UCC 5G cnSGWc Release Notes, Release 2024.03.0

First Published: 2024-07-31

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	31-Jul-2024
End of Life	EoL	31-Jul-2024
End of Software Maintenance	EoSM	29-Jan-2026
End of Vulnerability and Security Support	EoVSS	29-Jan-2026
Last Date of Support	LDoS	31-Jan-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-2024.03.0.tgz	2024.03.0
NED package	ncs-5.6.8-ccg-nc-2024.03.0 ncs-6.1-ccg-nc-2024.03.0
NSO	6.1.11

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

Note The ccg.<*version*>.SPA.tgz software package is common to both the cnSGWc and SMF 5G Network Functions (NF). The deployment and configuration procedure determines the NF deployment.

Verified Compatability

Products	Version
Ultra Cloud Core SMI	2024.03.1.12
Ultra Cloud CDL	1.11.8.1
Ultra Cloud Core UPF	2024.03.0
Ultra Cloud SMF	2024.03.0

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	cnSGWc provides the following support: • Consistent event failure logs for PDN Setup, Idle or Active, PDN Modify, and PDN Disconnect procedures across pods • Configurable logs at pod type • Inclusion of request and response details in a single-line format The significant volume of unnecessary system-generated logs resulted in increased memory consumption, performance impact, and ineffective management and utilization of logs. To prevent these issues, the consistent error log message format across various pods is introduced for reduced memory consumption, minimized number of log generations by the system, and efficient troubleshooting. The single-line log format display enhances the readability. **Default Setting:** Not Applicable
Notification for UPF-initiated PFCP Association Release	This feature enables cnSGWc to receive notification on UPF-initiated PFCP Association Release Session procedure. This notification indicates to clear the sessions and association simultaneously in UPF and cnSGWc. If the cnSGWc is not notified, the call remains connected until UPF receives the next Session Modify Request from cnSGWc. This leads to loss of subscriber usage reports. Here, the Enhanced PFCP Association Release feature (EPFAR) improves the signalling efficiency and effective handling of usage reports by cnSGWc. **Default Setting:** Disabled – Configuration Required to Enable
UCS C220 M7 Server Qualification	In this release, cnSGWc is functionally qualified on the Cisco UCS C220 M7 server. The Cisco UCS C220 M7 Rack Server is a versatile general-purpose infrastructure and application server. This high-density, 1RU, 2-socket rack server delivers industry-leading performance and efficiency for a wide range of workloads, including virtualization and bare-metal applications.
Validation of Uplink Packets for IP Source Violation	This feature enables cnSGW to detect packets with invalid source IP addresses. The packet detection is done by validating the source IP address against the UE IP address received in the uplink traffic endpoint. cnSGW provides configuration options to either drop or ignore the invalid packets based on the IP Source Violation IE. This feature also stops the immediate TEID reuse for another subscriber, which avoids the wrong subscriber being tapped and reported by LI agencies. This feature enhances the security and privacy of the subscribers by preventing the leakage of their data to unauthorized parties. This feature further reduces the risk of legal and regulatory issues for the service provider by complying with the lawful interception requirements. This feature introduces the new CLI command **ip source-violation [ignore | discard]** in the DNN profile. **Default Setting**: Disabled – Configuration Required to Enable

Behavior Changes

There are no behavior changes in this 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

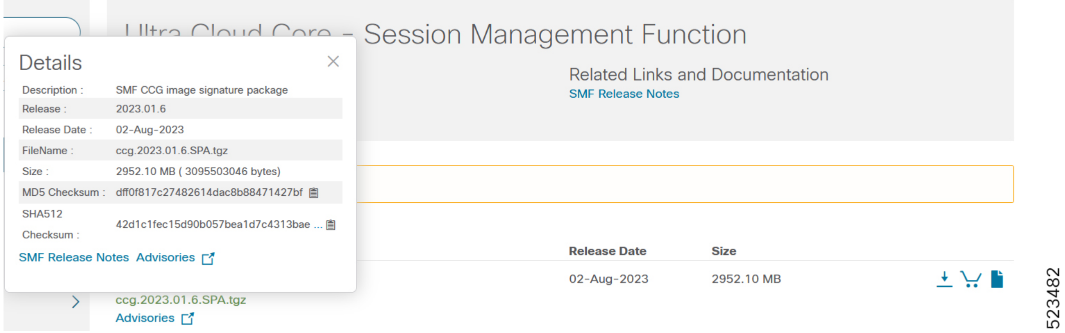
Installation and Upgrade Notes

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.



