Release Notes for UCC 5G SMF, Release 2026.03.0

Contents

Ultra Cloud Core - Session Management Function, Release 2026.03.0

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:

- In-service upgrades and high availability: Enhances system uptime and session continuity by enabling seamless software upgrades and node recovery across multi-server clusters with minimal service disruption.
- ULB integration for GTPC and PFCP traffic: Enhances network reliability and scalability by leveraging the ULB to intelligently distribute control-plane traffic, ensuring consistent performance and optimal resource utilization.
- Common charging IDs in roaming scenarios: Simplifies billing processes by maintaining consistent charging records across different networks, ensuring accurate and unified quota management.
- High uptime and session continuity: Introduces capability that ensures the services remain active and user sessions are preserved during software updates or system recoveries, providing a seamless experience for customers and maintaining high network reliability even at large scales.
- Automated power and performance optimization: Reduces operational costs by automatically optimizing energy consumption while ensuring the network maintains peak performance and service reliability.
- Standardized S-NSSAI mapping for roaming: Improves the reliability of roaming services by ensuring accurate network slice mapping, which prevents session failures and enhances interoperability between different mobile networks.
- Standardized session state reporting: Improves network reliability and 3GPP compliance by ensuring the AMF receives the correct session status during failed connection attempts, enabling better error recovery and more consistent service.
- WPS priority paging enhancement: Guarantees the successful delivery of high-priority services by dynamically updating paging requests to ensure critical calls receive the necessary network precedence.
- SCP model-D resilience: Enhances service continuity and network reliability by enabling seamless failover and optimized routing between critical network functions.

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 2026.03.0

Milestone	Date
First Customer Ship (FCS)	23-July-2026
End of Life (EoL)	23-July-2026

Milestone	Date
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

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

Table 2. New software features for UCC SMF, Release 2026.03.0

Product impact	Feature	Description
Software Reliability	SCP model-D support for SBI binding headers	This release enhances SCP Model-D communication by supporting SBI binding headers for AMF, PCF, and CHF interactions. The SMF stores and uses binding information to improve routing, enable alternate NF selection during failover by SCP.
Software Reliability	ULB integration for GTPC traffic	This release introduces ULB-based ingress and egress routing for GTPC traffic, enabling scalable traffic distribution. The enhancement optimizes control-plane traffic handling and supports efficient scaling in cloud-native deployments.
Software Reliability	Mapped NSSAI support for inbound roaming	vSMF supports inclusion of the mapped S-NSSAI in PDU Session Establishment Accept messages for home-routed inbound roaming sessions. This enhancement ensures 3GPP-compliant NSSAI mapping, improves interoperability between visited and home networks, and prevents session activation failures caused by missing mapped slice information. No additional configuration is required.
Software Reliability	ULB integration for PFCP traffic	This release introduces ULB-based ingress and egress routing for PFCP traffic, enabling scalable traffic distribution. The enhancement optimizes PFCP control-plane traffic handling and supports efficient scaling in cloud-native deployments.
Upgrade	Common charging IDs in roaming scenarios	When a user roams between networks, both the visited and home SMF must use the same Charging ID for the PDU session. This prevents charging data fragmentation, avoids duplicate or mismatched records, and ensures accurate billing and quota management. The Charging ID acts as a session anchor, supporting both online and offline charging in converged deployments.
Upgrade	Upgrade and resiliency for multi-server HA deployment in SMF	This feature helps maintain high uptime and session continuity by scaling the control plane across multi-server clusters. It enables the large-all deployment model to have node resiliency with minimal session loss using in-service software upgrades. This feature allows to upgrade or recover nodes with lesser disruption, supporting ongoing service availability at scale.

Product impact	Feature	Description
Software Reliability	IPM control-plane power optimization	This feature optimizes energy efficiency for the control-plane workloads by automatically tuning BIOS, NIC, and CPU power settings using Intel ® Intelligent Power Management (IPM). This integration ensures the Cisco UCS clusters maintain peak performance while significantly reducing power consumption. This feature enables these savings through the SMI Cluster Manager with simplified, automated configuration.
Software Reliability	Heartbeat skew for NRF interworking	This feature allows the network operators to configure a heartbeat skew to send heartbeat messages earlier than the negotiated interval for NRF interworking. It helps prevent NF suspensions due to network delay, improving reliability of SMF communication with the NRF. Command introduced: **hearbeat interval** seconds **skew** value
Software Reliability	WPS priority paging enhancement	Ensures high-priority (WPS) calls receive correct network priority precedence by enabling the SMF to dynamically update or re-issue paging requests if an elevated priority is detected during an active paging procedure.

