UCC 5G SMF Release Notes, Release 2025.01.0

First Published: 2025-01-29

5G Converged Core Session Management Function

Introduction

This Release Notes identifies changes and issues related to this software release.

Release Lifecycle Milestones

Release Lifecycle Milestone	Milestone	Date
First Customer Ship	FCS	31-Jan-2025
End of Life	EoL	31-Jan-2025
End of Software Maintenance	EoSM	1-Aug-2026
End of Vulnerability and Security Support	EoVSS	1-Aug-2026
Last Date of Support	LDoS	31-Aug-2027

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.

Release Package Version Information

Software Packages	Version
ccg-2025.01.0.SPA.tgz	2025.01.0
NED package	ncs-5.6.8-ccg-nc-2025.01.0 ncs-6.1.14-ccg-nc-2025.01.0
NSO	5.6.8 6.1.14

Descriptions for the various packages provided with this release are available in the Release Package Descriptions, on page 9 section.

Verified Compatibility

Products	Version
Ultra Cloud Core SMI	2025.01.1.14
Ultra Cloud CDL	1.12.0
Ultra Cloud Core UPF	2025.01.0
Ultra Cloud cnSGWc	2025.01.0

For information on the Ultra Cloud Core products, refer to the documents for this release available at:

- https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-subscriber-microservices-infrastructure/products-installation-and-configuration-guides-list.html
- https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-user-plane-function/products-installation-and-configuration-guides-list.html
- https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-serving-gateway-function/products-installation-and-configuration-guides-list.html

What's New in this Release

Features and Enhancements

This section covers a brief description of the features and enhancements introduced in this release. It also includes links to detailed documentation, where available.

Feature	Description
SMF	
3GPP LI Support	The 3GPP LI support is introduced to adhere to the 3GPP standards for lawful interception. **Important** This feature is fully qualified in this release. Contact your Cisco account representative for more information.

Feature	Description
Enabling User Plane Confidentiality Protection	The User Plane Confidentiality Protection (UPCP) is a user plane security mechanism to enable ciphering of user data between the UE and the gNB. Based on the UDM subscription data and local configuration, SMF determines the UPCP status for a PDU session during the PDU Session Establishment process. The SMF provides this UP security policy for a PDU session to the gNB during the PDU Session Establishment Procedure. The gNB shall activate the UP confidentiality depending upon the received UP security policy. **Commands Introduced:** • A CLI is introduced to configure the UPCP status locally: **[no] upcp status { required | preferred | not-needed }** • A new CLI is introduced to deactivate the UPCP feature in the SMF profile: **[no] instances** *instance_id* **deactivate-features { upcp | upip }** **Default Settings:** Enabled—Always-on
Enhancement in 5G to 4G Handover Process for Compliance with 3GPP Release 16	During the SM context retrieval, the SMF may send N4 Session modification to UPF to establish the CN tunnel for each EPS bearer. If the UPF is not reachable, it was not returning a proper cause to the AMF. This feature enhances the 5G to 4G handover process by introducing a new response value **UPF_NOT_RESPONDING**, which is sent by SMF if the UPF is unresponsive.
Enhancement in AMF-initiated PDU Session Release for Compliance with 3GPP Release 16	The AMF releases the PDU session upon receiving notification of UE Subscription changes. However, it was not specifying the cause for the PDU session release. This feature enhances the PDU session release process by introducing a new PDU session release cause as **REL_DUE_TO_SUBSCRIPTION_CHANGE** to indicate the PDU session release due to UE subscription changes.
Enhancement in PDU Session Management Process for Compliance with 3GPP Release 16	During any PDU Session Management processes, upon receiving the subsequent N1N2 Message Transfer Request, the AMF cannot determine whether this request was issued by the newly or originally selected SMF. This feature allows the SMF to send **NFInstanceID** in the N1N2 Message Transfer Request, in the existing nfId attribute.
Enhancement in Subscription (POST) process for Compliance with 3GPP Release 16	This feature enhances the Subscription (POST) process by including **reqNfType** attribute, which contains the NF type of the NF Service Consumer. The NRF uses it for authorizing the request.
Event Failure Logs for Session Report procedure	With this feature, the consistent event failure logs are enhanced to support the Session Report procedure for the SMF, PGW, hSMF, and vSMF interfaces.

