	23.4.9
38005208	Field(s): {Default} does not exist in DB when trying to change config settings for UM	While trying to edit some parameters in the Usage Monitoring menu, the error message was displayed after clicking the **Save** button. **Doc Impact:** There is no doc impact.	3	24.2.3
37421457	cnPCRF - Network Element - Capability Usage-Report-26	In cnPCRF, CCA was getting the "USAGE_REPORT (33) while generating the TAI_change report. **Doc Impact:** There is no doc impact.	3	23.2.8
37943466	Policy evaluation error: main is not a function	While calling a policy inside the main policy, the policy evaluation failed if the policy name starts with an integer value. **Doc Impact:** There is no doc impact.	3	24.2.3
37919387	PCF ATS 24.2.4:Feature continue to execute even after before_stage failure for stages 100-102	The features of a particular stage continued to execute even if the “Before_stage” step failed. **Doc Impact:** There is no doc impact.	3	24.2.4
36987393	PCRF-CORE traffic pattern is different for one POD	It was observed that the traffic pattern was different for a PCRF-Core POD from all other pods. **Doc Impact:** There is no doc impact.	3	22.4.7
37344625	In complete shutdown not seeing CEA from diam gw in pcap towards pgw	Provisioning Gateway was sending multiple CER to the Diameter Gateway, but not getting CEA response with 3004 (error code configured in PCF) from the Diameter Gateway in pcap. However, CEA with 3004 can be seen in the Diameter Gateway logs. **Doc Impact:** There is no doc impact.	3	22.4.7

Table 4-5 (Cont.) Policy 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36776263	PCRF-Core does not send SSV information to a second Gx session	On CCR-I or CCR-U, there is a case where PRE runs 2 actions in parallel: • Reauthorize all gxsessions with the same USER or IP_CAN_SESSION (depending on policy)). • Trigger SSV Update. When this happens, the other gxsessions that were reauthorized internally would never query PDS on internal reauth, therefore the changes from that SSV Update would not be present for these other sessions, making policy execution for those reauth call flows to lead to unintended behavior as SSV information was not up to date. **Doc Impact:** There is no doc impact.	3	23.2.8
38058428	URSP Install Failure	There are no validations for URSP rules, allowing invalid URSP entries to be accepted and leading to exceptions during N1 Message Transfer. **Doc Impact:** There is no doc impact.	3	23.4.6
38150314	Pending_Transaction_N7_Fast_Lock_Bulwark_with_SM_Error_handler Failure	“Pending_Transaction_N7_Fast_Lock_Bulwark_with_SM_Error_handler” has three scenarios. Among them, the scenario Pending_Transaction_FastLock_Client_SMUpdate_SM_Error_handling fails during the initial full regression pipeline but passes on rerun or when run individually. **Doc Impact:** There is no doc impact.	3	25.1.100
38406710	PCF-ATS 25.1.200 | User_Agent_Policy_Propagation Features Failing in Regression Pipeline	User_Agent_Policy_Propagation features were failing due to metrics validation. **Doc Impact:** There is no doc impact.	3	25.1.200
38240819	cnPCRF 24.2.4: "endDate" being set to the 30th, despite the billing day being the 31st	The system did not generate the endDate properly with the configured reset day, causing inconsistencies. **Doc Impact:** There is no doc impact.	3	24.2.4

Table 4-5 (Cont.) Policy 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38210891	PCF_BSF_Audit_Revalidation feature failure in New Feature pipeline	When update bsf connection API was getting called, contextId from path variable was not added to SessionBindingMapping bindingId object. **Doc Impact:** There is no doc impact.	3	25.1.200
38030059	Wrong Policy tags are sent from the UM to the PCRF-CORE for PRE policy evaluation	Few inconsistencies were seen for policyDecisionTags at UM and at PCRF-Core, as the policyDecisionTags were not updated in the UM database properly after sent to the PCRF-Core. **Doc Impact:** There is no doc impact.	3	24.2.3
37722614	AM-PCF Is Not Retrying After Getting 404 For N1N2MessageTransfer (namf-comm)	When N1N2 messages failed to retry because of an exception, the logs in warn level were required to identify the issue. **Doc Impact:** There is no doc impact.	3	23.4.4
38444909	Metrics validation failing in AMPolicy Feature in PCF 25.1.200	Metrics were getting pegged on time, so more wait time was required. **Doc Impact:** There is no doc impact.	3	25.1.100

4.2.8 SCP Resolved Bugs

Release 25.2.100

Table 4-6 SCP 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38121230	SCP is returning a 500 NRF Request Timeout error when initiating traffic for Model-D, while scale up and scale down worker pods	SCP returned a 500 NRF Request Timeout error when you initiated Model-D traffic during worker pod scale-up and scale-down operations. **Doc Impact**: There is no doc impact.	2	25.1.200

Table 4-6 (Cont.) SCP 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38582165	High CPU Utilization Observed on Load Manager reached upto 98% at 1200 NF Profiles (730K MPS)	During traffic runs at 730K MPS with 1,200 NF profiles, Load Manager CPU utilization reached up to 98%. **Doc Impact**: There is no doc impact.	2	25.2.100
38573314	Exception occurred while inserting ALLOWED_TLS_CIPHERS entries in ENGINEERING_CONFIGURATIONS table	The upgrade from SCP 23.4.3 to 25.1.100 failed due to an exception that occurred while inserting ALLOWED_TLS_CIPHERS entries in the ENGINEERING_CONFIGURATIONS table. **Doc Impact**: There is no doc impact.	2	25.1.100
38192165	Mediation pod goes to continuous crashloopbackoff state & Overall Success rate dropped when mediation pod is restarted on SCP Image - 300% load pumped to single mediation pod	After a restart on the SCP image with 300% load directed to a single mediation pod, the mediation pod entered a continuous restart loop and the overall success rate dropped. **Doc Impact**: There is no doc impact.	2	25.1.200
38543693	Add a flag control for the metric ocscp_metric_coherence_request_processing_time_total to control its cardinality	A parameter to control the cardinality of the metric ocscp_metric_coherence_request_processing_time_total was not available. **Doc Impact**: There is no doc impact.	3	25.1.100
38536707	Fix pseudo-header matching in mediation trigger points	The Pseudo header values were not considered at the request ingress mediation trigger point. **Doc Impact**: There is no doc impact.	3	25.2.100
38531178	SCP rejecting profiles due to canaryReleaseConfigName	SCP 25.1.100 rejected profiles due to canaryReleaseConfigName. **Doc Impact**: There is no doc impact.	3	25.1.100

