UCC 5G SMF Release Notes, Release 2024.03.0

First Published: 2024-07-31

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-Jul-2024
End of Life	EoL	31-Jul-2024
End of Software Maintenance	EoSM	29-Jan-2026
End of Vulnerability and Security Support	EoVSS	29-Jan-2026
Last Date of Support	LDoS	31-Jan-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-2024.03.0.SPA.tgz	2024.03.0
NED package	ncs-5.6.8-ccg-nc-2024.03.0 ncs-6.1-ccg-nc-2024.03.0
NSO	6.1.11

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

Verified Compatibility

Products	Version
Ultra Cloud Core SMI	2024.03.1.12

Products	Version
Ultra Cloud CDL	1.11.8.1
Ultra Cloud Core UPF	2024.03.0
Ultra Cloud cnSGWc	2024.03.0

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	
Configuration-based Control of Subscription Notification with Immediate Report Indication on N10 Interface	With the "immediateReport" attribute enabled on UDM, the SMF ignores the UDM subscription fetch message and continues with the Subscription Notification Request, in which Subscription Management Data is received in the Subscription Notification Response. With this controlled UDM notification subscription with the immediate report indication, the interactions between SMF and UDM over the N10 interface are minimized during the 4G, 5G, and Wi-Fi attach procedures and hence prevents message overload and failures. This feature introduces the new CLI command **subscription notify-immediate** in the DNN profile. **Default Setting:** Disabled – Configuration Required
Event Failure Logs for Release procedure	With this feature, the consistent event failure logs are enhanced to support the Release procedure for SMF, 4G, and hSMF interfaces. **Default Setting:** Not Applicable

Feature	Description
N3IWF Enhancement	Following are the additional enhancements to the N3IWF for the seamless communication between the Wi-Fi network and the cellular network. • UE-initiated Service Request through N3IWF • Wi-Fi to NR Handover (HO) through N3IWF • NR to N3IWF Wi-Fi HO • UE-initiated idle mode entry and exit procedure • Voice or Video Call Over Wi-Fi with N3IWF and HO support with Active Bearer. SMF also supports Evolved Packet System (EPS) fallback during handover. • Handling of RAT Type for N3IWF Sessions
UCS C220 M7 Server Qualification	In this release, SMF is functionally qualified on the Cisco UCS C220 M7 server. The Cisco UCS C220 M7 Rack Server is a versatile general-purpose infrastructure and application server. This high-density, 1RU, 2-socket rack server delivers industry-leading performance and efficiency for a wide range of workloads, including virtualization and bare-metal applications.
UE IP Address Hold and Reuse Functionality	This feature allows SMF to allocate the same IP address and session ID to a user session if the user reattaches within a configurable session hold timer after session release. This improves the user experience and reduces the IP address exhaustion in scenarios where users frequently attach and detach. **Important** This feature is not fully validated and qualified in this release. Contact your Cisco account representative for more information. **Command introduced**: **session-hold duration** in Converged Core profile and DNN profile configurations. **Default Setting:** Disabled – Configuration Required
Mobile IoT	
Indication for UPF-initiated PFCP Association Release	This feature enables SMF to receive notification on UPF-initiated PFCP Association Release procedure. This notification indicates to clear the sessions and association simultaneously in UPF and SMF. If the SMF is not notified, the call remains connected until UPF receives the next Session Modify Request from the SMF. This leads to loss of subscriber usage reports. Here, the Enhanced PFCP Association Release (EPFAR) feature improves the signalling efficiency and effective handling of usage reports by SMF. **Default Setting:** Disabled – Configuration Required to Enable

Feature	Description
Modification of QCI, ARP, and Online/Offline Charging Attributes	With this release, SMF supports modification of these additional AVPs included in the dynamic ADC rule: • QCI • ARP • Online • Offline These modifications allow the service providers to classify the traffic more efficiently.
Rolling Upgrade Optimization for Endpoint Pods	SMF provides the rolling upgrade optimization support for the following pods: • RADIUS endpoint pod • Diameter endpoint pod • UDP proxy pod • GTPP endpoint pod This optimization is an enhancement to the existing optimization. This feature uses the existing CLI command **supported-features [app-rx-retx-cache | app-tx-retx | rolling-upgrade-all | rolling-upgrade-enhancement-infra]** in the converged core profile.
UCS C220 M6 Server Performance and Scalability	With this release, the SMF (with Legacy Interfaces) was tested and validated for 7 million sessions scale for IoT use cases using the M6 based UCS systems with published call model including Modeled CEPS and DNN/IP pool configuration. To improve the scalability, SMF also provides new configuration options at GR instance level to • enable sharding on IPAM cache data using the CLI command **data-sharding num-shards** *ipam_data_shards*. • disable chunk throttling using the CLI command **chunk-throttling false**.

