Oracle® Communications

Cloud Native Core Release Notes

Release 2.5.0
F50692-23
June 2022

Oracle Communications Cloud Native Core Release Notes, Release 2.5.0

F50692-23

Contents

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

This section introduces the documentation updates for Release 2.5.0 in Oracle Communications Cloud Native Core (CNC) Release Notes.

Release 2.5.0 - F50692-23, June 2022

The following sections are updated for CNC Policy 1.15.5:

- Media Pack: Added Media pack details
- Compliance Matrix: Updated the compliance matrix information
- Common Services Load Lineup: Added Common Services Load Lineup details
- CNC Policy Resolved Bugs: Added resolved bugs list

Release 2.5.0 - F50692-22, June 2022

The following sections are updated for SCP 1.15.4:

- Media Pack: Added Media pack details
- Compliance Matrix: Added the compliance matrix information
- Common Services Load Lineup: Added Common Services Load Lineup details
- Security Certification Declaration : Added Security Compliance information
- SCP Resolved Bugs: Added resolved bugs list

Release 2.5.0 - F50692-22, April 2022

The following sections are updated for DBTier 1.10.3 and CNE 1.10.3:

- Media Pack: Added Media pack details
- CNE Resolved Bugs: Added DBTier 1.10.3 and CNE 1.10.3 resolved bugs list

Release 2.5.0 - F50692-21, April 2022

The following sections are updated for UDR 1.15.2:

- Media Pack: Added Media pack details
- Compliance Matrix: Added the compliance matrix information
- Common Services Load Lineup: Added Common Services Load Lineup details
- Security Certification Declaration : Added Security Compliance information

Release 2.5.0 - F50692-20, April 2022

The following sections are updated for NRF 1.15.2:

- Media Pack: Added Media pack details
- Compliance Matrix: Added the compliance matrix information
- Common Services Load Lineup: Added Common Services Load Lineup details
- Security Certification Declaration : Added Security Compliance information

Release 2.5.0 - F50692-19, April 2022

The following sections are updated for SCP 1.15.3:

- Media Pack: Added Media pack details
- Compliance Matrix: Added the compliance matrix information
- Common Services Load Lineup: Added Common Services Load Lineup details
- Security Certification Declaration : Added Security Compliance information
- SCP Resolved Bugs: Added resolved bugs list
- SCP Customer Known Bugs: Added customer known bugs list

Release 2.5.0 - F50692-17, April 2022

The following sections are updated for CNC Console 1.9.2:

- Media Pack: Added Media pack details
- Compliance Matrix: Updated the compliance matrix information
- Common Services Load Lineup: Added Common Services Load Lineup details

The following sections are updated for CNC Policy 1.15.4:

- Media Pack: Added Media pack details
- Compliance Matrix: Updated the compliance matrix information
- Common Services Load Lineup: Added Common Services Load Lineup details
- CNC Policy Resolved Bugs: Added resolved bugs list

Release 2.5.0 - F50692-16, March 2022

The following sections are updated for DBTier 1.10.2:

- Media Pack: Added Media pack details
- CNE Resolved Bugs: Added DBTier 1.10.2 resolved bugs list

Release 2.5.0 - F50692-15, March 2022

The following sections are updated for SCP 1.15.2:

- Media Pack: Added Media pack details
- Compliance Matrix: Added the compliance matrix information
- Common Services Load Lineup: Added Common Services Load Lineup details
- SCP Resolved Bugs: Added resolved bugs list
- SCP Customer Known Bugs: Added known bugs list

Release 2.5.0 - F50692-14, February 2022

The following sections are updated for SCP 1.15.1:

- Media Pack: Added Media pack details
- Compliance Matrix: Added the compliance matrix information
- Common Services Load Lineup: Added Common Services Load Lineup details

- SCP Resolved Bugs: Added resolved bugs list
- SCP Customer Known Bugs: Added known bugs list

Release 2.5.0 - F50692-13, February 2022

CNC Policy 1.15.3

The following sections are updated for CNC Policy 1.15.3:

- Media Pack: Added Media pack details
- Compliance Matrix: Updated the compliance matrix information
- Common Services Load Lineup: Added Common Services Load Lineup details
- CNC Policy Resolved Bugs: Added resolved bugs list

Release 2.5.0 - F50692-12, February 2022

The following section is updated for CNE 1.10.1:

- CNE Resolved Bugs: Updated CNE 1.10.1 resolved bug details

Release 2.5.0 - F50692-11, February 2022

CNE 1.10.1

The following sections are updated for CNE 1.10.1:

- Media Pack: Added Media pack details
- CNE Resolved Bugs: Added CNE 1.10.1 resolved bug details

Release 2.5.0 - F50692-10, January 2022

NRF 1.15.1

The following sections are updated for NRF 1.15.1:

- Media Pack: Added Media pack details
- Compliance Matrix: Updated compliance matrix
- Common Services Load Lineup: Updated common services load lineup
- NRF Resolved Bugs: Added NRF 1.15.1 resolved bug details

UDR 1.15.1

Added a Note in the Media Pack section.

Release 2.5.0 - F50692-09, January 2022

DBTier 1.10.1

The following sections are updated for DBTier 1.10.1:

- Media Pack: Added Media pack details
- CNE Resolved Bugs: Added DBTier 1.10.1 resolved bug details

Release 2.5.0 - F50692-08, January 2022

UDR 1.15.1

The following sections are updated for UDR 1.15.1:

- Media Pack: Added Media pack details
- Compliance Matrix: Updated the compliance matrix information
- Common Services Load Lineup: Added Common Services Load Lineup details

Release 2.5.0 - F50692-07, December 2021

CNC Policy 1.15.1

The following sections are updated for CNC Policy 1.15.1:

- Media Pack: Added Media pack details
- Compliance Matrix: Updated the compliance matrix information
- Common Services Load Lineup: Added Common Services Load Lineup details
- CNC Policy Resolved Bugs: Added resolved bugs list

Release 2.5.0 - F50692-06, December 2021

SEPP Release 1.7.1

The following sections are updated for SEPP Release 1.7.1:

- Media Pack: Added Media pack details
- Compliance Matrix: Updated the compliance matrix information
- Common Services Load Lineup: Added Common Services Load Lineup details
- SEPP Resolved Bugs: Added resolved bugs list
- Security Compliance Information: Added Security Compliance Information

CNC Console Release 1.9.1

The following sections are updated for CNC Console Release 1.9.1:

- Media Pack: Added Media pack details
- Compliance Matrix: Updated the compliance matrix information
- Common Services Load Lineup: Added Common Services Load Lineup details
- CNC Console Resolved Bugs: Added resolved bugs list
- Security Compliance Information: Added Security Compliance Information

Release 2.5.0 - F50692-05, December 2021

- Cloud Native Environment (CNE): Added a OCCNE feature

Release 2.5.0 - F50692-04, December 2021

- Compliance Matrix: Added 3GPP version numbers supported by SCP
- Compliance Matrix: Updated the compliance matrix information for CNC Policy and Binding Support Function
- Compliance Matrix: Updated the OSO version for UDR
- Common Services Load Lineup: Updated the ATS version

Release 2.5.0 - F50692-03, December 2021

- Compliance Matrix: Updated the SEPP and CNE compliance matrix information
- Common Services Load Lineup: Updated the ATS versions for NRF and NSSF
- CNE Customer Known Bugs: Added customer impact information

Release 2.5.0 - F50692-02, November 2021

- Common Services Load Lineup: Updated the ASM Configuration details

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 2.5.0.

Automated Testing Suite (ATS)

There are no new features or updates implemented in CNC 2.5.0 release.

