Release Notes for UCC 5G SMF, Release 2026.01.1

Contents

Ultra Cloud Core – Session Management Function, Release 2026.01.1 3

New software features 3

Changes in behavior 3

Resolved issues 5

Open issues 5

Compatibility 5

Supported software packages 6

Related resources 8

Legal information 8

Ultra Cloud Core - Session Management Function, Release 2026.01.1

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

Release lifecycle milestones

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

Table 1. EoL milestone information for UCC SMF, Release 2026.01.1

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

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.

Table 2. Behavior changes for UCC SMF, Release 2026.01.1

Description	Behavior changes
Handling of conditional or optional IEs and Supportedfeatures in N11/N16 messages [CSCwt28379]	**Previous Behavior**: Conditional or optional IEs were sent with null/empty values in compliance with specification for nsmf-pdusession v.16. Supportedfeatures with 0 value were sent in nsmf-pdusession specification v.15, and mandatory feature flags HOFAIL, ES3XX, and AASN were included in Supportedfeatures in nsmf-pdusession specification v.16. **New Behavior**: To optimize N11 and N16 messaging, the SMF now omits null or empty conditional and optional IEs. • nsmf-pdusession specification v.15: SupportedFeatures are omitted if the value is empty. • Following the nsmf-pdusession v16 specification, the HOFAIL, ES3XX, and AASN flags are now excluded by default. A new CLI parameter has been added to the SMF profile to enable these flags if required: `profile smf > instances > supported-features [hofail es3xx aasn]` • By default, only the VQOS bit is included; DTSSA and ACSCR bits are sent only when explicitly enabled. **Customer Impact**: Null or empty conditional/optional IEs and supportedfeatures with empty values are skipped on N11/N16 messages, and mandatory feature flags are excluded unless explicitly enabled using a new CLI parameter.
SNSSAI encoding in N1 accept message during roaming [CSCwt33699]	**Previous Behavior**: SNSSAI was not encoded properly in N1 accept when both visitor SNSSAI (SST only) and mapped SNSSAI (SST and SD) were sent during roaming scenarios. **New Behavior**: SNSSAI is now encoded correctly in N1 accept with both visitor SNSSAI (SST with or without SD) and mapped SNSSAI (SST with or without SD) during roaming scenarios.
qosFlowDescription IE handling in EPCO/PCO within bearer context of CBR message [CSCwt09790]	**Previous Behavior**: qosFlowDescription IE in EPCO/PCO within Bearer-Context of a CBR message included EPS Bearer Identity (EBI) IE containing the previous call's dedicated bearer EBI. **New Behavior**: qosFlowDescription IE in EPCO/PCO within Bearer-Context of a CBR message no longer includes EBI IE. **Customer Impact**: Prevents semantic errors on the UE caused by EBI IE.
Sequence number handling for MBC-triggered UBR [CSCwt13922]	**Previous Behavior**: When SMF received an MBC without AMBR or Default QoS changes, the resulting UBR was sent directly to sgw-service and did not reuse the MBC's sequence number. **New Behavior**: The MBC-triggered UBR now always uses the same sequence number as the original MBC, regardless of AMBR or Default QoS changes. **Customer Impact**: Ensures consistent sequence number handling, resolving issues where UBR did not reuse the MBC sequence number in certain scenarios.

Description	Behavior changes
NRF subscription request – subscriptionId field handling [CSCwt26067]	**Previous Behavior**: SMF included the subscriptionId field with an empty value (" subscriptionId" : " ") in the NRF subscription creation request (POST /nnrf-nfm/v1/subscriptions). As per 3GPP specification v.29.510, subscriptionId is a read-only attribute generated by NRF in the response and must not be present in the request. **New Behavior**: SMF omits the subscriptionId field from the NRF subscription creation request when it is not set. NRF generates and returns the subscriptionId only in the response, in accordance with 3GPP specification v.29.510. **Customer Impact**: This change aligns the implementation with 3GPP specification 29.510 and ensures standards compliance.

