UCC 5G SMF - Release Change Reference

Features and Changes Quick Reference

Features / Behavior Changes	Release Introduced / Modified
3GPP Compliance Changes for 5G to Wi-Fi Handover Scenarios—CSCvv81958, on page 5	2021.01.0
Case Insensitive DNN Configuration, on page 6	2021.01.0
Change in Default Values of N1 Timer t3591—CSCvu79719, on page 7	2021.01.0
Co-located UPF Selection, on page 8	2021.01.0
Converged Core Support, on page 9	2021.01.0
DCNR-Based UPF Selection, on page 12	2021.01.0
DNN Configuration Limits, on page 13	2021.01.0
DSCP Marking for Control Plane Signaling, on page 14	2021.01.0
Emergency Services Support, on page 15	2021.01.0
Enhanced Limits in Bandwidth Policy Configuration, on page 15	2021.01.0
Handling EPS Fallback Failures, on page 17	2021.01.1
Handling RADIUS Disconnect and CoA Requests, on page 18	2021.01.0
Handling Session Report Rejection Procedure, on page 19	2021.01.0
IPv6 Interface ID Generation—CSCvw93433, on page 20	2021.01.1
Local Breakout-based Roaming Support, on page 22	2021.01.0
Multiple PLMN Support, on page 22	2021.01.0
N2 Handover with Data Radio Bearer IE—CSCvw93447, on page 23	2021.01.1
New Outer Header Format, on page 24	2021.01.0
PAP, CHAP, MSCHAP-based RADIUS Authentication, on page 25	2021.01.0

Features / Behavior Changes	Release Introduced / Modified
Prioritization of Router Advertisement Procedure—CSCvu19134, on page 27	2021.01.0
RADIUS Access Response Attributes, on page 28	2021.01.0
RADIUS Accounting, on page 29	2021.01.0
RADIUS NAS-IP Address Support , on page 30	2021.01.0
Randomization of P-CSCF Addresses, on page 31	2021.01.0
RAT Type Configuration for UDM Failure Handling, on page 32	2021.01.1
Restoration of Old Deployment CLI for Grafana Dashboard—CSCvx73885, on page 33	2021.01.1
SBI Message Priority Mechanism, on page 34	2021.01.0
Session-level URR Limitation, on page 35	2021.01.1
SMF Deployment on Bare Metal Server, on page 36	2021.01.0
Support for Dynamic Change in ACS Configuration, on page 37	2021.01.0
TAI Selection From AMF, on page 38	2021.01.0
VRF Support, on page 39	2021.01.0
TFT Handling for Wi-Fi Handovers, on page 38	2021.01.0
Zero Usage Report Suppression, on page 40	2021.01.0

Feature Defaults Quick Reference

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

Feature	Default
3GPP Compliance Changes for 5G to Wi-Fi Handover Scenarios—CSCvv81958	Enabled – Configuration Required
Case Insensitive DNN Configuration	Disabled – Configuration Required
Change in Default Values of N1 Timer t3591—CSCvu79719	Enabled – Configuration Required
Co-located UPF Selection	Disabled – Configuration Required
Converged Core Support	Disabled – Configuration Required

Feature	Default
DCNR-Based UPF Selection	Disabled – Configuration Required
DNN Configuration Limits	Disabled – Configuration Required
DSCP Marking for Control Plane Signaling	Disabled – Configuration Required
Emergency Services Support	Enabled – Always-on
Enhanced Limits in Bandwidth Policy Configuration	Disabled – Configuration Required
Handling EPS Fallback Failures	Disabled – Configuration Required
Handling RADIUS Disconnect and CoA Requests	Disabled – Configuration Required
Handling Session Rejection Procedure	Disabled – Configuration Required
IPv6 Interface ID Generation—CSCvw93433	Disabled – Configuration Required
Local Breakout-based Roaming Support	Enabled – Always-on
Multiple PLMN Support	Disabled – Configuration Required
N2 Handover with Data Radio Bearer IE—CSCvw93447	Enabled - Always-on
New Outer Header Format	Enabled – Always-on
PAP, CHAP, and MSCHAP-based RADIUS Authentication	Disabled – Configuration Required
Prioritization of Router Advertisement Procedure—CSCvu19134	Enabled – Always-on
RADIUS Access Response Attributes	Disabled – Configuration Required
RADIUS Accounting	Disabled – Configuration Required
RADIUS NAS-IP Address Support	Disabled – Configuration Required
Randomization of P-CSCF Addresses	Disabled – Configuration Required
RAT Type Configuration for UDM Failure Handling	Disabled - Configuration Required
Restoration of Old Deployment CLI for Grafana Dashboard—CSCvx73885	Disabled - Configuration Required
SBI Message Priority Mechanism	Disabled – Configuration Required
Session-level URR Limitation	Disabled – Configuration Required
SMF Deployment on Bare Metal Server	Disabled – Configuration Required
Support for Dynamic Change in ACS Configuration	Disabled – Configuration Required