Binding Support Function (BSF)

BSF 1.11.0 has been updated with the following enhancement:

- **Support for Diameter Error Codes**: This feature allows users to configure Diameter error codes for BSF by adding customized values for a defined condition. For any defined condition, give customized Error Message, Experimental Result Code, and Vendor Id as per your requirements. For more information about this feature, see the "Diameter Error Codes" section in *Oracle Communications Cloud Native Core Binding Support Function User Guide*.
- **Support for binding selection in session viewer using SUPI/GPSI only:** BSF is enhanced to support querying PCF bindings sessions using SUPI or GPSI on the Session Viewer page on CNC Console. For more information on how to query bindings sessions using CNC Console, see the "Session Viewer" section in Oracle Communications Cloud Native Core Binding Support Function User Guide. For information on available APIs for this feature, see *Oracle Communications Cloud Native Core Binding Support REST Specification Guide*.
- **Support for manual delete from Session Viewer:** BSF is enhanced to support manual deletion of PCF bindings sessions using SUPI or GPSI on the Session Viewer page on CNC Console. For more information on how to delete bindings sessions using CNC Console, see the "Session Viewer" section in Oracle Communications Cloud Native Core Binding Support Function User Guide. For information on available APIs for this feature, see *Oracle Communications Cloud Native Core Binding Support REST Specification Guide*.
- **Support for NF Sets and Binding Headers**: Oracle Communications Cloud Native Core Binding Support Function (BSF) supports the 3GPP NF Sets and Binding Headers in Model-B (Direct communication) and Model-C (Indirect communication). Using this feature, BSF can construct and send a binding header in the response messages to PCF for successful call processing. For more information on how to configure this feature using CNC Console, see the "Support for 3GPP NF Sets and Binding Headers" section in Oracle Communications Cloud Native Core Binding Support Function User Guide. For information on available APIs for this feature, see *Oracle Communications Cloud Native Core Binding Support REST Specification Guide*.
- **Support for Stale Session Handling in BSF**: With this feature, you can use Oracle Communications Cloud Native Core Binding Support Function to detect and remove stale PCF session bindings to avoid unlimited use of memory and other system resources. For more information on how to configure this feature using CNC Console, see the "Stale

Session Handling in BSF" section in Oracle Communications Cloud Native Core Binding Support Function User Guide. For information on available APIs for this feature, see *Oracle Communications Cloud Native Core Binding Support REST Specification Guide*.

Cloud Native Core Console (CNC Console)

Cloud Native Core Console (CNC Console) 1.9.x has been updated with the following enhancements:

CNC Console Release 1.9.2

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

CNC Console Release 1.9.1

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

CNC Console Release 1.9.0

Cloud Native Core Console (CNC Console) 1.9.0 has been updated with the following enhancements:

- **Secure Communication between CNCC Master and Agent**: CNC Console supports for mTLS configuration in Multi Cluster deployment to provide secure communication between CNC Console Manager and Agent. This feature is an extension of Multi-Cluster deployment. For more information, see *Oracle Communications Cloud Native Core Console Installation and Upgrade Guide*.
- **LDAPS Support**: CNC Console supports s Lightweight Directory Access Protocol Secure (LDAPS) to provide secure connection between LDAP server and CNCC IAM.

  For more information, see *Oracle Communications Cloud Native Core Console Installation and Upgrade Guide* and *Oracle Communications Cloud Native Core Console User Guide.*
- **Authorizing CNE Common Services and Audit/Security Logging Enhancements**

  This feature supports the additional functionalities as follows:

  - RBAC (Role Based Access Control) based authorization for CNE Common Services.
  - Audit Logs capture CNE Applications authorization events.
  - Security Logs capture CNE Applications requests and responses.
  - For more information, see *Oracle Communications Cloud Native Core Console Installation and Upgrade Guide* and *Oracle Communications Cloud Native Core Console User Guide*.

Cloud Native Environment (CNE)

Oracle Communications Cloud Native Environment (OCCNE) 1.10.0 has been updated with the following enhancements:

OCCNE

Virtual OCCNE on VMware Infrastructure: OCCNE supports vCNE installation on VMWare. This is a limited availability feature. For more information, see *Oracle Communications Cloud Native Environment Installation Guide*.

DBTier

DBTier Disaster Recovery automation: DBTier Disaster Recovery procedures are automated by introducing scripts that reduced the manual steps considerably as compared to the previous released Disaster Recovery procedures. For more information, see *Oracle Communications Cloud Native Core DBTier Disaster Recovery Guide*.

Cloud Native Core Policy (CNC Policy)

Oracle Communications Cloud Native Core Policy (CNC Policy) 1.15.x has been updated with the following enhancements:

CNC Policy 1.15.5

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

CNC Policy 1.15.4

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

CNC Policy 1.15.3

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

CNC Policy 1.15.1

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

CNC Policy 1.15.0

- **Support for Stale Session Handling in PDS**: CNC Policy supports the stale session handling support for Policy Data Service (PDS). For more information on how to configure this feature using CNC Console, see the "PDS Settings" section in Oracle Communications Cloud Native Core Policy User Guide. For information on available APIs for this feature, see Oracle Communications Cloud Native Core Policy REST Specification Guide.
- **Support for 3GPP NF Sets and Binding Headers**: CNC Policy supports the 3GPP NF Sets and Binding Headers in Direct communication and Indirect communication for AM, UE, PA, and Binding services. For more information on how to configure this feature using CNC Console, see the "NF Communication Profiles" section in Oracle Communications Cloud Native Core Policy User Guide. For information on available APIs for this feature, see Oracle Communications Cloud Native Core Policy REST Specification Guide.
- **Support for Pending Transactions on N7**: CNC Policy supports the Pending Transactions on N7 interface to handle race conditions in a deterministic manner. For more information on how to configure this feature using CNC Console, see the "Pending Transaction on N7" section in Oracle Communications Cloud Native Core Policy User Guide. For information on available APIs for this feature, see Oracle Communications Cloud Native Core Policy REST Specification Guide.

- **Support for Handling of Late Arrival Requests**: CNC Policy supports the detection and handling of late arrival requests on PCF to detect the response time for the components received in the headers from the Ingress Gateway. For more information on how to configure this feature using CNC Console, see the "Detection and Handling of Late Arrival Requests on PCF" section in Oracle Communications Cloud Native Core Policy User Guide.
- **Support for GET/DELETE based on SUPI or GPSI:** CNC Policy supports the retrieval and deletion of queried results for session type as ALL using SUPI or GPSI as the identifier. When the identifier is selected as GPSI for deletion, the associated diameter session, binding data, and user data is also deleted. For more information on how to configure this feature using CNC Console, see the "Session Viewer" section in Oracle Communications Cloud Native Core Policy User Guide. For information on available APIs for this feature, see Oracle Communications Cloud Native Core Policy REST Specification Guide.

Service Communication Proxy (SCP)

SCP Release 1.15.4

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

SCP Release 1.15.3

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

SCP Release 1.15.2

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

SCP Release 1.15.1

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

SCP Release 1.15.0

SCP 1.15.0 has been updated with the following enhancements:

- **Alternate Routing based on the DNS SRV Records:** This feature enables SCP to find an alternate Network Function (NF) service by performing the Domain Name System (DNS) Service Record (SRV) query with the DNS server. For more information about this feature, see *Oracle Communications Cloud Native Core Service Communication Proxy User Guide.*
- **Support for Multiple Signaling Service IPs:** Using multiple signaling IPs, SCP can expose multiple signaling service IPs from the same or a different network to all Network Functions (NFs) to accept 5G Service Based Interface (SBI) signaling traffic. This feature provides the flexibility to achieve maximum redundancy in the IP path. For more information about this feature, see *Oracle Communications Cloud Native Core Service Communication Proxy User Guide.*
- **Pod Overload Control**: This feature throttles only ingress 5G Service Based Interface (SBI) request messages based on CPU utilization of the scp-worker microservice pods. When CPU utilization of the scp-worker pod exceeds the configured threshold level, SCP responds with configured error codes or throttles the traffic based on the Pod Overload Action Policy configuration. For more information about this feature, see *Oracle Communications Cloud Native Core Service Communication Proxy User Guide.*

- **Enhanced 5G SBI Message Failure Handling**: This feature enables SCP to send information of all the routing attempts made on the producer NF. SCP has enhanced the server header format to include all the routing information while forwarding error responses with server header to consumer NFs. For more information about this feature, see *Oracle Communications Cloud Native Core Service Communication Proxy User Guide.*
- **SCP Performance and Capacity Improvements:** SCP can support 50K Transactions Per Second (TPS) per SCP instance.
- **SCP is Compliant with Kubernetes and ASM:** SCP is complaint with Kubernetes 1.20.x and Aspen Service Mesh (ASM) 1.9.x.

Security Edge Protection Proxy (SEPP)

Security Edge Protection Proxy (SEPP) 1.7.0 has been updated with the following enhancements:

- **Alternate Routing Across Remote SEPPs:** This feature enables the consumer SEPP to route the n32f traffic messages based on the availability of Primary, Secondary, or Tertiary producer SEPPs. For more information about the features, see *Oracle Communications Cloud Native Core Security Edge Protection Proxy User Guide*.

