



UCC 5G cnSGWc Release Notes, Release 2024.04.0

First Published: 2024-10-25

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-2024.04.0.SPA.tgz	2024.04.0
NED package	ncs-5.6.8-ccg-nc-2024.04.0 ncs-6.1.12-ccg-nc-2024.04.0
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 6](#) section.

Verified Compatibility

Products	Version
Ultra Cloud Core SMI	2024.04.1.14
Ultra Cloud CDL	1.11.9.1
Ultra Cloud Core UPF	2024.04.0
Ultra Cloud SMF	2024.04.0

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
Event Failure Logs for Service Pods	With this feature, the consistent event failure logs are enhanced to support the Create Bearer, Update Bearer, Delete Bearer, PDN Modify List, and Modify Bearer Command procedures for the service pods.
Rolling Upgrade Optimization for Protocol PFCP Pods	For the protocol (PFCP) pods, Converged Core Gateway introduces a session-level response messages cache at the service pod for handling the retransmitted requests. This optimization helps in reduced session and Call Events Per Second (CEPS) loss during the upgrade procedure.

Behavior Changes

This section covers a brief description of behavior changes introduced in this release.

Behavior Change	Description
Rate Limiting Configuration for S11 GTPC Endpoints	<p>In high-traffic mobile networks, the S11 GTPC endpoint can receive a large number of Create Session Request messages, especially during peak times or in densely populated areas.</p> <p>With Rate Limiting configuration, you can control the flow of incoming Create Session Request messages to the GTPC endpoints. This ensures that the GTPC endpoint can handle high traffic volumes effectively.</p> <p>Previous Behavior: There was no rate limiting functionality for Create Session Requests on S11. This resulted in all requests being accepted, which led to an out-of-memory (OOM) issue.</p> <p>New Behavior: cnSGWc now supports rate limiting for Create Session Requests on S11 with the following configuration:</p> <pre> config instance instance-id 1 endpoint gtp interface s11 overload-control msg-type create-session-request reject-action reject-req rate-limit rate_limit queue-size queue_size reject-threshold threshold_limit pending-request pending_requests exit exit exit exit </pre> <p>Note If the rate limiting configuration is enabled, it will also apply to emergency calls and WPS sessions, potentially causing Create Session Request messages for these calls to be rejected or dropped.</p> <p>This new configuration helps manage high traffic volumes by controlling the number of Create Session Requests that the GTPC endpoint can process at any given time.</p>

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>

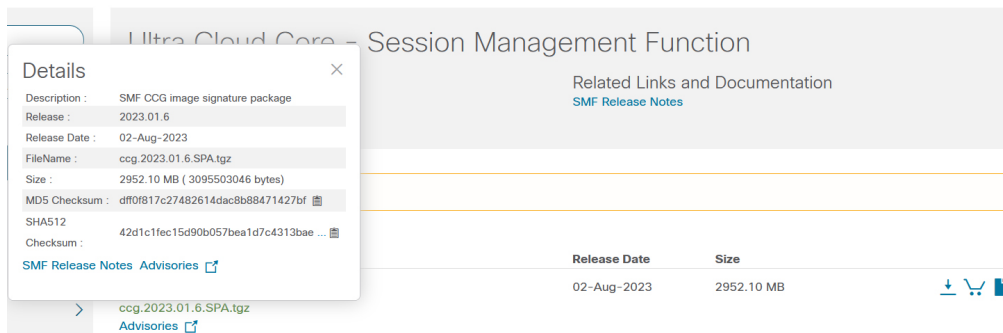
Installation and Upgrade Notes

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.



523482

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: <pre>> certutil.exe -hashfile filename.extension SHA512</pre>
Apple MAC	Open a terminal window and type the following command: <pre>\$ shasum -a 512 filename.extension</pre>
Linux	Open a terminal window and type the following command: <pre>\$ sha512sum filename.extension</pre> <p>OR</p> <pre>\$ shasum -a 512 filename.extension</pre>
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 bug 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
CSCwm90737	sgw service restart at BearerInfo PdnInfo SubscriberInfo SubsContext

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
CSCwk68678	Encrypt all the CLEAR Data in ETCD DB	No
CSCwm05677	UDP endpoints are not Started - 2 0.0.0.0:16002 0.0.0.0:16002 Udp Starting S5E false	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>.