Ultra Cloud Core 5G Session Management Function, Release 2022.04 - Release Change Reference

First Published: 2022-10-20

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

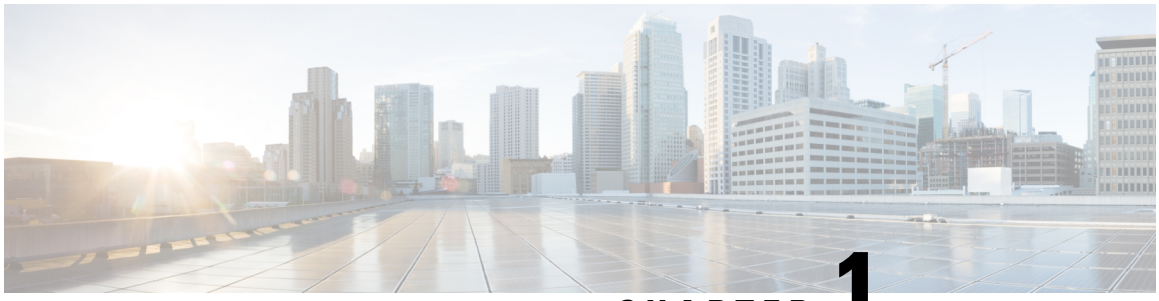
CONTENTS

About this Guide

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. While any existing biased terms are being substituted, exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

This Release Change Reference (RCR) describes new and modified feature and behavior change information for the applicable 5G SMF release(s).

About this Guide



CHAPTER 1

UCC 5G SMF - Release Change Reference

Features and Changes Quick Reference

Features / Behavior Changes	Release Introduced / Modified
Batch ID Allocation, Release, and Reconciliation Support, on page 6	2022.04.0
CDL Flush Interval and Session Expiration Tuning Configuration, on page 7	2022.04.0
Dedicated Multi-bearer Creation—CSCwa91602, on page 9	2022.04.0
Domain-based User Authorization Using Ops Center, on page 9	2022.04.0
Edge Echo Implementation, on page 10	2022.04.0
EDR Logging Support, on page 11	2022.04.0
ETCD Peer Optimization Support, on page 13	2022.04.0
Flag DB Database Updates, on page 14	2022.04.0
Geo-Redundancy Pod Hardening—CSCwc27740	2022.04.0
Grafana Dashboard Visibility during Deployment—CSCwa78001	2022.04.0
GR Maintenance Mode, on page 17	2022.04.0
Handling PDU Session Modifications based on RRC Inactive Cause Codes—CSCwb13529, on page 19	2022.04.0
Handover Failure when TGT-gNB does not Support IDFT - CSCwd58407	2022.04.0
Interservice Pod Communication, on page 21	2022.04.0
IPAM Data Reconciliation—CSCwc26796	2022.04.0
IP Pool Allocation per Slice and DNN	2022.04.0
IPv6 Support on SMF Interfaces, on page 24	2022.04.0
IPv6 Support on UPF Tunnel Endpoint, on page 26	2022.04.0
Modification of Standalone CLI Changes during Deployment in GTPC Split Mode Not Allowed—CSCwb89776	2022.04.0

Features / Behavior Changes	Release Introduced / Modified
Mutual TLS Support for LI and SBI Interfaces, on page 28	2022.04.0
N4 Modification Request Rejection—CSCwc93668, on page 29	2022.04.0
N4 Over IPSec, on page 30	2022.04.0
PAPN Support, on page 32	2022.04.0
SMF and cnSGW Optimization for GTPC IPC Cross-rack Support Messages—CSCwb88088, on page 34	2022.04.0
SMF Deployment Validation on VMware vSphere Hypervisor (ESXi) 7.0.x	2022.04.0
TCP Support for LI, on page 36	2022.04.0
Unique IP Pools for UPF, on page 37	2022.04.0
User Plane Integrity Protection Support, on page 39	2022.04.0
VoNR Hardening for PCF-initiated Flow Deletion Failure Handling—CSCwc12894	2022.04.0

Feature Defaults Quick Reference

The following table indicates what features are enabled or disabled by default.

Feature	Default
Batch ID Allocation, Release, and Reconciliation Support	Disabled – Configuration required to enable
CDL Flush Interval and Session Expiration Tuning Configuration	Enabled – Configuration required to disable
Dedicated Multi-bearer Creation—CSCwa91602	Not Applicable
Domain-based User Authorization Using Ops Center	Not Applicable
Edge Echo Implementation	Enabled – Always-on
EDR Logging Support	Enabled – Configuration required to disable
ETCD Peer Optimization Support	Enabled – Always-on
Flag DB Database Updates	Enabled – Always-on
Geo-Redundancy Pod Hardening—CSCwc27740	Enabled – Configuration required to disable