Network Repository Function (NRF)

OCNRF Release 1.15.2

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

OCNRF Release 1.15.1

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

OCNRF Release 1.15.0

OCNRF 1.15.0 has been updated with the following enhancement:

- **Support of CHF-GroupID**: Support for SLF based discovery lookup for CHF NfType. For more information about Subscriber Location Function (SLF) feature, see the "Subscriber Location Function" chapter in *Oracle Communications Cloud Native Core Network Repository Function User Guide*.
- **Support for Location Set based NfDiscovery**: OCNRF supports configuration of multiple location in Preferred Locality triplet. NfDiscovery service checks the locationSet configured under Extended Preferred Locality Priority attributes locationSets and performs discovery of a producer NF type. For more information about location set feature, see the "Extended Preferred Locality Priority Handling" chapter in *Oracle Communications Cloud Native Core Network Repository Function User Guide*.
- **Support for 3GPP based errorCause attribute in ProblemDetails for NRF generated error responses**: OCNRF supports for errorCause attribute as per 3GPP 29.500, R17 for all the service operations. For more information about errorCause, see *Oracle Communications Cloud Native Core Network Repository Function REST Specification Guide*.
- **Support for configurable ephemeral-storage request and limit during NRF installation/upgrade**: OCNRF supports configuration of ephemeral containers for temporary storage of data of your instances. The Pods use ephemeral local storage for

scratch space, caching, and logs. For more information about ephemeral-storage resource requirements, see the "Resource Requirement" section in *Oracle Communications Cloud Native Core Network Repository Function Installation and Upgrade Guide*.

Network Slice Selection Function (NSSF)

OCNSSF 1.8.0 has been updated with the following enhancements:

- **Support for Optimized Network Slice Selection Assistance Information (ONSSAI):** ONSSAI is one of the 3GPP Specification 29.531 supported optional features that OCNSSF negotiates using Feature Negotiation. When this feature is supported by AMF and NSSF, it allows NSSAI Availability data to be signaled per list or per range(s) of a Tracking Area Identifier (TAI).
- **Support for Tracking Area Identifier (TAI) Range**: ONSSAI also extends the support for TAI ranges in OCNSSF. This feature reduces the memory consumption at NSSF by eliminating the need for storage of redundant data. It reduces the size of supported NSSAI towards NF Service Consumer, which in turn improves the overall network throughput by decreasing the network latency.

For more information about the support for ONSSAI and TAI range in OCNSSF, see *Oracle Communications Cloud Native Core Network Slice Selection Function User Guide*.

Unified Data Repository (UDR)

UDR Release 1.15.2

There are no new enhancements in UDR Release 1.15.2.

UDR Release 1.15.1

There are no new enhancements in UDR Release 1.15.1.

UDR Release 1.15.0

UDR 1.15.0 has been updated with the following enhancements:

- **Support for SBI message priority for Overload Control:** UDR supports discard of messages during Overload scenarios based on SBI message priority. For more information, see the **Overload Handling** section in *Oracle Communications Cloud Native Core Unified Data Repository User Guide*.
- **Support of 3GPP SBI Co-relation header:** UDR supports 3GPP SBI Co-relation header in the messages. For more information, see the **3gpp-Sbi-Correlation-Info Header** section in *Oracle Communications Cloud Native Core Unified Data Repository User Guide*.
- **Support of Ingress Rate Limiting:** UDR supports rate limiting of Ingress traffic per route. For more information, see the **Rate Limiting** section in *Oracle Communications Cloud Native Core Unified Data Repository User Guide*.
- **Support of Pod disruption budget:** UDR supports pod disruption budget to enable availability of minimum replicas for microservices. For more information, see the **Debugging PodDisruptionBudget Related Issues** section in *Oracle Communications Cloud Native Core Unified Data Repository Troubleshooting Guide*.

- **UDM APIs enhancements:** UDM subscription APIs are enhanced to support creation of subscriptions with sdmSubscritpions. For more information, see the **Configuring User Parameters** section in *Oracle Communications Cloud Native Core Unified Data Repository Installation and Upgrade Guide*.
- **CHFGrpID support:** SLF supports provisioning of CHFGrpId, which are not mapped under SLFGroup name. For more information, see the **Configuring User Parameters** section in *Oracle Communications Cloud Native Core Unified Data Repository Installation and Upgrade Guide*.
- **Import and Export of Provisioning Gateway Configuration Data:** UDR Provisioning Gateway supports import and export of the configuration data from the REST APIs. For more information, see *Oracle Communications Cloud Native Core Unified Data Repository Provisioning Gateway Interface Specification Guide*.
- **UDR custom entity enhancements:** UDR is enhanced to add custom fields under subscriber profile. For more information, see the Supported SOAP or XML Request Operations for Custom Entities section in *Oracle Communications Cloud Native Core Provisioning Gateway Interface Specification Guide.*
- **Mano 21.03 compliance:** UDR CSAR has been updated with Mano 21.03 compliance.

3
Media and Documentation

Media Pack

This section lists the media package for Cloud Native Core 2.5.0. To download the media package, refer to 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 Cloud Native Core 2.5.0

Description	Versions	ATS Package Available (Y/N)	Upgrade Supported
Oracle Communications Cloud Native Core Binding Support Function (BSF)	1.11.0	Y	BSF 1.11.0 supports fresh installation and upgrade from 1.10.x. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Binding Support Function Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Console (CNCC)	1.9.2	N	CNC Console 1.9.2 supports fresh installation and upgrade from: • 1.8.x to 1.9.2. • 1.9.x to 1.9.2. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Console Installation and Upgrade Guide*.

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.5.0

Description	Versions	ATS Package Available (Y/N)	Upgrade Supported
Oracle Communications Cloud Native Core Console (CNCC)	1.9.1	N	CNC Console 1.9.1 supports fresh installation and upgrade from: • 1.8.x to 1.9.1. • 1.9.0 to 1.9.1. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Console Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Console (CNCC)	1.9.0	N	CNC Console 1.9.0 supports fresh installation and upgrade from 1.8.x to 1.9.0. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Console Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Cloud Native Environment (CNE)	1.10.3	N	CNE 1.10.3 supports fresh installation. The upgrade from CNE 1.9.x, 1.10.x to 1.10.3 is supported. For more information on installation or upgrading, see *Oracle Communications Cloud Native Environment Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Cloud Native Environment (CNE)	1.10.2	N	CNE 1.10.2 supports fresh installation. The upgrade from CNE 1.9.x, 1.10.x to 1.10.2 is supported. For more information on installation or upgrading, see *Oracle Communications Cloud Native Environment Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Cloud Native Environment (CNE)	1.10.1	N	CNE 1.10.1 supports fresh installation. The upgrade from CNE 1.9.1 to 1.10.1 is supported. For more information on installation or upgrading, see *Oracle Communications Cloud Native Environment Installation and Upgrade Guide*.

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.5.0

Description	Versions	ATS Package Available (Y/N)	Upgrade Supported
Oracle Communications Cloud Native Core Cloud Native Environment (CNE)	1.10.0	N	CNE 1.10.0 supports fresh installation. The upgrade from CNE 1.9.1 to 1.10.0 is supported. For more information on installation or upgrading, see *Oracle Communications Cloud Native Environment Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core DBTier	1.10.3	N	DBTier 1.10.3 supports fresh installation. The upgrade from DBTier 1.8.x, 1.9.x, 1.10.x to 1.10.3 is supported. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core DBTier Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core DBTier	1.10.2	N	DBTier 1.10.2 supports fresh installation. The upgrade from DBTier 1.8.x, 1.9.x, 1.10.x to 1.10.2 is supported. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core DBTier Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core DBTier	1.10.1	N	DBTier 1.10.1 supports fresh installation. The upgrade from DBTier 1.8.x, 1.9.x, 1.10.x to 1.10.1 is supported. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core DBTier Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Policy (CNC Policy)	1.15.5	Y	CNC Policy 1.15.5 supports fresh installation and upgrade from 1.14.x and 1.15.x. For more information on installing or upgrading CNC Policy, see *Oracle Communications Cloud Native Core Policy Installation and Upgrade Guide*.

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.5.0

Description	Versions	ATS Package Available (Y/N)	Upgrade Supported
Oracle Communications Cloud Native Core Policy (CNC Policy)	1.15.4	Y	CNC Policy 1.15.4 supports fresh installation and upgrade from 1.14.x and 1.15.x. For more information on installing or upgrading CNC Policy, see *Oracle Communications Cloud Native Core Policy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Policy (CNC Policy)	1.15.3	Y	CNC Policy 1.15.3 supports fresh installation and upgrade from 1.14.x and 1.15.x. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Policy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Policy (CNC Policy)	1.15.1	Y	CNC Policy 1.15.1 supports fresh installation and upgrade from 1.14.x and 1.15.0. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Policy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Policy (CNC Policy)	1.15.0	Y	CNC Policy 1.15.0 supports fresh installation and upgrade from 1.14.x. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Policy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Network Exposure Function (NEF)	1.3.0	N	NA
Oracle Communications Cloud Native Core Network Repository Function (NRF)	1.15.2	Y	OCNRF 1.15.2 supports fresh installation and upgrade from 1.14.x, 1.15.x to 1.15.2. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Network Repository Function Installation and Upgrade Guide*.