Behavior Changes

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

Behavior Change	Description
AVP Validation for Call Processing in Gx and Gy Endpoints	**Previous Behavior**: SMF did not validate the presence and values of the mandatory AVPs used for call processing. **New Behavior**: SMF verifies that the mandatory base AVPs are present and have valid values for the AVPs. If the validation fails, SMF informs service with action as terminate and sub-action as with-term-req for both Gx and Gy.

Behavior Change	Description
Change in RAT Type Validation for N3IWF Sessions	**Previous Behavior**: SMF used to process the PDU session establishment request received for N3IWF-based sessions with RAT type set to NR. **New Behavior**: SMF now rejects PDU session establishment requests for N3IWF-based sessions with RAT type set to NR. SMF processes the requests only if the RAT type is set to WLAN. **Customer Impact**: You might observe call failure due to the rejection of PDU session establishment request for N3IWF sessions with NR RAT type.
Changes to Naming of usedUnitContainer Attribute on N40	**Previous Behavior**: The attribute "usedUnitContainer" was sent with upper case "UsedUnitContainer" when 3GPP release 16 (16.8.1) version was configured for N40 interface on SMF. **New Behavior**: The case of the usedUnitContainer attribute on N40 interface changes when 3GPP release 16 is activated at SMF. It becomes lowercase "usedUnitContainer" instead of uppercase "UsedUnitContainer". **Customer Impact**: For each 3GPP release version, handle N40 messages based on the case change.
Generate Pod Logs in JSON Format	**Previous Behavior**: SMF did not have functionality to generate pod logs in JSON format. However, this functionality was present in the CDL application. **New Behavior**: SMF can now generate pod logs in JSON format using the **logging json-logging [application | monitor-subscriber | transaction]** CLI command. Once this feature is activated, all SMF-related application pods begin generating logs in JSON for the selected log types.
Managing 3gpp-Sbi-Discovery-service-names IE in SCP Header	**Previous Behavior**: SMF does not send 3gpp-Sbi-Discovery-service-names IE in the SCP header. **New Behavior**: SMF lets you manage the inclusion of 3gpp-Sbi-Discovery-service-names IE in the SCP header. This IE can be made conditional by using a new CLI command **discovery-params [service-names]** in SCP network element profile. **Customer Impact**: If you are downgrading SMF, make sure you first disable this CLI configuration. If this CLI command is configured after the upgrade, you will observe that only the new sessions will include the discovery service names as one of the headers in SCP.

Behavior Change	Description
N10 Registration during Wi-Fi to 5G Handover	**Previous Behavior**: N10 registration did not occur during Wi-Fi to 5G handover. **New Behavior**: If UDM registration was skipped during Wi-Fi attach, SMF tries to register with UDM again during Wi-Fi to 5G handover. Note that this behavior change is observed from 2024.02 release.
NF Discovery through SUPI Query Parameter	**Previous Behavior**: SMF didn't have the capability to discover the peer NFs based on the SUPI query parameter. **New Behavior**: SMF allows you to additionally configure SUPI as the query parameter to discover the peer NF profile. Use the **query-params** CLI command in the respective **NF client profile** configuration mode. For more information on the command, see the UCC 5G SMF CLI Command Reference.
PDRs in N4 Modification Request during Dedicated Bearer Deletion	When inter-plmn-ho configuration is enabled for a user with VoWi-Fi call and dedicated flow, the Wi-Fi to NR handover begins. If a flow failure is observed during this handover, SMF performs the EPS fallback and subsequently removes the Packet Detection Rules (PDRs) for the failed flows. **Previous Behavior**: In this scenario, when a peer NF triggers dedicated bearer deletion after EPS fallback, SMF sends the previously deleted PDRs in the N4 modification request. **New Behavior**: When the peer NF triggers dedicated bearer deletion, SMF no longer sends the deleted PDRs in the N4 modification request.
Quota Management for Online URRs in CCA Messages	**Previous Behavior**: SMF used to send the maximum quota to UPF for all online URRs if FHT with CONTINUE action and NONE/UNKNOWN sub-action was received in CCA-I message. **New Behavior**: SMF now relays the maximum quota for online URRs only when FHT with action CONTINUE and Sub-action NONE/UNKNOWN is received in Gy CCA-U. SMF disables the Gy online charging for the session if the corresponding FHT action is set to CONTINUE in Gy CCA-I.
Retransmission of Create Session Request Response	**Previous Behavior**: If the SMF received the retransmitted Create Session Request before the Create Session Response, then SMF dropped the retransmitted request. **New Behavior**: With the rolling updates, the Create Session Response to the retransmitted Create Session Request is sent only if the SMF receives the Create Session Request before the Create Session Response.