Table 4-6 (Cont.) SCP 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38489414	SCP not allowing Format3: NFTYPE-NFINSTANCEID to be provisioned for User Agent Format and not screening correctly when using only NFTYPE	SCP did not allow provisioning of Format3: NFTYPE-NFINSTANCEID for User Agent Format and did not screen correctly when using only NFTYPE. **Doc Impact**: Updated the description of the `userAgentHeaderFormat` parameter in " Table 2-343 ConsumerInfo" in *Oracle Communications Cloud Native Core, Service Communication Proxy REST Specification Guide*.	3	24.2.5
38476699	Replace == with .equals() and + with StringBuilder.append()	During the 25.2.100 code audit, "==" was not replaced with .equals() and "+" was not replaced with StringBuilder.append() in the reviewed files. **Doc Impact**: There is no doc impact.	3	25.1.100
38476671	Misprinted Logs and Missing Debug Check Before Printing Large Objects	During the 25.2.100 code audit, some logs were misprinted and debug checks were missing before printing large objects. **Doc Impact**: There is no doc impact.	3	25.1.100
38471581	SCP not returning all 3 mediation trigger points as configured. The same metrics work on old release 23.4	SCP did not return all three configured mediation trigger points in SCP 24.1.2, while the same metrics worked in SCP 23.4. **Doc Impact**: Updated the "Configuring Mediation Trigger Point" section in *Oracle Communications Cloud Native Core, Service Communication Proxy REST Specification Guide*.	3	24.1.2
38449920	Accept header added by SCP if it is not in the original request	SCP added the header "Accept: application/json" to requests that did not originally contain it before forwarding to the producer NF, resulting in rejection by the producer NF that only supported "Accept: application/problem+json" or no Accept header. **Doc Impact**: There is no doc impact.	3	25.1.201

Table 4-6 (Cont.) SCP 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38440704	SCP Ingress Rate Limit not applied - SCP_INTERNAL_ERROR	SCP did not limit traffic to 200 transactions per second as defined in the configuration when a load of 500 transactions per second was applied to the nbsf-management service with nfType set to PCF. **Doc Impact**: There is no doc impact.	3	24.2.5
38412225	message info is not mentioned for notification request message in ocscp_worker_routing_options_selected_total Metrics.	Message information was not mentioned for notification request messages in the ocscp_worker_routing_options_selected_total metric. **Doc Impact**: Updated the `ocscp_worker_routing_options_selected_total` metric dimension `Message type` in "Table 5-251 ocscp_worker_routing_options_selected_total" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	3	25.2.100
38385864	Traffic dip observed during upgrade and blank gaps in multiple graphs on Grafana	A traffic dip was observed during the upgrade, with blank gaps appearing in multiple Grafana graphs. **Doc Impact**: There is no doc impact.	3	25.1.201
38384483	SCP does not allow 0.1 second as timeout configuration value.	SCP did not configure the response timeout value as 0.1 seconds in the routing configuration set, as specified in the Rest Guide. **Doc Impact**: Added a note "This parameter must be an integer, not a decimal. If the value is provided as a decimal, convert it to an integer unit. For example, 0.1 s becomes 100 ms." for all the occurrences of "totalTransactionLifetime" and "responseTimeout" in the "Configuring Routing Config Set" section of *Oracle Communications Cloud Native Core, Service Communication Proxy REST Specification Guide*.	3	25.2.100

Table 4-6 (Cont.) SCP 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38376331	ocscp_notification_duplicate_profile_ignored_total metric not getting incremented while trying to register duplicate profile	The ocscp_notification_duplicate_profile_ignored_total metric did not increment when attempting to register a duplicate profile. **Doc Impact**: Renamed the `ocscp_notification_duplicate_profile_ignored_total` metric to `ocscp_notification_profile_ignored_total` in the "Metrics" section of *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	3	25.1.201
38375508	SCP is not allowed to configure valid format of user Agent "NFTYPE-FQDN-NFINSTANCEID" in consumer info configuration in CNCC.	SCP did not allow to configure the valid User-Agent format "NFTYPE-FQDN-NFINSTANCEID" in the consumer info configuration on the CNC Console. **Doc Impact**: Updated the value of `userAgentHeaderSeparator` parameter in *Oracle Communications Cloud Native Core, Service Communication Proxy REST Specification Guide*.	3	25.2.100
38339384	Applied certificate not checked before primary certificate reload on SSL config details SSE	The primary server certificate was reloaded upon receiving the SSL configuration details SSE, instead of verifying the applied certificate and then reloading it as required. **Doc Impact**: There is no doc impact.	3	25.2.100
38310934	apiSpecificResourceUri is configured successfully in incorrect regex while configuring Sender NF type in Routing option config.	The apiSpecificResourceUri parameter was configured successfully with an incorrect regular expression when you configured the Sender NF type in the Routing option configuration. **Doc Impact**: Updated the description of `apiSpecificResourceUri` in "Table 2-20 routingOptionsConfigData Parameters" in *Oracle Communications Cloud Native Core, Service Communication Proxy REST Specification Guide*.	3	25.2.100

Table 4-6 (Cont.) SCP 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38253718	SCP Same OID for some Alerts	Some of the alerts had duplicate OIDs in SCP 24.3.0. **Doc Impact**: There is no doc impact.	3	24.3.0
38245751	Reduced the number of API calls to Kubernetes API server	The getStorePassword functionality in WorkerSSLConfig was implemented using a Kubernetes secret mount inline instead of using CoreV1Api. **Doc Impact**: There is no doc impact.	3	25.1.200
38231339	When either one of Primary Server or Client Certificate is Expired, the Monitor Cert Expire spawns a thread in infinite loop for switching to secondary certificate.	When either the primary server or client certificate expired, the Monitor Cert Expire function spawned a thread in an infinite loop to switch to the secondary certificate. **Doc Impact**: There is no doc impact.	3	25.1.100
38231308	When Primary Server Certificate is Expired and scp-worker pod is restarted, it continues to use the Expired Primary Server Certificate	When the primary server certificate expired and the scp-worker pod was restarted, it continued to use the expired primary server certificate. **Doc Impact**: There is no doc impact.	3	25.1.100
38231282	When Secondary Server or Client TLS secret is patched, it doesn't switch to new Server/Client Certificate for new TLS connections	When the secondary server or client TLS secret was patched, new TLS connections did not switch to the updated server or client certificate. **Doc Impact**: There is no doc impact.	3	25.1.100
38209694	SCP Generated 500 Internal Server Error Observed for mediation traffic	It was observed that for mediation traffic, 500 internal server error responses were generated. **Doc Impact**: There is no doc impact.	3	25.1.200
38202573	SCP Errors generated during the upgrade are not captured in the ocscp_metric_scp_generated_response_total metrics	SCP errors generated during the upgrade from SCP 25.1.100 to 25.1.200 were not captured in the ocscp_metric_scp_generated_response_total metrics. **Doc Impact**: There is no doc impact.	3	25.1.200

