Release Notes for UCC 5G SMF, Release 2026.01.3

Contents

Ultra Cloud Core - Session Management Function, Release 2026.01.3

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 2026.01.3

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

Table 2. Behavior changes for UCC SMF, Release 2026.01.3

Description	Behavior changes
Optimized DNS cache retrieval and synchronization [CSCwu05697]	**Previous Behavior**: When executing the show `dns-cache` command, the system retrieved information from all `dns-proxy` instances because the cache entries were not synchronized across the various instances. **New Behavior**: All `dns-proxy` instances are now synchronized. Consequently, the show `dns-cache` command only needs to retrieve information from a single instance to provide a complete view of the cache. **Customer Impact**: This change improves the performance and response time of the show `dns-cache` command, particularly in high-scale environments, by reducing the internal overhead required to aggregate data from multiple instances.

Description	Behavior changes
Updated N4 FAR handling for unreachable UEs [CSCwu08006]	**Previous Behavior**: When AMF responded to an N11N1N2MessageTransfer message with a 504 error and the cause "UE_NOT_REACHABLE", the SMF updated the Forwarding Action Rule (FAR) to the UPF with the flags BUFF=1, NOCP=1, and DROPBU=1. **New Behavior**: When AMF responds with a 504 error ("UE_NOT_REACHABLE"), SMF now updates the FAR to UPF with the flags DROP=1 and DROPBU=1. **Customer Impact**: This change modifies how UPF handles traffic when a UE is in idle mode and unreachable. Instead of attempting to buffer packets, the system will now drop them, preventing unnecessary resource consumption or the delivery of stale data.

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 2026.01.3

Bug ID	Description
CSCwt81979	SMF not updating RAT-TYPE when changed in between HO.
CSCwt85627	Unnecessary EBI Assignment during VoNR Flow multiparty calls.
CSCwu00785	Error logs for specific etcd keys "C.GR.1.etcd.checkpoint" and "C.GR.2.etcd.checkpoint" randomly observed in service pod log.
CSCwu05697	FQDN Resolution issue when dns-proxy Pod Failover to Secondary Node.
CSCwu08006	504 "GATEWAY TIMEOUT" with Cause=UE_NOT_REACHABLE.

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 2026.01.3

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

Product	Supported Release
Ultra Cloud cnSGWc	2026.01.3

Supported software packages

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

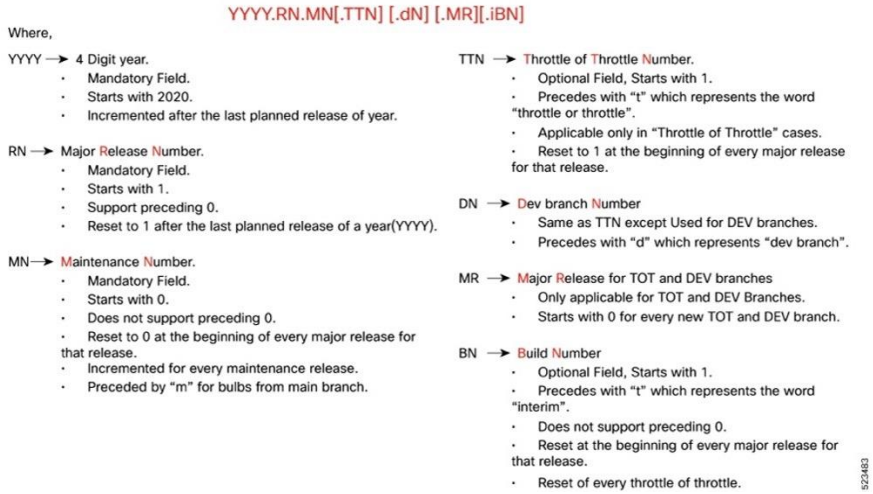
Table 5. Software packages for UCC SMF, Release 2026.01.3

Software Package	Description	Release
ccg-2026.01.3.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.	2026.01.3
ncs-6.4.8.2-ccg-nc-1.1.2026.01.3.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-1.1.2026.01.3.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



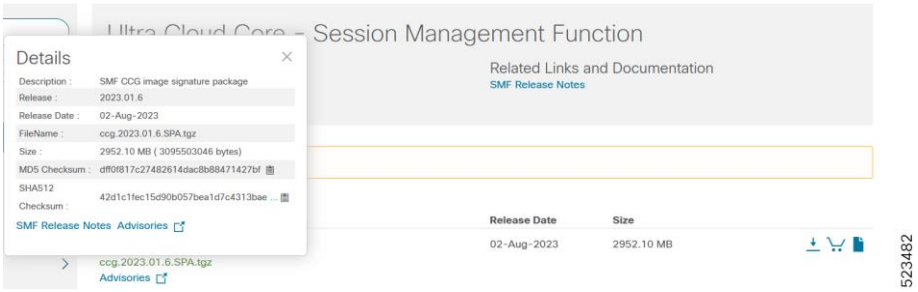
The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research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