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 2026.03.0

Description	Behavior changes
PDU session rejection for barred subscribers [CSCwt85164]	**Previous Behavior**: The SMF continued with PDU session establishment even if Operator Determined Barring (ODB) was active in the subscription data received from the UDM. **New Behavior**: The SMF now correctly enforces Operator Determined Barring. If the SessionManagementSubscriptionData received from the UDM includes the odbPacketServices attribute set to ALL_PACKET_SERVICES, the SMF will reject the PDU session establishment request. **Customer Impact**: This change ensures compliance with 3GPP standards and allows network operators to successfully restrict data services for specific subscribers via ODB, preventing unauthorized PDU session creation.
Handling incorrect display of metrics and EDR status [CSCwu66341]	For a PDU session established in 5G, if SMF receives a Modify Bearer Request while there is no active 5G-to-4G handover, SMF sends the MBR with a failure cause. **Previous Behavior**: The SMF sends the MBR with a failure cause the, however incorrectly pegs the stats " smf_gtpc_msg_stats" and " smf_service_stats" as Success. The EDR is also marked as Success. This displays incorrect status of the metrics and EDR. **New Behavior**: The SMF sends MBR with failure cause and correctly pegs the " smf_gtpc_msg_stats" and " smf_service_stats" metrics as failure with a reason " invalid_rat_type" . The EDR is also marked as Failure. Customer impact: The metrics and EDR status are displayed correctly.

Description	Behavior changes
Change in timing for PDU session type comparison in SMF [CSCws22886]	**Previous Behavior:** When processing a PDU session setup, the SMF compared the UE-requested PDU session type with the DNN-configured PDU session type after receiving the UDM subscription. If the types did not match, the PDU session setup was rejected at this stage. **New Behavior:** The SMF now performs the comparison between the UE-requested PDU session type and the DNN-configured PDU session type before interacting with the UDM. If there is a mismatch, the PDU session setup is rejected immediately, eliminating the need for further UDM interaction. This change streamlines the setup process, reduces resource usage, and prevents avoidable signaling with the UDM when the session types are incompatible.
SMF includes upCnxState=DEACTIVATED in 404 error responses during PDU session reactivation [CSCwj98519]	**Previous Behavior:** For an absent or cleared PDU session, SMF returned a 404 Context Not Found response when it received an SmContextUpdate request with upCnxState=ACTIVATING. The response did not include upCnxState=DEACTIVATED. **New Behavior**: For an absent or cleared PDU session, SMF returns a 404 Context Not Found response when it receives an SmContextUpdate request with upCnxState=ACTIVATING. The response now includes upCnxState=DEACTIVATED. **Customer Impact**: • Improves compliance with 3GPP TS 29.502. • Provides the AMF with the correct PDU session state during failed reactivation attempts.
UE-initiated release request forwarding without 5GSM cause in roaming [CSCwv25316]	**Previous Behavior**: In roaming scenarios, when the vSMF received a UE-initiated release request without a 5GSM cause in the NAS message, it did not forward the UE NAS message to the hSMF. As a result, the hSMF responded with a failure because it expected the UE NAS message to be included during the UE-initiated release procedure, even when the 5GSM cause was absent. **New Behavior**: The vSMF now forwards the UE NAS message to the hSMF for UE-initiated release requests in roaming scenarios regardless of whether the NAS message contains a 5GSM cause. Consequently, the N16 message now includes the UE NAS message even when the 5GSM cause is not present, ensuring interoperability with hSMF implementations that expect the NAS message to be forwarded.
Enforcement of RFC-compliant HTTP/2 callback URL in SBI messages [CSCwv61002]	**Previous Behavior**: The SMF accepted callback URLs from SBI peers where the full absolute URL (including scheme, authority, and path) was carried in the HTTP/2 :path pseudo-header. For example, a full URL like http://192.0.2.10/callbacks/v2/notifyUri/2097157/chargingNotification was accepted in the :path header. **New Behavior**: The SMF now accepts only the RFC-compliant path component in the HTTP/2: path pseudo-header. The host and port must be carried separately in the :authority header. If a request carries a non-conforming: path (i.e., includes scheme and authority), the SMF rejects the request and closes the stream. For example, the accepted :path would be /callbacks/v2/notifyUri/2097157/chargingNotification without the scheme and authority.