Table 4-6 (Cont.) SCP 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38188009	In case of scale down of NRF proxy/mediation pods, scp-worker map keep sending message to old IP Address of already deleted nrfproxy pod	After a scale-down of NRF proxy and mediation pods, scp-worker kept sending messages to the old IP address of the deleted nrfproxy pod. **Doc Impact**: There is no doc impact.	3	25.1.200
38187991	Exceptions were observed on the worker pod while running traffic at a rate of 400K MPS with the Model-D cache enabled	Some exceptions were observed on the worker pod while running traffic at 400K MPS with the Model-D cache enabled. **Doc Impact**: There is no doc impact.	3	25.1.200
38179423	nrf-proxy Pod restarts observed under Overload Conditions(300%)	While running 400K MPS on SCP with 20% Model-D and 80% Model-C, sequentially scaling nrf-proxy pods from 15 to 7 and then to 3 overloaded them by about 200% of the expected load and caused restarts; after reducing from 7 to 3, all nrf-proxy pods restarted unexpectedly. **Doc Impact**: There is no doc impact.	3	25.1.200
38172901	SCP Discrepancies between SCP User Guide and `ScpAlertrules.yaml` file	Some discrepancies in metric names were observed between the `ScpAlertrules.yaml` file and the alerts documented in the SCP User Guide. **Doc Impact**: Updated the metric names in the "Alerts" section of *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	3	24.3.0
38154297	trafficFeed_attempted_total metric in SCP is intermittently pegged with an unknown value for the NFServiceType dimension during Notification RxRequest	The trafficFeed_attempted_total metric in SCP was intermittently set to an unknown value for the NFServiceType dimension during Notification RxRequest. **Doc Impact**: There is no doc impact.	3	25.1.200
38112967	"ocscp_authority" dimension missing in "ocscp_metric_http_rx_res_total" metric	The ocscp_authority dimension was missing from the ocscp_metric_http_rx_res_total metric. **Doc Impact**: There is no doc impact.	3	24.3.0

Table 4-6 (Cont.) SCP 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37971770	ocscp producer service instance id and ocscp producer nf instance id is same in ocscp_metric_http_rx_res_total and ocscp_metric_http_tx_req_total.	The ocscp producer service instance ID and ocscp producer NF instance ID were the same in ocscp_metric_http_rx_res_total and ocscp_metric_http_tx_req_total. **Doc Impact**: There is no doc impact.	3	25.1.200
37951970	Unable to edit services of the Registered NF's even if TSI is changed to Local	The services could not be edited for registered NFs even after Topology Source Information (TSI) was changed to Local. **Doc Impact**: There is no doc impact.	3	25.1.200
37936773	TLS, Jetty & micronaut exceptions are continuously logged at worker & nrf proxy on SCP 25.1.200-beta.57 Image	TLS, Jetty, and Micronaut exceptions were continuously logged on the worker of SCP 25.1.200 image. **Doc Impact**: There is no doc impact.	3	25.1.200
37627403	Incorrect Message is getting populated when query parameters are given as nf-type="PCF" under NF Rule Profile Data Section	An incorrect message was displayed when you set the query parameter nf-type="PCF" in the NF Rule Profile Data section. **Doc Impact**: There is no doc impact.	4	25.1.100
38646204	Incorrect Metric Name: Extra Space in ocscp_notification_ nf_profiles_count	The `ocscp_notification_nf_profiles_count` metric contained an unintended extra space before "nf" in its name, which may have caused issues in monitoring or fetching the metric. **Doc Impact**: Updates the `ocscp_notification_nf_profiles_count` metric name in the "Table 5-259 ocscp_notification_nf_profiles_count" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	4	25.2.100

Table 4-6 (Cont.) SCP 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38457711	Incorrect text in the SCP Response Timeout Extension section of SCP User Guide	The "SCP Response Timeout Extension" section in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide* incorrectly stated that the 200 MPS limit applies only to the Namf interface, when it should apply to all NF services with Namf given as an example. **Doc Impact**: Replaced "The SCP supports up to 200 messages per second (MPS) for all NF Service-Based Interface (SBI) traffic through the Namf interface" with "A single SCP deployment supports up to 200 messages per second (MPS) for all NF Service-Based Interface (SBI) traffic through multiple interfaces." in the "SCP Response Timeout Extension" section in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	4	24.3.0
38031000	SCP is selecting the alternate destination on the bases of NF_SET even alternateNFGroupRoutingOptions mode is DNS_SRV and altRoutingDnsSrvModeSupported flag is false	SCP selected an alternate destination based on NF_SET even though alternateNFGroupRoutingOptions was set to DNS_SRV and the altRoutingDnsSrvModeSupported parameter was false. **Doc Impact**: There is no doc impact.	4	25.1.200
38079582	Notification: Remove .getName() from LogManager invocation	A code audit found that logger calls still used getName(), and all such uses should have been removed. **Doc Impact**: There is no doc impact.	4	25.1.200

Table 4-6 (Cont.) SCP 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38441396	ocscp_consumer_host attribute is missing in ocscp_metric_5gsbi_rx_req_total and ocscp_metric_5gsbi_tx_req_total in user Guide.	The ocscp_consumer_host parameter was missing from the ocscp_metric_5gsbi_rx_req_total and ocscp_metric_5gsbi_tx_req_total metrics in the User Guide. **Doc Impact**: Added the `ocscp_consumer_host` dimension to `ocscp_metric_5gsbi_rx_req_total` and `ocscp_metric_5gsbi_tx_req_total` metrics in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	4	25.2.100
38221723	Update Log level details in verbose logging of SCP-Worker and nrfProxy as per the code.	The log level details in verbose logging for SCP-Worker and nrfProxy were not aligned with the code and required an update. **Doc Impact**: Added the missing event IDs in the "Verbose Logging for SCP" section of *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	4	25.2.100
38250006	Incorrect description of status field in MediationRulesConfig table in REST Guide	The REST Guide contained an incorrect description of the status field in the MediationRulesConfig table. **Doc Impact**: Updated the description of `state` and `status` parameters in the "Configuring Mediation Rule" section of *Oracle Communications Cloud Native Core, Service Communication Proxy REST Specification Guide*.	4	25.1.200
38375894	SCP Transaction Success Rate showing 0% by default on Grafana	The SCP transaction success rate displayed as 0% by default on the Grafana dashboard when using the *ocscp_metric_dashboard_promha_25.1.201.json* file of SCP 25.1.201, and the correct success rate appeared only after the *Transform* section was removed from the dashboard. **Doc Impact**: There is no doc impact.	4	25.1.201

Table 4-6 (Cont.) SCP 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38418107	Description of event ID OSCP-NTF-RULUPD-EV010 missing in SCP User Guide	The description of event ID OSCP-NTF-RULUPD-EV010 was missing from the SCP User Guide. **Doc Impact**: Added the missing event IDs in the "Verbose Logging for SCP" section of *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	4	25.1.201
38435655	Document maximum values of a counter metric.	A query was raised regarding the maximum values for incremental counters and their reset behavior. **Doc Impact**: Added a note "The maximum value of the incremental counter for SCP metrics is 1.7976931348623157 × 10^308 (1.7976931348623157E308). When this value is reached, SCP resets the counter to 0 per pod." in the "Metric" section of *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	4	24.2.0

> **Note**
>
> Resolved bugs from 25.1.100 and 25.1.200 have been forward ported to Release 25.2.100.

