Release Notes for UCC 5G SMF and cnSGWc, Release 2026.04.0

© 2026 Cisco and/or its affiliates. All rights reserved.

Contents

Ultra Cloud Core – Session Management and Serving Gateway Function, Release 2026.04.0 3
New software features 4
Changes in behavior 6
Resolved issues 8
Open issues 9
Compatibility 9
Supported software packages 9
Related resources 11
Legal information 11

© 2026 Cisco and/or its affiliates. All rights reserved.

Ultra Cloud Core - Session Management and Serving Gateway Function, Release 2026.04.0

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

The key highlights of this release include:

- Dynamic URI resolution and simplified integration: Automatically resolves relative location URI headers, simplifying integration across PCF and CHF communication paths and improving operational reliability.
- Intelligent NF set failover and session resiliency: Enhances Service-Based Architecture reliability by automatically routing retries within the same NF Set, ensuring session affinity and minimizing service disruptions during PCF failure events.
- Enhanced subscriber-aware NRF discovery: Improves network resource selection and correlation accuracy by dynamically including subscriber identifiers in discovery requests, enabling the NRF to perform more precise, context-aware NF selection.
- Cilium CNI support for SMF and cnSGWc: Enables the deployment of SMF and cnSGWc on Kubernetes clusters using Cilium as the Container Network Interface (CNI) to provide enhanced networking performance and security.
- Operator Determined Barring (ODB) enforcement: Enables service providers to enforce data access restrictions based on subscriber profiles, ensuring seamless policy management and 3GPP compliance across both 4G and 5G networks.
- Enhanced pre-emptive quota management: This feature is designed to improve network efficiency and reduce service latency by optimizing session charging for predefined rules.
- Streamlined license management for SMF: Simplifies the tracking and management of software entitlements, ensuring easier compliance and more efficient resource allocation across the network.
- Resilient N40 charging fallback: Improves session charging reliability by implementing a local quota fallback mechanism, ensuring service continuity during N40 interface failures.
- Optimized network resource management: Improves traffic distribution and ensures balanced use of network resources by enabling more intelligent selection of available service instances.
- Enhanced routing and service reliability: Provides the flexibility to prioritize FQDNs over IP addresses for service discovery, enabling advanced DNS-based load balancing and more resilient network routing.
- Seamless and stable system upgrades: Improves service availability and prevents unnecessary disruptions during maintenance by optimizing how the system manages background tasks while nodes are being updated.
- High-capacity session scaling: Increases total network capacity to support up to 32 million concurrent sessions and enhances resource selection flexibility to meet growing subscriber demands.

© 2026 Cisco and/or its affiliates. All rights reserved.

- Enhanced ULB service optimization: Improves network performance and service continuity by enabling the ULB to handle REST/SBI messages and automate traffic recovery during node transitions.

For more information about Ultra Cloud Core – Session Management Function and Serving Gateway Control Plane Function (cnSGWc), see the Related resources section.

Release lifecycle milestones

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

Table 1. EoL milestone information for UCC SMF and cnSGWc, Release 2026.04.0

Milestone	Date
First Customer Ship (FCS)	5-Nov-2026
End of Life (EoL)	5-Nov-2026
End of Software Maintenance (EoSM)	5-May-2028
End of Vulnerability and Security Support (EoVSS)	5-May-2028
Last Date of Support (LDoS)	31-May-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 and cnSGWc, Release 2026.04.0

Product impact	Feature	Description
Software Reliability	Operator Determined Barring (ODB) of PDU session from UDM	This feature allows SMF to reject PDU Session Establishment (5G) or PDN Connection Setup (4G) requests when the User Data Management (UDM) indicates ODB in the subscriber's subscription data. This ensures compliance with 3GPP standards by using appropriate cause codes for rejection and supports both roaming and non-roaming scenarios.
Software Reliability	Enhanced pre-emptive quota management	This feature is designed to optimize session charging for predefined or static rules.
Software Reliability	Support for 3gpp-Sbi-Correlation-Info in NRF discovery requests	The 3gpp-Sbi-Correlation-Info in HTTP header is included in NRF discovery requests when subscriber identification is available. The header carries the SUPI when SUPI is available; otherwise, it carries the PEI if available. If neither SUPI nor PEI is available, the 3gpp-Sbi-Correlation-Info header is not included in the NRF discovery request.