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.5.0

Description	Versions	ATS Package Available (Y/N)	Upgrade Supported
Oracle Communications Cloud Native Core Network Repository Function (NRF)	1.15.1	Y	OCNRF 1.15.1 supports fresh installation and upgrade from 1.14.x, 1.15.0 to 1.15.1. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Network Repository Function Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Network Repository Function (NRF)	1.15.0	Y	OCNRF 1.15.0 supports fresh installation and upgrade from 1.14.x to 1.15.0. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Network Repository Function Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Network Slice Selection Function (NSSF)	1.8.0	Y	OCNSSF 1.8.0 supports only fresh installation. For more information on installation, see *Oracle Communications Cloud Native Core Network Slice Selection Function Installation Guide*.
Oracle Communications Cloud Native Core Service Communications Proxy (SCP)	1.15.4	Y	SCP 1.15.4 supports a fresh installation and upgrade from: • 1.12.x to 1.15.4 • 1.14.x to 1.15.4 • 1.15.x to 1.15.4 For more information about installation and upgrade, see *Oracle Communications Cloud Native Core Service Communication Proxy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Service Communications Proxy (SCP)	1.15.3	Y	SCP 1.15.3 supports a fresh installation and upgrade from: • 1.12.x to 1.15.3 • 1.14.x to 1.15.3 • 1.15.x to 1.15.3 For more information about installation and upgrade, see *Oracle Communications Cloud Native Core Service Communication Proxy Installation and Upgrade Guide*.

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.5.0

Description	Versions	ATS Package Available (Y/N)	Upgrade Supported
Oracle Communications Cloud Native Core Service Communications Proxy (SCP)	1.15.2	Y	SCP 1.15.2 supports a fresh installation and upgrade from: • 1.12.x to 1.15.2. • 1.14.x to 1.15.2. For more information about installation and upgrade, see *Oracle Communications Cloud Native Core Service Communication Proxy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Service Communications Proxy (SCP)	1.15.1	Y	SCP 1.15.1 supports a fresh installation and upgrade from: • 1.12.x to 1.15.1. • 1.14.x to 1.15.1. For more information about installation and upgrade, see *Oracle Communications Cloud Native Core Service Communication Proxy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Service Communications Proxy (SCP)	1.15.0	Y	SCP 1.15.0 supports a fresh installation and upgrade from: • 1.12.x to 1.15.0. • 1.14.x to 1.15.0. For more information about installation and upgrade, see *Oracle Communications Cloud Native Core Service Communication Proxy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Security Edge Protection Proxy (SEPP)	1.7.1	Y	SEPP 1.7.1 supports fresh installation. For more information on installation, see *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation Guide*.
Oracle Communications Cloud Native Core Security Edge Protection Proxy (SEPP)	1.7.0	Y	SEPP 1.7.0 supports fresh installation. For more information on installation, see *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation Guide*.

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.5.0

Description	Versions	ATS Package Available (Y/N)	Upgrade Supported
Oracle Communications Cloud Native Core Unified Data Repository (UDR)	1.15.2	Y	OCUDR 1.15.2 supports fresh installation and upgrade from 1.14.x or 1.15.0 to 1.15.2. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core United Data Repository Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Unified Data Repository (UDR)	1.15.1	Y	OCUDR 1.15.1 supports fresh installation and upgrade from 1.14.x and 1.15.0. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core United Data Repository Installation and Upgrade Guide*. **Note**: Upgrade from 1.14.x to 1.15.1 is supported. Due to rollback issues from 1.15.1 to 1.15.0, avoid upgrading from 1.15.0 to 1.15.1.
Oracle Communications Cloud Native Core Unified Data Repository (UDR)	1.15.0	Y	OCUDR 1.15.0 supports fresh installation and upgrade from 1.14.x to 1.15.0. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core United Data Repository Installation and Upgrade Guide*.

Compliance Matrix

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

Table 3-2 Compliance Matrix

CNC NF	NF Versions	OCCNE	cnDBTier	CNC Console	OSO	Kubernetes	3GPP
BSF	1.11.0	• 1.10.x • 1.9.x • 1.8.x	• 1.10.x • 1.9.x • 1.8.x	1.9.x	1.6.x	• 1.20.x • 1.19.x • 1.18.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.514 • 3GPP TS 29.521 • 3GPP TS 29.214
CNC Console	1.9.2	• 1.10.x • 1.9.x • 1.8.x	• 1.10.x • 1.9.x • 1.8.x	NA	1.6.x	• 1.20.x • 1.19.x • 1.18.x	NA
CNC Console	1.9.1	• 1.10.x • 1.9.x • 1.8.x	• 1.10.x • 1.9.x • 1.8.x	NA	1.6.x	• 1.20.x • 1.19.x • 1.18.x	NA
CNC Console	1.9.0	• 1.10.x • 1.9.x • 1.8.x	• 1.10.x • 1.9.x • 1.8.x	NA	1.6.x	• 1.20.x • 1.19.x • 1.18.x	NA
CNC Policy	1.15.5	• 1.10.x • 1.9.x • 1.8.x	• 1.10.x • 1.9.x • 1.8.x	1.9.x	1.6.x	• 1.20.x • 1.19.x • 1.18.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.507 • 3GPP TS 29.512 • 3GPP TS 29.513 • 3GPP TS 29.514 • 3GPP TS 29.519 • 3GPP TS 29.521 • 3GPP TS 29.525 • 3GPP TS 29.594 • 3GPP TS 29.214

Table 3-2 (Cont.) Compliance Matrix

CNC NF	NF Versions	OCCNE	cnDBTier	CNC Console	OSO	Kubernetes	3GPP
CNC Policy	1.15.4	• 1.10.x • 1.9.x • 1.8.x	• 1.10.x • 1.9.x • 1.8.x	1.9.x	1.6.x	• 1.20.x • 1.19.x • 1.18.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.507 • 3GPP TS 29.512 • 3GPP TS 29.513 • 3GPP TS 29.514 • 3GPP TS 29.519 • 3GPP TS 29.521 • 3GPP TS 29.525 • 3GPP TS 29.594 • 3GPP TS 29.214
CNC Policy	1.15.3	• 1.10.x • 1.9.x • 1.8.x	• 1.10.x • 1.9.x • 1.8.x	1.9.x	1.6.x	• 1.20.x • 1.19.x • 1.18.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.507 • 3GPP TS 29.512 • 3GPP TS 29.513 • 3GPP TS 29.514 • 3GPP TS 29.519 • 3GPP TS 29.521 • 3GPP TS 29.525 • 3GPP TS 29.594 • 3GPP TS 29.214
CNC Policy	1.15.1	• 1.10.x • 1.9.x • 1.8.x	• 1.10.x • 1.9.x • 1.8.x	1.9.x	1.6.x	• 1.20.x • 1.19.x • 1.18.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.507 • 3GPP TS 29.512 • 3GPP TS 29.513 • 3GPP TS 29.514 • 3GPP TS 29.519 • 3GPP TS 29.521 • 3GPP TS 29.525 • 3GPP TS 29.594 • 3GPP TS 29.214

Table 3-2 (Cont.) Compliance Matrix

CNC NF	NF Versions	OCCNE	cnDBTier	CNC Console	OSO	Kubernetes	3GPP
CNC Policy	1.15.0	• 1.10.x • 1.9.x • 1.8.x	• 1.10.x • 1.9.x • 1.8.x	1.9.x	1.6.x	• 1.20.x • 1.19.x • 1.18.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.507 • 3GPP TS 29.512 • 3GPP TS 29.513 • 3GPP TS 29.514 • 3GPP TS 29.519 • 3GPP TS 29.521 • 3GPP TS 29.525 • 3GPP TS 29.594 • 3GPP TS 29.214
OCCNE	1.10.0	NA	• 1.10.x • 1.9.x • 1.8.x	NA	1.10.0, 1.6.x	1.20.x	NA
NRF	1.15.2	• 1.10.x • 1.9.x • 1.8.x	• 1.10.x • 1.9.x • 1.8.x	1.9.x	1.6.x	• 1.20.x • 1.19.x • 1.18.x	• 3GPP TS 29.510 v15.5 • 3GPP TS 29.510 v16.3.0 • 3GPP TS 29.510 v16.7
NRF	1.15.1	• 1.10.x • 1.9.x • 1.8.x	• 1.10.x • 1.9.x • 1.8.x	1.9.x	1.6.x	• 1.20.x • 1.19.x • 1.18.x	• 3GPP TS 29.510 v15.5 • 3GPP TS 29.510 v16.3.0 • 3GPP TS 29.510 v16.7
NRF	1.15.0	• 1.10.x • 1.9.x • 1.8.x	• 1.10.x • 1.9.x • 1.8.x	1.9.x	1.6.x	• 1.20.x • 1.19.x • 1.18.x	• 3GPP TS 29.510 v15.5 • 3GPP TS 29.510 v16.3.0 • 3GPP TS 29.510 v16.7
NSSF	1.8.0	• 1.10.x • 1.9.x • 1.8.x	• 1.10.x • 1.9.x • 1.8.x	NA	1.6.x	• 1.20.x • 1.19.x • 1.18.x	• 3GPP TS 29.510 v15.5