Table 4-7 SCP ATS 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38592919	SCP_RoutingRules_R16_API_P0 failing on re-run as initial and cleanup scenario is not running.	SCP_RoutingRules_R16_API_P0 failed on re-run because the initial and cleanup scenarios did not execute. **Doc Impact**: There is no doc impact.	3	25.2.100
38537989	Parallel execution causes ConsumerInfo API to get corrupted and persist stale values in database, leading to downstream FT failures	Parallel test execution caused the ConsumerInfo API to become corrupted and persist stale values in the database, which led to downstream feature test failures. **Doc Impact**: There is no doc impact.	3	25.2.100

Table 4-7 (Cont.) SCP ATS 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38451676	Parallel execution causes ConsumerInfo API to get corrupted and persist stale values in database, leading to downstream FT failures	The parallel test execution caused the ConsumerInfo API to become corrupted and persist stale values in the database, which led to downstream feature test failures. **Doc Impact**: There is no doc impact.	3	25.2.100
38385323	DDClient stub is by default having DEBUG level logs instead of INFO level logs	The log level for ddclientstub was set to DEBUG even though the environment and configmap specified INFO, which caused pod restarts during ATS runs. **Doc Impact**: There is no doc impact.	4	25.2.100

4.2.9 SEPP Resolved Bugs

Release 25.2.100

Table 4-8 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

Table 4-8 (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

Table 4-8 (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

Table 4-8 (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

Table 4-8 (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

Table 4-8 (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

Table 4-8 (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

Table 4-8 (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

Table 4-8 (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

Table 4-8 (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

Table 4-8 (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

Table 4-8 (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

Table 4-8 (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

Table 4-8 (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

4.2.10 UDR Resolved Bugs

Release 25.2.100

Table 4-9 UDR 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38296509	SLF failing- Open API specification file contains error validations	The `ocudr_mgm_api_25.1.100.yaml` and `ocudr_nudr_config_api_25.1.100.yaml` files contained format errors when checked with the YAMLLint tool. **Doc Impact:** There is no doc impact.	3	25.1.100
38083572	SLF - We observed restart on dr-service pods when we performed negative test case on cndb	During a test on the cnDBTier, the dr-service pods restarted. This happened when the ndbapp pod was scaled down from seven to zero for 15 minutes and then scaled back up. **Doc Impact:** There is no doc impact.	3	25.1.200
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
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 did not expose `containerPortNames`, requiring users to manually locate them in charts for provisioning `backendPortName` in Cloud Native Load Balancer (CNLB) annotations. **Doc Impact:** There is no doc impact.	3	25.1.100
37837227	SLF - Complete traffic drop observed when we tried to induced latency between cndb and slf during performance run	There was loss of lookup and provisioning traffic when latency was introduced between cnDBTier and SLF. **Doc Impact:** There is no doc impact.	3	25.1.100

Table 4-9 (Cont.) UDR 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
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 run 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
38376438	UDR 25.1.200 - CSV Export of Policy Data - Export is failing with vsaJson Null Error	Incoming messages did not appear in the user interface because the message handling module encountered a null pointer exception. **Doc Impact:** There is no doc impact.	3	25.1.200
38305513	Empty ocslf_alertrules_empty_<version>.yaml is not present in OSO Package	The empty configuration file `ocslf_alertrules_empty_<version>.yaml` was not included in the OSO software package. Instead, the file was located in the `ocudr_custom_configtemplates` directory of the UDR package. **Doc Impact:** Updated the "Alert section" section in *Oracle Communications Cloud Native Core, Unified Data Repository Installation, Upgrade, and Fault Recovery Guide*.	3	25.1.200

Table 4-9 (Cont.) UDR 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38294162	SLF-We observed incorrect metrics oc_ingressgateway_http_request_ratelimit_count in the user guide	The user guide incorrectly listed the metric `oc_ingressgateway_http_request_ratelimit_count`, which is not present in Prometheus. The correct metric is `oc_ingressgateway_http_request_ratelimit_values_total`. **Doc Impact:** Updated the correct metrics name in the "Ingress Gateway Metrics " section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.	3	25.1.200
37776157	SLF- We are observing ERROR logs on ingress gateway signaling pods after upgrading slf from 23.4.x release to 25.1.100 release	ERROR logs appeared in ingress gateway signaling pods after upgrading SLF from 23.4.x to 25.1.100 due to a old resource version. **Doc Impact:** There is no doc impact.	3	25.1.100
38089584	PROVGW- We observed ERROR related to alternate-route on PROVGW egress pod	Alternate route errors were observed on the Provisioning gateway egress pod during a scaling operation. **Doc Impact:** There is no doc impact.	3	25.1.200
38055372	Need improvement in LOG messages in DR Service & IGW_POD Logs	Log messages in the dr-service and Ingress Gateway pods needed improvement. The dr-service logs did not include subscriber ID details during auto enrollment, and Ingress Gateway logs showed many warning messages due to mismatched response codes. **Doc Impact:** There is no doc impact.	4	24.2.4
37167720	WARNING MSG "Response code received from back-end service doesnot match errorCodeSeries configured" appears in IGW_SIG continously	The warning message "Response code received from back-end service does not match errorCodeSeries configured" was continuously appearing in Ingress Gateway signaling logs, which resulted in excessive logging and impacting log storage. **Doc Impact:** There is no doc impact.	4	24.3.0

> **Note**
>
> Resolved bugs from 24.2.x and 25.1.2xx have been forward ported to Release 25.2.100.

4.2.11 Common Services Resolved Bugs

4.2.11.1 ATS Resolved Bugs

Release 25.2.100

Table 4-10 ATS 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38188247	When before_stage hooks fails, the build or run passes instead of being failed or unstable	The build or run passed even when a before_stage for a stage failed, whereas it was expected to be marked as failed or unstable. **Doc Impact:** There is no doc impact.	3	25.2.100
38274149	CNCATS- Trace Validation scenario failures with ServiceNameError exception	Trace validation scenarios failed with the ATS framework due to an InvalidServiceNameError indicating no available service on the specified trace_query_server. **Doc Impact:** There is no doc impact.	3	25.2.100
38203983	Overall Results and NewFeature OverAll Result counts are mismatched when Features were skipped in execution.	Overall Results and NewFeature OverAll Result counts were mismatched when features were skipped during the test case run. When no features were run, the test case run count was incorrectly shown as 1 for the skipped feature under NewFeature OverAll Result instead of zero. **Doc Impact:** There is no doc impact.	4	25.1.200

4.2.11.2 ASM Configuration Resolved Bugs

Release 25.2.100

There are no resolved bugs in this release.

4.2.11.3 Alternate Route Service Resolved Bugs

Release 25.2.104

There are no resolved bugs in this release.

Release 25.2.103

There are no resolved bugs in this release.

Release 25.2.102

There are no resolved bugs in this release.

Release 25.2.101

Table 4-11 Alternate Route Service 25.2.101 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38363339	Alternate Route pod servc restart in staging during Upgrade (25.2.100)	During an upgrade, the Alternate Routes Service pods restarted while four pods were running in production. **Doc Impact:** There is no doc impact.	3	23.4.10

> **Note**
>
> A resolved bug from 23.4.10 has been forward ported to Release 25.2.101.

Release 25.2.100

Table 4-12 Alternate Route Service 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38193180	The port is not considered when endpoint is resolved as part of jetty destination resolver	The port was not considered during endpoint resolution in the jetty destination resolver, which caused requests to be directed to the exposed port instead of the actual service port after DNS resolution. **Doc Impact:** There is no doc impact.	2	25.2.100

> **Note**
>
> A resolved bug from 25.1.100 has been forward ported to Release 25.2.101.

