Release Notes for UCC 5G SMF, Release 2026.01.2

Contents

Ultra Cloud Core - Session Management Function, Release 2026.01.2

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:

- Duplicate static IP detection on Attach over Attach PDU sessions: Enables RAT-aware IP conflict detection to prevent session rejections during 4G/5G transitions.
- Enhanced geo-redundant Lawful Interception: Ensures continuous regulatory compliance and data integrity across geographically distributed.
- Seamless 2G/3G and 5G interoperability: Allows legacy 2G/3G systems to work seamlessly with new 5G technology.
- Optimized NRF routing via custom API roots: Gives operators better control over where network traffic is sent, making it easier to manage complex or multi-vendor setups.

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 2026.01.2

Milestone	Date
First Customer Ship (FCS)	30-Jan-2026
End of Life (EoL)	30-Jan-2026
End of Software Maintenance (EoSM)	31-July-2027
End of Vulnerability and Security Support (EoVSS)	31-July-2027
Last Date of Support (LDoS)	31-July-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 2026.01.2

Product impact	Feature	Description
Software reliability	Duplicate static IP detection on Attach over Attach PDU sessions	This feature provides duplicate IP detection to be RAT-aware. The mechanism now restricts conflict detection to the same RAT type, preventing erroneous session rejection when users transition between 4G and 5G sessions. Command introduced: **rat no-match** and **attributes session-type all** – when both these commands are configured in the Event Management policy, the system rejects new session and releases the old session.
Software Reliability	3GPP-compliant Lawful Interception support for geo-redundant deployments	This support enables automatic replication of LI data across geo-redundant. For more information about this feature, contact Cisco account representative.
Software Reliability	2G and 3G session handling with legacy PCF/CHF support	SMF supports 2G and 3G sessions over N7 and N40 interfaces with PCF and CHF. For Release 15 and Release 16 PCF/CHF, the SMF excludes unsupported attributes (for example, RAT Type and ULI) and does not include the UserLocationInfoTime information element when ULI is not present, ensuring backward compatibility.
Software Reliability	3gpp-sbi-target-apiroot header for NRF	The 3GPP-SBI-target-APIroot header lets operators set a target API root URI for registration, deregistration, subscription, unsubscription, update, and discovery messages. SMF includes this header in each HTTP request to NRF, ensuring requests reach the desired destination based on deployment needs. Command introduced: • **profile message-handling nf-type** *nf_type* **{ mh-profile** *mh_profile_name* **{ service name type** *service_name_type* **{ message type [nf-register { header 3gpp-sbi target-apiroot** *api_root_uri* **} | nf-deregister { header 3gpp-sbi-target apiroot** api_root_uri **} | nf-update { header 3gpp-sbi-target-apiroot** *api_root_uri* **} | nf-status-subscribe { header 3gpp-sbi-target-apiroot** *api_root_uri* **} | nf-status unsubscribe { header 3gpp-sbi-target-apiroot** *api_root_uri* **}] } } }** – Used to configure the target API root URI for NF management messages. • **profile message-handling nf-type nf_type { mh-profile** mh_profile_name **{service name type** service_name_type **{message type nf-discover {header 3gpp-sbi target-apiroot** api_root_uri **} } } }**–Used to configure the target API root URI for NF discovery. Default Setting: Disabled – Configuration Required

Changes in behavior

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

Table 3. Behavior changes for UCC SMF, Release 2026.01.2

Description	Behavior changes
Incorrect PLMN_CH trigger in CHF update during inter-RAT HO [CSCwt35295]	**Previous Behavior**: During an inter-RAT handover (HO), the SMF was incorrectly sending a CHF Update with a PLMN_CH trigger to the CHF, even when no actual PLMN change had occurred. **New Behavior**: The PLMN change detection logic has been corrected. The SMF now sends a CHF Update with a PLMN_CH trigger to the CHF only when a verified PLMN change is detected during an inter-RAT HO. **Customer Impact**: This correction eliminates unnecessary signaling to the CHF, leading to improved system efficiency and reduced load on the CHF.