Table 3-2 (Cont.) Compliance Matrix

CNC NF	NF Versions	OCCNE	cnDBTier	CNC Console	OSO	Kubernetes	3GPP
SCP	1.15.4	• 1.10.x • 1.9.x • 1.8.x	• 1.10.x • 1.9.x • 1.8.x	1.9.x	1.6.x	• 1.20.x • 1.19.x • 1.18.x	• 3GPP TS 23.501 v16.7.0 • 3GPP TS 29.500 v16.6.0 • 3GPP TS 29.501 v16.5.0 • 3GPP TS 29.571 v16.7.0
SCP	1.15.3	• 1.10.x • 1.9.x • 1.8.x	• 1.10.x • 1.9.x • 1.8.x	1.9.x	1.6.x	• 1.20.x • 1.19.x • 1.18.x	• 3GPP TS 23.501 v16.7.0 • 3GPP TS 29.500 v16.6.0 • 3GPP TS 29.501 v16.5.0 • 3GPP TS 29.571 v16.7.0
SCP	1.15.2	• 1.10.x • 1.9.x • 1.8.x	• 1.10.x • 1.9.x • 1.8.x	1.9.x	1.6.x	• 1.20.x • 1.19.x • 1.18.x	• 3GPP TS 23.501 v16.7.0 • 3GPP TS 29.500 v16.6.0 • 3GPP TS 29.501 v16.5.0 • 3GPP TS 29.571 v16.7.0
SCP	1.15.1	• 1.10.x • 1.9.x • 1.8.x	• 1.10.x • 1.9.x • 1.8.x	1.9.x	1.6.x	• 1.20.x • 1.19.x • 1.18.x	• 3GPP TS 23.501 v16.7.0 • 3GPP TS 29.500 v16.6.0 • 3GPP TS 29.501 v16.5.0 • 3GPP TS 29.571 v16.7.0
SCP	1.15.0	• 1.10.x • 1.9.x • 1.8.x	• 1.10.x • 1.9.x • 1.8.x	1.9.x	1.6.x	• 1.20.x • 1.19.x • 1.18.x	• 3GPP TS 23.501 v16.7.0 • 3GPP TS 29.500 v16.6.0 • 3GPP TS 29.501 v16.5.0 • 3GPP TS 29.571 v16.7.0
SEPP	1.7.1	• 1.10.x • 1.9.x • 1.8.x	• 1.10.x • 1.9.x • 1.8.x	1.9.x	NA	• 1.20.x • 1.19.x • 1.18.x	• 3GPP TS 29.573 v 16.3.0

Table 3-2 (Cont.) Compliance Matrix

CNC NF	NF Versions	OCCNE	cnDBTier	CNC Console	OSO	Kubernetes	3GPP
SEPP	1.7.0	• 1.10.x • 1.9.x • 1.8.x	• 1.10.x • 1.9.x • 1.8.x	1.9.x	NA	• 1.20.x • 1.19.x • 1.18.x	• 3GPP TS 29.573 v 16.3.0
UDR	1.15.2	• 1.10.x • 1.9.x • 1.8.x	• 1.10.x • 1.9.x • 1.8.x	1.9.x	1.10.x, 1.6.x	• 1.20.x • 1.19.x • 1.18.x	NA
UDR	1.15.1	• 1.10.x • 1.9.x • 1.8.x	• 1.10.x • 1.9.x • 1.8.x	1.9.x	1.10.0, 1.6.x	• 1.20.x • 1.19.x • 1.18.x	NA
UDR	1.15.0	• 1.10.x • 1.9.x • 1.8.x	• 1.10.x • 1.9.x • 1.8.x	1.9.x	1.10.0, 1.6.x	• 1.20.x • 1.19.x • 1.18.x	NA

Common Services Load Lineup

This section provides information about common services and ATS for the specific NF versions in Cloud Native Core Release 2.5.0.

Table 3-3 Common Services Load Lineup for Network Functions

CNC NF	NF Versions	Alternate Route Svc	App-Info	ASM Configuration	ATS Framework	Config-Server	Debug-tool	Egress Gateway	Ingress Gateway	Helm Test	NRF-Client	Perf-Info
BSF	1.11.0	1.6.4	1.15.0	1.14.0 (Retagged as 1.0.0)	1.9.2	1.15.0	1.2.0	1.15.3	1.15.3	1.15.1	1.9.1	1.15.0
CNC Console	1.9.2	NA	NA	NA	NA	NA	1.2.1	NA	1.15.9	1.15.5	NA	NA
CNC Console	1.9.1	NA	NA	NA	NA	NA	1.2.0	NA	1.15.7	1.15.3	NA	NA
CNC Console	1.9.0	NA	NA	NA	NA	NA	1.2.0	NA	1.15.5	1.15.1	NA	NA

Table 3-3 (Cont.) Common Services Load Lineup for Network Functions

CNC NF	NF Versions	Alternate Route Svc	App-Info	ASM Configuration	ATS Framework	Config-Server	Debug-tool	Egress Gateway	Ingress Gateway	Helm Test	NRF-Client	Perf-Info
CNC Policy	1.15.5	1.6.8	1.15.4	1.14.0 (Retagged as 1.0.0)	1.9.2	1.15.4	1.2.1	1.15.9	1.15.9	1.15.5	1.9.6	1.15.4
CNC Policy	1.15.4	1.6.8	1.15.4	1.14.0 (Retagged as 1.0.0)	1.9.2	1.15.4	1.2.1	1.15.9	1.15.9	1.15.5	1.9.6	1.15.4
CNC Policy	1.15.3	1.6.6	1.15.3	1.14.0 (Retagged as 1.0.0)	1.9.2	1.15.1	1.2.0	1.15.7	1.15.7	1.15.3	1.9.5	1.15.1
CNC Policy	1.15.1	1.6.6	1.15.1	1.14.0 (Retagged as 1.0.0)	1.9.2	1.15.1	1.2.0	1.15.7	1.15.7	1.15.3	1.9.3	1.15.1
CNC Policy	1.15.0	1.6.4	1.15.0	1.14.0 (Retagged as 1.0.0)	1.9.2	1.15.0	1.2.0	1.15.4	1.15.4	1.15.1	1.9.1	1.15.0
NRF	1.15.2	NA	1.15.4	1.12.0 (Retagged as 1.1.0)	1.9.1	NA	1.2.1	1.15.9	1.15.9	1.15.5	NA	NA
NRF	1.15.1	NA	1.15.2	1.12.0 (Retagged as 1.1.0)	1.9.0	NA	1.2.0	1.15.8	1.15.8	1.15.4	NA	NA
NRF	1.15.0	NA	1.15.0	1.12.0 (Retagged as 1.1.0)	1.9.0	NA	1.2.0	1.15.4	1.15.4	1.15.1	NA	NA
NSSF	1.8.0	NA	1.15.0	NA	1.9.2	1.15.0	1.2.0	1.15.4	1.15.4	1.15.0	1.9.1	1.15.0
SCP	1.15.4	NA	NA	NA	1.9.4	NA	1.2.0	NA	NA	1.15.5	NA	NA
SCP	1.15.3	NA	NA	NA	1.9.4	NA	1.2.0	NA	NA	1.15.5	NA	NA
SCP	1.15.2	NA	NA	NA	1.9.0	NA	1.2.0	NA	NA	1.15.1	NA	NA
SCP	1.15.1	NA	NA	NA	1.9.0	NA	1.2.0	NA	NA	1.15.1	NA	NA
SCP	1.15.0	NA	NA	NA	1.9.0	NA	1.2.0	NA	NA	1.15.1	NA	NA
SEPP	1.7.1	NA	1.15.1	NA	1.9.2	1.15.1	NA	1.15.7	1.15.7	NA	1.9.3	1.15.1
SEPP	1.7.0	NA	1.15.0	NA	1.9.2	1.15.0	NA	1.15.5	1.15.5	NA	1.9.1	1.15.0
UDR	1.15.2	1.6.8	1.15.4	1.14.0	1.9.4	1.15.4	1.2.0	1.15.9	1.15.9	1.15.5	1.9.6	1.15.4
UDR	1.15.1	1.6.7	1.15.2	1.14.0	1.9.2	1.15.2	1.2.0	1.15.8	1.15.8	1.15.4	1.9.4	1.15.2
UDR	1.15.0	1.6.4	1.15.0	1.14.0	1.9.2	1.15.0	1.2.0	1.15.4	1.15.4	1.15.1	1.9.1	1.15.0

Security Certification Declaration

The following table lists the security tests and the corresponding dates of compliance for each network function.