Feature	Default
TAI Selection From AMF	Enabled – Always-on
TFT Handling for Wi-Fi Handovers	Disabled – Configuration Required
VRF Support	Enabled – Always-on
Zero Usage Report Suppression	Disabled – Configuration Required

3GPP Compliance Changes for 5G to Wi-Fi Handover Scenarios—CSCvv81958

Behavior Change Summary and Revision History

Summary Data

Table 1: Summary Data

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

Revision History

Table 2: Revision History

Revision Details	Release
First introduced. CDETS ID: CSCvv81958	2021.01.0

Behavior Change

Previous Behavior: During 5G to Wi-Fi handover, SMF sent the following messages:

- N1 PDU Session Release command to UE without Skip-Indication flag in N1N2Transfer message
- N2 Resource Release Command Transfer message to gNB
- SmContextStatusNotify message to AMF

New Behaviour: The SMF now supports June 2019 compliance of 3GPP TS 23.502, Release 15.4.1. For 5G to Wi-Fi handover, the SMF sends the following messages:

- N2 Resource Release Command Transfer message if the user plane tunnel is active.
- N1 PDU Session Release command if the following configuration is NOT configured:

  ```
  config
     profile compliance compliance_profile_name
        service threegpp23502
           version uri v1
           version full 1.0.2
           version spec 15.6.0
           exit
  ```

  When N1 is sent, SMF includes Skip-Indication flag in N1N2Transfer message based on configuration under dnn-profile.

- SmContextStatus Notify message to AMF only in the following cases:
  - When the SMF does not send N1N2Transfer message and if the following configuration exists:

    ```
    config
       profile compliance compliance_profile_name
          service threegpp23502
             version uri v1
             version full 1.0.2
             version spec 15.6.0
             exit
    ```

  - When SMF sends N1N2Transfer message and AMF responds with status code other than 4xx.

Case Insensitive DNN Configuration

Feature Summary and Revision History

Summary Data

Table 3: 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 4: Revision History

Revision Details	Release
The limit for the following configurations in SMF is increased from 512 to 2048: • 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

The SMF supports case insensitive DNN configuration. The configuration accepts an alphanumeric string of 1 to 62 alphanumeric characters that is not case sensitive. It can also contain dots (.) and/or dashes (-).

For more information, refer to the UCC 5G SMF - Release Change Reference 2021.01 > Multiple and Virtual DNN Support chapter.

Change in Default Values of N1 Timer t3591—CSCvu79719

Behavior Change Summary and Revision History

Summary Data

Table 5: Summary Data

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

Revision History

Table 6: Revision History

Revision Details	Release
First introduced. CDETS ID: CSCvu79719	2021.01.0

Behavior Change

During the collision of events, SMF must control the maximum retry attempts of N1 PDU Modification Command to avoid looping of procedure. This operation is accomplished by using the **n1 t3591-pdu-mod-cmd timeout** *timeout* **max-retry** *retry_count* command in Access Profile Configuration mode.

Previous Behavior: The default value of N1 PDU Modification Command retransmission timeout was 4 seconds. The default value of maximum retry count was 4.

New Behavior: The default value of N1 PDU Modification Command retransmission timeout is 2 seconds. The default value of maximum retry count is 2.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > Network-Initiated Service Request chapter.

