

Oracle® Communications

Cloud Native Core, Certificate Management

Network Impact Report



Release 23.4.4
F88117-05
October 2024

ORACLE®

Copyright © 2023, 2024, Oracle and/or its affiliates.

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

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

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

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

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

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

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

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

1	Introduction	
1.1	Purpose and Scope	1
1.2	OCCM Compatibility Matrix	1
1.3	Common Services Load Lineup	2
1.4	Software Requirements	3
1.5	Orchestration	4
1.6	Resource Requirements	7
2	Features	
3	Supported Upgrade and Rollback Paths	
4	Configuration	
4.1	Helm	1
4.2	REST API	2
4.3	CNC Console	2
5	Observability	
5.1	Metrics	1
5.2	Alerts	1
5.3	KPIs	2

Acronyms

The following table lists the acronyms and the terminologies used in the document:

Table Acronyms and Terminologies

Acronym	Definition
3GPP	3rd Generation Partnership Project
API	Application Programming Interface
CCA	Client Credentials Assertions
CMP	Certificate Management Protocol
CNC	Cloud Native Core
CNC Console	Cloud Native Configuration Console
OCCM	Oracle Communications Certificate Management
CA	Certification Authority is a trusted entity that issues Secure Sockets Layer (SSL) certificates. CAs are also called issuer in this document.
DNS	Domain Name Server
EE	End Entity
ECC	Elliptic Curve Cryptography
HSM	Hardware Security Module
IDP	Identity Provider
LCM	Life Cycle Management
PKI	Public Key Infrastructure
RA	Registration Authority
RSA	Rivest-Shamir-Adleman
SAN	Subject Alternative Name
URI	Uniform Resource Indicator
URN	Uniform Resource Name
CMP Identity Key	Private Key used by Certificate Management to sign the CMPv2 requests and establish trust between Certificate Management and CA.
CMP Identity Certificate	Certificate that corresponds to and certifies the CMP Identity Key. It is included in the CMPv2 requests for authentication by CA.

What's New in This Guide

This section introduces the documentation updates for release 23.4.x.

Release 23.4.4 - F88117-05, October 2024

- Updated the [Common Services Load Lineup](#) with the latest Helm Test and Debug Tool version.
- Updated the orchestration details in the [Orchestration](#) section.
- Updated the [Helm](#) section.
- Updated the [Alerts](#) section.

Release 23.4.3 - F88117-04, July 2024

- Updated the [Common Services Load Lineup](#) with the latest Helm Test and Debug Tool version.

Release 23.4.2 - F88117-03 April 2024

There are no updates in this release.

Release 23.4.1 - F88117-02 March 2024

- [Orchestration](#)

Release 23.4.0 - F88117-01 December 2023

This is the initial release of this document.

1

Introduction

1.1 Purpose and Scope

The purpose of this document is to highlight the changes made in OCCM in Release 23.4.x. These changes may have an impact on the customer network operations and should be considered by the customer while planning the deployment.

1.2 OCCM Compatibility Matrix

This section lists the versions of added or updated components in release 23.4.x. To know the list of all the supported versions, see Oracle Communications Cloud Native Core Release Notes.

Release 23.4.4

There is no change in the compatibility matrix in this release.

Release 23.4.3

The following table lists the versions of added or updated components in release 23.4.3:

Table 1-1 Compatibility Matrix

Components	Compatible Versions
CNE	23.4.x, 23.3.x, 23.2.x
CDCS	23.4.x, 23.3.x

Release 23.4.2

The following table lists the versions of added or updated components in release 23.4.2:

Table 1-2 Compatibility Matrix

Components	Compatible Versions
CNE	23.4.x, 23.3.x, 23.2.x
CDCS	23.4.x, 23.3.x

Release 23.4.1

The following table lists the versions of added or updated components in release 23.4.1:

Table 1-3 Compatibility Matrix

Components	Compatible Versions
CNE	23.4.x, 23.3.x, 23.2.x

Table 1-3 (Cont.) Compatibility Matrix

Components	Compatible Versions
CDCS	23.4.x, 23.3.x

Release 23.4.0

The following table lists the versions of added or updated components in release 23.4.0:

Table 1-4 Compatibility Matrix

Components	Compatible Versions
CNE	23.4.x, 23.3.x, 23.2.x
CDCS	23.4.x, 23.3.x

1.3 Common Services Load Lineup

This section lists the versions of added or updated common services in release 23.4.x. To know the list of all the supported versions, see *Oracle Communications Cloud Native Core Release Notes*.