Feature	Description
FQDN for Peer Communication	SMF allows you to configure FQDN for communicating with NRF and peer NFs. Command introduced: • **fqdn** *fqdn_value* — Used to configure FQDN at endpoint, interface, and NF client level. **Default Setting**: Disabled – Configuration Required • **smf-fqdn** *fqdn_value* — Used to configure SMF's FQDN under SMF profile for each instance. **Default Setting**: Disabled – Configuration Required
Session management based on UDM data change notification	With this feature, SMF terminates or continues the session on receiving the data change notification with REPLACE operation from Unified Data Management (UDM). This feature enables the User Equipment (UE) to avail new subscription changes. This feature introduces a new event **subscription-change** in the existing Event Management Policy configuration. **Command Enhanced**: **policy eventmgmt** *policy_eventmgmt_name***priority** *priority_number* **event** *subscription-change* **Default Setting**: Disabled–Configuration Required
IoT	
FWA Support	SMF validates and supports 4G Fixed Wireless Access (FWA) for separate subscriber groups: those using 4G interfaces (RADIUS and Gz) and those using 5G SBA interfaces (N7 and N40).
SMF Metrics – View Peer Status Through Grafana	With this release, SMF provides the ability to view the connection status of Diameter (Gx and Gy), RADIUS, CGF, and N4 peers using Grafana queries on Grafana cloud. In a single pane view, you can see the peer status across various deployments, aiding in faster identification and resolution of connectivity issues. The Grafana query shows the current status of the peers and also shows the peer status if it is connected or not connected. For more information about SMF metrics, see the UCC 5G SMF Metrics Reference Guide.
Traffic Prioritization based on Flows of Dynamic ADC Rules	SMF uses TosTrafficClass field in dynamic ADC rules from PCRF to prioritize the traffic flows associated with IoT applications during network congestion.

Behavior Changes

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

Behavior Change	Description
SMF	
Enhancement in SMF Behaviour Post the Peer OCI Validity Timeout	**Previous Behavior:** After peer OCI Validity Timeout, if the SMF received an OCI from the peer (SGW, MME) with the same sequence number, it ignored the received OCI. **New Behavior:** After the peer OCI Validity Timeout, the SMF deletes the expired peer OCI and its entry. It uses the new OCI value received from the peer, even if it has the same sequence number.
Enhancement in UPIP Feature to Deactivate Manually	**Previous Behavior:** The operator did not have the flexibility to deactivate the User Plane Integrity Protection feature on SMF manually. **New Behavior:** A new CLI is added under **deactivate-features** under the SMF profile to deactivate the User Plane Integrity Protection feature on SMF manually. **New CLI**: **profile smf** *smf_profile_name* **[no] instances** *instance_id* **deactivate-features upip**
Enhancement in UPIP Failure Handling during Xn Handover Process	**Previous Behavior**: During the Xn handover process, If the target gNB is unable to apply the UPIP, then it was sending Xn handover pathswitch setup failure with cause "CauseRadioNetwork-up-integrity-protection-not-possible" and was releasing the PDU session. SMF was moving the session to idle state. **New Behavior**: During the Xn handover procedure, If the target gNB is unable to apply the UPIP, then it sends pathswitch setup failure response with radio network cause as “up-integrity-protection-not-possible" to SMF and releases the PDU session. Based on the target gNB’s failure response, SMF also releases the session.
Support for Visitor LBO scenario in UPIP Implementation	**Previous Behavior**: The SMF did not support the roaming scenarios for UPIP implementation. **New Behavior**: As part of this release, the SMF supports Visitor Local Break-Out scenario in the roaming cases. For Visitor LBO scenario, the UPIP implementation works the same as the homer scenario. However, during the UPIP status negotiation SMF prioritizes the local configuration over the UPIP status received from the UDM. **Customer Impact**: Due to this enhancement, the operator can enable UPIP for Visitor LBO scenario.
IoT	

Behavior Change	Description
Increase max limit for rate of clearing subscribers	**Previous Behavior:** The maximum limit for the rate of clearing the subscribers using **clear subscriber nf-service smf rate** *<rate_val>* CLI command is 500. **New Behavior:** The maximum limit for the rate of clearing subscribers is increased to 1500. Thus, now all the subscribers can be cleared at the maximum rate value of 1500 using the **clear subscriber nf-service smf rate** *<rate_val>* CLI command. **Customer Impact:** You can clear the subscribers at a higher rate which help in scenarios where the system has huge number of sessions.

Related Documentation

For the complete list of documentation available for this release, see https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-session-management-function/products-installation-and-configuration-guides-list.html.

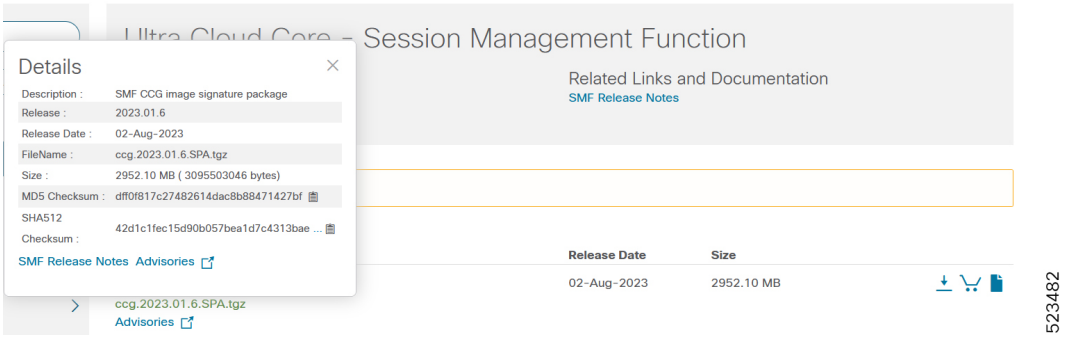
Installation and Upgrade Notes

This Release Note does not contain general installation and upgrade instructions. Refer to the existing installation documentation for specific installation and upgrade considerations.