4.2.11.4 Common Configuration Service Resolved Bugs

Release 25.2.104

There are no resolved bugs in this release.

Release 25.2.103

There are no resolved bugs in this release.

Release 25.2.101

Table 4-13 Common Configuration Service 25.2.101 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38154277	Observing NullPointerException for custom header feature when defaultVal: null, after that any new routes are not getting updated. All calls are failing with NullPointerException.	A NullPointerException occurred for the custom header feature when the defaultVal was set to null, after which new routes were not updated and all calls failed with a NullPointerException. **Doc Impact:** There is no doc impact.	3	24.2.100
36826534	SBIWeightBased routing option not visible in routes config GUI screen of PLMN EGW	In the PLMN Egress Gateway GUI, the routes configuration did not display the `sbiRoutingWeightBasedEnabled` option. **Doc Impact:** There is no doc impact.	3	24.2.0

> **Note**
>
> Resolved bugs from 25.1.100 have been forward ported to Release 25.2.101.

Release 25.2.101

There are no resolved bugs in this release.

Release 25.2.100

There are no resolved bugs in this release.

4.2.11.5 Egress Gateway Resolved Bugs

Release 25.2.104

There are no resolved bugs in this release.

Release 25.2.103

There are no resolved bugs in this release.

Release 25.2.102

Table 4-14 Egress Gateway 25.2.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38353944	Egress gateway pods restarted post upgrade of policy from 24.2.5 to 25.1.200	Egress Gateway pod restarted after upgrading Policy, and this issue occurred once during the testing and was intermittent. **Doc Impact:** There is no doc impact.	3	25.2.100
38342233	Observing SSL Exception with "Tag Mismatch" error message during SM Create	SSL exception was observed with an error message, "Tag Mismatch", during SM creation. **Doc Impact:** There is no doc impact.	2	25.2.100

> **Note**
>
> Resolved bugs from 25.2.100 have been forward ported to Release 25.2.102.

Release 25.2.101

Table 4-15 Egress Gateway 25.2.101 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38299966	EnvoyFilter Connection Repaving causes , requests to fail	When EnvoyFilter was used for connection repaving based on parameters such as max_requests_per_connection, the immediate request after the connection was repaved failed. **Doc Impact:** There is no doc impact.	2	25.2.100
37801259	SBIWeightBased routing option not visible in routes config GUI screen of PLMN EGW	The sbiRoutingWeightBasedEnabled option was not displayed in the routes configuration on the PLMN Egress Gateway GUI. **Doc Impact:** There is no doc impact.	3	24.2.0

Table 4-15 (Cont.) Egress Gateway 25.2.101 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38154277	Observing NullPointerException for custom header feature when defaultVal: null, after that any new routes are not getting updated. All calls are failing with NullPointerException.	A NullPointerException occurred for the custom header feature when the defaultVal was set to null, after which new routes were not updated and all calls failed with a NullPointerException. **Doc Impact:** There is no doc impact. .	3	25.2.100
37648493	Issue with message copy feature for the access token request generated at EGW towards NRF	The access token request generated at Egress Gateway was not sent to Kafka. However, the response received at Egress Gateway from the access token was fed into Kafka. **Doc Impact:** There is no doc impact.	3	25.1.200

> **Note**
>
> Resolved bugs from 25.2.100 have been forward ported to Release 25.2.101.

Release 25.2.100

Table 4-16 Egress Gateway 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38174384	EGW is rejecting the request when enableOutgoingHTTP1 flag is enabled and oc-http-version: http1 is sent in request header	When the enableOutgoingHTTP1 parameter was set to true and a request with the header oc-http-version: http1 was sent to Egress Gateway, the request was rejected with a 500 error due to a class cast exception in the HTTP connection handling. **Doc Impact:** There is no doc impact.	2	25.2.100
37564746	Missing Metric for Blacklisted SCP in SBI Routing Flows at EGW	During testing, it was found that there was no metric to identify when an SCP was blacklisted during SBI Routing flows in the Egress Gateway, which limited observability for tracking blacklisting conditions and their duration. **Doc Impact:** There is no doc impact.	3	25.1.200

Table 4-16 (Cont.) Egress Gateway 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37578043	In oc_ingressgateway_http_responses_total metric UNKNOWN status updated for the NFTYPE and NFSERVIE type for UDR service notification	In the `oc_ingressgateway_http_responses_total` metric, NFTYPE and NFSERVICE types were updated as UNKNOWN. **Doc Impact:** There is no doc impact.	4	25.1.100

4.2.11.6 Ingress Gateway Resolved Bugs

Release 25.2.104

Table 4-17 Ingress Gateway 25.2.104 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38563676	X-Forward host header not added by Ingress gateway	The X-Forward host header was not added by Ingress Gateway. **Doc Impact:** Added the "Forwarded Header Configuration" section in *Oracle Communications Cloud Native Core, Ingress Gateway User Guide*.	2	25.2.102

Release 25.2.103

There are no resolved bugs in this release.

Release 25.2.102

Table 4-18 Ingress Gateway 25.2.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38342233	Observing SSL Exception with "Tag Mismatch" error message during SM Create	SSL exception was observed with an error message, "Tag Mismatch", during SM creation. **Doc Impact:** There is no doc impact.	2	25.2.100
38353944	Egress gateway pods restarted post upgrade of policy from 24.2.5 to 25.1.200	Egress Gateway pod restarted after upgrading Policy, and this issue occurred once during the testing and was intermittent. **Doc Impact:** There is no doc impact.	3	25.2.100

Table 4-18 (Cont.) Ingress Gateway 25.2.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38352595	High latency was observed at IGW when scaling the pods horizontally to support higher traffic	When Ingress Gateway is scaled from 20 pods (handling 80K TPS at 70–75% CPU) to 32 pods to target 96K to 120K TPS, latency at Ingress Gateway increased for the worst 10% of the traffic. **Doc Impact:** There is no doc impact.	2	25.2.101

> **Note**
>
> Resolved bugs from 25.1.100 have been forward ported to Release 25.2.102.

Release 25.2.101

Table 4-19 Ingress Gateway 25.2.101 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38299966	EnvoyFilter Connection Repaving causes , requests to fail	When EnvoyFilter was used for connection repaving based on parameters such as max_requests_per_connection, the immediate request after the connection was repaved failed. **Doc Impact:** There is no doc impact.	2	25.2.100
38154277	Observing NullPointerException for custom header feature when defaultVal: null, after that any new routes are not getting updated. All calls are failing with NullPointerException.	A NullPointerException occurred for the custom header feature when the defaultVal was set to null, after which new routes were not updated and all calls failed with a NullPointerException. **Doc Impact:** There is no doc impact.	3	24.2.100
37801259	SBIWeightBased routing option not visible in routes config GUI screen of PLMN EGW	The sbiRoutingWeightBasedEnabled option was not displayed in the routes configuration on the PLMN Egress Gateway GUI. **Doc Impact:** There is no doc impact.	3	24.2.0

> **Note**
>
> Resolved bugs from 25.1.100 have been forward ported to Release 25.2.101.