Co-located UPF Selection

Feature Summary and Revision History

Summary Data

Table 7: 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 8: Revision History

Revision Details	Release
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
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

The SMF performs UPF selection based on the SGW-U node name received in the Create Session Request (CSR) message. The SMF selects the co-located UPF during the initial EPS Attach procedure.

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

Converged Core Support

Feature Summary and Revision History

Summary Data

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

Related Documentation	Not Applicable

Revision History

Revision Details	Release
First introduced.	2021.01.0

Feature Description

The converged core solution provides an advanced, cloud native, converged control plane with the capability to support 4G and 5G devices, and use cases.

Important This release supports only the cloud native integrated S-GW and SMF instance with S5C and SGW-C functionalities.

The converged core network supports the following converged control plane and user plane functions.

- Converged Control Plane Function:
    - Integrated SGW and SMF network functions as a single deployment, under a single Kubernetes namespace, to support 4G and 5G devices from E-UTRAN/NR (Converged Core gateway)
    - Support for logical network functions (data only)
- Converged User Plane Function:
    - Integrated UPF and SGW-U functionalities as a single network function
    - Simultaneous support for N4 and Sxa interfaces
    - Terminate multiple control planes in a single deployment

Converged Core Refactoring

With the converged core support, the changes to the SMF architecture have resulted in modifications to the configuration maps, helm charts, Ops Center configuration, common naming formats, and so on.

The following list describes the high-level changes related to refactoring in the documentation.

CLI Enhancements

The **endpoint** CLI command is enhanced to include the new interface keywords.

- **endpoint gtp [interface s11]**
- **endpoint pfcp [interface sxa]**
- **endpoint protocol [interface sxa]**

Deprecated CLI Commands

The following commands are deprecated in 2021.01 and later releases.

- **k8 smf local [etcd | datastore | tracing]**
- **deployment [app-name | cluster-name | dc-name]**
- RCM configurations under Active Charging Services:
  - **accelerate-flow**
  - **tethering-detection**
  - **statistics-collection**
  - **port-map**
  - **edr-format**
  - **subs-class**
  - **service-scheme**
  - **host-pool**
  - **trigger-condition**
  - **subscriber-base**
  - **trigger-action**

Namespaces

The **namespace** keyword option is added to the following commands to display the output pertaining to the respective SMF or SGW namespace.

- **monitor subscriber supi** *supi_id* **namespace [smf | sgw]**
- **show subscriber all namespace [smf | sgw]**

Naming Formats

Common naming formats are introduced in this release, wherein the pod names, statistic names, message names, and procedure type names with the **smf** and **n4** prefixes are removed.

For more information, refer to the *Converged Core Refactoring Changes* section in the respective feature chapters of the UCC 5G SMF Configuration and Administration Guide.

For more information on the CLI commands, refer to the UCC 5G SMF CLI Command Reference.

DCNR-Based UPF Selection

Feature Summary and Revision History

Summary Data

Table 9: Summary Data

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

Revision History

Table 10: Revision History

Revision Details	Release
4g-UE and Option-3x Support phase-2 includes: • DCNR based UPF selection • Handling SecondaryRatDataUsageReport from SGW/MME and relaying it to CHF • UE Presence-Reporting Feature Support • Handling Gtpv1 Messages for 4g-3g HO • SUPI+IP session and affinity key for 4G/WIFI HO • Avoiding sending of 5G QoS for 4G-Only UE • Handling 5GCNRS and 5GCNRI indication flags from SGW/MME	2021.01.0
First introduced.	2020.03.0

Feature Description

With this release SMF selects DCNR supported UPF for DCNR enabled session when DCNR is configured under query parameters. DCNR isn't a mandatory query parameter for UPF selection. DCNR can be configured in profile network-element UPF. Query parameters / Filter criteria configuration under nf-profile is enhanced to include DCNR support.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > PDU Session Establishment from 4G-Only and Option 3x Capable Devices chapter.

DNN Configuration Limits

Feature Summary and Revision History

Summary Data

Table 11: 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 12: Revision History

Revision Details	Release
The limit for the following configurations in SMF is increased from 512 to 2048: • 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

The limit for the DNN configurations in SMF is increased from 512 to 2048.