Table 3-4 Security Certification Declaration

CNC NF	NF Versions	Systems test on functional and security features	Regression testing on security configuration	Vulnerability testing	Fuzz testing on external interfaces
BSF	1.11.0	N/A (no new security feature)	November 19, 2021	November 19, 2021	November 19, 2021
CNC Console	1.9.2	NA	November 11, 2021	April 13, 2022	November 11, 2021
CNC Console	1.9.1	NA	November 11, 2021	December 22, 2021	November 11, 2021
CNC Console	1.9.0	NA	November 11, 2021	November 11, 2021	November 11, 2021
CNC Policy	1.15.5	June 3, 2022	June 3, 2022	June 10, 2022	May 25, 2022
CNC Policy	1.15.4	N/A (no new security feature)	November 19, 2021	April 11, 2022	November 19, 2021
CNC Policy	1.15.0	N/A (no new security feature)	November 19, 2021	November 19, 2021	November 19, 2021
NRF	1.15.2	N/A (no new security feature)	April 22, 2022	April 22, 2022	November 11, 2021
NRF	1.15.0	N/A (no new security feature)	November 17, 2021	November 17, 2021	November 11, 2021
NSSF	1.8.0	November 17, 2021	NA	November 17, 2021	November 17, 2021
SCP	1.15.4	NA	NA	April 19, 2022	November 15, 2021
SCP	1.15.3	NA	NA	April 19, 2022	November 15, 2021
SCP	1.15.2	NA	NA	November 15, 2021	November 15, 2021
SCP	1.15.1	NA	NA	November 15, 2021	November 15, 2021
SCP	1.15.0	NA	NA	November 15, 2021	November 15, 2021
SEPP	1.7.1	NA	NA	December 21,2021	November 10, 2021
SEPP	1.7.0	NA	NA	October 10, 2021	November 10, 2021

Table 3-4 (Cont.) Security Certification Declaration

CNC NF	NF Versions	Systems test on functional and security features	Regression testing on security configuration	Vulnerability testing	Fuzz testing on external interfaces
UDR	1.15.2	NA (no new security features)	April 20, 2022	April 20, 2022	November 15, 2021
UDR	1.15.1	NA (no new security features)	November 15, 2021	November 15, 2021	November 15, 2021
UDR	1.15.0	NA (no new security features)	November 15, 2021	November 15, 2021	November 15, 2021

Documentation Pack

All documents for Cloud Native Core (CNC) 2.5.0 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.

4
Resolved and Known Bugs

This chapter lists the resolved and known bugs for Cloud Native Core release 2.5.0.

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

Severity Definitions

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

Severity 1

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

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

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

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

Severity 2

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

Severity 3

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

Severity 4

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

Resolved Bug List

The following Resolved Bugs tables list the bugs that are resolved in Cloud Native Release 2.5.0.

BSF Resolved Bugs

Table 4-1 BSF 1.11.0 Resolved Bugs

Bug Number	Title	Severity	Found in Release
33595031	Update VNFD in all CSAR to not point to SM Helm	3	1.10.0
33595019	servicemesh RequestAuthentication template labelselector key hardcoded as "app" template changes	3	1.10.0
33262764	Ephemeral storage requirement for BSF	3	1.9.0

CNC Console Resolved Bugs

CNC Console Release 1.9.2

There are no resolved bugs in CNC Console Release 1.9.2.

CNC Console Release 1.9.1

Table 4-2 CNC Console 1.9.1 Resolved Bugs

Bug Number	Title	Severity	Found in Release
33640184	CNCC 1.9.0 cncc-iam-kc CrashLoopBackOff w/ keycloak-add-user.json (Permission denied)	3	1.9.0

Table 4-2 (Cont.) CNC Console 1.9.1 Resolved Bugs

Bug Number	Title	Severity	Found in Release
33587376	Console GUI - Appending edit in service page heading When the user keeps edit operation in an incomplete state and moves to a new screen, the new screen heading is appending with the edit.	4	1.9.0

CNC Console Release 1.9.0

There are no resolved bugs in CNC Console Release 1.9.0.

CNE Resolved Bugs

OCCNE Resolved Bugs

OCCNE 1.10.3 Resolved Bugs

There are no resolved bugs for this release.

Table 4-3 OCCNE 1.10.2 Resolved Bugs

Bug Number	Title	Severity	Found in Release
33983820	LBVM Switchover fails when active lbvm physical host is down in openstack.	4125	1.10.0

Table 4-4 OCCNE 1.10.1 Resolved Bugs

Bug Number	Title	Severity	Found in Release
33734043	LBVM Switchover for ports failing	3	1.10.0
33734043	LBVM Switchover port remove failing	3	1.10.0
33831653	LB-Controller removes LBVM IP when a pod is restarted	3	1.10.0
33734036	LBVM: Duplicate svc names causing LBVMs to go into FAILED state	3	1.10.0
33564120	LBVM: createFailedLbvm does not update haproxy template files	3	1.9.1
33564120	LBVM: addPeerAddrPool.py does not update haproxy template files	3	1.9.1
33733703	Fix PUSHGATEWAY alert rules to use correct reference of pushgateway service name	3	1.9.1, 1.10.0
33749146	LBVM: lb_controller lb_monitor.log growing excessively	3	1.9.1

Table 4-4 (Cont.) OCCNE 1.10.1 Resolved Bugs

Bug Number	Title	Severity	Found in Release
33749273	Special Character in openstack password results in openstack commands failing within lb controller	3	1.9.1
33755419	Deploy.sh trying to set Openstack port post terraform apply from the hostfile input	3	1.9.1

Table 4-5 OCCNE 1.10.0 Resolved Bugs

Bug Number	Title	Severity	Found in Release
33550838	Error using run_cmd causes lb_monitor to crash	2	1.9.0
33550811	cncc_enabled=false in hosts.ini causes pipeline.sh fail with NotLoadBalancer	3	1.9.1
33550858	LB-Controller switchover fails in VCD 10.1.2	3	1.9.0
33550875	chronyd syncing to central repo instead of NTP server specified as an installation input	3	1.9.1

DBTier Resolved Bugs

Table 4-6 DBTier 1.10.3 Resolved Bugs

Bug Number	Title	Severity	Found in Release
34084015	Update Spring boot to 2.6.6 for DB Tier K8s applications	2	1.10.2
34084849	Use ASM acceptable port name in the cnDBTier helm chart	2	22.1.0
34094355	Correction in updateclusterdetails.sh dr-procedure script	2	1.10.1
34108029	Update Spring boot to 2.6.7 for DB Tier K8s applications	2	1.10.2
34084036	Mysql hosts are frequently getting blocked	3	1.10.1

Table 4-7 DBTier 1.10.2 Resolved Bugs

Bug Number	Title	Severity	Found in Release
33837602	Fixing issues reported in Dish PI-D DB Tier security scan	2	1.10.0
33923166	Remove auto mounting of default service account	2	1.9.0

Table 4-7 (Cont.) DBTier 1.10.2 Resolved Bugs

Bug Number	Title	Severity	Found in Release
33713253	Upgrade Tomcat to 9.0.58 for DB Tier K8s applications	2	1.10.1
33978772	Increase ephemeral storage size for different cnDBTier containers	3	1.10.0
33964190	cnDBTier 1.10.1 DR restore_replication.sh doesn't specify which SVC_IP to ente	3	1.10.1
33964215	DBTier DR procedure is missing the cleaning of mysql.ndb_apply_status	3	1.10.1
33959954	DBTier 1.10.1 dr-procedure scripts use pod's default container on some "exec" and "cp" cmds	4	22.1.0

Table 4-8 DBTier 1.10.1 Resolved Bugs

Bug Number	Title	Severity	Found in Release
33713253	Update Spring boot to 2.6.2 for DBTier K8s applications	2	1.10.0
33684194	Remove max 63 character length constraint from the cnDBTier FQDN name configurations	3	1.10.0
33701019	Make the Prometheus alerts rule loading user configurable in cnDBTier	3	1.10.0
33725640	Failed to find backup 2147483647 in path /var/ndbbackup/dbback/BACKUP/BACKUP-2201041013	3	1.10.0
33728580	Steps to transfer backup compress file from workcluster to restorecluster missing in Restore DB from Backup with ndb_restore	3	1.10.0

