Release Notes for UCC 5G SMF and cnSGWc, Release 2026.03.5

© 2026 Cisco and/or its affiliates. All rights reserved.

Contents

Ultra Cloud Core – Session Management and Serving Gateway Function, Release 2026.03.5 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

© 2026 Cisco and/or its affiliates. All rights reserved.

Ultra Cloud Core - Session Management and Serving Gateway Function, Release 2026.03.5

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 (cnSGWc), 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 2026.03.5

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 introduced in this release.

Changes in behavior

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

© 2026 Cisco and/or its affiliates. All rights reserved.

Table 2. Behavior changes for UCC SMF and cnSGWc, Release 2026.03.5

Description	Behavior changes
Optimized context retrieval during PDU session setup [CSCwx15023]	**Previous Behavior**: If a Retrieve Request was received while a PDU session was still being established, SMF waited for the setup process to complete before responding. If the PDU session setup was delayed, the MME would time out while waiting for the session context, causing the entire handover process, including other established PDU sessions, to fail. **New Behavior**: When a Retrieve Request arrives while a PDU session setup is in progress, SMF now immediately rejects the request with a "500 - SYSTEM_FAILURE" error. This provides AMF with an immediate response, allowing it to proceed with handover for all other established PDU sessions without being blocked by the pending session. **Customer Impact**: This change improves the reliability of 5G to 4G handovers by preventing a single pending PDU session setup from causing a timeout that fails the entire mobility procedure. While the specific session under establishment may not hand over, all other active sessions will transition successfully.

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 2026.03.5

Bug ID	Description
CSCwx15023	SMF collision handling of PDU RESOURCE SETUP RESPONSE and retrieve sm-context > SMF waits for 10 seconds.
CSCwx30448	WPS Voice call setup failure | 404 in response to N7UN.
CSCww78954	HO cancellation and service request collision results in 403 Errors KPI spike.
CSCww85596	UE stuck due to failure handling for policy Update.
CSCww88466	stopTime and startTime use localtime(JST) with UTC format.
CSCww57469	SMF path-based ingress fails when NF HTTPRoute creates shared Gateway listener without ReferenceGrant.

Open issues

There are no open issues in this specific software release.

© 2026 Cisco and/or its affiliates. All rights reserved.

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 cnSGWc software.

Table 4. Compatibility information for UCC SMF and cnSGWc, Release 2026.03.5

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	2026.03.5

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 2026.03.5

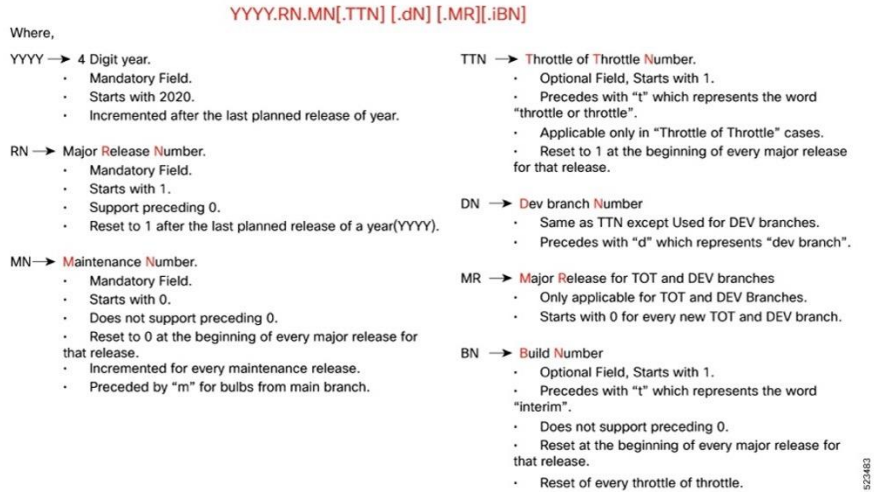
Software Package	Description	Release
ccg-2026.03.5.SPA.tgz	The SMF and cnSGWc offline release signature package. This package contains the SMF deployment software, NED package, as well as the release signature, certificate, and verification information.	2026.03.5
ncs-6.4.8.3-ccg-nc-1.1.2026.03.5.tar.gz	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.	6.4.8.3
ncs-6.1.14-ccg-nc-1.1.2026.03.5.tar.SPA.tgz		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.

© 2026 Cisco and/or its affiliates. All rights reserved.

Figure 1. Cloud native product versioning format and description



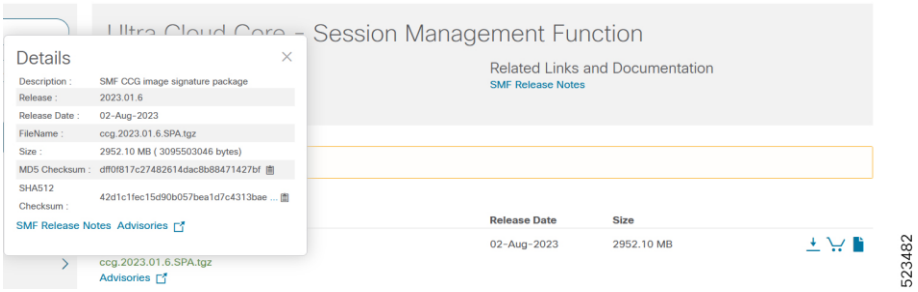
The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research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



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:

© 2026 Cisco and/or its affiliates. All rights reserved.

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.