The specific DNN configurations are:

- Precedence — The precedence value associated with the subscriber policy.
- Operator policy — The operator policy associated with the subscriber policy.
- DNN policy — The DNN policy.
- DNN profile — The network DNN profile.

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

DSCP Marking for Control Plane Signaling

Feature Summary and Revision History

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

Revision Details	Release
Provided support for DSCP marking of control plane signaling messages	2021.01.0
First introduced.	Pre-2020.02.0

Feature Description

The SMF supports per-interface configurable DSCP marking for control plane signaling messages.

Note The current implementation of DSCP marking supports only per RPC and Endpoint. Also, the customers must be aware of the DSCP code value range and its denoted priority.

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

Emergency Services Support

Feature Summary and Revision History

Summary Data

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

Revision History

Table 13: Revision History

Revision Details	Release
First introduced.	2020.02.5.t1

Feature Description

"Emergency Services" refers to functionalities provided by the serving network when the network is configured to support Emergency Services. Emergency Services are provided to support IMS emergency sessions.

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

Enhanced Limits in Bandwidth Policy Configuration

Feature Summary and Revision History

Summary Data

Table 14: 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 15: Revision History

Revision Details	Release
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
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

The bandwidth policy configuration supports the following maximum limits in this release.

- Up to a maximum of 64 bandwidth policies
- 1000 groups per bandwidth policy
- 1000 bandwidth IDs per bandwidth policy

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

Handling EPS Fallback Failures

Feature Summary and Revision History

Summary Data

Table 16: Summary Data

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

Revision History

Table 17: Revision History

Revision Details	Release
Introduced procedure to support dynamic configuration of the Access Profile configuration.	2020.03.0
New CLI command in the DNN profile configuration to reject calls from 4G-only UE devices.	2020.02.1
First introduced.	Pre-2020.02.0

Feature Description

The EPS fallback failures occurred when the SMF received temporary errors with the N1N2 Transfer Request message during N2HO or XnHO collision.

The SMF sent N1N2TransferReq for PCF-Init-Modify procedure to enforce voice flows. The AMF detected collision with ongoing N2HO or XnHO and responded back with N1N2TransferResp — "409-Conflict" HTTP status code, "Handover-In-Progress" cause, or "Temporary-Reject-Registration-Ongoing" cause. The SMF was unable to retransmit the N1N2TransferReq message after N2HO or XnHO so that gNB could send N2Resp with EPS fallback. Since the SMF was unable to send the N1N2TransferReq message, it led to EPSFB failures.

To handle the EPSFB failures, the SMF performs retransmissions for the N1N2TransferReq message based on **N11-failure-profile** configured under access-Profile. Once all the retries are exhausted, the SMF increments with failure reason "N1N2XferMaxRetryExhausted" under PDU Modify procedure.

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

Handling RADIUS Disconnect and CoA Requests

Feature Summary and Revision History

Summary Data

Table 18: 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 19: Revision History

Revision Details	Release
Added support for the following: • PAP, CHAP, and MSCHAP-based RADIUS authentication • Multiple RADIUS NAS-IP source addresses • Handling RADIUS Disconnect and CoA Requests • RADIUS Accounting on SMF • New attributes in the RADIUS Access Response message	2020.02.5.t1
First introduced.	Pre-2020.02.0

Feature Description

The SMF supports the following attributes in the Disconnect-Message (DM) request to identify the NAS and the user sessions to be terminated.

- 3GPP-IMSI
- 3GPP-NSAPI
- ACCT-SESSION-ID

- CALLED-STATION-ID (DNN)
- FRAMED-IP-ADDR
- FRAMED-IPV6-PREFIX

The SMF supports the following attributes in the DM ACK or NAK response.

- ERROR-CAUSE
- REPLY-MESSAGE

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > RADIUS Client for SMF chapter.

Handling Session Report Rejection Procedure

Feature Summary and Revision History

Summary Data

Table 20: 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 21: Revision History

Revision Details	Release
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

The SMF rejects the UPF-originated Session Report Request during any mismatch in the charging configuration of SMF and UPF. Subsequently, the UPF purges the sessions.