Feature	Default
Grafana Dashboard Visibility during Deployment—CSCwa78001	Not Applicable
GR Maintenance Mode	Disabled – Configuration required to enable
Handling PDU Session Modifications based on RRC Inactive Cause Codes—CSCwb13529	Disabled – Configuration required to enable
Handover Failure when TGT-gNB does not Support IDFT - CSCwd58407	Not Applicable
Interservice Pod Communication	Disabled – Configuration required to enable
IPAM Data Reconciliation	Enabled – Always-on
IP Pool Allocation per Slice and DNN	Disabled – Configuration required to enable
IPv6 Support on SMF Interfaces	Not Applicable
IPv6 Support on UPF Tunnel Endpoint	Enabled – Always-on
Modification of Standalone CLI Changes during Deployment in GTPC Split Mode Not Allowed—CSCwb89776	Not Applicable
Mutual TLS Support for LI and SBI Interfaces	Not Applicable
N4 Modification Request Rejection - CSCwc93668	Not Applicable
N4 Over IPSec	Enabled – Configuration required to disable
PAPN Support	Disabled – Configuration required to enable
SMF and cnSGW Optimization for GTPC IPC Cross-rack Support Messages—CSCwb88088	GTPC IPC Cross-rack Support: Disabled – Configuration required to enable
SMF Deployment Validation on VMware vSphere Hypervisor (ESXi) 7.0.x	Not Applicable
TCP Support for LI	Disabled – Configuration required to enable
Unique IP Pools for UPF	Disabled – Configuration required to enable
User Plane Integrity Protection Support	Disabled – Configuration required to enable
VoNR Hardening for PCF-initiated Flow Deletion Failure Handling— CSCwc12894	Not Applicable

3GPP Spec Version Compliance Configuration for CHF Server—CSCwe29701

Behavior Change Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 2: Revision History

Revision Details	Release
Added support for: • N4 interface over IPsec • IPv6 address on all SMF interfaces • User plane integrity protection • Mutual TLS for the SBI interface • 3GPP specification version compliance configuration for CHF server	2022.04.0
Added support for configuration-based control of UDM and PCF messages.	2021.02.3.t3
Added support for N2 cause and diagnostic IEs.	2021.02.3

Revision Details	Release
Added support for: • Cause IE on the N11 interface. • NAS messages compliance with invalid protocol data handling. • ProblemDetails JSON object on the N11 interface. • Error handling with HTTP error codes. • HTTP/2 TLS support for the SBA interface.	2021.02.0
First introduced.	Pre-2020.02.0

Behavior Change

Previous Behavior: CHF used to reject the charging data request from SMF due to the invalid format of the subscriberIdentifier included in the request message.

New Behavior: 3GPP TS 32.291 specification introduces a new subscriberIdentifier type in Release 15.4.0. The compliance profile configuration for the **nchf-convergedcharging** service now supports the 15.4.0 specification version. That means, the CHF server is configured to use the 15.4.0 3GPP specification compliance version to avoid rejection of the charging data request.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > Interfaces Support chapter.

Batch ID Allocation, Release, and Reconciliation Support

Feature Summary and Revision History

Summary Data

Table 3: Summary Data

Applicable Products or Functional Area	cnSGW-C, SMF
Applicable Platforms	SMI
Feature Default Setting	Disabled – Configuration required to enable
Related Documentation	*UCC Serving Gateway Control Plane Function - Configuration and Administration Guide* and *UCC 5G SMF Configuration and Administration Guide*

Revision History

Table 4: Revision History

Revision Details	Release
First introduced.	2022.04.0

Feature Description

The nodemgr allocates a unique ID to the subscriber that is in the attached state. When the subscriber detaches, the unique ID is released to the nodemgr. If the allocation and deallocation procedures increase, the nodemgr performance is impacted and the sgw-service continues to wait longer to complete these procedures.

The Batch ID Allocation, Release, and Reconciliation Support feature provide a mechanism to reduce the interaction between the sgw-service and nodemgr, which in turn optimizes the nodemgr's performance.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > Performance Optimization Support chapter.

CDL Flush Interval and Session Expiration Tuning Configuration

Feature Summary and Revision History

Summary Data

Table 5: Summary Data

Applicable Products or Functional Area	cnSGW-C, SMF
Applicable Platforms	SMI
Feature Default Setting	Enabled – Configuration required to disable
Related Documentation	*UCC Serving Gateway Control Plane Function - Configuration and Administration Guide* and *UCC 5G SMF Configuration and Administration Guide*

Revision History

Table 6: Revision History

Revision Details	Release
First introduced.	2022.04.0

Feature Description

You can modify the default service-pod parameters to fine-tune the throughput performance and optimize the load performance.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > Performance Optimization Support chapter.

Changes to the Range of responsetimeout Value—CSCwb73053

Behavior Change Summary and Revision History

Summary Data

Table 7: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 8: Revision History

Revision Details	Release
First introduced. CDETS ID: CSCwb73053	2022.04.0

Behavior Change

Previous Behaviour: The upper and lower range of timeout values were not configured. The **responsetimeout** field allowed any value in service or failure handling profile in SMF. This behavior caused failure scenarios.

New Behaviour: Now, the **responsetimeout** field is configured to allow values in the range of 1 to 10000 milliseconds. This behavior prevents the failure scenarios.

