UCC 5G cnSGWc Release Notes, Release 2024.04.1

First Published: 2024-11-26

Ultra Cloud Serving Gateway Control Plane Function

Introduction

This Release Notes identifies changes and issues related to this software release.

Release Lifecycle Milestones

Release Lifecycle Milestone	Milestone	Date
First Customer Ship	FCS	30-Oct-2024
End of Life	EoL	30-Oct-2024
End of Software Maintenance	EoSM	30-Apr-2026
End of Vulnerability and Security Support	EoVSS	30-Apr-2026
Last Date of Support	LDoS	30-Apr-2027

These milestones and the intervals between them are defined in the Cisco Ultra Cloud Core (UCC) Software Release Lifecycle Product Bulletin available on cisco.com.

Release Package Version Information

Software Packages	Version
ccg-2024.04.1.SPA.tgz	2024.04.1
NED package	ncs-5.6.8-ccg-nc-2024.04.1 ncs-6.1.12-ccg-nc-2024.04.1
NSO	5.6.8 6.1.12

Descriptions for the various packages provided with this release are available in the Release Package Descriptions, on page 5 section.

Verified Compatability

Products	Version
Ultra Cloud Core SMI	2024.04.1.14
Ultra Cloud CDL	1.11.9.1
Ultra Cloud Core UPF	2024.04.1
Ultra Cloud SMF	2024.04.1

For information on the Ultra Cloud Core products, refer to the documents for this release available at:

- https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-subscriber-microservices-infrastructure/products-installation-and-configuration-guides-list.html

- https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-user-plane-function/products-installation-and-configuration-guides-list.html

- https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-session-management-function/products-installation-and-configuration-guides-list.html

What's New in this Release

Features and Enhancements

This section covers a brief description of the features and enhancements introduced in this release. It also includes links to detailed documentation, where available.

Feature	Description
Overload Optimization for GTPC Messages using Message Priority Negotiation	During WPS sessions, cnSGWc ensures smooth communication by defining the message priority for incoming messages and negotiating the message priority value for outgoing messages. This feature allows the network operator to exempt the incoming WPS session messages by configuring the message priority under the overload exclude profile. This feature also compares the message priority value of the incoming GTPC messages with the configured value and sets the lowest value for that session. **Commands Introduced: message-priority { any | s5e | s11 | sxa } upto** *message_priority* **Default Setting:** Disabled—Configuration required to Enable
Handling the Incoming Sx Messages at Self-overload State	The load and overload control capability of cnSGWc is enhanced to handle the incoming Sx message during the self-overload state. This feature allows the cnSGWc to throttle the incoming DLDR session report request messages in the self-protection mode.

Behavior Changes

There are no behavior changes in this software release.

Related Documentation

For the complete list of documentation available for this release, go to:

https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-serving-gateway-function/products-installation-and-configuration-guides-list.html

Installation and Upgrade Notes

This Release Note does not contain general installation and upgrade instructions. Refer to the existing installation documentation for specific installation and upgrade considerations.

Software Integrity Version

To verify the integrity of the software image you have from Cisco, you can validate the SHA512 checksum information against the checksum identified by Cisco for the software.

Image checksum information is available through **Cisco.com Software Download Details**. To find the checksum, hover the mouse pointer over the software image you have downloaded.
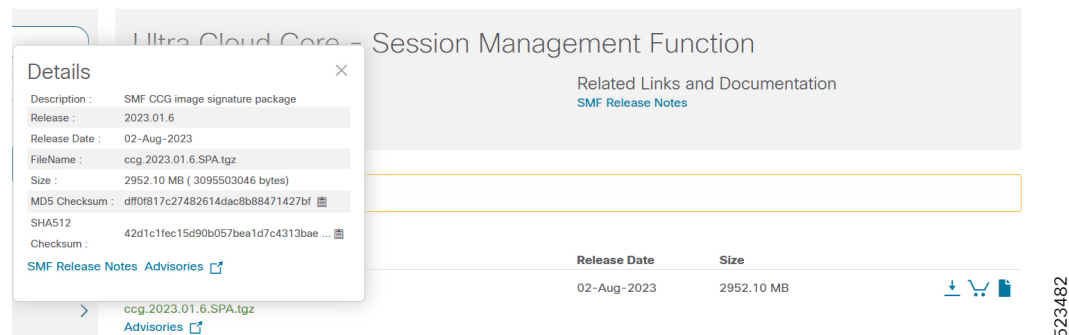
At the bottom you find the SHA512 checksum, if you do not see the whole checksum you can expand it by pressing the "..." at the end.