Table 4-9 DBTier 1.10.0 Resolved Bugs

Bug Number	Title	Severity	Found in Release
33551223	restart_cndbtier_cluster.sh fails if cnDBTier installed with the pod prefixes	3	1.9.2

CNC Policy Resolved Bugs

Table 4-10 CNC Policy 1.15.5 Resolved Bugs

Bug Number	Title	Severity	Found In Release
34317062	SOAP notification schema, Replication failure with Binding service	3	1.15.4

Table 4-11 CNC Policy 1.15.4 Resolved Bugs

Bug Number	Title	Severity	Found In Release
34084838	Policyds not sending CHF un-subscribe to chf-connector when one subscriber have multiple dnn sessions	3	1.15.0
34084869	5063 error codes for some of AAA messages	3	1.15.0

Table 4-12 CNC Policy ATS 1.15.4 Resolved Bugs

Bug Number	Title	Severity	Found In Release
34084906	ATS shall wait before SNR message	3	1.15.0

Table 4-13 CNC Policy 1.15.3 Resolved Bugs

Bug Number	Title	Severity	Found In Release
33843822	PCF nfServiceStatus Suspended while NRF is Registered	3	1.15.1
33843782	nchf-spendinglimitcontrol content type wrong	3	1.15.1

Table 4-14 CNC Policy 1.15.1 Resolved Bugs

Bug Number	Title	Severity	Found In Release
33691565	PCF does not cleanup PDS records when CHF responds with 404 not found	2	1.14.0
33683221	PCF 1.15.0 CSAR includes ocdebug-tools:1.2.0.tar but helm chart includes 1.0.0	3	1.15.0
33683226	PDS receives smPolicyData in UDR notification but doesn't pass "smPolicyAttrs" to smService	3	1.14.0
33670406	PCF(1.15.0)/ ATS(1.15.0):Internal: Issue in Policy Evaluation	3	1.15.0

Table 4-14 (Cont.) CNC Policy 1.15.1 Resolved Bugs

Bug Number	Title	Severity	Found In Release
33651230	BT: Referenced Match List changes in activer Policy ,when any change done in Matchlist	3	1.14.0
33670282	PCF1.14- Policy Export with dependencies failing in exporting custom yaml schemas	3	1.14.0
33670288	Data corruption for "Yaml Schema" when imported using bulk import	3	1.14.0
33388403	Policy Table sort by blockly intermittently fails to load correctly when switching policy projects	3	1.14.0
33706478	Data Type change required from "bigint" to "bigint unsigned" in binding service tables	3	1.15.0

Table 4-15 CNC Policy 1.15.0 Resolved Bugs

Bug Number	Title	Severity	Found In Release
33593798	Policy engine stops after evaluation of Object expression	2	1.15.0
33594763	PRE pod fails to come up after upgrade when any policy has issues	2	1.15.0
33542427	PCF sending NULL smPolicyDecision in audit messages	3	1.11.4
33424744	Bulk Export and Policy Export results in similar file name	3	1.14.0
33459271	PCF: Timer profile export fails with Bulk Export Operation due to incorrect data getting saved in the db from cm GUI	3	1.14.0
33593646	Offline AVP not set in the outgoing CCA message at IP-CAN Session level	3	1.14.0
33593708	HorizontalPodAutoscaler (hpa) support for pcrf-core	3	1.14.0
33593753	SM PCF cnDBTier 1.8.8 db replication failure	3	1.12.0

Table 4-15 (Cont.) CNC Policy 1.15.0 Resolved Bugs

Bug Number	Title	Severity	Found In Release
33593935	pdssubscriber DB leak observed in case of UDR resource based subscription for sm-data	3	1.15.0
33594137	CNCP 1.14 not sending RAR when receiving a SNR in Sy interface when pcs1.ppci1.time is set	3	1.14.0
33594801	servicemesh RequestAuthentication template labelselector key hardcoded as "app" template changes	3	1.15.0
33594775	Update VNFD in all CSAR to not point to SM Helm	3	1.15.0
33263667	Ephemeral storage requirement for CNC Policy	3	1.14.0
33459825	Blockly "default" not working 1.12.x onwards	3	1.12.3
33593578	PCF diam-connector svc as prometheus scrape target for metrics	4	1.14.0

NRF Resolved Bugs

NRF 1.15.2 Resolved Bugs

There are no resolved bugs for this release.

NRF 1.15.1 Resolved Bugs

Table 4-16 NRF 1.15.1 Resolved Bugs

Bug Number	Title	Severity	Found In Release
33760081	SLF lookup with Subscriber not provisioned resulting into NRF forwarding	2	1.11.3
33760243	NRF Forwarding forwarded request the SNSSAI is replacing %5B%7B with { resulting in EGW failed to send	2	1.11.3
33760313	NRF sending unmatched UDMs when SLF returns a valid Group-ID.	3	1.11.3
33763632	Loop detection validation failing when more than one value is present in the via header	3	1.11.3

NRF 1.15.0 Resolved Bugs

Table 4-17 NRF 1.15.0 Resolved Bugs

Bug Number	Title	Severity	Found In Release
33508869	FQDN in NFProfile and NFservice is not getting replaced using InterPLMNFqdn present in Inter-PLMN Notification Messages and Discovery responses	3	1.14.0
33521092	Create database users with NDB_STORED_USER for non-root user	4	1.14.0
33521073	NRF does not send 204 when it receives HB request	4	1.14.0
33517608	Requester-plmn-list can be present in intra-plmn request as well	4	1.14.0

NSSF Resolved Bugs

There are no resolved bugs in NSSF Release 1.8.0.

SCP Resolved Bugs

Table 4-18 SCP 1.15.4 Resolved Bugs

Bug Number	Title	Severity	Found in Release
34249989	Configuration module restarts when scp-worker pod replica count is 0	3	1.15.3
34173869	SCP silently discarding messages due to sbi message priority even when configuration is set to 100% discard with error	3	1.15.2
34189588	SCP not able to extract message type when multiple parameters are there in dataset-names in ingres request URI	3	1.15.3
34189601	Fix NoNFInstance metric pegging issue	3	1.15.3
34178268	SCPAuditEmptyNFArrayResponse alert expression not correct	4	1.15.3
34212879	Change memory utilization percentages to 85% instead of current 70% in alerts of scp-worker and notification pods	4	1.15.3
34212846	Fix Null pointer exception in silent discard	4	1.15.3
34212819	Set HTTP Response with query parameters not working in ATS	4	1.15.2

Table 4-19 SCP 1.15.3 Resolved Bugs

Bug Number	Title	Severity	Found in Release
33990755	SCP responding with incorrect 3gpp-sbi-producer-id header to consumer NF	2	22.1.1
34041750	Circuit Breaking not working in case of Multiple IP endpoints for a service host	3	1.15.0
33966523	Location header is incorrectly updated in response when headers to be addition to apiPrefix for reverse proxy routing	3	1.15.0
33966476	SCP is adding "accept-encoding:gzip" header to requests while routing out	3	22.1.0
33966463	SCP should not add "User-agent" header in indirect communication	3	1.14.1
33966543	ATS enhancement to support timeout at configuration client, if response is not received by configuration client	3	1.15.1
33956765	Even with reverseProxyEnabled set to false, SCP appends UDR and its own rootapi in location header back to PCF POST request	3	22.1.0
34037543	SCP sending incorrect format for 3gpp-sbi-target-apiroot header in response	3	22.1.0
34093590	jaeger tracing not working for some SCP generated error responses	3	1.15.0
34093613	SCP responds with 508 LOOP_DETECTED for the UDM Notification request	3	1.15.0

Table 4-20 SCP 1.15.2 Resolved Bugs

Bug Number	Title	Severity	Found in Release
33904805	SCP sends duplicate subscription/ unsubscription request towards NRF	4	1.15.0
33904845	Helm chart changes to bypass sidecar proxy for DNS queries	3	1.15.0
33914225	Correct apiPrefix in R15 Regression Egressratelimiting_INTERSCP feature testcase	4	1.15.1