Customer Impact: With this change, customers need to validate the configuration as per the allowed range of values for the **responsetimeout** field.

Dedicated Multi-bearer Creation—CSCwa91602

Behavior Change Summary and Revision History

Summary Data

Table 9: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 10: Revision History

Revision Details	Release
First introduced.	2022.04.0

Behavior Change

Previous Behavior: When a CBR is triggered after deletion (due to N4 Reject scenario) of the same bearer, it was considered as a bearer update. This behavior was because the entry for the bearer was not deleted from the policy data in SMF.

New Behavior: Whenever PCF triggers bearer creation after the same bearer deletion (due to N4 Reject scenario), SMF creates a dedicated bearer.

Domain-based User Authorization Using Ops Center

Feature Summary and Revision History

Summary Data

Table 11: Summary Data

Applicable Products or Functional Area	SMF, cnSGW-C

Applicable Platform(s)	SMI
Feature Default Setting	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 12: Revision History

Revision Details	Release
First introduced.	2022.04.0

Feature Description

SMF and cnSGW-C support domain-based user authorization using the Ops Center. To control the access on a per-user basis, use the TACACS protocol in Ops Center AAA. This protocol provides centralized validation of users who attempt to gain access to a router or NAS.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > Performance Optimization Support chapter.

Edge Echo Implementation

Feature Summary and Revision History

Summary Data

Table 13: Summary Data

Applicable Products or Functional Area	cnSGW-C, SMF
Applicable Platforms	SMI
Feature Default Setting	Enabled – Always-on
Related Documentation	*UCC Serving Gateway Control Plane Function - Configuration and Administration Guide* and *UCC 5G SMF Configuration and Administration Guide*

Revision History

Table 14: Revision History

Revision Details	Release
First introduced.	2022.04.0

Feature Description

In a nonmerged mode, the udp-proxy pod acts as an endpoint, and the gtpc-ep responds to the Echo Requests from the peer node.

The gtpc-ep experiences traffic when the system receives a high number of inputs CEPS leading to a discrepancy between the rate at which gtpc-ep picks up the messages from udp-proxy and the rate at which udp-proxy gets the messages.

If the gtpc-ep is loaded, the queue between the udp-proxy and gtpc-ep gets full, and some of the messages at udp-proxy might get dropped. The peer detects path failure if these are Echo Request messages because an Echo Response is not received. Further, the peer clears all the sessions sent to the sgw-service.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > Performance Optimization Support chapter.

EDR Logging Support

Feature Summary and Revision History

Summary Data

Table 15: Summary Data

Applicable Products or Functional Area	SMF
Applicable Platforms	SMI
Feature Default Setting	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 16: Revision History

Revision Details	Release

Introduced support for the following enhancements:
• EDR generation for dedicated bearer and handover (pathswitchreq (Xn handover), pdun2ho, pdn5g4gHo, nrtountrustwifiho, pdun26ho, utn3gppto5g) procedures
• Archival of EDR files in EDR Monitor pod
• New commands to
  • Enable EDR for all subscribers
  • Configure transaction EDR rate, CPU threshold, session threshold, and file archival policy
	2022.04.0

Introduced EDR support for PDU session modification procedure for roaming and non-roaming scenarios	2021.02.2
Provided support for event-level EDR generation	2021.02.0
Custom EDR Generation	2021.01.0

Feature Description

SMF supports transaction logging and generation of detailed event records for all PDU session modification, deletion, handover, and dedicated bearer procedures except the following scenarios:

- Xn HO, N2 HO, 5G to 4G HO, 4G to 5G HO, 5G to Wi-Fi HO, and Wi-Fi to 5G HO
- Idle-Active transition
- Active-Idle transition
- 4G PDN modification

For more information, see the UCC 5G SMF Configuration and Administration Guide > Event Detail Records chapter.

ETCD Peer Optimization Support

Feature Summary and Revision History

Summary Data

Table 17: Summary Data

Applicable Products or Functional Area	cnSGW-C, SMF
Applicable Platforms	SMI
Feature Default Setting	Enabled – Always-on
Related Documentation	*UCC Serving Gateway Control Plane Function - Configuration and Administration Guide* and *UCC 5G SMF Configuration and Administration Guide*

Revision History

Table 18: Revision History

Revision Details	Release
First introduced.	2022.04.0

Feature Description

When large numbers of GTPC peers are connected with SMF or cnSGW-C, the performance of ETCD is impacted. Each peer is a considered as a record in the ETCD, and the timestamp is updated every 30 seconds for each peer. This causes continuous updates on ETCD and generates huge traffic that impacts the overall system performance.

The ETCD Peer Optimization feature facilitates optimization in peer management and enables reduced performance impact on ETCD.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > Performance Optimization Support chapter.

Flag DB Database Updates

Feature Summary and Revision History

Summary Data

Table 19: Summary Data

Applicable Products or Functional Area	cnSGW-C, SMF
Applicable Platforms	SMI
Feature Default Setting	Enabled – Always-on
Related Documentation	*UCC Serving Gateway Control Plane Function - Configuration and Administration Guide* and *UCC 5G SMF Configuration and Administration Guide*

Revision History

Table 20: Revision History

Revision Details	Release
First introduced.	2022.04.0

Feature Description

cnSGW-C and SMF update the CDL whenever the subscriber state changes from idle to active, and the ULI, UeTz, UCI, or the serving network is modified.

