UCC 5G SMF Release Notes, Release 2024.04.0

First Published: 2024-10-25

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	30-Oct-2024
End of Life	EoL	30-Oct-2024
End of Software Maintenance	EoSM	30-Apr-2026
End of Vulnerability and Security Support	EoVSS	30-Apr-2026
Last Date of Support	LDoS	30-Apr-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-2024.04.0.SPA.tgz	2024.04.0
NED package	ncs-5.6.8-ccg-nc-2024.04.0 ncs-6.1.12-ccg-nc-2024.04.0
NSO	5.6.8 6.1.12

Descriptions for the various packages provided with this release are available in the Release Package Descriptions, on page 10 section.

Verified Compatibility

Products	Version
Ultra Cloud Core SMI	2024.04.1.14
Ultra Cloud CDL	1.11.9.1
Ultra Cloud Core UPF	2024.04.0
Ultra Cloud cnSGWc	2024.04.0

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 not fully qualified in this release. Contact your Cisco account representative for more information.
Event Failure Logs for vSMF interface	With this feature, the consistent event failure logs are enhanced to support the Create, Insert, Release, and Update procedures for the vSMF interface.

Feature	Description
IPv6 Prefix Delegation from Local Pool	The SMF supports IPv6 Prefix Delegation, allowing User Equipment (UE) and Customer Premises Equipment (CPE) to request additional IPv6 prefixes for configuring routers or cellular gateway devices. The delegated prefix length range allowed is from 48 to 62. This IPv6 prefix delegation is especially beneficial for service providers as it helps manage subscriber networks more effectively by assigning a prefix to CPE devices acting as routers between the subscriber's internal network and the core network Command introduced: **ipv6-prefix-delegation prefix length** *prefix_length* **dnn prefix-delegation** *vdnn* in DNN Profile Configuration mode **Default Setting**: Disabled – Configuration Required to Enable
Rolling Upgrade Optimization for Protocol PFCP Pods	For the protocol (PFCP) pods, Converged Core Gateway introduces a session-level response messages cache at the service pod for handling the retransmitted requests. This optimization helps in reduced session and Call Events Per Second (CEPS) loss during the upgrade procedure.
Support for UE IP Address Hold and Reuse	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 feature improves the user experience and reduces the IP address exhaustion in scenarios where users frequently attach and detach. Command introduced: **session-hold duration** in Converged Core profile and DNN profile configurations
IoT	

Feature	Description
Support Seven Million Sessions on UCS 220 M7 Platform	This feature involves optimizing the SMF infrastructure to support up to seven million IoT call sessions on the UCS 220 M7 platform. The optimizations include improvements in radius-ep and GTPC-ep components and communication towards CDL component. This optimization improves the reliability and scalability of the system, thereby ensuring efficient handling of large-scale IoT deployments. CLI Console Changes: Releases prior to 2024.04.0, the help string for **detect-dead-server consecutive-failures** displayed 10 as the default value. In release 2024.04.0 and later, the help string for **detect-dead-server consecutive-failures** has been updated to reflect that the default value is disabled. Commands introduced: • **enable-async { false | true }** in the RADIUS endpoint configuration mode to enable asynchronous communication from RADIUS endpoint for RADIUS authentication, accounting, and CoA request messages. The default value is **false**. • **overload-control msg-type create-session-request** in S5 interface configuration mode to apply rate limiting for Create Session Request messages.

Behavior Changes

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

Behavior Change	Description
SMF	
Change in Log Level for MemoryCache	**Previous Behavior**: CDL pods and other app infrastructure pods displayed warning logs for ETCD operations, such as Update, Get, and Delete. **New Behavior**: The log level for ETCD operations changed from warning to debug level, as these logs are intended for debugging purposes.
Message Priority Negotiation for High Priority Messages	**Previous Behavior:** SMF was not considering the message priority of the incoming messages that are coming over N4, GTPC, and SBA interfaces. SMF used to send the message priority in outgoing messages. **New Behavior:** SMF extracts the message priority of the incoming messages and negotiates the extracted MP value with the configured interface specific MP value and sends out best among them in outgoing message priorities.