Without knowing about the purge operation, the SMF continues to send the N4 message to the UPF. This action triggers the UPF to send “context not found” message to the SMF for the locally purged sessions.

This behavior impacts the UE experience and results in the loss of charging data. So, the current implementation of handling the session report errors is modified to avoid local purging of sessions on the UPF and also to support graceful clearing of sessions.

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

IPv6 Interface ID Generation—CSCvw93433

Behavior Change Summary and Revision History

Summary Data

Table 22: 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 23: Revision History

Revision Details	Release
First introduced. CDETS ID: CSCvw93433	2021.01.1

Behavior Change

The SMF generates the IPv6 interface ID without International Mobile Subscriber Identity (IMSI) or Extended Unique Identifier (EUI).

Previous Behavior: The SMF generated the IPv6 interface ID in EUI-64 format based on configured or default virtual-mac under DNN. The interface ID is common for all subscribers under DNN. This operation resulted in apps like Google Duo to reject connections due to security policy.

New Behavior: The SMF generates unique 64-bit interface ID which is non-EUI-64 format by using SBI VIP address and CommonId of the subscriber.

That is, IPv6 interface ID = VIP-IP (4 bytes) + CommonId (4 bytes)

By default, **virtual-mac** CLI command is now disabled under DNN configuration.

Table 24: Interface ID for Different Messages

Call Model	PDU Session Establishment Accept	Create Session Response
5G	N11-SBI-VIP+CommonID	Not Applicable
4G	Not Applicable	GTP-VIP+CommonID
WiFi	Not Applicable	GTP-VIP+CommonID
5G->4G	Not Applicable	Not Applicable (N26 HO - there are NAS contents during handover)
4G->5G	Not Applicable (N26 HO - there are NAS contents during handover)	Not Applicable
4G->WiFi	Not Applicable	GTP-VIP+CommonID (Same as 4G)
WiFi->4G	Not Applicable	GTP-VIP+CommonID (Same as 4G)
5G->WiFi	Not Applicable	N11-SBI-VIP+CommonID (Same as 5G)
WiFi->5G	GTP-VIP+CommonID (Same as WiFi)	Not Applicable

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

Local Breakout-based Roaming Support

Feature Summary and Revision History

Summary Data

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

Revision History

Table 25: Revision History

Revision Details	Release
First introduced.	2021.01.0

Feature Description

SMF supports local breakout functionality for in-roamers with this release.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > Local Breakout-based Roaming Support chapter.

Multiple PLMN Support

Feature Summary and Revision History

Summary Data

Table 26: 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 27: Revision History

Revision Details	Release
First introduced.	2021.01.0

Feature Description

The multi-PLMN feature supports multiple PLMNs for homer and roamer networks. A maximum number of 32 PLMNs can be configured.

The primary PLMN configured under profile DNN is used by SMF for peer discovery. This feature also supports emergency calls from 4G and 5G RATs from roamer UEs with SIM (unauthenticated IMSI) and without SIM.

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

N2 Handover with Data Radio Bearer IE—CSCvw93447

Behavior Change Summary and Revision History

Summary Data

Table 28: Summary Data

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

Revision History

Table 29: Revision History

Revision Details	Release
First introduced. CDETS ID: CSCvw93447	2021.01.0

Behavior Change

Once the N2 handover procedure is initiated, the SMF sends Data Radio Bearer (DRB) List IE to the source gNB through the Handover Command Transfer message.

Previous Behavior: The SMF incorrectly sends N3 Uplink (UP) Tunnel Information in Downlink (DL) Forwarding Tunnel IE of Handover Command Transfer message.

New Behavior: The SMF no longer forwards the N3 UP Tunnel Information over Handover Command Transfer message. The SMF forwards DL Forwarding Tunnel Information in Handover Command Transfer message if the same is received from Handover Request Acknowledge Transfer message.

The SMF sends Data Radio Bearer (DRB) List IE to the source gNB through the Handover Command Transfer message if it is received from target gNB in the Handover Request Acknowledge Transfer message. This operation is in compliance with the 3GPP specification 38.413, version 9.3.4.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > Inter gNodeB Handover chapter.