Release 25.2.100

Table 4-20 Ingress Gateway 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38174384	EGW is rejecting the request when enableOutgoingHTTP1 flag is enabled and oc-http-version: http1 is sent in request header	When the enableOutgoingHTTP1 parameter was set to true and a request with the header oc-http-version: http1 was sent to EGW, the request was rejected with a 500 error due to a class cast exception in the HTTP connection handling. **Doc Impact:** There is no doc impact.	2	25.2.100
37032005	IGW is timing out with 408 request intermittently	Ingress Gateway timed out for certain messages, and logs indicated the presence of a race condition during these occurrences. **Doc Impact:** There is no doc impact.	2	24.3.0
38216940	Message Copy Cases Failing due to missing headers	Message Copy cases failed due to the absence of required headers, such as 'nettylatency' and 'requestmethod', which impacted backward compatibility with the network. **Doc Impact:** There is no doc impact.	3	25.2.100
38042890	66K traffic with POP25 and CCA enabled - CPU utilization is more than 90 percent	When the Client Credentials Assertions header was enabled at the global level and the Pod Protection feature was activated during a 66K traffic run, CPU utilization exceeded 90 percent. **Doc Impact:** There is no doc impact.	3	25.1.200
37188113	WARNING MSG "Response code received from back-end service does not match errorCodeSeries configured" appears in IGW continously	The warning message "Response code received from back-end service does not match errorCodeSeries configured" appeared continuously in IGW_SIG logs while running traffic, indicating that the back-end response code did not align with the configured error code series. **Doc Impact:** There is no doc impact.	3	24.3.0

Table 4-20 (Cont.) Ingress Gateway 25.2.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37860609	/oauth2/token returns 403 error unless 3gpp-sbi-client-credentials includes 'Bearer'	The request was refused with a 403 error unless the 3gpp-sbi-client-credentials header attribute included 'Bearer' before the JWT, although the specification indicated that 'Bearer' should not be present in the attribute content. **Doc Impact:** There is no doc impact.	3	24.3.0
37578043	In oc_ingressgateway_http_responses_total metric UNKNOWN status updated for the NFTYPE and NFSERVIE type for UDR service notification	In the `oc_ingressgateway_http_responses_total` metric, NFTYPE and NFSERVICE types were updated as UNKNOWN. **Doc Impact:** There is no doc impact.	4	25.1.100
38178922	The same Congestion level for resource logs are being repeatedly generated in the IGW pod	The same congestion level for resource logs were repeatedly generated in the Ingress Gateway pod. **Doc Impact:** There is no doc impact.	4	25.1.203

> **Note**
>
> Resolved bugs from 24.3.0 have been forward ported to Release 25.2.100.

4.2.11.7 Helm Test Resolved Bugs

Release 25.2.1xx

There are no resolved bugs in this release.

4.2.11.8 App-Info Resolved Bugs

Release 25.2.1xx

There are no resolved bugs in this release.

4.2.11.9 Mediation Resolved Bugs

Release 25.2.100

There are no resolved bugs in this release.

4.2.11.10 NRF-Client Resolved Bugs

Release 25.2.102

Table 4-21 NRF-Client 25.2.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38562170	Priority set to UNKNOWN for requests for AutonomousNfSubscriptionUpdate and AutonomousNfUnSubscribe (Nrf-Client 25.2.102)	After enabling Traffic Prioritization in the Egress Gateway Helm configuration, the default `trafficPrioritization` setting did not assign priority levels to `AutonomousNfUnSubscribe` and `AutonomousNfSubscriptionUpdate` messages, leaving them incorrectly marked as `UNKNOWN`.	2	25.2.200

Release 25.2.101

Table 4-22 NRF-Client 25.2.101 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38450018	NRF-Client sending user-agent header while sending registration or hearbeat even when userAgentFlag set to false (25.2.101)	The NRF-Client was incorrectly sending the `User-Agent` header to the Egress Gateway microservice even when the `userAgent` flag was disabled.	2	25.2.100

Release 25.2.100

There are no resolved bugs in this release.

4.2.11.11 Perf-Info Resolved Bugs

Release 25.2.1xx

There are no resolved bugs in this release.

4.2.11.12 Debug Tool Resolved Bugs

Release 25.2.1xx

There are no resolved bugs in this release.

4.3 Known Bug List

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

4.3.1 BSF Known Bugs

Release 25.2.100

There are no new known bugs for this release.

4.3.2 CNC Console Known Bugs

Release 25.2.100

Table 4-23 CNC Console 25.2.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38319858	POLICY_READ Role enabled but user is also able to edit the parameters	A user with only the POLICY_READ role enabled is able to edit parameters.	There is no functional impact. A user with only the POLICY_READ role enabled will be able to edit parameters. **Workaround**: Uses can be assigned both POLICY_READ and POLICY_WRITE roles until the issue is resolved.	3	24.2.3

4.3.3 cnDBTier Known Bugs

Release 25.2.100

Table 4-24 cnDBTier 25.2.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38166191	Traffic Failure After Enabling Exception Table Cleanup Feature	After enabling the Exception Table Cleanup feature on the deployment, traffic failures were observed.	During certain Webscale cluster maintenance procedures, unexpected restarts of cnDBTier data pods may interrupt the PCF process. This interruption can result in the loss of nologging tables within PCF. **Workaround**: If a maintenance procedure fails, resulting in loss of nologging table data, initiate the Georeplication Recovery (GRR) process. This will restore PCF service and recover the data from the nologging tables.	2	23.4.4

Table 4-24 (Cont.) cnDBTier 25.2.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38267894	SM-PCF RCKL 002 Ingress and Egress Traffic	Following a rollback of the SM PCF (from version 23.4.6 to 23.4.4) at the RCKL 002 site due to a Helm upgrade failure, it was observed that all ingress and UDR traffic dropped to 0%.	During certain Webscale cluster maintenance procedures, unexpected restarts of cnDBTier data pods may interrupt the PCF process. This interruption can result in the loss of nologging tables within PCF. **Workaround**: If a maintenance procedure fails, resulting in loss of nologging table data, initiate the Georeplication Recovery (GRR) process. This will restore PCF service and recover the data from the nologging tables.	2	23.4.4
38426377	SM SLK West 004 Mgm pods getting crashed	In the SM SLK West 004 environment, management pods are repeatedly crashing, and node 50 is disconnected from the cluster.	One of the two mgmd pods is currently disconnected from the rest of the cnDBTier pods. However, since the second mgmd pod remains operational, there is no impact on database queries from the application or on geo-replication. **Workaround**: During the next maintenance window, restart both the mgmd pods at the same time to restore connectivity between both mgmd pods and the rest of the cnDBTier pods.	2	23.4.6
38414831	ndbmtd-1 is in a CrashLoopBackOff state on the AM-PCF rcklca63vzwcpcf-y-or-am-w1-003 deployment.	On the AM-PCF rcklca63vzwcpcf-y-or-am-w1-003 deployment, the ndbmtd-1 pod is continuously observed in a CrashLoopBackOff state before and after restart attempts.	One of the data pods is repeatedly restarting. However, since the other data pod remains operational, there is no impact on database queries from the application or on geo-replication. **Workaround**: During the next maintenance window, scale down all data pods and then scale them back up to restore normal operation across all data pods.	2	23.4.6