Behavior Change	Description
Roaming-status Configuration and Inter-PLMN Roaming Handovers	**Previous Behavior**: Inter-PLMN roaming handovers were successful even if roaming-status was configured in operator policy. **New Behavior**: The inter-PLMN roaming handovers may not work as expected if roaming-status is specified in the operator policy. PLMNs decide the roaming status. Use the roaming-status configuration to override the status determined by PLMNs only in rare situations. **Customer Impact**: The success rate of inter-PLMN roaming call flows may be affected by the roaming-status configuration.
SMF Disconnect Reason Statistics for Invalid Release Requests	**Previous Behavior**: Disconnect reason statistics (smf_disconnect_stats) were pegged even when network- or UE-initiated release request has failed for the sessions which were not present or in different RAT type. **New Behavior**: When the release requests fail with either session not exist or session in different RAT type, the SMF disconnect reason statistics do not increase.
UE Location Validation for Idle Mode Entry and Exit Procedures	**Previous Behavior**: SMF does not validate the UE location against the received RAT type or the RAT type available in SMF as part of PDU session context. **New Behavior**: SMF validates the UE location against the received RAT type or the RAT type in the PDU session context. SMF rejects the Idle Mode (IM) procedure if there is a mismatch during the validation.
Updated "show subscriber" CLI Output for Full Database Record Update	**Previous Behavior**: Any change to the subscriber parameters resulted in full db record update. The **show subscriber** CLI command displayed old parameter values as the flagdb record was not reset. **New Behavior**: Whenever the subscriber parameters change and the full db record gets updated, the **show subscriber** CLI shows the updated parameter values as the flag db record is reset now.
Updated Gaumi IE Encoding as per 3GPP Release 16.0	**Previous Behavior**: The plmnId within the Guami IE was encoded wrongly on the N7 interface. The incorrect Guami encoding caused the interoperability issue. **New Behavior**: The plmnId is correctly encoded as plmnIdNid type. Now, the Guami encoding is corrected to resolve the interoperability issue and complies with the 3GPP Release 16 and above specifications.

Behavior Change	Description
Validation of APN String in 4G Attach Requests	**Previous Behavior**: For 4G attach requests received at cnSGWc, SMF, or cnPGWc, there was no validation being done for the allowed characters in the APN string. **New Behavior**: SMF validates the APN string included in the 4G attach requests. If the APN string contains any characters other than ASCII printable characters (33-126), the attach request gets rejected with a cause "Missing or unknown APN (78)".
V-SMF Update Response for the H-SMF-initiated PDU Modification Procedure	**Previous Behavior**: For the H-SMF-initiated PDU Modification procedure, V-SMF sent the N1 N2 Transfer Request to AMF. In the N1 N2 Transfer Response timeout, V-SMF used to send the Update Response to H-SMF. **New Behavior**: For the H-SMF-initiated PDU Modification procedure, V-SMF sends the N1 N2 Transfer Request to AMF. In case of the N1 N2 Transfer Response timeout, V-SMF sends the Update Failure Response with the "PeerNotResponding" cause and "HTTP_STATUS_CODE_504_GATEWAY_TIMEOUT" cause code to H-SMF.

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.

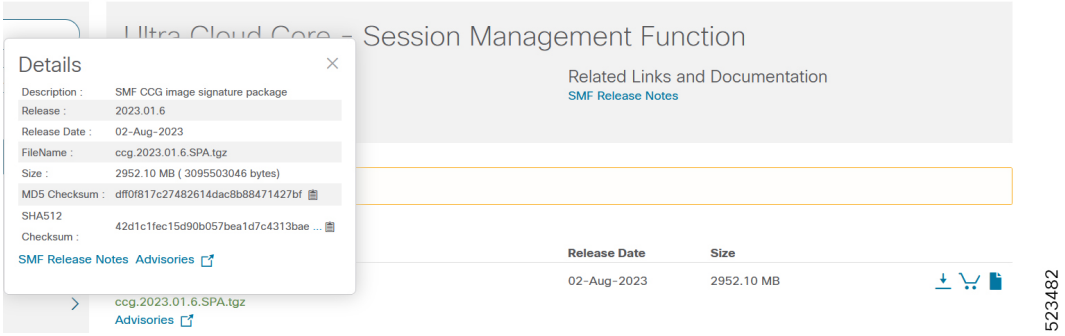
Installation and Upgrade Notes

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 Verification

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: Checksum Calculations per Operating System 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 bugs 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
CSCwk65884	SMF-LI : Encrypt all the CALEA Data in ETCD DB
CSCwk71020	IP ReUse fails for reattaches (500 v4v6_make/break) and these IPs becomes stale entries in IPAM
CSCwk71127	With ~420k calls ID Deallocation Failed with error couldn't identify the ID Handle