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 4. Resolved issues for UCC SMF, Release 2026.03.0

Bug ID	Description
CSCwj98519	SMF does not send upCnxState attribute set to DEACTIVATED during PDU session reactivation.
CSCws22886	Session with PDN type not matching DNN config is successful when UDM fails to respond to subscription fetch.
CSCwt85164	PDU/PDN setup: After subscription response, check ODB status and reject create if enabled.
CSCwt96713	Support for VoNR after location fetch.
CSCwu38206	Discovery response with multiple profiles priority, no capacity.
CSCwu45357	Unexpected URR ID was assigned by the SMF for session-level monitoring, resulting in the UPF not reporting usage for that URR.
CSCwu67051	SMF does DNS query for FQDN resolution of SEPP and SMF instance id from hSMF.
CSCwu68441	SMF sending local query to dns-server.
CSCwu69528	SMF Metric- udmEndpoint not coming in msg_status="accepted" for N10.
CSCwu87707	SMF-monsub - unsent parameters from chf set -1.
CSCwu97511	smf service restart generic.nasEncodePduSessionReleaseRequest.
CSCwv19763	vSMF stalls roaming PDU Session Modification when home-side SEPP rejects the update.
CSCwv25316	vSMF fails to forward NAS message to hSMF when release cause code is missing.
CSCwv40068	vSMF release due to qos flow descriptor missing.

Open 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 5. Open issues for UCC SMF, Release 2026.03.0

Bug ID	Description
CSCwu87850	gtpc s11 pod go routine constantly showing high during longevity run post SMI upgrade.

Bug ID	Description
CSCwv54983	Temporary idle-to-active procedure failures during CCG and SMI rolling upgrade.
CSCwv57461	Multiple ipm-agent pods restarting with exit code 0 during longevity run.
CSCwv57478	S5/S11 CEPS degradation and GTPC-EP pod restart during CCG and SMI rolling upgrade.

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 2026.03.0

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	2026.03.0

Supported software packages

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

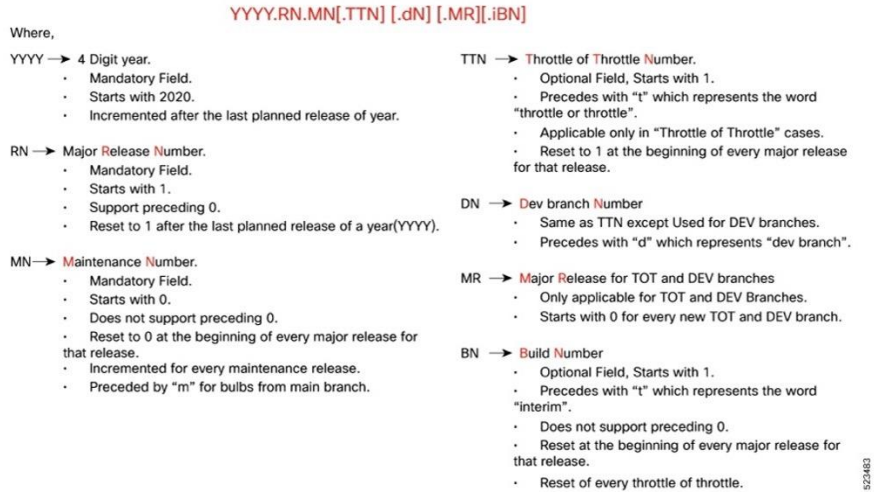
Table 7. Software packages for UCC SMF, Release 2026.03.0

Software Package	Description	Release
ccg-2026.03.0.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.	2026.03.0
ncs-6.4.8.3-ccg-nc-1.1.2026.03.0.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-1.1.2026.03.0.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



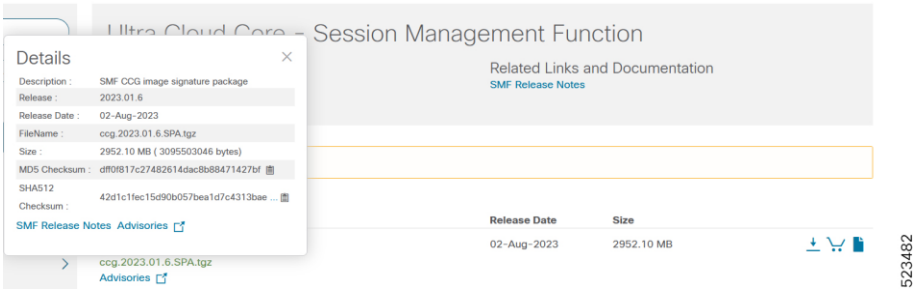
The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research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