© 2026 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
Software Reliability	NFSet-aware routing and intelligent failover for PCF	Enables NFSet-aware routing and failover for PCF interactions by utilizing 3gpp-Sbi-Binding headers and NRF discovery data. This ensures retry attempts are contained within the same NF Set, effectively preserving session affinity and improving overall SBA resiliency.
Software Reliability	Smart licensing support for SMF	This feature introduces new entitlement tags to support Smart Licensing for SMF.
Software Reliability	Support for relative location URIs without apiRoot	Supports relative Location URIs received from PCF and CHF in session-specific responses. When a relative URI is received, the complete URI is automatically constructed using the available scheme, FQDN or IP address, and port information. Both absolute and relative Location URIs are supported across direct communication, NRF-based discovery, and SCP-based communication, without requiring additional configuration.
Hardware Reliability	Support for Cilium CNI with SMF and cnSGWc	SMF and cnSGWc are now qualified to operate on Kubernetes clusters using Cilium as the Container Network Interface (CNI). This provides greater flexibility for cloud-native deployments, allowing operators to leverage Cilium's advanced networking and security capabilities.
Software Reliability	Local charging quota for N40 failures	This feature provides a fallback mechanism for N40 charging failures. Commands introduced: • local-quota: Configures local quota under charging profile • max-time-quota-refresh: Configure the threshold for refreshing local quota under charging profile. Default settings: Disabled-Configuration required to Enable.
Software Reliability	Priority attribute support in NRF registration	SMF now supports priority and capacity at Profile level during NRF registration to ensure balanced traffic distribution and prevent instance underutilization. This allows any NF to make informed selection decisions, promoting consistent session anchoring and more efficient resource use across the network.
Software Reliability	FQDN preference for HTTP-based NF discovery	This feature allows SMF to prioritize FQDNs over IP addresses for HTTP-based communication during Network Function (NF) discovery. This supports advanced DNS-based load balancing and geo-redundancy while maintaining standard FQDN preference for HTTPS.
Software Reliability	SMI rolling upgrade and ISSU enhancements	With this release, the Kubernetes descheduler is temporarily disabled during ISSU upgrade to prevent unnecessary pod disruptions while nodes are restarting.
Software Reliability	Session count re-architecture	Introduces an enhanced 26-bit session ID allocation model for converged core deployments, increasing the maximum configurable SMF session capacity to 32 million sessions and enabling UPF selection based on PGW-U or SGW-U IP addresses.

© 2026 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
Software Reliability	2G and 3G connected IRI events	The lawful intercept support for 2G and 3G subscribers delivers connected IRI events and LI_X2 xIRI records for session management procedures the LI_X2 interface. For more information about this feature, contact your Cisco account representative.
Software Reliability	ULB REST/SBI integration and service optimizations	Enhanced ULB support for Converged Core to handle REST/SBI messages, improve resiliency during node changes, and optimize service processing using Flex-Fused mode. The enhancement provides NodeIndex-based routing and Common ID-based affinity for REST/SBI messages, supports resilient traffic redistribution when nodes become unavailable or recover, and reduces internal processing overhead by enabling direct GTP-C and PFCP session-message handling within the service processing context.

Changes in behavior

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

Table 3. Behavior changes for UCC SMF and cnSGWc, Release 2026.04.0

Description	Behavior changes
Refined Incrementing Logic for smf_fail_open_stats [CSCww12760]	**Previous Behavior**: Following a Network Function (NF) failure, the smf_fail_open_stats counter continued to increment for every subsequent procedure associated with that session until a successful NF response was received. This resulted in inflated statistics, as the counter was incremented even by procedures that did not independently trigger a fail-open condition. **New Behavior**: The smf_fail_open_stats counter is now incremented only once per fail-open episode per session. The increment occurs during the first procedure that encounters the fail-open condition; subsequent procedures remaining in the same state do not trigger further increments. The counter only re-arms if the session's fail-open status changes (i.e., a new fail-open condition is added or an existing one is cleared). **Customer Impact**: Reported smf_fail_open_stats values will be lower and more accurate compared to previous releases for identical traffic patterns. While the metric name and labels remain unchanged, It is recommended that you review and potentially recalibrate monitoring dashboards or alert thresholds that were baselined on the previous behavior. No configuration changes are required.
Inclusion of 3GPP correlation headers in NRF discovery [CSCwv02874]	**Previous Behavior**: SMF did not include the 3gpp-sbi-correlation-info HTTP header in NRF Discovery Request messages. **New Behavior**: SMF now includes the 3gpp-sbi-correlation-info header in NRF Discovery Request messages. This header is populated with either the Subscription Permanent Identifier (SUPI) or the Permanent Equipment Identifier (PEI), Depending on the received user identity value for the subscriber. **Customer Impact**: This change improves network observability and troubleshooting. It allows the NRF and other network elements to correlate specific discovery requests with individual user sessions using standard 3GPP identifiers.

© 2026 Cisco and/or its affiliates. All rights reserved.