The following table lists the versions of added or updated common services in release 23.4.4:

Table 1-5 Common Services Load Lineup

Common Service	Version
Helm Test	23.4.3
Debug Tool	23.4.3

The following table lists the versions of added or updated common services in release 23.4.3:

Table 1-6 Common Services Load Lineup

Common Service	Version
Helm Test	23.4.2
Debug Tool	23.4.2

The following table lists the versions of added or updated common services in release 23.4.2:

Table 1-7 Common Services Load Lineup

Common Service	Version
Helm Test	23.4.1
Debug Tool	23.4.1

The following table lists the versions of added or updated common services in release 23.4.1:

Table 1-8 Common Services Load Lineup

Common Service	Version
Helm Test	23.4.0
Debug Tool	23.4.1

The following table lists the versions of added or updated common services in release 23.4.0:

Table 1-9 Common Services Load Lineup

Common Service	Version
Helm Test	23.4.0
Debug Tool	23.4.0

1.4 Software Requirements

This section lists the software that must be installed before installing OCCM:

Install the following software before installing OCCM:

Table 1-10 Preinstalled Software

Software	Version
Kubernetes	1.27.x, 1.26.x, 1.25.x
Helm	3.12.3
Podman	4.4.1

To check the current Helm and Kubernetes version installed in the CNE, run the following commands:

```
kubectl version
```

```
helm version
```

The following software are available if OCCM is deployed in CNE. If you are deploying OCCM in any other cloud native environment, these additional software must be installed before installing OCCM. To check the installed software, run the following command:

```
helm ls -A
```

The list of additional software items, along with the supported versions and usage, is provided in the following table:

Table 1-11 Additional Software

Software	Version
containerd	1.7.5

Table 1-11 (Cont.) Additional Software

Software	Version
Calico	3.25.2
MetallLB	0.13.11
Prometheus	2.44.0
Grafana	9.5.3
Jaeger	1.45.0
Istio	1.18.2
Kyverno	1.9.0
cert-manager	1.12.4
Oracle OpenSearch	2.3.0
Oracle OpenSearch Dashboard	2.3.0
Fluentd OpenSearch	1.16.2
Velero	1.12.0

1.5 Orchestration

This section provides information about orchestration changes in release 23.4.x.

The following table provides information about orchestration changes in release 23.4.4:

Table 1-12 Orchestration

Orchestration Changes	Status	Notes
Support for in-service upgrade	Yes	Upgrade and Rollback is supported. Note that OCCM microservices are single pod.
Changes in the custom_values.yaml file	Yes	For information about changes in the custom_values.yaml file, see Helm section
Changes in the resource information for custom_values.yaml file	No	No changes have been made in this release.
Changes in the CSAR package	No	No changes have been made in this release. CSAR package is supported. Note: For more information on specific CSAR changes, please contact My Oracle Support.
Changes in Role-Based Access Control (RBAC) policy	No	No changes have been made in this release. OCCM deployment needs Service Account. Appropriate permissions must be assigned to OCCM using Kubernetes Service Account, Role and Role Binding, based on the selected deployment model.

Table 1-12 (Cont.) Orchestration

Orchestration Changes	Status	Notes
Changes in Life Cycle Management (LCM) Operations	No	No changes have been made in this release. OCCM deployment using helm install and CDCS is supported.
Helm Test Support	Yes	Helm test is supported.

The following table provides information about orchestration changes in release 23.4.3:

Table 1-13 Orchestration

Orchestration Changes	Status	Notes
Support for in-service upgrade	Yes	Upgrade and Rollback is supported. Note that OCCM microservices are single pod.
Changes in the custom_values.yaml file	No	No changes have been made in this release.
Changes in the resource information for custom_values.yaml file	No	No changes have been made in this release.
Changes in the CSAR package	No	No changes have been made in this release. CSAR package is supported. Note: For more information on specific CSAR changes, please contact My Oracle Support.
Changes in Role-Based Access Control (RBAC) policy	No	No changes have been made in this release. OCCM deployment needs Service Account. Appropriate permissions must be assigned to OCCM using Kubernetes Service Account, Role and Role Binding, based on the selected deployment model.
Changes in Life Cycle Management (LCM) Operations	No	No changes have been made in this release. OCCM deployment using helm install and CDCS is supported.
Helm Test Support	Yes	Helm test is supported.

The following table provides information about orchestration changes in release 23.4.2.

Table 1-14 Orchestration

Orchestration Changes	Status	Notes
Support for in-service upgrade	Yes	Upgrade and Rollback is supported. Note that OCCM microservices are single pod.