Resolved Bugs for this Release

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

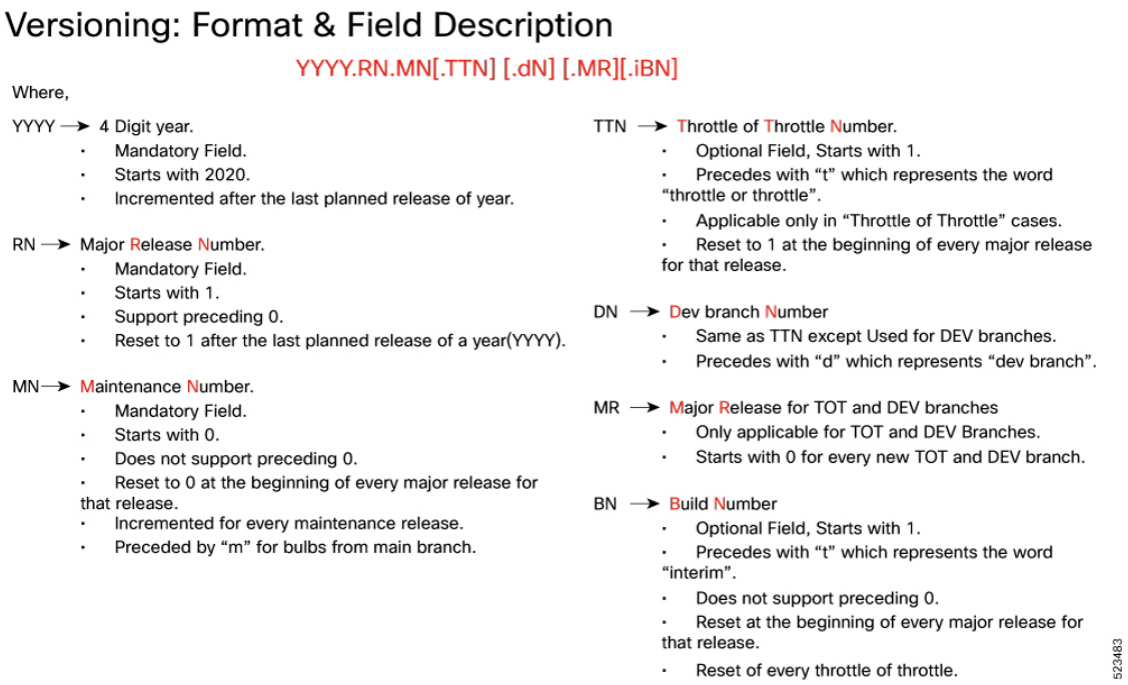
Bug ID	Headline	Behavior Change
CSCwh88576	Evaluation of smf for HTTP/2 Rapid Reset Attack vulnerability	No
CSCwj56131	SMF - Accounting interim request not triggered when CHF is down	No
CSCwj59562	SMF is keeping a PCSCF MW IP in failed list which is not even configured in the system	No
CSCwj71200	SMF isn't updating GateStatus on N4 when there is change in TFT along with FlowStatus from PCF	No
CSCwj71969	SMF- 4G to 5G Handover abort due to Release from AMF - not cleaning up PDRs	Yes
CSCwj75235	Routes are not advertised when there are logical smfs	No
CSCwj77282	SMF: R16 Guami encoding wrongly in N7 interface	Yes
CSCwj81934	SMF P4: UDM NRF discovery by SUPI	Yes

Bug ID	Headline	Behavior Change
CSCwj94079	GR pod did not take correct role (instance-1) info after SMI upgrade,and was stuck in INIT state	No
CSCwk07393	SMF Rest-ep Leader fails to send NRF HB after K8-M1-1 node HW failure	No
CSCwk07395	Edr sftp transfer is appending the same Tx file	No
CSCwk15822	Stale TEID in shortcircuit MBResp post GR switchback	No
CSCwk17411	CHF - 3GPP 32.291 attribute usedUnitContainer (lowercase u) instead of UsedUnitContainer	Yes
CSCwk40075	SMF Emergency call fails SMF with 3GPP September21 compliance for N7, works with June19 compliance	No
CSCwk47954	3gpp-Sbi-Discovery-service-name missing in header	Yes
CSCwk48422	When more than one restart happens on all 3 ETCDs, backup data like Li Taps fail to get loaded	No
CSCwk57817	Mismatch in ip chunks between SMF and UPF	No
CSCwk74710	Ops center confd logs print user values like supi, gpsi and event id for lawful tap	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.