Table 4-21 SCP 1.15.1 Resolved Bugs

Bug Number	Title	Severity	Found in Release
33804949	SCP to create routing rules based on mate Site info provided at deployment time	3	1.15.0
33890294	scp-worker is not re-routing to other producer if 307 response has incorrect location header	3	1.15.0
33890341	Jaeger traces are missing NF IP End point details	4	1.15.0
33791959	SCP-worker exception when updating location header for reverse proxy routing	3	1.15.0
33882889	Exception in scp-worker on metric peg during message discard due to pod overload control	3	1.15.0
33885113	Update metric for SCPAuditEmptyArrayResponse	4	1.15.0
33894405	Metric pegging is missing for ondemand audit	4	1.15.0
33791930	Fix of FT for "VZW:- Getting AttributeError "NoneType' while running Routing_Rules_API_R16.feature	3	1.15.0
33673751	Cluster domain is not getting updated in few New feature files	3	1.15.0
33888551	Update EgressRateLimiting_InterSCP.feature to remove extra space in update json step	4	1.15.0
33883105	Fix the FT <Worker_Pod_Overload_Ctrl_Policy_Config_API.feature> for validating the response step	4	1.15.0
33883148	Enable automatic ATS cleanup to revert default values for different levels (WANR, MINOR, MAJOR, CRITICAL) for CPU overload control policy	4	1.15.0
33883056	Update rate limiting scenario with high rate and tolerane	4	1.14.1

Table 4-22 SCP 1.15.0 Resolved Bugs

Bug Number	Title	Severity	Found in Release
33429818	Addition/deletion of service in NF profile results in incorrect destination rules on SCP	2	1.9.2
33595612	Duplicate IP Endpoints in different profile results in stale service entries.	3	1.14.0
33460911	Application User missing NDB_STORED_USER permissions	3	1.14.0

Table 4-22 (Cont.) SCP 1.15.0 Resolved Bugs

Bug Number	Title	Severity	Found in Release
33460931	Audit microservice upgrade failure due to namespace and releasename variable missing in upgrade hooks	3	1.14.0
33460935	Duplicate rules creation on scp worker pod restart	3	1.14.0
33460944	Hostmpper null pointer exception observed in scp worker	3	1.14.0
33465417	Add Pod scale up in cleanup of NRF Registration feature file	3	1.12.0
33460920	Document update for privileged user permissions	4	1.14.0
33460956	Enable pasing R15 as input to New features ATS	4	1.14.0
33460975	Fix comments in ATS custom deployment file	4	1.14.0

SEPP Resolved Bugs

Table 4-23 SEPP 1.7.1 Resolved Bugs

Bug Number	Title	Severity	Found in Release
33668005	SEPP 1.7.0 handshake failure due to missing helm configuration	3	1.7.0
33682982	Authority header port not used	3	1.7.0
33696703	SEPP 1.7.0 adding extra http2 headers to hSMF response	3	1.7.0
33667946	SEPP 1.7.0 shows incorrect app version	4	1.7.0

Table 4-24 SEPP 1.7.0 Resolved Bugs

Bug Number	Title	Severity	Found in Release
33577511	NRF Discovery fails with 400-Bad request at hNRF	2	1.6.1
33322009	Cache not getting updated for deleted entries	3	1.6.1
33323304	DB operations taking approximately 60seconds to reflect in N32f services	3	1.6.1

Table 4-24 (Cont.) SEPP 1.7.0 Resolved Bugs

Bug Number	Title	Severity	Found in Release
33593942	Mismatch between metric names used in KPI formulas for SEPP in User Guide v 1.6.0.	4	1.6.0

UDR Resolved Bugs

UDR Release 1.15.2

There are no resolved bugs in UDR Release 1.15.2.

UDR Release 1.15.1

There are no resolved bugs in UDR Release 1.15.1.

UDR Release 1.15.0

Table 4-25 UDR 1.15.0 Resolved Bugs

Bug Number	Title	Severity	Found in Release
30774750	Notify Service delays notifications to PCF during traffic run	4	1.3.0
32377439	De-Registration fails when egressgateway goes down before nrf-client during UDR deletion	4	1.10.0

Customer Known Bug List

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

BSF Customer Known Bugs

There are no customer known bugs in BSF Release 1.11.0.

CNC Console Customer Known Bugs

CNC Console Release 1.9.2

There are no customer known bugs in CNC Console Release 1.9.2.

CNC Console Release 1.9.1

There are no customer known bugs s in CNC Console Release 1.9.1.

CNC Console Release 1.9.0

Table 4-26 CNC Console 1.9.0 Customer Known Bugs

Bug Number	Title	Severity	Found in Release	Customer Impact
33587376	Console GUI - Appending Edit in the service page heading When user keep edit operation in incomplete state and move to new screen, new screen heading is appending with Edit.	3	1.9.0	No customer impact. When the user keep edit operation in incomplete state and move to new screen, new screen heading is appending with **Edit**. **Workaround**: User can click on the **Cancel** button available in **Edit** screen.

CNE Customer Known Bugs

Table 4-27 CNE 1.10.0 Customer Known Bugs

Bug Number	Title	Severity	Found in Release	Customer Impact
32211087	Updating the Alerts, Varbind and alert groups of prometheus.	2	1.4.0	No customer impact.
33564120	createFailedLbvm does not update haproxy template files	3	1.9.1	A switchover will not work properly as the services will not work because the template files are not on the new LBVMs to generate the service configurations in the haproxy.cfg file on the LBVM.
33564120	addPeerAddrPool.py does not update haproxy template files	3	1.9.1	A switchout to that LBVM will work but the services will not work (get created properly) on the new LBVM.
33356061	Modify NETWORK_INTERFACE_FAILED alert to fire separate alert for gen10 and gen8 h/w	3	1.7.0	The current definition of NETWORK_INTERFACE_FAILED alert sends a false alarm for gen10 hardware.

CNC Policy Customer Known Bugs

CNC Policy 1.15.5

There are no customer known bugs in CNC Policy 1.15.5.

CNC Policy 1.15.4

There are no customer known bugs in CNC Policy 1.15.4.

CNC Policy 1.15.3

There are no customer known bugs in CNC Policy 1.15.3.

CNC Policy 1.15.1

There are no customer known bugs in CNC Policy 1.15.1.

CNC Policy 1.15.0

Table 4-28 CNC Policy 1.15.0 Customer Known Bugs

Bug Number	Title	Severity	Found in Release	Customer Impact
33594728	MatchList cannot be created with IP Addresses & Subnet	3	1.14.0	MatchList cannot be created with IP Addresses & Subnet. This support is not there in the software and customer will not be able to use the support IP Address with Subnet
33388403	Conflict Resolution detection in Policy Table	3	1.14.0	Policy Table in the imported file will replace the Policy Table in the DB if they are same and thus will make the Policies using the Policy Table unusable
33388333	Export operation on the Yaml Schema screen is not working after doing Bulk Import of data including Yaml Schema	3	1.14.0	Bulk Import will throw error for the custom yaml configuration and custom yaml will fail to import.

Table 4-28 (Cont.) CNC Policy 1.15.0 Customer Known Bugs

Bug Number	Title	Severity	Found in Release	Customer Impact
33594749	BS Binding Header: Data to pcfId, pcfSetId parameters not sent in pcfBinding request object	3	1.15.0	The two parameters pcfSetd and pcfId will go as null to BSF in CREATE request. These two values are saved in BSF database but only required when request comes from AF in 5G. And since this flow is not implemented yet, these two values will not be used by BSF. So it wont have any impact for now
33595266	PDS Workflow json file not into zip Bulk export file	3	1.15.0	PDS workflow will not get exported from a system while doing Bulk Export. User needs to manually add workflow in PDS Workflow page on CNC Console. Then, if export is performed, the json file should appear in exported zip file.

NRF Customer Known Bugs

Table 4-29 NRF 1.15.x Customer Known Bugs

Bug Number	Title	Severity	Found in Release	Customer Impact
33521288	Last value of keyDetailsList in nfAccessTokenOptions cannot be cleared using CNC Console	4	1.12.0	Using CNCC GUI, the last Key Id from the keyDetailsList can't be removed
33521204	NRF CNCC SLF Look up configuration delete is not available	4	1.12.0	Using CNCC GUI, the SLF Details can't be removed

NSSF Customer Known Bugs

There are no customer known bugs in NSSF Release 1.8.0.

SCP Customer Known Bugs

Table 4-30 SCP 1.15.x Customer Known Bugs

Bug Number	Title	Severity	Found In Release	Customer Impact
33594355	Wrong ASM Server Header implementation causes ATS test case failures	4	1.15.0	Due to ASM issue, some ATS test cases are removed.

SEPP Customer Known Bugs

There are no customer known bugs in SEPP Release 1.7.0.

UDR Customer Known Bugs

Table 4-31 UDR 1.15.0 and 1.15.1 Customer Known Bugs

Bug Number	Title	Severity	Found in Release	Customer Impact
30774755	Headers for few resources are not implemented as per spec 29505-v15.4.0	3	1.4.0	No impact.
30774742	UDR is not validating the conditional attributes for UDM APIs.	4	1.3.0	No impact. UDM(consumer of UDM APIs) does not send conditional attributes to UDR.