Ultra Cloud Core – Session Management Function

Details

Description :	SMF CCG image signature package
Release :	2023.01.6
Release Date :	02-Aug-2023
FileName :	ccg.2023.01.6.SPA.tgz
Size :	2952.10 MB (3095503046 bytes)
MD5 Checksum :	dff0f817c27482614dac8b88471427bf
SHA512 Checksum :	42d1c1fec15d90b057bea1d7c4313bae ...

SMF Release Notes Advisories

Related Links and Documentation
SMF Release Notes

	Release Date	Size
ccg.2023.01.6.SPA.tgz Advisories	02-Aug-2023	2952.10 MB

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

There are no open bugs in this software release.

Resolved Bugs for this Release

The following table lists the known bug that is resolved 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.

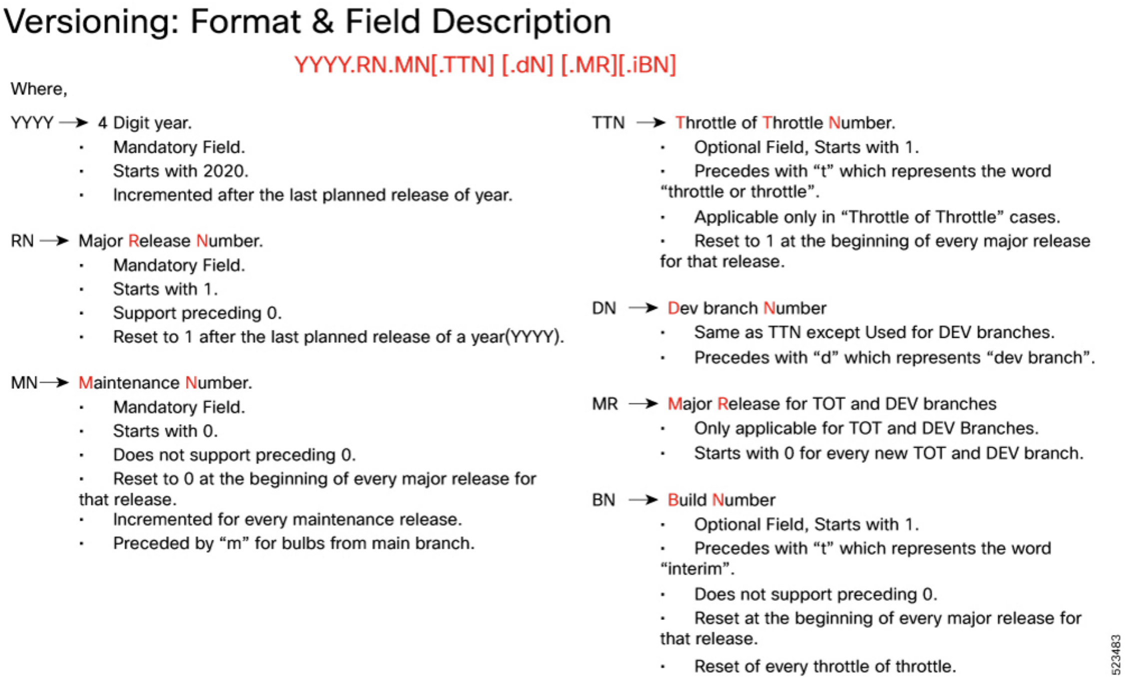
Bug ID	Headline	Behavior Change
CSCwi11657	Evaluation of sgw for HTTP/2 Rapid Reset Attack vulnerability	No

Bug ID	Headline	Behavior Change
CSCwk17311	Once cnSGW receive this MBRsp it will fail the validation. But no MBRsp sent towards S11 side.	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.

Software Packages	Description
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.