Table 1-14 (Cont.) Orchestration

Orchestration Changes	Status	Notes
Changes in the custom_values.yaml file	No	No changes have been made in this release.
Changes in the resource information for custom_values.yaml file	No	No changes have been made in this release.
Changes in the CSAR package	No	No changes have been made in this release. CSAR package is supported. Note: For more information on specific CSAR changes, please contact My Oracle Support.
Changes in Role-Based Access Control (RBAC) policy	No	No changes have been made in this release. OCCM deployment needs Service Account. Appropriate permissions must be assigned to OCCM using Kubernetes Service Account, Role and Role Binding, based on the selected deployment model.
Changes in Life Cycle Management (LCM) Operations	No	No changes have been made in this release. OCCM deployment using helm install and CDCS is supported.
Helm Test Support	Yes	Helm test is supported.

The following table provides information about orchestration changes in release 23.4.1.

Table 1-15 Orchestration

Orchestration Changes	Status	Notes
Support for in-service upgrade	Yes	Upgrade and Rollback is supported. Note that OCCM microservices are single pod.
Changes in the custom_values.yaml file	No	No changes have been made in this release.
Changes in the resource information for custom_values.yaml file	No	No changes have been made in this release.
Changes in the CSAR package	No	No changes have been made in this release. CSAR package is supported. Note: For more information on specific CSAR changes, please contact My Oracle Support.

Table 1-15 (Cont.) Orchestration

Orchestration Changes	Status	Notes
Changes in Role-Based Access Control (RBAC) policy	No	No changes have been made in this release. OCCM deployment needs Service Account. Appropriate permissions must be assigned to OCCM using Kubernetes Service Account, Role and Role Binding, based on the selected deployment model.
Changes in Life Cycle Management (LCM) Operations	No	No changes have been made in this release. OCCM deployment using helm install and CDCS is supported.
Helm Test Support	Yes	Helm test is supported.

The following table provides information about orchestration changes in release 23.4.0.

Table 1-16 Orchestration

Orchestration Changes	Status	Notes
Support for in-service upgrade	Yes	Upgrade and Rollback is supported. Note that OCCM microservices are single pod.
Changes in the custom_values.yaml file	Yes	OCCM and OCCM Network Polices Helm chart and custom values are made available as part of OCCM package.
Changes in the resource information for custom_values.yaml file	Yes	OCCM resource requirement is updated in custom values file.
Changes in the CSAR package	Yes	CSAR package is supported. Note: For more information on specific CSAR changes, please contact My Oracle Support.
Changes in Role-Based Access Control (RBAC) policy	Yes	OCCM deployment needs Service Account. Appropriate permissions must be assigned to OCCM using Kubernetes Service Account, Role and Role Binding, based on the selected deployment model.
Changes in Life Cycle Management (LCM) Operations	Yes	OCCM deployment using helm install and CDCS is supported.
Helm Test Support	Yes	Helm test is supported.

1.6 Resource Requirements

This section lists the resource requirements to install and run OCCM

Resource Profile

Table 1-17 Resource Profile

Microservice Name	Pod Replica	Limits			Requests		
		CPU	Memory (Gi)	Ephemeral Storage (Mi)	CPU	Memory (Gi)	Ephemeral Storage (Mi)
OCCM	1	2	2	1102	2	2	57
Helm Test	1	0.5	0.5	1102	0.5	0.5	57
Total		2.5	2.5	2204	2.5	2.5	114

Note

- Helm Test Job - This job is executed on demand when helm test command is executed. It will execute the helm test and stops after completion. These are short-lived jobs which gets terminated after the work is done. So, they are not part of Active deployment Resource but needs to be considered only during helm test procedures.
- Troubleshooting Tool (Debug tool) Container - If Troubleshooting Tool Container Injection is enabled during OCCM deployment/upgrade, this container will be injected to OCCM pod. These containers will stay till pod/deployment exists. Debug tool resources are not considered in the calculation. Debug tool resources usage is per pod, if debug tool is enabled then max 0.5vCPU and 0.5Gi Memory per occm pod is needed.

2

Features

This chapter lists the added or updated features in release 23.4.x. For more information about the features, see *Oracle Communications Cloud Native Core Certificate Management User Guide*.

Release 23.4.4

There are no new features or enhancements in this release.

Release 23.4.3

There are no new features or enhancements in this release.

Release 23.4.2

There are no new features or enhancements in this release.

Release 23.4.1

There are no new features or enhancements in this release.