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.



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 Table 1 and verify that it matches either the one provided on the software download page.

To calculate a SHA512 checksum on your local desktop, refer to the table below.

Table 1: 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 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 to not 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.

Open Bugs for this Release

The following table lists the open bug in this specific software release.

Note This software release may contain open bugs first identified in other releases. Additional information for all open bugs for this release are available in the Cisco Bug Search Tool.

Bug ID	Headline
CSCwn61822	fqdn update in offline mode makes SMF discoverable again on the NRF

Bug ID	Headline
CSCwn66612	service pod restart not complete for about 20 mins
CSCwn82914	Enable and disable camp-on LI tap gives error "Unable to do LI Tap" and "LI Tap Disable Error"

Resolved Bugs for this Release

The following table lists the resolved bugs in this specific software release.

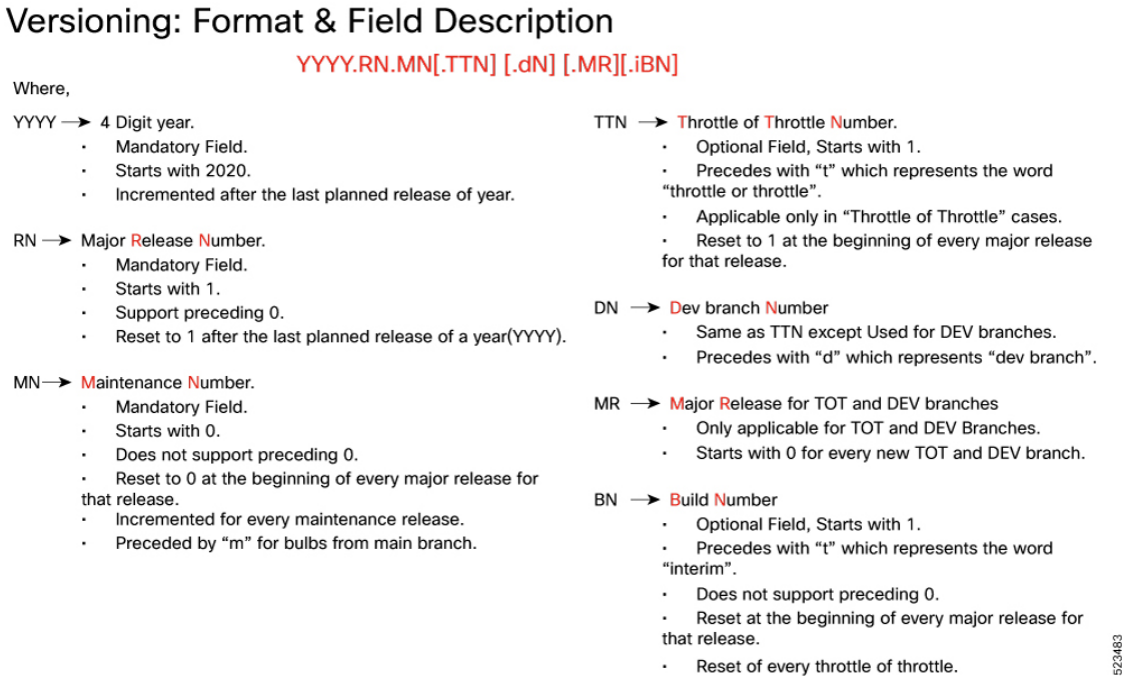
Note This software release may contain bug fixes first introduced in other releases. Additional information for all resolved bugs for this release are available in the Cisco Bug Search Tool.

Bug ID	Headline	Behavior Change
SMF		
CSCwn00894	Active LI tap is not working on SMF post upgrade from old build	No
CSCwn14845	Xn_handover procedures failed without a reason label being pegged	No
CSCwn15086	delete_bearer_command, Attempted!=(Success+Failure)- issue with smf_servce metrics	No
CSCwn17969	Addition of new IPv4 prefix-range on existing pool not Working	No
CSCwn24482	When subscribers cleared on UPF with EPFAR, IP Hold-timer is not proper for subscriber	No
CSCwn33214	GR switchback results in GR Instance detecting false overload and throttling happens for 10 mins	No
CSCwn71445	Rejects activateTask w/x2&x3 when createDest DID1 carries X2Only & DID2 is with X3only	No
IoT		
CSCwk82318	clear sub CLI did not clear all active sessions	Yes
CSCwm73549	show peers all interfaceName Gz not showing all peers on dynamic config change	No
CSCwm86970	Rolling Upgrade Async/SendNotification support validation for IOT	No

Operator Notes

Cloud Native Product Version Numbering System

The show helm list command displays detailed information about the version of the cloud native product currently deployed.



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.

Release Package Descriptions

The following table provides descriptions for the packages that are available with this release.

Table 2: Release Package Information

Software Packages	Description
ccg.<version>.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.
ncs-<nso_version>-ccg-nc-<version>.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.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, refer to https://www.cisco.com/c/en/us/support/index.html.