



Release Notes for the 5G Converged Core (SMF and cnSGWc), Release 2024.03.7

First Published: 2025-03-19

5G Converged Core Session Management 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
cgc-2024.03.7.SPA.tgz	2024.03.7
NED package	ncs-5.6.8-cgc-nc-2024.03.7 ncs-6.1-cgc-nc-2024.03.7
NSO	5.6.8 6.1.11

Descriptions for the various packages provided with this release are available in the [Release Package Descriptions](#) section.

Verified Compatibility

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 cnSGWc	2024.03.7

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-serving-gateway-function/products-installation-and-configuration-guides-list.html>

What's New in this Release

Features and Enhancements

There are no new features and enhancements introduced in this release.

Behavior Changes

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

Behavior Change	Description
Encoding of QoS Rules in ePCO	<p>Previous Behavior: Initially, the SMF sent two separate "0023H" containers, each with two QoS rules, allowing UEs to process all four rules. In the 2024.03.3 release, this behavior changed to using a single "0023H" container for all four QoS rules. This changed behavior is as per the 3GPP standard.</p> <p>New Behavior: To maintain compatibility with older UEs, which are not compliant with release 16 and experience crashes with the changed behavior, the SMF is reverting to the previous method. It will again send two "0023H" containers, each containing two QoS rules, as in the 2023.04.1 ER release.</p> <p>Customer Impact: This change resolves RTT failures for certain UE devices, ensuring seamless operation and service continuity across all compatible devices.</p>

Related Documentation

For the complete list of documentation available for this release, see <https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-session-management-function/products-installation-and-configuration-guides-list.html>.

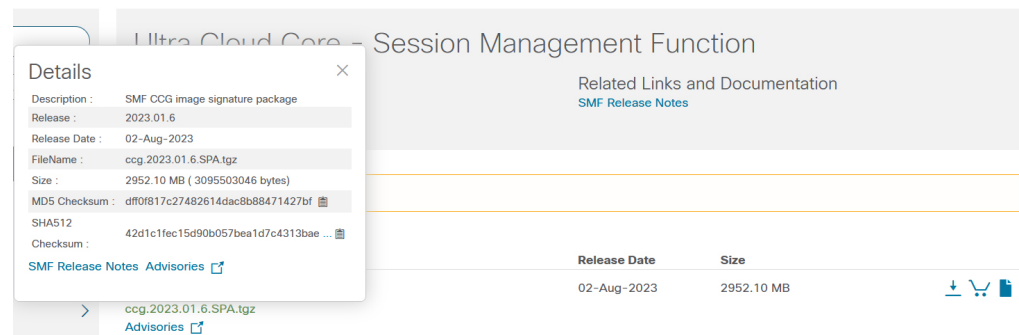
Installation and Upgrade Notes

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 Verification

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: Checksum Calculations per Operating System](#) 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	<p>Open a command line window and type the following command:</p> <pre>> certutil.exe -hashfile filename.extension SHA512</pre>
Apple MAC	<p>Open a terminal window and type the following command:</p> <pre>\$ shasum -a 512 filename.extension</pre>

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

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

SMF software images are signed via x509 certificates. Please view the .README file packaged with the software for information and instructions on how to validate the certificates.

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 bugs that are 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
CSCwo03689	Logs does not display the username/account that fails authentication	No
CSCwo39466	UE decoding problem - SMF sending multiple QOS rules in same container	Yes

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
cgc.<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>-cgc-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>.