Release 23.4.0

The OCCM documentation has been updated with the following features:

- **Automated Certificate Management:**

Oracle Communications Certificate Management (OCCM) is an automated solution for managing the certificates needed for Oracle 5G Network Functions (NFs). OCCM constantly monitors and renews the certificates based on their validity or expiry period.

OCCM integrates with the Certificate Authority(s) using Certificate Management Protocol Version 2 (CMPv2) and RFC4210 to facilitate these certificate management operations:

- Operator-initiated certificate creation
- Operator-initiated certificate recreation
- Automatic certificate monitoring and renewal

OCCM supports transport of CMPv2 messages using HTTP-based protocol.

OCCM provides the following mechanisms to establish initial trust between OCCM and CA(s):

1. Certificate-based message signing
2. Pre-shared key or MAC based authentication

All the subsequent CMPv2 procedures are authenticated using the certificate-based mechanism in compliance with 3GPP TS 33.310.

The keys and X.509 certificates are managed using Kubernetes secrets.

- **OCCM Deployment Models:**

OCCM provides the following deployment models to support certificate management for the integrated NF(s) instantiated within the same cluster:

- Dedicated deployment model - OCCM resides in the same Kubernetes namespace as the NF or Components.
- Shared deployment model - OCCM is deployed in a separate Kubernetes namespace and can manage certificates of multiple NFs or components deployed in other Kubernetes namespaces.

Appropriate permissions must be assigned to OCCM using Kubernetes Service Account, Role and Role Binding, based on the selected deployment model.

- **Console Support for OCCM Configuration:**
Console support for OCCM configuration is enabled. OCCM configuration can be performed through Console GUI or by invoking REST API by passing Console Access Token. Following OCCM GUI screens are supported at Console:
 - Issuer Configuration
 - Certificate Configuration
 - Logging Configuration
- **Support for Kubernetes Network Policies:** OCCM has implemented the Network policies framework to enable the user to specify how a pod communicates with network entities. It enables OCCM to create pod-level rules needed for OCCM data flows, to manage Ingress and Egress traffic.
- **Support for OCCM Deployment Using Continuous Delivery Control Server (CDCS):**
In addition to OCCM's Command Line Interface (CLI) deployment method, OCCM can be deployed using the Continuous Delivery Control Server (CDCS), which is a centralized server that automates OCCM deployment processes such as downloading the OCCM package, installation, upgrade, and rollback. For more information about CDCS, see *Oracle Communications Cloud Native Core CD Control Server User Guide*. For information about OCCM deployment using CDCS, see the Overview section in *Oracle Communications Cloud Native Core Certificate Management Installation, Upgrade, and Fault Recovery Guide*.

3

Supported Upgrade and Rollback Paths

This chapter lists the supported upgrade and rollback paths in release 23.4.x. For more information about upgrade and rollback, see *Oracle Communications Cloud Native Core Certificate Management Installation, Upgrade, and Fault Recovery Guide*.

OCCM 23.4.4

Supported Upgrade Paths

The following table lists the supported upgrade path in release 23.4.4

Table 3-1 Supported Upgrade Paths

Source OCCM Release	Target OCCM Release
23.4.x	23.4.x

Supported Rollback Paths

The following table lists the supported rollback path in release 23.4.4:

Table 3-2 Supported Rollback Paths

Source OCCM Release	Target OCCM Release
23.4.x	23.4.x

OCCM 23.4.3

Supported Upgrade Paths

The following table lists the supported upgrade path in release 23.4.3:

Table 3-3 Supported Upgrade Paths

Source OCCM Release	Target OCCM Release
23.4.x	23.4.x

Supported Rollback Paths

The following table lists the supported rollback path in release 23.4.3:

Table 3-4 Supported Rollback Paths

Source OCCM Release	Target OCCM Release
23.4.x	23.4.x

OCCM 23.4.2

Supported Upgrade Paths

The following table lists the supported upgrade path in release 23.4.2:

Table 3-5 Supported Upgrade Paths

Source OCCM Release	Target OCCM Release
23.4.x	23.4.x

Supported Rollback Paths

The following table lists the supported rollback path in release 23.4.2:

Table 3-6 Supported Rollback Paths

Source OCCM Release	Target OCCM Release
23.4.x	23.4.x

OCCM 23.4.1

Supported Upgrade Paths

The following table lists the supported upgrade path in release 23.4.1:

Table 3-7 Supported Upgrade Paths

Source OCCM Release	Target OCCM Release
23.4.x	23.4.x

Supported Rollback Paths

The following table lists the supported rollback path in release 23.4.1:

Table 3-8 Supported Rollback Paths

Source OCCM Release	Target OCCM Release
23.4.x	23.4.x

OCCM 23.4.0

Supported Upgrade Paths

The following table lists the supported upgrade path in release 23.4.0:

Table 3-9 Supported Upgrade Paths

Source OCCM Release	Target OCCM Release
23.4.x	23.4.x

Supported Rollback Paths

The following table lists the supported rollback path in release 23.4.0:

Table 3-10 Supported Rollback Paths

Source OCCM Release	Target OCCM Release
23.4.x	23.4.x

4

Configuration

This chapter lists the configuration changes in release 23.4.x.