Table 4-24 (Cont.) cnDBTier 25.2.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38582579	Rest API of db-replication-svc will not be accessible outside db-replication-svc during migration of http	During migration between HTTPS and HTTP, the REST API of db-replication-svc will not be accessible externally. This is due to a misconfiguration in a newly created internal service, where the replication-svc is set to use HTTPS even though it is not fully enabled. As a result, while the replication service is configured for HTTPS, clients such as monitor-svc and helm test see HTTPS as disabled, leading to access issues during the transition.	During migration between HTTP and HTTPS, when the DB Tier is set with HTTPS disabled and supportDualProtocol, Helm tests and REST APIs that use db-replication-svc will fail. This also affects certain console GUI screens such as replication health and heartbeat status, and GRR cannot be performed through the console during this transition. **Workaround**: This issue occurs only during the migration between HTTP and HTTPS. To minimize errors in certain REST APIs, it is recommended to complete the migration as quickly as possible.	3	25.2.100

4.3.4 CNE Known Bugs

Release 25.2.100

Table 4-25 CNE 25.1.200 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 platform agnostic bmCNE deployment procedure of X9-2 servers" from *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*. • Use CNE 24.3.1 or older version on X9-2 servers.	2	23.4.0

4.3.5 OCCM Known Bugs

Release 25.2.100

There are no known bugs in this release.

4.3.6 OSO Known Bugs

Release 25.2.100

There are no known bugs in this release.

4.3.7 Policy Known Bugs

Release 25.2.100

Table 4-26 Policy 25.2.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38293751	SM-PCF: Policy Table is missing a row in CNCC GUI	While using the policy_tables_check script, it was observed that the tMedia_039 table has a row missing in the CNCC UI for site SM-PCF.	Incorrect policy was installed, modified, or removed. **Workaround**: • Export the table "<table_name>" from UI from a good site, POLICY ->Policy Data Configuration -> Common -> Policy Table • Select tMedia_039 table, click on arrow sign on right to export it locally on desktop. • Once it is downloaded, import it on the bad site's SM-PCF UI where the row is missing for table "<table_name>"POLICY -> Policy Data Configuration -> Common -> Policy Table • Click Import, click Drag and Drop and select the downloaded file, Select Merge and Retain, Verify that file is selected and once verified, click Import. • Verify by clicking on Open icon for Policy Table <table_name>, ensure you have all the rows in it now.	2	23.4.6
38414790	ndbmtd-1 in CrashLoopBackOff on one of the sites	CrashLoopBackOff occurred in ndbmtd-1 on one of the sites.	cnDBTier cluster failure triggers retry for signaling traffic on other site. **Workaround**: Run single data pod fault recovery from *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*. That will include delete PVC on ndbmtd-1 and restart pod.	2	23.4.6

Table 4-26 (Cont.) Policy 25.2.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38412963	After GRR DB Entries are Not in sync in Site-1 and Site-2 (failed Site)	DB Entries are not in sync in Site-1 and Site-2 (failed Site) after performing GRR.	There is a mismatch in the record count after performing GRR procedure, where failed site record count is slightly higher than healthy site. **Workaround**: None	3	25.1.200
38412996	Bulk export is partial success due to policy project internal server error after the upgrade from 25.1.200 to 25.2.100	While upgrading from 25.1.200 to 25.2.100, the Bulk export is partial successful due to policy project internal server error.	• If there are issues in the policy projects or any configurations, the export will not occur, and the report will show Internal_Server_Error. • While this behavior is expected due to validations, the report currently does not provide details explaining why the export failed. Including these details would help users understand the cause of the failure. This does not impact any other functionality. **Workaround**: None	3	25.2.100
38486279	PCF 24.2.3 has more than 4 (max_connection_per_destination) Connection with SCP	PCF 24.2.3 has more than 4 max_connection_per_destination connection with SCP.	PCF is establishing double the connections towards SCP than what is configured under MAX_CONNECTIONS_PER_DESTINATION **Workaround**: None	3	24.2.3
35847911	Not able to access Overload Control Threshold Tab from Policy UI after Rollback	While accessing the **Overload Control Threshold** tab from the Policy UI, a rollback error is displayed and a subsequent successful upgrade.	Due to duplicate entries in common config db after rollback failure common-comon api's are not working, due to which some of the GUI screens are not working as expected. **Workaround**: Performing the proper cleanup if upgrade/rollback fails, Deleting the duplicate entries from common_config_db.	3	23.1.7

Table 4-26 (Cont.) Policy 25.2.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38196773	Exception table entries getting generated resulting in DB Entries on Site-1 and Site-2 out of sync after doing an in service upgrade from 24.2.6 to 25.1.200 on a 2 site GR setup	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 two-site GR setup for tables SmPolicyAssociation_1, SmPolicyAssociation_2, pdsprofile, and pdssubscriber. Also, the exception entries were created for the below tables SmPolicyAssociation_EX, AppSession_EX, pdsprofile_EX, pdssubscriber_EX, contextbinding_EX, and dependentcontextbinding_EX.	During the MySQL upgrade or rollback, entries in the exception tables may continuously increase, leading to temporary data inconsistency. This can result in data inconsistency across sites, and if subsequent requests are routed to other sites, some data may appear missing. Over time, the system will reach eventual consistency, particularly if follow-up requests are directed to the same site **Workaround**: None	3	25.1.200

4.3.8 SCP Known Bugs

Release 25.2.100

Table 4-27 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

Table 4-27 (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

Table 4-27 (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

Table 4-27 (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

Table 4-27 (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

Table 4-27 (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

4.3.9 SEPP Known Bugs

Release 25.2.100

Table 4-28 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

Table 4-28 (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

Table 4-28 (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

Table 4-28 (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

Table 4-28 (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

Table 4-28 (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

SEPP 25.2.100 Gateway Known Bugs

Table 4-29 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

Table 4-29 (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

4.3.10 UDR Known Bugs

Release 25.2.100

Table 4-30 UDR 25.2.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38420558	Certificate expired ALERT missing in alert.yaml file	The certificate expiry alert is missing in the alert.yaml file.	There is no impact. **Workaround:** The `alert.yaml` file must be created manually.	3	24.2.4

4.3.11 Common Services Known Bugs

4.3.11.1 ATS Known Bugs

Release 25.2.100

There are no known bugs in this release.

4.3.11.2 ASM Configuration Known Bugs

Release 25.2.100

There are no known bugs in this release.