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 4. Resolved issues for UCC SMF, Release 2026.01.2

Bug ID	Description
SMF	
CSCwt01329	GeoPod TriggerGR takes more time when multiple etcd get operation timed-out
CSCwt29933	Add Retry mechanism to etcd Grant during setTTL.
CSCwt35295	PLMN_CH trigger getting armed for inter-RAT HO.
CSCwt39953	Debug message required when N16 update is suppressed.
CSCwt47973	Redirect URL sent from PCF is observed only in the FAR of the access side for 5G calls.
CSCwt51430	ConfigMap with null values seen as <no value> with scale config.
CSCwt53190	Upon session report with zero usage for online RG, CDR drop is not happening.
CSCwt55728	Incorrect BCM in Create PDP Context Response in SMF.
CSCwt68370	SMF does not handle create over create from different RAT (4G to wifi/5G).
IoT	
CSCwt55728	Incorrect BCM in Create PDP Context Response in SMF.

Open issues

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

Note: This software release may contain open bugs first identified 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 5. Open issues for UCC SMF, Release 2026.01.2

Bug ID	Description
IoT	
CSCwt66542	GSN Address format is not correct in Create PDP Context response in SMF.

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 6. Compatibility information for UCC SMF, Release 2026.01.2

Product	Supported Release
Ultra Cloud Core SMI	2026.01.1.i08
Ultra Cloud CDL	2.1
Ultra Cloud Core UPF	2026.01.0
Ultra Cloud cnSGWc	2026.01.2

Supported software packages

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

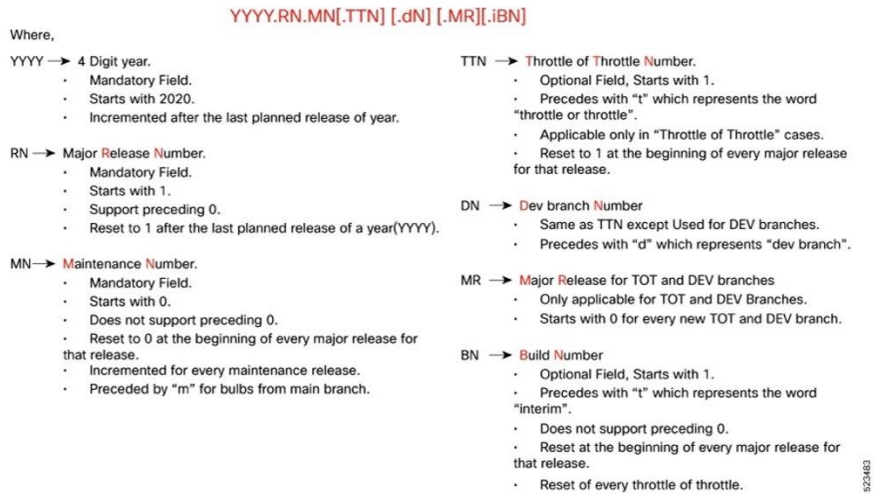
Table 7. Software packages for UCC SMF, Release 2026.01.2

Software Package	Description	Release
ccg-2026.01.2.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.	2026.01.2
ncs-6.4.8.2-ccg-nc-1.1.2026.01.2.tar.SPA.tgz	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.	6.4.8.2
ncs-6.1.14-ccg-nc-1.1.2026.01.2.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.

Figure 1. Cloud native product versioning format and description



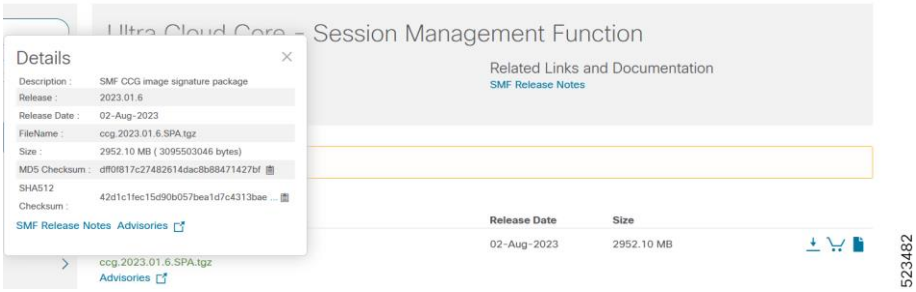
The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research 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 8. 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 cnSGWc and other Ultra Cloud Core (UCC) products.

Table 9. 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.