Description	Behavior changes
Optimized EDR file transfer mechanism [CSCwv61372]	**Previous Behavior**: The edr-monitor pod used kubectl exec based commands to transfer NAS EDR files from the service pods. This method was less efficient and could result in higher resource overhead during large-scale data transfers. **New Behavior**: A new dedicated HTTP endpoint is now available on each service pod to facilitate the retrieval of EDR records. The edr-monitor pod now utilizes a more efficient curl-based transfer method to collect these files, replacing the previous kubectl exec process. **Customer Impact**: This change improves the performance and reliability of EDR file collection. While the internal mechanism for moving files has changed to improve system efficiency, the end-user experience and the final EDR data remain unchanged.
Enhanced logging controls and mandatory asynchronous logging [CSCwv33320]	**Previous Behavior**: Logs were not subject to rate-limiting, and no warnings or confirmation prompts were issued when a user selected high-verbosity log levels (such as debug or trace). Additionally, users had the option to manually enable or disable asynchronous logging. **New Behavior**: Log rate-limiting is now implemented and is active whenever the logs_per_second value is configured to be greater than zero. To optimize system performance, asynchronous logging is now the permanent default and the option to disable it has been removed. Furthermore, the CLI now generates a warning and requires explicit confirmation when a user attempts to commit a change to "debug" or "trace" log levels. New metrics have also been added to track the number of logs dropped due to rate-limiting. **Customer Impact**: These changes improve system stability and performance by preventing logging processes from overwhelming system resources. Operators should monitor the new "dropped logs" metrics to ensure sufficient visibility. Users will also notice a new confirmation step in the CLI when enabling high-verbosity logging.
Separation of bidirectional PCC flows into discrete Uplink and Downlink filters [CSCww32527]	**Previous Behavior**: A bidirectional (BIDI) flow was installed as a single bidirectional packet filter. When a subsequent update changed the flow from bidirectional to either uplink (UL) only or downlink (DL) only, the system generated new packet-filter IDs. because the User Equipment (UE) often retained the original BIDI filter instead of replacing it, a mismatch occurred, leading to one-way audio issues. **New Behavior**: SMF now encodes a bidirectional PCC flow (without a packFiltId) as two separate packet filters: one for the uplink and one for the downlink. This applies to N1 QoS rules, N4 SDF filters, and EPS Traffic Flow Templates (TFTs). When subsequent UL or DL updates occur, SMF modifies these existing filters in place rather than creating new ones. **Customer Impact:** This change resolves intermittent one-way audio issues by ensuring the UE correctly synchronizes and updates its packet filters. Note that there will be a slight increase in the total packet-filter count per QoS rule when using bidirectional flows without explicit IDs.
Downgraded logging level for PCF reconciliation [CSCwu13705]	**Previous Behavior:** The REST-EP pod logged the "Triggering PCF Reconciliation" message at the ERROR level. Because PCF reconciliation is a standard recovery procedure initiated after a PCF failure or restart, these logs were incorrectly perceived as system faults. In large-scale environments, this caused an influx of error logs for every affected subscriber session, often triggering false alarms. **New Behavior**: The "Triggering PCF Reconciliation" log is now categorized at the INFO level. The message content and the functional logic of the reconciliation process remain unchanged. **Customer Impact:** This change reduces log "noise" and prevents unnecessary troubleshooting by removing the "Error" designation from a standard recovery process. Customers should note that these messages will no longer appear if the logging level is set strictly to ERROR. If you use external monitoring tools or automated scripts to track these events, ensure they are updated to look for the message at the INFO level.

© 2026 Cisco and/or its affiliates. All rights reserved.

Description	Behavior changes
Accurate user location reporting during PDU session release [CSCwu52319]	**Previous Behavior**: When AMF sent an SM Context Release request that included updated user location information, SMF ignored this new location. Consequently, SMF sent the previously stored (outdated) location to the PCF in the SM Policy Association termination request. **New Behavior**: SMF now captures and stores the latest user location information received in the SM Context Release request. This updated location is then included in the SM Policy Association termination request sent to the PCF, ensuring the PCF receives the subscriber's actual location at the time of session release. **Customer Impact**: The PCF and downstream systems now receive accurate location data at session termination. This improves the reliability of location-based policy decisions, final usage reporting, and analytics. No configuration changes are required for this update.