When the transaction requests driven to CDL increases, cnSGW-C and SMF incur a higher CPU utilization. To prevent the needless CPU utilization, cnSGW-C and SMF update only a subset of the CDL with the changed attributes.

Flag DB Database for the DDN Procedure

When the DDN procedure completes, sgw-service updates the CDL which impacts the CPU utilization. To optimize the CPU usage, the CDL is notified about the DDN only with the partial updates.

DDN Internal timer

cnSGW-C and SMF implement the DDN Retry Timer by applying the CDL's timer functionality. Every DDN transaction starts the DDN Retry Timer that requires the complete CDL instance to be updated, which results in an increase in the CPU usage of the CDL and sgw-service.

cnSGW-C is modified to have an integrated DDN Retry Timer that is configurable from sgw-profile. With this approach, the performance is improved because the cnSGW-C and SMF do not communicate with the

CDL for starting the DDN Retry Timer as it is an internal timer. The DDN Retry Timer is started for a duration of 10 seconds.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > Performance Optimization Support chapter.

Geo-Redundancy Pod Hardening—CSCwc27740

Behavior Change Summary and Revision History

Summary Data

Table 21: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Default Setting	Enabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 22: Revision History

Revision Details	Release
First introduced.	2022.04.0

Behavior Change

Switchover of Role of STANDBY to PRIMARY due to Traffic Hit

Previous Behaviour: Due to traffic hit, the primary rack published new multiple exit discriminator (MED) values on change of role to FAILOVER_INIT. In addition, if there was a STANDBY rack moving to a PRIMARY role, it did not replicate the final time pull.

New Behaviour: Now, the existing primary rack does not publish the new MED values on change of role from PRIMARY to FAILOVER_INIT. In addition, the lower MED values are published when the role changes to STANDBY_ERROR.

Attempt of Final Pull on Traffic Hit

Previous Behaviour: Due to traffic hit, the georeplication-pod did not attempt replication of final pull before changing the role from STANDBY to PRIMARY.

New Behaviour: Now, the georeplication-pod attempts a one-time replication data pull in the STANDBY rack before moving a role to PRIMARY.

Grafana Dashboard Visibility during Deployment—CSCwa78001

Behavior Change Summary and Revision History

Summary Data

Table 23: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 24: Revision History

Revision Details	Release
First introduced.	2022.04.0

Behavior Change

Previous Behaviour: The App-infra dashboard pod was deployed from infra-charts.

New Behaviour: Now, the app-infra dashboard pod is not deployed from infra-charts. Hence, the Grafana dashboard is not visible.

Customer Impact: This change prevents confusion with only one panel. Customers can load the `dashboard.json` file manually to view the old Grafana dashboard for checking the required statistics.

GR Maintenance Mode

Feature Summary and Revision History

Summary Data

Table 25: Summary Data

Applicable Products or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 26: Revision History

Revision Details	Release
First introduced.	2022.04.0

Feature Description

SMF supports the maintenance mode flag to disable the impact on a cluster if the cluster in GR setup is scheduled for in-service (rolling upgrade). This is useful so that the other mated cluster executes its responsibility and other activities on the targeted cluster without any issue.

If the maintenance mode flag is set to **true**, cluster role change and GR trigger for the rack is allowed only in case of CLI-based failover.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > Redundancy Support chapter.

GTPC Endpoint Initialization With and Without UDP Proxy

Behavior Change Summary and Revision History

Summary Data

Table 27: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	*UCC SMF Configuration and Administration Guide* and *UCC cnSGWc Configuration and Administration Guide*

Revision History

Table 28: Revision History

Revision Details	Release
First introduced.	

Behavior Change

Previous Behavior: The UDP proxy pod was used as an endpoint for the GTPC, PFCP, and RADIUS messages. If GTP default VIP, such as S11, S5, S5e, and S2b, was configured, the GTP endpoints started into the UDP proxy. Multiple protocol microservices depend on UDP proxy for UDP transport. Hence, UDP proxy was a scaling bottleneck. A surge of messages led to packet drops.

New Behavior: The UDP proxy functionality merges into the respective protocol microservice to mitigate the scaling bottleneck. The UDP proxy bypass improves the CPU usage by reducing one hop across microservices in the signaling path. With this new behavior:

- If the GTP interface VIP is configured in the endpoint protocol, the GTP endpoints start into the UDP proxy.
- If only the GTP default VIP is configured in the GTP endpoint and no VIP is configured in the endpoint protocol, then the GTP endpoints start into the GTPC endpoint.

Note In this software release, you must deploy SMF in merged mode only. For more information on this mode, see the *UCC SMF Configuration and Administration Guide* and *UCC cnSGWc Configuration and Administration Guide*.