Behavior Change	Description
SMF Handling of SmContextStatusNotify for WiFi (N3IWF) to NR Handover	**Previous Behavior:** By default, SMF sends the SmContextStatusNotify to AMF without checking the "3GPP 23.502" compliance version for "WiFi (N3IWF) to NR" and "NR to WiFi" handover in intra PLMN scenarios. **New Behavior:** SMF now sends the SmContextStatusNotify to AMF only if the compliance profile for "3GPP 23.502" is configured to be greater than 15.4.0 for "WiFi (N3IWF) to NR" and "NR to WiFi" handover in intra PLMN scenarios. If the compliance profile is 15.4.0, SMF does not send the SmContextStatusNotify message to AMF.
IoT	
Destination-Host and Destination-Realm AVP Support for Dynamic Route	**Previous Behavior**: • For CCR-U/T, if the route list of bounded peer does not have active dynamic route, it continues to refer the route list of same peer for sending out the request. • Whenever the peer switch happens for an existing session, the destination-host is set as per the switched peer • Whenever the peer switch happens for an existing session, the destination-realm is set as per the switched peer. • If the route list has only dynamic routes based on host/realm details, the static or patchcache route of bounded peer is not added to list of route. **New Behavior**: • For CCR-U/T, if the route list of primary does not have any dynamic route then secondary is considered for sending the message. • When peer switch occurs for an existing session, the Destination-Host value is set as empty. • When peer switch occurs for an existing session, Destination-Realm AVP is set as the origin-realm received in the previous CCA-I/U. • If the route list of host has only dynamic routes, static or patchcache route of peer associated with route is added to the list.
Destination-Host Handling in Realm-Based Routes	**Previous Behavior**: When routing based on realms, SMF used the destination-host value of the selected host instead of the destination-host of the peer associated with the route. **New Behavior**: When routing based on realms, SMF now uses the destination-host value specified in the peer configuration within the endpoint profile.

Behavior Change	Description
Expiry Time Handling for Dynamic Diameter Routes	**Previous Behavior**: In Diameter, once the dynamic route is created, the expiration time of dynamic route is not updated even if there is a message exchange using that dynamic route or the response is pointing to that dynamic route where the origin-host and origin-realm in response is different from the destination-host and destination-realm of request. **New Behavior**: The expiration time of dynamic route is updated with the new expiration time if there is a message exchange using that dynamic route or if the response is pointing to that dynamic route where the origin-host and origin-realm in response is different from the destination-host and destination-realm of request.
Enhancement in EDR Configuration to Capture Transaction Priority	**Previous Behavior:** In SMF, the transaction priority of a message was not getting recorded in the EDR. **New Behavior:** The EDR configuration is enhanced to capture the priority class of a message. Enabling this CLI displays an additional field in the EDR transaction files with an additional field containing one of the following two values: • DefaultPriority • HighPriority Following is the new CLI: **[no] edr file transaction field priorityClass**

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.

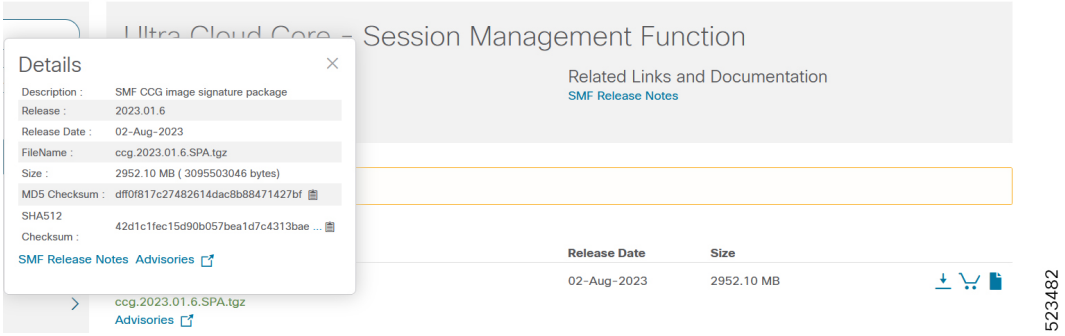
Installation and Upgrade Notes

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 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
SMF	
CSCwm98056	3gpp li provisioning results in call failures and CEPS loss
IoT	
CSCwk82318	Clear sub CLI did not clear all active sessions
CSCwm73549	show peers all interfaceName Gz not showing all peers on dyanmic config change
CSCwm86970	Rolling Upgrade Async/SendNotification support validation for IOT
CSCwm94697	"mode debug exec attributes" cli pushing two ip chunks to UPF instead of one

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.