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, Release 2026.01.1

Bug ID	Description
CSCwt28379	Suppressing IE with null values on N16.
CSCwt16290	Static IP allocation fails after GR switchover when new static IP pools and dnn added multiple times.
CSCwt31579	PAPN SMF is not allocating IPAM from dynamic pool and unable to recover the same as well.
CSCwt33699	vSMF does not send correct value of Mapped Slice SST and SD in PDU Session establishment accept.
CSCwt33061	Roaming-flow - AMF-N11 released EBI error log.
CSCwt09790	SMF - EBI in PCO CBR sent wrongly post EPSFB.
CSCwt13922	CC Enable-bypass UBR sent with wrong sequence number
CSCwt26067	SubscriptionId is empty in request to NRF.

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 2026.01.1

Product	Supported Release
Ultra Cloud Core SMI	2026.01.1.08
Ultra Cloud CDL	2.1
Ultra Cloud Core UPF	2026.01.0
Ultra Cloud cnSGWc	2026.01.1

Supported software packages

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

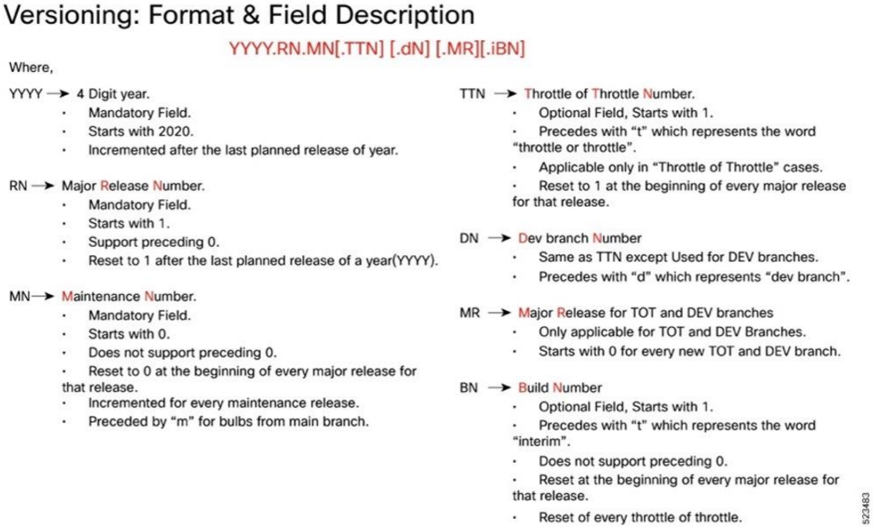
Table 5. Software packages for UCC SMF, Release 2026.01.1

Software Package	Description	Release
ccg-2026.01.1.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.	2026.01.1
ncs-6.4.8.2-ccg-nc-1.1.2026.01.1.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-1.1.2026.01.1.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**



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.

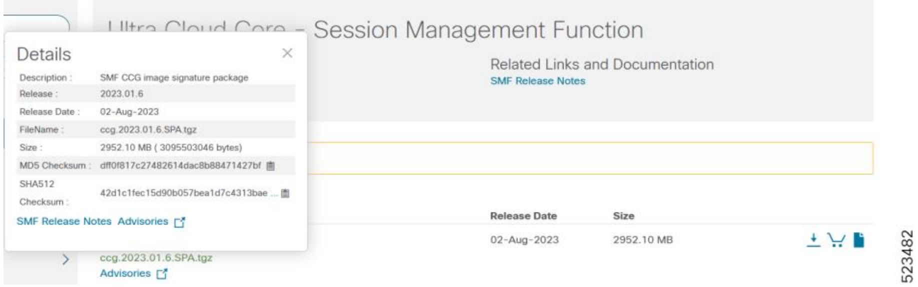
The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research 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 :	dff0f817c27482614dac8b88471427bf
SHA512 Checksum :	42d1c1fec15d90b057bea1d7c4313bae ...

SMF Release Notes Advisories

Related Links and Documentation
SMF Release Notes

	Release Date	Size
ccg.2023.01.6.SPA.tgz Advisories	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: `> 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 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.