Handling PDU Session Modifications based on RRC Inactive Cause Codes—CSCwb13529

Behavior Change Summary and Revision History

Summary Data

Table 29: Summary Data

Applicable Products or Functional Area	SMF
Applicable Platforms	SMI
Feature Default Setting	Handling PDU Session Modifications based on RRC Inactive Cause Codes: Disabled – Configuration required to enable
Related Changes in this Release	Not Applicable
Related Documentation	*UCC 5G SMF Configuration and Administration Guide* *UCC 5G SMF CLI Command Reference*

Revision History

Table 30: Revision History

Revision Details	Release
The following supplementary feature under the Performance Optimization Support feature was introduced and supported: • Handling PDU Session Modifications based on RRC Inactive Cause Codes • CDETS ID: CSCwb13529	2022.04.0
First introduced.	2021.02.3

Feature Description

The Radio Resource Control (RRC) is a layer within the 5G NR protocol stack. It exists only in the control plane, in the UE, and in the gNB. The existing state of PDU sessions controls the behaviour and functions of the RRC.

During the PCF-initiated modification, the AMF sends those received unsuccessful transfer radio networks cause codes in the N2 content of the SmContextUpdate message to the SMF under the following conditions:

- When the Xn-handover is in progress.
- When the AN is released.
- When the UE is in the RRC inactive state.
- When the UE isn't reachable.

The SmContextUpdate message with the N2 cause codes acts as a bridge and converter from AMF to SMF or from SMF to AMF.

Behavior Change

Previous Behavior—The details regarding the performance optimization support feature in the SMF, the Inactive RRC Support wasn't defined.

New Behavior—From this release, details about the Inactive RRC Support feature is now available under the *Performance Optimization Support* chapter in the *UCC 5G SMF Configuration and Administration Guide*.

The Radio Resource Control (RRC) is a layer within the 5G NR protocol stack. It exists only in the control plane, in the UE, and in the gNB. The existing state of the RRC controls the behaviour and functions of the RRC.

Customer Impact—Enhanced feature and configuration details.

Handover Failure when TGT-gNB does not Support IDFT - CSCwd58407

Behavior Change Summary and Revision History

Summary Data

Table 31: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Default Setting	Not Applicable
Related Changes in this Release	Not Applicable

Related Documentation	Not Applicable

Revision History

Table 32: Revision History

Revision Details	Release
First introduced.	2022.04.0

Behavior Change

Previous Behavior: In N2 handover, if direct path is not available between S-RAN and T-RAN then SMF may decide to enable IDFT for data forwarding. So, SMF expects DL forwarding UP tunnel information from T-RAN for indirect data forwarding. If T-ran doesn't provide the DL forwarding UP tunnel information then SMF rejects the handover.

New Behavior: Now, If T-ran doesn't provide the DL forwarding UP tunnel information then SMF continues the HO without IDFT.

Interservice Pod Communication

Feature Summary and Revision History

Summary Data

Table 33: Summary Data

Applicable Products or Functional Area	cnSGW-C
Applicable Platforms	SMI
Feature Default Setting	Disabled – Configuration required to enable
Related Documentation	*UCC Serving Gateway Control Plane Function - Configuration and Administration Guide*

Revision History

Table 34: Revision History

Revision Details	Release
First introduced.	2022.04.0

Feature Description

When the IMS PDN sgw-service and smf-service selected for a subscriber are on the same cluster and same RACK, the following message flow occurs when sgw-service sends a message to smf-service:

- The message is sent from S5e gtpc-ep interface to network interface.
- The message returns to the S5 interface from gtpc-ep to smf-service.

For the subscribers that are collocated, the communication happens between the sgw-service and the smf-service. This approach reduces the processing load on the gtpc-ep.

IPAM Data Reconciliation—CSCwc26796

Feature Summary and Revision History

Summary Data

Table 35: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	IPAM: Enabled – Always-on Unique IP Pools for UPF: Disabled – Configuration required to enable
Related Changes in this Release	Not Applicable
Related Documentation	*UCC 5G SMF Configuration and Administration Guide*

Revision History

Table 36: Revision History

Revision Details	Release
First introduced. CDETS ID: CSCwc26796	2022.04.0

Feature Description

SMF supports IPAM reconciliation at instance level, pool level, and chunk level.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > IP Address Management chapter.

IP Pool Allocation per Slice and DNN

Feature Summary and Revision History

Summary Data

Table 37: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 38: Revision History

Revision Details	Release
Added support for IP pool allocation per slice and DNN.	2022.04.0
Added support for: • Charging Characteristics lookup parameter in the subscriber policy configuration. • Extension in Charging Characteristics ID range values.	2021.02.3.t3
Added support for IPv6 interface ID generation based on SBI VIP address and CommonId of the subscriber.	2021.01.1
SMF supports the maximum limit of 2048 for the following configurations: • Precedence • Operator policy • DNN policy • DNN profile	2021.01.0
SMF supports case insensitive DNN configuration.	2020.02.5.t1
First introduced.	Pre-2020.02.0

Feature Description

SMF supports IP pool allocation per slice with the same DNN. A slice is a logical end-to-end network that is created dynamically. A user equipent (UE) can access multiple slices over one access network, such as over the same radio interface.