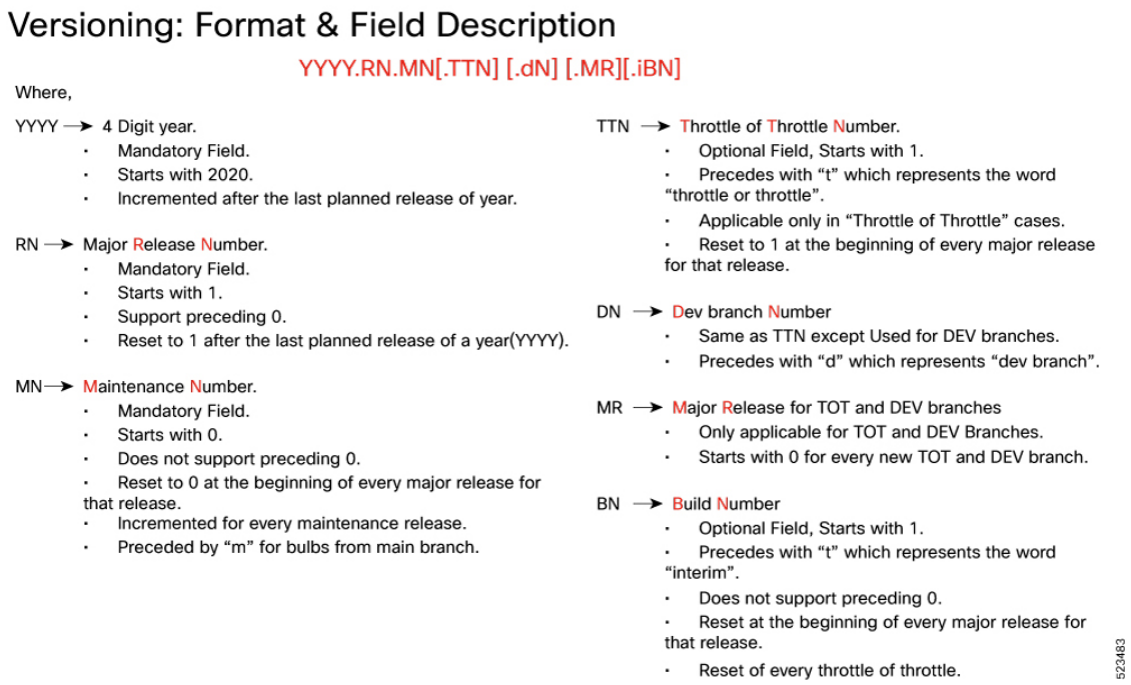
Bug ID	Headline	Behavior Change
CSCwe15107	AMF sends duplicate NRF subscription req intermittently during retry for expired validity	No
CSCwk65884	Encrypt all the CALEA Data in ETCD DB	No
CSCwm65123	GR switchover resulted in huge go routine spikes on nodemgr pods	No

Bug ID	Headline	Behavior Change
CSCwj98129	Ops center needs to validate the IP format in CLI	No
CSCwk73687	Registration Time during LTE to wifi sent wrongly	No
CSCwm58741	Service pod Panic Message during Intial attach with - Release request	Yes
CSCwk11285	"Show nrf discovery-info" with AMF set filter key need to print all service level info	No
CSCwm10198	"show subscriber all" showing rat as NR and WLAN - after handover from wlan to nr	No
CSCwm86027	show subscriber count nf-specific updating wrongly after upgrade	No
CSCwm47828	SMF does not suspend IDLE mode exit proc with incoming context retrieve request	No
CSCwm28044	SMF not sending usage stats under charging request to CHF with EPFAR - Converged call clear	No
CSCwm05930	SMF picking wrong CA inconsistently when static and dynamic rules' CA have same RG	No
CSCwm45589	SMF takes 2 seconds (after a failed attempt to AMF) when NRF has already notified the AMF failure	No
CSCwm41162	Stuck sessions, no clear event sent towards northbound- ipHoldTimer(issue with both 4G /5G)	No
CSCwk40753	Sytax error in amf RegionID related CLI	No
CSCwm05677	UDP endpoints are not Started - 2 0.0.0.0:16002 0.0.0.0:16002 Udp Starting S5E false	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.