Release Notes for UCC 5G SMF, Release 2026.02.1

Contents

Ultra Cloud Core - Session Management Function, Release 2026.02.1

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

The key highlights of this release include:

- Subsequent N7 message routing via resource URI: Ensures reliable communication between the SMF and PCF by accurately routing subsequent N7 signaling messages to the correct PCF instance. This provides flexible control to customize routing behaviors based on specific service requirements.
- Simultaneous handling of QCI and rule base change during inter-PLMN handover: Enhances service continuity during network inter-PLMN handover process by efficiently processing QCI and Rulebase changes simultaneously.

For more information about Ultra Cloud Core - Session Management Function, see the Related resources section.

Release lifecycle milestones

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

Table 1. EoL milestone information for UCC SMF, Release 2026.02.1

Milestone	Date
First Customer Ship (FCS)	23-Apr-2026
End of Life (EoL)	23-Apr-2026
End of Software Maintenance (EoSM)	22-Oct-2027
End of Vulnerability and Security Support (EoVSS)	22-Oct-2027
Last Date of Support (LDoS)	31-Oct-2028

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

This section provides a brief description of the new software features introduced in this release.

Table 2. New software features for UCC SMF, Release 2026.02.1

Product impact	Feature	Description
Software Reliability	Subsequent message routing using resource URI on N7 interface	This feature enables the SMF to store the resourceUri received from PCF N7 notifications for each DNN and use it as the destination address for all subsequent N7 signalling messages. By doing so, it ensures requests are routed to the correct PCF instance. The feature also supports dynamic updates to the stored resourceUri upon receiving notifications from a different PCF instance. Granular, per-DNN configuration is provided to allow operators to enable or disable this behaviour based on specific service requirements. Command introduced: **supported-features [n7-resource-uri]** – Configured within the DNN profile, this command activates the use of the N7 resource URI to ensure accurate message routing to the appropriate PCF instance. **Example:** profile dnn dnn_name supported-features [n7-resource-uri] exit **Default Setting:** Disabled – Configuration required to enable.
Software Reliability	Simultaneous handling of QCI and Rule base change during inter-PLMN handover	This feature allows the SMF to process both the attributes simultaneously by splitting the combined N7 update into two internal events, rulebase change event and QCI change event respectively.

Changes in behavior

There are no behavior changes in this specific software release.

Resolved issues

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 Ultra Cloud Core – Session Management Function, Release 2026.02.1

Bug ID	Description
CSCwt35295	PLMN_CH trigger getting armed for inter-RAT HO
CSCwu54894	A mon sub shows a rATType" : 2 in the usedUnitContainer, although a pcap shows the " rATType" : " EUTRA"
CSCwu98822	Revoking of Threshold-hit IP chunk is not working.

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 software.

Table 4. Compatibility information for UCC SMF, Release 2026.02.1

Product	Supported Release
Ultra Cloud Core SMI	2026.02.1.07
Ultra Cloud CDL	2.2.0
Ultra Cloud Core UPF	2026.02.0
Ultra Cloud cnSGWc	2026.02.1

Supported software packages

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

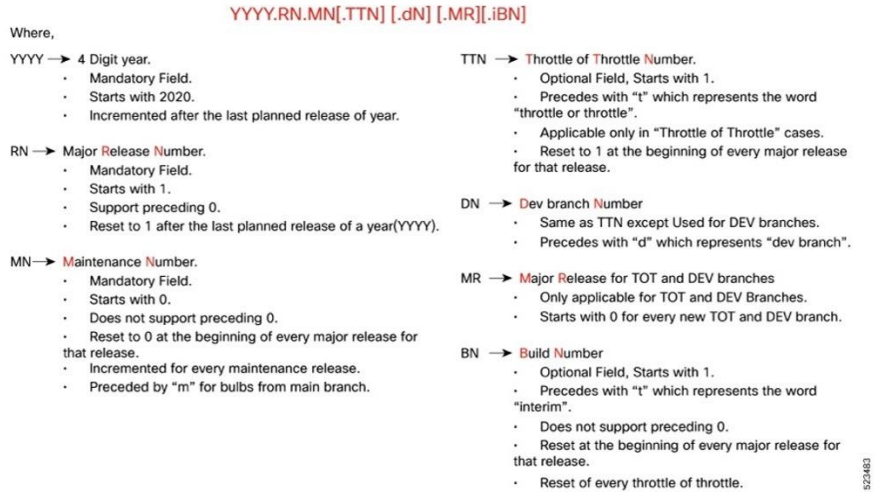
Table 5. Software packages for UCC SMF, Release 2026.02.1

Software Package	Description	Release
ccg-2026.02.1.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.	2026.02.1
ncs-6.4.5-ccg-nc-2026.02.1.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.	6.4.5
ncs-6.1.14-ccg-nc-2026.02.1.tar.gz		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



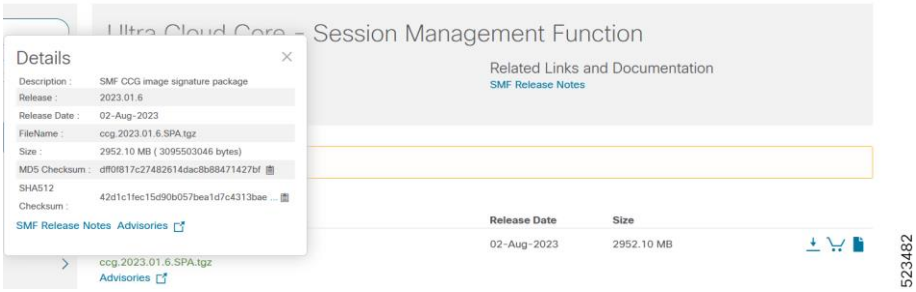
The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research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

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 SMF and other 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

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.