For this feature, SMF performs the following tasks:

- Register, discover, subscribe, and send traffic to all the external NFs based on the slice ID.
- Provide slice-based procedure and session statistics.
- Provide slice information on an EDR.
- Provide slice information on logs.
- Limit the maximum number of supported slices on SMF to 512.

For more details, refer to the UCC 5G SMF Configuration and Administration Guide > Multiple and Virtual DNN Support, IP Address Management, NF Discovery and Management, and Troubleshooting Information chapters.

IPv6 Support on SMF Interfaces

Feature Summary and Revision History

Summary Data

Table 39: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 40: Revision History

Revision Details	Release

Added support for:
• Multiple 3GPP specification compliance for SMF interfaces.
• Gz Interfaces and associated features:
  • PDN Attach and Detach with Gz Interface
  • Gz Usage Reporting
• Indirect communication for NFs through SCP Model D.
• Excluding the optional IE for Locality in the NRF messages.
	2023.03.0

Added support for: • N4 interface over IPsec • IPv6 address on all SMF interfaces • User plane integrity protection • Mutual TLS for the SBI interface • 3GPP specification version compliance configuration for CHF server	2022.04.0
Added support for configuration-based control of UDM and PCF messages.	2021.02.3.t3
Added support for N2 cause and diagnostic IEs.	2021.02.3
Added support for: • Cause IE on the N11 interface. • NAS messages compliance with invalid protocol data handling. • ProblemDetails JSON object on the N11 interface. • Error handling with HTTP error codes. • HTTP/2 TLS support for the SBA interface.	2021.02.0
First introduced.	Pre-2020.02.0

Feature Description

SMF interfaces can now send and receive the IPv6 addresses along with IPv4 addresses. To support the IP addresses, both the endpoint and interfaces configuration must include unique VIP IP and port details.

Important At a given time, the SBI interfaces (N7, N10, N11, and N40) support only IPv4 or IPv6 address. However, the N3, N4 and GTPC interfaces support either IPv4 or IPv6 address or both.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > Interfaces Support chapter.

IPv6 Support on UPF Tunnel Endpoint

Feature Summary and Revision History

Summary Data

Table 41: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 42: Revision History

Revision Details	Release
IPv6 address support introduced to UPF tunnel end point address.	2022.04.0
Introduced support for the selection of UPF nodes based on the query parameters, such as DNN, location, and PDU session type.	2020.03.0
First introduced.	Pre-2020.02.0

Feature Description

SMF is now capable of sending an IPv6 address of UPF tunnel endpoint to the AMF or gNB through the CN-Tunnel_information. The IPv6 address information is used to establish the N3 tunnel.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > UP Session Activation and Deactivation Service Request Procedures chapter.

Modification of Standalone CLI Changes during Deployment in GTPC Split Mode Not Allowed—CSCwb89776

Behavior Change Summary and Revision History

Summary Data

Table 43: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 44: Revision History

Revision Details	Release
First introduced. CDETS ID: CSCwb89776	2022.04.0

Behavior Change

Previous Behaviour: During deployment, new Standalone CLIs, such as **standalone**, **internal-vip**, and **cpu** could be modified.

New Behaviour: Now, the standalone CLIs can be modified only after the system shutdown. Changes in deployed system are rejected.

Mutual TLS Support for LI and SBI Interfaces

Feature Summary and Revision History

Summary Data

Table 45: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 46: Revision History

Revision Details	Release
Added support for: • N4 interface over IPsec • IPv6 address on all SMF interfaces • User plane integrity protection • Mutual TLS for SBI interface	2022.04.0
Added support for configuration-based control of UDM and PCF messages.	2021.02.3.t3
Added support for N2 cause and diagnostic IEs.	2021.02.3
Added support for: • Cause IE on N11 interface. • NAS messages compliance with invalid protocol data handling. • ProblemDetails JSON object on N11 interface. • Error handling with HTTP error codes. • HTTP/2 TLS support for SBA interface.	2021.02.0

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

SMF supports Mutual TLS (mTLS) for the following interfaces:

- LI X1 and X2
- SBI

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > Interfaces Support chapter.

Note For more information on mTLS support on LI interfaces, contact your Cisco Account representative.

N4 Modification Request Rejection—CSCwc93668

Behavior Change Summary and Revision History

Summary Data

Table 47: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 48: Revision History

Revision Details	Release
First introduced.	2022.04.0

Behavior Change

Previous Behaviour: The Outer Header Removal IE was sent with value as 0 in UPDATE_PDR IE of N4 modification request to UPF.

New Behaviour: Now, the Outer Header Removal IE is not sent in UPDATE_PDR IE of N4 modification request to UPF.