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 and cnSGWc, Release 2026.04.0

Bug ID	Description
CSCww02524	cnSGW CDR's showing GPR Charging ID of 0.
CSCww12754	Fail open logging enhancement on N10 interface.
CSCww12760	Post a UDM failure, Fail Open statistics continue to be incremented until a successful UDM response is received.
CSCww19703	Clear subscriber rate along with options not working.
CSCww32527	SMF sends Update Bearer Request with TFT operation " Replace packet filters in existing TFT" , but uses new packet filter IDs instead of replacing the original packet filter IDs.
CSCww49168	clear sub non-volte with reactivation not working properly.
CSCww57469	SMF path-based ingress fails when NF HTTPRoute creates shared Gateway listener without ReferenceGrant.
CSCww78954	403 Errors KPI spike.
CSCww85596	UE stuck due to Failure handling for policy Update.
CSCww88466	stopTime and startTime use localtime(JST) with UTC format.
CSCwx13165	protocol vip-ipv6 and interface rendering issue.

© 2026 Cisco and/or its affiliates. All rights reserved.

Open issues

This table lists the open 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 5. Open issues for UCC SMF and cnSGWc, Release 2026.04.0

Bug ID	Description
CSCwx54981	Local quota allocation is not done as SMF wrongly considers URR sequence number to be out of order.
CSCwx55039	SMF local quota session budget debited without a corresponding N4 Update URR grant during N40 fail-open.

Compatibility

This section lists compatibility information of the Cisco UCC software products that are verified to work with this version of the UCC SMF and cnSGWc software.

Table 6. Compatibility information for UCC SMF and cnSGWc, Release 2026.04.0

Product	Supported Release
Ultra Cloud Core SMI	2026.04.1.10
Ultra Cloud CDL	2026.04.1.10
Ultra Cloud Core UPF	2026.04.0
Ultra Cloud cnSGWc	2026.04.0

Supported software packages

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

Table 7. Software packages for UCC SMF and cnSGWc, Release 2026.04.0

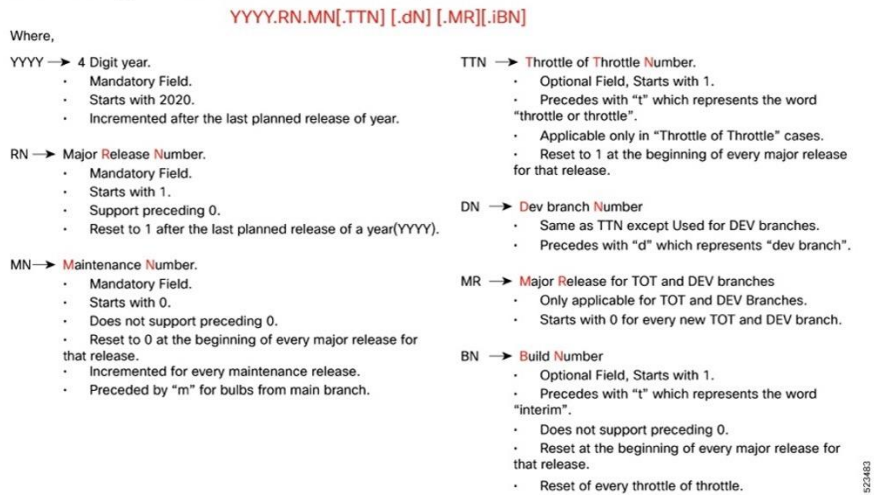
Software Package	Description	Release
ccg-2026.04.0.SPA.tgz	The SMF and cnSGWc offline release signature package. This package contains the SMF deployment software, NED package, as well as the release signature, certificate, and verification information.	2026.04.0
ncs-6.4.15-ccg-nc-1.1.2026.04.0.tar.gz	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.	6.4.15
ncs-6.1.14-ccg-nc-1.1.2026.04.0.tar.gz		6.1.14

© 2026 Cisco and/or its affiliates. All rights reserved.

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



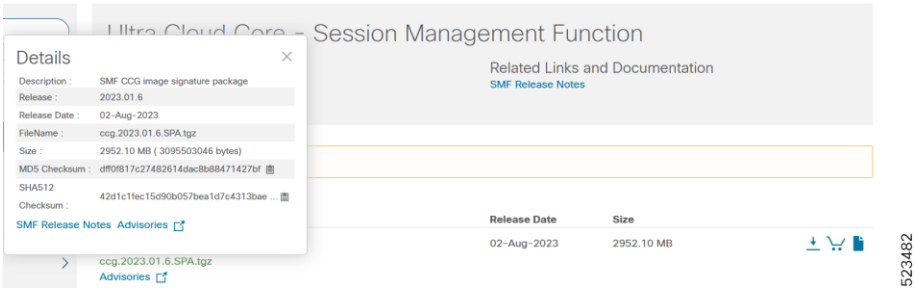
The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research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

© 2026 Cisco and/or its affiliates. All rights reserved.

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 related 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

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.

© 2026 Cisco Systems, Inc. All rights reserved.