To validate the information, calculate a SHA512 checksum using the information in Table 1 and verify that it matches either the one provided on the software download page.

To calculate a SHA512 checksum on your local desktop, refer to the table below.

Table 1: Checksum Calculations per Operating System

Operating System	SHA512 checksum calculation command examples
Microsoft Windows	Open a command line window and type the following command: `> certutil.exe -hashfile` filename.extension `SHA512`

Operating System	SHA512 checksum calculation command examples
Apple MAC	Open a terminal window and type the following command: `$ shasum -a 512` filename.extension
Linux	Open a terminal window and type the following command: `$ sha512sum` filename.extension OR `$ shasum -a 512` filename.extension
Note filename is the name of the file. extension is the file extension (for example, .zip or .tgz).	

If the SHA512 checksum matches, you can be sure that no one has tampered with the software image or the image has not been corrupted during download.

If the SHA512 checksum does not match, we advise you to not attempt upgrading any systems with the corrupted software image. Download the software again and verify the SHA512 checksum again. If there is a constant mismatch, please open a case with the Cisco Technical Assistance Center.

Certificate Validation

The software images are signed via x509 certificates. For information and instructions on how to validate the certificates, refer to the .README file packaged with the software.

Open Bugs for this Release

The following table lists the open bugs in this specific software release.

> **Note** This software release may contain open bugs first identified in other releases. Additional information for all open bugs for this release are available in the Cisco Bug Search Tool.

Bug ID	Headline
CSCwn26804	S5DeleteBearerReq Failing with Error Message : Session not found
CSCwn29556	Disabling the oveload feature results in single instance of sgw-service restart

Resolved Bugs for this Release

The following table lists the resolved bugs in this specific software release.

Note This software release may contain bug fixes first introduced in other releases. Additional information for all resolved bugs for this release are available in the Cisco Bug Search Tool.

Bug ID	Headline	Behavior Change
CSCwm90737	sgw service restart at BearerInfo PdnInfo SubscriberInfo SubsContext	No
CSCwn01354	S11_gtpc pod crash with Panic trace during collision scenario	No

Operator Notes

Cloud Native Product Version Numbering System

The show helm list command displays detailed information about the version of the cloud native product currently deployed.

Versioning: Format & Field Description

YYYY.RN.MN[.TTN] [.dN] [.MR][.iBN]

Where,

YYYY → 4 Digit year.
- Mandatory Field.
- Starts with 2020.
- Incremented after the last planned release of year.

RN → Major Release Number.
- Mandatory Field.
- Starts with 1.
- Support preceding 0.
- Reset to 1 after the last planned release of a year(YYYY).

MN → Maintenance Number.
- Mandatory Field.
- Starts with 0.
- Does not support preceding 0.
- Reset to 0 at the beginning of every major release for that release.
- Incremented for every maintenance release.
- Preceded by "m" for bulbs from main branch.

TTN → Throttle of Throttle Number.
- Optional Field, Starts with 1.
- Precedes with "t" which represents the word "throttle or throttle".
- Applicable only in "Throttle of Throttle" cases.
- Reset to 1 at the beginning of every major release for that release.

DN → Dev branch Number.
- Same as TTN except Used for DEV branches.
- Precedes with "d" which represents "dev branch".

MR → Major Release for TOT and DEV branches.
- Only applicable for TOT and DEV Branches.
- Starts with 0 for every new TOT and DEV branch.

BN → Build Number.
- Optional Field, Starts with 1.
- Precedes with "t" which represents the word "interim".
- Does not support preceding 0.
- Reset at the beginning of every major release for that release.
- Reset of every throttle of throttle.

523483

The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research software releases.

Release Package Descriptions

The following table provides descriptions for the packages that are available with this release.

Table 2: Release Package Information

Software Packages	Description
ccg.<version>.SPA.tgz	The SMF offline release signature package. This package contains the SMF deployment software, NED package, as well as the release signature, certificate, and verification information.
ncs-<nso_version>-ccg-nc-<version>.tar.gz	The NETCONF NED package. This package includes all the yang files that are used for NF configuration. Note that NSO is used for the NED file creation.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, refer to https://www.cisco.com/c/en/us/support/index.html.