N4 Over IPSec

Feature Summary and Revision History

Summary Data

Table 49: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 50: Revision History

Revision Details	Release

Added support for:
• Multiple 3GPP specification compliance for SMF interfaces.
• Gz Interfaces and associated features:
  • PDN Attach and Detach with Gz Interface
  • Gz Usage Reporting
• Indirect communication for NFs through SCP Model D.
• Excluding the optional IE for Locality in the NRF messages.
	2023.03.0

Revision Details	Release
Added support for: • N4 interface over IPsec • IPv6 address on all SMF interfaces • User plane integrity protection • Mutual TLS for the SBI interface • 3GPP specification version compliance configuration for CHF server	2022.04.0
Added support for configuration-based control of UDM and PCF messages.	2021.02.3.t3
Added support for N2 cause and diagnostic IEs.	2021.02.3
Added support for: • Cause IE on the N11 interface. • NAS messages compliance with invalid protocol data handling. • ProblemDetails JSON object on the N11 interface. • Error handling with HTTP error codes. • HTTP/2 TLS support for the SBA interface.	2021.02.0
First introduced.	Pre-2020.02.0

Feature Description

SMF supports Internet Protocol Security (IPSec) on N4 interface for secure network traffic.

The N4 Over IPSec feature requires some basic configurations to be enabled on SMF, UPF and SMI. For complete information on this feature, see the *UCC 5G UPF Configuration and Administration Guide* applicable for the release.

For SMI strongSwan configuration details, see the UCC 5G SMF Configuration and Administration Guide > Interfaces Support chapter.

PAPN Support

Feature Summary and Revision History

Summary Data

Table 51: Summary Data

Applicable Products or Functional Area	cnSGW-C, SMF
Applicable Platform(s)	SMI
Feature Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 52: Revision History

Revision Details	Release
First introduced.	2022.04.0

Feature Description

In private APN deployments, the SMF can support multiple PAPNs, requiring authentication and accounting with the enterprise AAA servers. As the AAA servers belong to different mobile virtual network operators (MVNOs), it is possible that their address ranges overlap. SMF uses Virtual Routing and Forwarding (VRF) functionality to support overlapping IP addresses for AAA servers.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > Virtual Routing and Forwarding chapter.

PDN-based UPF Selection

Feature Summary and Revision History

Summary Data

Table 53: Summary Data

Applicable Product(s) or Functional Area	SMF

Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 54: Revision History

Revision Details	Release
Added support for SMF— • to allocate UPFs with unique IP pools • to select the UPF based on PDN type	2022.04.0
Introduced support for Diff-Serv-Code-Point (DSCP) or Type of Service (ToS) QoS functions during interaction with PCF.	2021.02.3.t3
Introduced support for the following features: • Usage Monitoring over PCF • N4 QoS Mismatch Correction • Dynamic QoS Flow-based Application Detection and Control • IP Threshold-based UPF Selection	2021.02.3
Introduced support for non-standard QCI for dynamic PCC and session rules	2021.02.2
Introduced support for the following features: • Bit rate mapping • UPF Selection based on Slice and Location • UP Optimization	2021.02.0
Introduced support for the following: • Co-located UPF Selection • Enhanced Limits for Maximum Groups in Bandwidth Policy Configuration • Handling Session Report Rejection Procedure • New Format of Outer Header information element (IE)	2021.01.0

Revision Details	Release
Introduced support for the following: • UPF node selection based on DNN and PDU Session type • Modification of authorized default QoS • Additional session report and UPF node report request	2020.03.0
First introduced.	Pre-2020.02.0

Feature Description

SMF supports UPF selection based on predefined query parameters including PDN type.

SMF performs co-located UPF selection based on the SGW-U node name received in the Create Session Request (CSR) message. In the absence of the SGW-U node name, the SMF follows the existing UPF selection algorithm.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > Policy and User Plane Management chapter.

SMF and cnSGW Optimization for GTPC IPC Cross-rack Support Messages—CSCwb88088

Behavior Change Summary and Revision History

Summary Data

Table 55: Summary Data

Applicable Product(s) or Functional Area	SMF cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	GTPC IPC Cross-rack Support: Disabled – Configuration required to enable
Related Changes in this Release	New feature as an enhancement

Related Documentation	*UCC 5G SMF Configuration and Administration Guide* *UCC 5G cnSGWc Configuration and Administration Guide*

Revision History

Table 56: Revision History

Revision Details	Release
First introduced. CDETS ID: CSCwb88088	2022.04.0

Feature Description

This is an enhancement to optimize GTPC messages between SMF and cnSGW-C across IMS and data racks clusters.

When you perform GR-setup activities with SMF and cnSGW-C, the GTPC message handling can be optimized between these two racks, as in the following scenarios:

- The set of IPC messages from cnSGW-C to SMF service pods flow over `gtpc-ep` pods twice leading to message encoding and decoding overheads.
- Within a GR pair, these IPC messages can avoid one more processing step, if service pods such as cnSGW-C and SMF can route messages to the corresponding peer GTPC nodes directly.

Before applying the configuration for enabling GTPC IPC on cnSGW or SMF interfaces, you must apply inter-rack routing networks using cluster sync. More configuration required to add BGP routes for supporting new routable networks across rack servers.

For more information, refer to the UCC 5G SMF - Configuration and Administration Guide > Performance Optimization Support chapter.

