



Release Notes for UCC 5G SMF and cnSGWc, Release 2026.03.2



Contents

Ultra Cloud Core – Session Management and Serving Gateway Function, Release 2026.03.2 3

New software features 3

Changes in behavior 3

Resolved issues 4

Open issues 4

Compatibility 5

Supported software packages 5

Related resources 7

Legal information 7

Ultra Cloud Core - Session Management and Serving Gateway Function, Release 2026.03.2

This Release Notes identifies changes and issues related to the software release of 5G Converged Core Session Management Function (SMF) and Serving Gateway Control Plane Function (cnSGWc).

For more information about Ultra Cloud Core - Session Management Function and Serving Gateway Control Plane Function, see the [Related resources](#) section.

Release lifecycle milestones

The following table provides EoL milestones for Cisco UCC SMF and UCC cnSGWc software:

Table 1. EoL milestone information for UCC SMF and cnSGWc, Release 2026.03.2

Milestone	Date
First Customer Ship (FCS)	23-July-2026
End of Life (EoL)	23-July-2026
End of Software Maintenance (EoSM)	22-Jan-2028
End of Vulnerability and Security Support (EoVSS)	31-Jan-2028
Last Date of Support (LDoS)	31-Jan-2029

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.

New software features

There are no new software features in this specific software release.

Changes in behavior

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

Table 2. Behavior changes for UCC SMF and cnSGWc, Release 2026.03.2

Description	Behavior changes
Optimized service request handling during DLDR collisions [CSCwv93061]	Previous Behavior: When a Service Request was queued while a Downlink Data Report (DLDR) was already activating the N3 interface, the SMF triggered a N3 deactivation and reactivation cycle (if the reactivation CLI was enabled). If N2 Setup Complete is not received during this process, the session could remain in an incomplete state with the N3 interface deactivated. New Behavior: The SMF now manages collisions between Service Requests and DLDR activations. If a Service Request is received before a DLDR-initiated N3 activation is finished, the SMF considers the request already fulfilled. It skips the unnecessary N3 deactivation/reactivation and N2 Setup steps, maintains the active N3 state. Customer Impact: This change prevents PDU sessions from becoming unresponsive or entering a stalled state during these specific race conditions, thereby eliminating associated downlink packet loss.

Description	Behavior changes
Enhanced SBI message priority handling for WPS sessions [CSCwv67253]	Previous Behavior: For transactions involving PFCP message interactions, the transaction priority sometimes overrides the SBI message priority based on the PFCP message priority. As a result, priority-subscriber signaling messages (such as paging/N1N2, N7) were sometimes sent with an incorrect priority. New Behavior: SMF now preserves the SBI priority for SBI interface messages and no longer allows the PFCP priority to override or be applied to SBI interface messages. Customer Impact: SBI priority and PFCP message priority are applied separately, ensuring clear and correct SBI message prioritization for Wireless Priority Services (WPS) sessions. This prevents incorrect priority assignment in subscriber signaling and improves priority handling consistency for WPS traffic.
Handover collision handling during voice bearer creation [CSCwv75684]	Previous Behavior: When a higher-priority handover arrived while the SMF was waiting for the first N4 Session Modification Response, the SMF immediately terminated the voice dedicated-bearer procedure and switched to handover processing without waiting for the UPF response. New Behavior: SMF defers terminating the dedicated-bearer procedure until it receives the first N4 Session Modification Response from the UPF. After processing this response, the SMF then terminates the dedicated-bearer procedure and switches to the higher-priority handover. Customer Impact: Handover processing may experience a brief wait for the pending UPF response instead of starting immediately. This change ensures graceful cleanup of the PFCP leg and prevents stale forwarding rules, which could otherwise cause downlink voice packet loss after handover.

Resolved issues

This table lists the resolved issues in this specific software release.

Note: This software release may contain bug fixes first introduced in other releases. To see additional information, click the bug ID to access the [Cisco Bug Search Tool](#). To search for a documented Cisco product issue, type in the browser: <bug_number> site:cisco.com

Table 3. Resolved issues for UCC SMF and cnSGWc, Release 2026.03.2

Bug ID	Description
CSCwv67253	WPS MP of PFCF need not be reflected at SBI.
CSCwv75684	VoWiFi CBR-LTE HO collision: only UL PDR removed on abort, stale DL PDR
CSCwv93061	DLDR Collision Causes Missing N2 Trigger after Queued Service Request Handling.
CSCwv99022	GTPV2 Peer restart observed in SGWc of Converged Core Gateway.

Open issues

There are no open bugs in this specific software release.

Compatibility

This section lists compatibility information of the Cisco UCC software products that are verified to work with this version of the UCC SMF and and cnSGWc software.

Table 4. Compatibility information for UCC SMF and cnSGWc, Release 2026.03.2

Product	Supported Release
Ultra Cloud Core SMI	2026.03.1.08
Ultra Cloud CDL	2.3.0
Ultra Cloud Core UPF	2026.03.0
Ultra Cloud cnSGWc	2026.03.2

Supported software packages

This section provides information about the release packages associated with UCC SMF and cnSGWc software.

Table 5. Software packages for UCC SMF and cnSGWc, Release 2026.03.2

Software Package	Description	Release
cgc-2026.03.2.SPA.tgz	The SMF and cnSGWc offline release signature package. This package contains the SMF deployment software, NED package, as well as the release signature, certificate, and verification information.	2026.03.2
ncs-6.4.8.3-cgc-nc-1.1.2026.03.2.tar.gz	The NETCONF NED package. This package includes all the yang files that are used for NF configuration.	6.4.8.3
ncs-6.1.14-cgc-nc-1.1.2026.03.2.tar.SPA.tgz	Note that NSO is used for the NED file creation.	6.1.14

Cloud native product version numbering system

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

Figure 1. Cloud native product versioning format and description
Versioning: Format & Field Description

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 "i" 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.

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.

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.

Figure 2. Sample of converged core gateway software image

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 : dff0817c27482614dac8b88471427bf

SHA512 Checksum : 42d1c1fec15d90b057bea1d7c4313bae ...

SMF Release Notes Advisories

cog.2023.01.6.SPA.tgz Advisories

Related Links and Documentation

SMF Release Notes

Release Date	Size
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 the following table and verify that it matches the one provided on the software download page.

To calculate a SHA512 checksum on your local desktop, see this table.

Table 6. Checksum calculations per operating system

Operating System	SHA512 checksum calculation command examples
Microsoft Windows	Open a command line window and type the following command:

Operating System	SHA512 checksum calculation command examples
	> certutil.exe -hashfile <filename.extension> SHA512
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 type 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 not to 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.

Related resources

This table provides key resources and links to the support information and essential documentation for related Ultra Cloud Core (UCC) products.

Table 7. Related resources and additional information

Resource	Link
SMF documentation	Session Management Function
cnSGWc documentation	Serving Gateway Function
SMI documentation	Subscriber Microservices Infrastructure
UPF documentation	User Plane Function
Service request and additional information	Cisco Support

Legal information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2026 Cisco Systems, Inc. All rights reserved.