4.1 Helm

This section lists the Helm parameter changes in release 23.4.x. For more information about the Helm parameters, see *Oracle Communications Cloud Native Core Certificate Management Installation, Upgrade, and Fault Recovery Guide*.

Release 23.4.4

- In `occm_network_policy_custom_values_<version>.yaml` file, policy `allow-ingress-from-cncc-pods` network policy is updated as follows:

```
# Allow ingress traffic from cncc pods
- metadata:
  name: allow-ingress-from-cncc-pods
  spec:
    podSelector:
      matchLabels:
        app.kubernetes.io/part-of: occm
    policyTypes:
      - Ingress
    ingress:
      - from:
          # Use this when OCCM and CNCC are deployed in different namespaces
          - namespaceSelector:
              matchLabels: { }
              ## kubernetes.io/metadata.name: cncc-ns # Uncomment and add this
              label for Namespace where cncc pods are located
            podSelector:
              matchLabels: { }
              ## app.kubernetes.io/app-name: cncc # Uncomment and add this
              label for CNCC pods

          # Use this when OCCM and CNCC are deployed in the same namespace
          - podSelector:
              matchLabels: { }
              ## app.kubernetes.io/app-name: cncc # Uncomment and add this
              label for CNCC pods
            ports:
              - protocol: TCP
                port: 8989 # OCCM Port
```

Release 23.4.3

There are no changes in this release.

Release 23.4.2

There are no changes in this release.

Release 23.4.1

There are no changes in this release.

Release 23.4.0

The following are the Helm parameters changes in release 23.4.0:

OCCM and OCCM Network Policies Helm chart and custom values are made available as part of OCCM package.

4.2 REST API

This section lists the REST API changes in release 23.4.x. For more information about the REST APIs, see *Oracle Communications Cloud Native Core Certificate Management REST Specification Guide*.

Release 23.4.4

There are no changes in the REST API in this release.

Release 23.4.3

There are no changes in this release.

Release 23.4.2

There are no changes in this release.

Release 23.4.1

There are no changes in this release.

Release 23.4.0

This is the initial release of this document.

4.3 CNC Console

This section lists the CNC Console changes in release 23.4.x. For more information about the CNC Console, see *Oracle Communications Cloud Native Core, Certificate Management User Guide*.

Release 23.4.4

There are no changes in this release.

Release 23.4.3

There are no changes in this release.

Release 23.4.2

There are no changes in this release.

Release 23.4.1

There are no changes in this release.

Release 23.4.0

GUI screens for OCCM APIs are available and have been documented in the *Oracle Communications Cloud Native Core Certificate Management User Guide*.

5

Observability

This chapter lists the observability changes in release 23.4.x.

5.1 Metrics

This section lists the added or updated metrics in release 23.4.x. For more information about metrics, see *Oracle Communications Cloud Native Core Certificate Management User Guide*.

Release 23.4.4

There are no changes in this release.

Release 23.4.3

There are no changes in this release.

Release 23.4.2

There are no changes in this release.

Release 23.4.1

There are no changes in this release.

Release 23.4.0

This is the initial release of this document.

5.2 Alerts

This section lists the added or updated alerts in release 23.4.x. For more information about alerts, see *Oracle Communications Cloud Native Core Certificate Management User Guide*.

Release 23.4.4

Updated the `OccmFailureMinor` alert description.

Release 23.4.3

There are no changes in this release.

Release 23.4.2

There are no changes in this release.

Release 23.4.1

There are no changes in this release.

Release 23.4.0

This is the initial release of this document.

5.3 KPIs

This section lists the added or updated KPIs in release 23.4.x. For more information about KPIs, see *Oracle Communications Cloud Native Core Certificate Management User Guide*.

Release 23.4.4

There are no changes in this release.

Release 23.4.3

There are no changes in this release.

Release 23.4.2

There are no changes in this release.

Release 23.4.1

There are no changes in this release.

Release 23.4.0

This is the initial release of this document.