SMF Deployment Validation on VMware vSphere Hypervisor (ESXi) 7.0.x

Feature Summary and Revision History

Summary Data

Table 57: Summary Data

Applicable Product(s) or Functional Area	SMF

Applicable Platform(s)	SMI
Feature Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 58: Revision History

Revision Details	Release
First introduced.	2022.04.0

Feature Description

SMI allows you to validate the deployment of SMF on VMware version 7.0 of VMware vSphere Hypervisor (ESXi).

TCP Support for LI

Feature Summary and Revision History

Summary Data

Table 59: Summary Data

Applicable Product(s) or Functional Area	5G-SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 60: Revision History

Revision Details	Release

Added support for:
• TCP LI. As part of this feature, added the following configurations:
  • Non-3GPP LI TCP
  • Non-3GPP LI UDP
• 3GPP LI ETSI encoding
• mTLS for LI interfaces
	2022.04.0

First Introduced	2020.02.0

Feature Description

SMF supports LI in two ways—3GPP-compliant LI and non-3GGP LI. With this feature, the non-3GGP LI is supported through TCP, along with the earlier supported UDP.

Note This feature is backward-compatible and supports both the TCP and the UDP.

For more information, contact your Cisco account representative.

Unique IP Pools for UPF

Feature Summary and Revision History

Summary Data

Table 61: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI

Feature Default Setting	• IPAM: Enabled – Always-on • Unique IP Pools for UPF: Disabled – Configuration required to enable • Auto-Reclamation of Under-Utilized IP Chunks: Disabled- Configuration required to enable • Identification of Corrupted Chunks: Disabled- Configuration required to enable. • Reconciliation of IP Chunks between SMF and UPF: Disabled- Configuration required to enable. • IP Chunk Auto-Throttle and ToD Chunk Clearance: Disabled- Configuration required to enable. • Route Aggregation to Handle Switch Limit: Disabled- Configuration required to enable. • NAT Support: Disabled- Configuration required to enable.
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 62: Revision History

Revision Details	Release
Added support for the following features: • IPAM reconciliation CLI commands for IPAM hardening. • IP pool allocation per slice and DNN feature. • SMF to allocate UPFs with unique IP pools.	2022.04.0
Added support for the following features: • New calls with a static IP address. • Quarantine queue size. • IP address validation with CDL Configuration and statistics.	2021.02.0
IP Address Validation with CDL Configuration introduced.	2021.02.0
Updated quarantine time range to 3600 seconds.	2021.02.0
VRF Support introduced.	2020.02.5

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

With this feature, SMF enables you to perform the following tasks:

- Allocate specific set of IP pools for edge UPFs in such a way that the UPFs do not share the same IP pool
- Fall back to centrally located UPF when the edge UPF is down

This feature introduces new CLI command to tag the IP pools with a name, and associate this name while configuring UPF selection for each DNN. The IP address allocation to UPF is unique per pool if the tag configuration is based on location DNN. The UPFs share the same IP pool if the IPAM tag is configured with the default DNN received from the service.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > IP Address Management chapter.

User Plane Integrity Protection Support

Feature Summary and Revision History

Summary Data

Table 63: Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 64: Revision History

Revision Details	Release

Added support for:
• Multiple 3GPP specification compliance for SMF interfaces.
• Gz Interfaces and associated features:
  • PDN Attach and Detach with Gz Interface
  • Gz Usage Reporting
• Indirect communication for NFs through SCP Model D.
• Excluding the optional IE for Locality in the NRF messages.
	2023.03.0

Added support for: • N4 interface over IPsec • IPv6 address on all SMF interfaces • User plane integrity protection • Mutual TLS for the SBI interface • 3GPP specification version compliance configuration for CHF server	2022.04.0
Added support for configuration-based control of UDM and PCF messages.	2021.02.3.t3
Added support for N2 cause and diagnostic IEs.	2021.02.3
Added support for: • Cause IE on the N11 interface. • NAS messages compliance with invalid protocol data handling. • ProblemDetails JSON object on the N11 interface. • Error handling with HTTP error codes. • HTTP/2 TLS support for the SBA interface.	2021.02.0
First introduced.	Pre-2020.02.0

Feature Description

SMF supports integrity protection of user data packets exchanged between UE and gNB. Though the 3GPP specification mandates the Integrity Protection feature on both the UE and the gNB, this feature remains optional to use due to the overhead of the packet size.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > Interfaces Support chapter.

VoNR Hardening for PCF-initiated Flow Deletion Failure Handling—CSCwc12894

Behavior Change Summary and Revision History

Summary Data

Table 65: Summary Data

Applicable Products or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 66: Revision History

Revision Details	Release
First introduced. CDETS ID: CSCwc12894	2022.04.0

Behavior Change

Previous Behaviour: When PCF-initiated flow deletion procedure failed due to access side failures or timeouts, SMF used to retain the PCC rules that PCF sent for deletion.

New Behaviour: In case of a failure during PCF-initiated flow deletion procedure, the SMF deletes the PCC rules and communicates the details on the deleted PCC rules to UPF and PCF.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > Network-initiated Session Modification Procedures chapter.