4.3.11.3 Alternate Route Service Known Bugs

Release 25.2.1xx

Table 4-31 Alternate Route Service 25.2.1xx Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38522842	First lookup call to ARS is failing for configured vFQDN	The first lookup call to Alternate Route Service fails for configured vFQDN.	As the DNS lookup fails on the first request, it causes calls to fail. Later, all calls are successful. **Workaround**: Send a manual lookup call before the application starts to send the request.	3	25.1.200

4.3.11.4 Egress Gateway Known Bugs

Release 25.2.1xx

Table 4-32 Egress Gateway 25.2.1xx Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37751607	Egress gateway throwing NPE when trying to send oauth token request to "Default NRF Instance" when unable to find NRF instance to forward the request	Egress Gateway failed to send requests to the configured *primaryNrfApiRoot* and *secondaryNrfApiRoot* endpoints specified in the configmap. Subsequently, it attempted to send an OAuth2 token request to the default NRF instance at "[http://localhost:port/oauth2/token]," but this request also failed. Egress Gateway displayed a NullPointerException.	This issue occurs only when an invalid host and port are provided. The port is mentioned with string value as "port" instead of a numeric port value, for example, 8080. **Workaround**: You must provide the valid host and port for the NRF client instance.	3	25.1.200
38339561	Metrics oc_ingressgateway_dd_unreachable and oc_egressgateway_dd_unreachable are not resetting to value zero after connection with DD is restored	After the connection with Oracle Communications Network Analytics Data Director is restored, the oc_ingressgateway_dd_unreachable and oc_egressgateway_dd_unreachable metrics do not reset to 0.	It has observability impact as even the connection is restored, the metric is not updated. **Workaround**: None	3	24.1.5
38504941	EGW/IGW should include LCI header when the current load is less than or equals to the difference between previously reported load and configured LoadThreshold value	Ingress Gateway and Egress Gateway do not include the LCI header when the current load is less than or equal to the difference between the previously reported load and the configured LoadThreshold.	It has an impact on consumer NF to decide for traffic load as LCI information is not shared when the current load is less than or equal to the difference between the previously reported load and the configured LoadThreshold. **Workaround**: None	3	25.2.102

Table 4-32 (Cont.) Egress Gateway 25.2.1xx Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38304085	EGW is not Validating 3gpp-sbi-message-priority Header parameters in case of POP25 and Overload	Egress Gateway do not validate the 3gpp-sbi-message-priority header parameters in the pod protection overload scenarios.	This Config validation issue causes the feature to malfunction in case invalid values are received. **Workaround**: The consumer NF should send valid values in the header to avoid any malfunctioning.	3	25.2.100
38294514	Observed NPE during oauth-acess-request message when "nrfClientQueryEnabled" flag enabled	An NPE is observed during the oauth-access-request message when the nrfClientQueryEnabled parameter is enabled.	Due to Null Pointer Exception (NPE), the OAuth access token request does not reach the NRF, and more calls fail because the OAuth token request is failing. **Workaround**: None	3	25.2.100
38279961	"oauthDeltaExpiryTime" functionality not working during traffic run. Somtimes EGW is requesting NRF oauthtoken even though still ""oauthDeltaExpiryTime" not expired.	The oauthDeltaExpiryTime functionality does not work during traffic run. Egress Gateway requests an NRF OAuth token before the configured oauthDeltaExpiryTime expires.	There is no traffic impact because token request processing occurs before timerExpiry. **Workaround**: None	3	25.2.100
38522816	EGW fails to build peer health table after initial ARS call fails	Egress Gateway fails to construct the peer health table after the first Alternate Route Service call fails.	None of the Alternate Route Service calls are able to reconstruct the peer health table back. **Workaround**: Restart the pod.	3	25.1.200

4.3.11.5 Ingress Gateway Known Bugs

Release 25.2.1xx

Table 4-33 Ingress Gateway 25.2.1xx 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 the controlledshutdownerrormapping and errorcodeprofiles are not present. This indicates that the required action of rejecting traffic will not occur. There must be a pre-check to check for these configurations before allowing the state to be changed. If the pre-check fails, the operational state should not be changed.	Request will be processed by Gateway Services when it is supposed to be rejected. **Workaround**: None	3	23.2.0
38339561	Metrics oc_ingressgateway_dd_unreachable and oc_egressgateway_dd_unreachable are not resetting to value zero after connection with DD is restored	After the connection with Oracle Communications Network Analytics Data Director is restored, the oc_ingressgateway_dd_unreachable and oc_egressgateway_dd_unreachable metrics do not reset to 0.	It has observability impact as even the connection is restored, the metric is not updated. **Workaround**: None	3	24.1.5
38405814	Post_rollback_SM_Validation fails at alternate-route logging level validation	The alternate-route logging level values are mismatching.	It has no impact because it is not a production use case. The log level is not changed from WARN to DEBUG. **Workaround**: None	3	25.2.100

Table 4-33 (Cont.) Ingress Gateway 25.2.1xx Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38310333	In TLS setup when IGW rejected with 401 then IGW Request/ Response Latency metrics are not updated	In a TLS setup, when Ingress Gateway rejects a request with HTTP 401, the Ingress Gateway request and response latency metrics are not updated.	It has observability impact because the latency metric is not being updated. **Workaround**: None	3	25.2.100
38293511	IGW is not Validating 3gpp-sbi-message-priority Header parameters in case of POP25 and Overload	Ingress Gateway does not validate the 3gpp-sbi-message-priority header parameters in the pod protection overload scenarios.	This Config validation issue causes the feature to malfunction in case invalid values are received. **Workaround**: The consumer NF should send valid values in the header to avoid any malfunctioning.	3	25.2.100
38181400	NPE seen in one of the IGW pod during pod initialization	In Ingress Gateway 25.1.203, an NPE occurs in one of the Ingress Gateway pods during initialization in an idle state when no traffic is sent.	Due to Null Pointer Exception (NPE), the OAuth access token request does not reach the NRF, and more calls fail because the OAuth token request is failing. **Workaround**: None	4	25.1.203

Table 4-33 (Cont.) Ingress Gateway 25.2.1xx Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37986338	For XFCC header failure case "oc_ingressgateway_http_responses_total" stats are not updated	When deploying Ingress Gateway with XFCC header validation enabled in a three-route configuration (for create, delete, and update operations), and sending traffic without the XFCC header, Ingress Gateway rejected the traffic due to XFCC header validation failure. However, the `oc_ingressgateway_http_responses_total` metric was not updated, but the `oc_ingressgateway_xfcc_header_validate_total` metric was updated.	The metric will not be pegged when the XFCC header validation failure is observed. **Workaround**: None	4	25.1.200
38461465	Sender Attribute should only consist SEPP-<sepp-fqdn> when addtional error logging in enabled in gw logging config	When any failure is observed in Gateway Services, the sender attribute format does not aligned with SEPP requirements when additional error logging is enabled in the Gateway Services logging configuration.	It has observability and debugging impact because it is a formatting issue for SEPP and SCP. **Workaround**: None	4	25.2.100

4.3.11.6 Common Configuration Service Known Bugs

Release 25.2.1xx

There are no known bugs in this release.

4.3.11.7 Helm Test Known Bugs

Release 25.2.1xx

There are no known bugs in this release.

4.3.11.8 Mediation Known Bugs

Release 25.2.100

There are no known bugs in this release.

4.3.11.9 NRF-Client Known Bugs

Release 25.2.1xx

There are no known bugs in this release.

4.3.11.10 App-Info Known Bugs

Release 25.2.1xx

There are no known bugs in this release.

4.3.11.11 Perf-Info Known Bugs

Release 25.2.1xx

There are no known bugs in this release.

4.3.11.12 Debug Tool Known Bugs

Release 25.2.1xx

There are no known bugs in this release.