New Outer Header Format

Feature Summary and Revision History

Summary Data

Table 30: 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 31: Revision History

Revision Details	Release
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
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

The SMF accepts new format of the Outer Header information element (IE) from the UPF. The Packet Detection Rule (PDR) of Packet Forwarding Control Protocol (PFCP) session includes this IE. The Outer Header IE is present in the N4 Session Establishment Request message sent over the Sx interface.

The new formtat of Outer Header IE complies to 3GPP TS 29.244 specification, version 16.4.0.

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

PAP, CHAP, MSCHAP-based RADIUS Authentication

Feature Summary and Revision History

Summary Data

Table 32: 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 33: Revision History

Revision Details	Release
Added support for the following: • PAP, CHAP, and MSCHAP-based RADIUS authentication • Multiple RADIUS NAS-IP source addresses • Handling RADIUS Disconnect and CoA Requests • RADIUS Accounting on SMF • New attributes in the RADIUS Access Response message	2020.02.5.t1
First introduced.	Pre-2020.02.0

Feature Description

In releases prior to 2021.01.0, the SMF used only MSISDN values for the user authentication. In this release, the SMF uses the user name and original password to support Point-to-Point Protocol (PPP), Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP), or Microsoft CHAP (MSCHAP) authentication.

The SMF configuration aids in the protocol selection for the user authentication. If the secondary authentication is enabled in DNN profile, the SMF interacts with the RADIUS server to perform RADIUS authentication.

To implement the authentication, the RADIUS client residing within the SMF sends the User-Name and User-Password attributes in Access-Request message to the RADIUS server.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > RADIUS Client for SMF chapter.

Prioritization of Router Advertisement Procedure—CSCvu19134

Behavior Change Summary and Revision History

Summary Data

Table 34: Summary Data

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

Revision History

Table 35: Revision History

Revision Details	Release
First introduced. CDETS ID: CSCvu19134	2021.01.0

Behavior Change

Previous Behavior: SMF queued the Router Advertisement (RA) and Router Solicitation (RS) messages when the PCF-initiated PDU Modification Request is triggered immediately after the Session Create Request.

New Behavior: The SMF sends the RA message and also responds to the RS message when the PCF-initiated PDU Modification Request is triggered immediately after the Session Create Request. That is, the SMF prioritizes the processing of RA and RS messages over the PCF-initiated PDU Modification Request.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > Router Solicit and Router Advertisement chapter.

RADIUS Access Response Attributes

Feature Summary and Revision History

Summary Data

Table 36: 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 37: Revision History

Revision Details	Release
Added support for the following: • PAP, CHAP, and MSCHAP-based RADIUS authentication • Multiple RADIUS NAS-IP source addresses • Handling RADIUS Disconnect and CoA Requests • RADIUS Accounting on SMF • New attributes in the RADIUS Access Response message	2020.02.5.t1
First introduced.	Pre-2020.02.0

Feature Description

This release supports new standard AVPs in the RADIUS Access Response message.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > RADIUS Client for SMF chapter.

RADIUS Accounting

Feature Summary and Revision History

Summary Data

Table 38: 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 39: Revision History

Revision Details	Release
Added support for the following: • PAP, CHAP, and MSCHAP-based RADIUS authentication • Multiple RADIUS NAS-IP source addresses • Handling RADIUS Disconnect and CoA Requests • RADIUS Accounting on SMF • New attributes in the RADIUS Access Response message	2020.02.5.t1
First introduced.	Pre-2020.02.0

Feature Description

The SMF implements the RADIUS Accounting functionality through the use of CLI configuration.

If the RADIUS accounting is enabled and server-group is configured within the DNN profile, then the SMF sends server-group as AAA group in charging-params in N4 session establishment request.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > RADIUS Client for SMF chapter.

RADIUS NAS-IP Address Support

Feature Summary and Revision History

Summary Data

Table 40: 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 41: Revision History

Revision Details	Release
Added support for the following: • PAP, CHAP, and MSCHAP-based RADIUS authentication • Multiple RADIUS NAS-IP source addresses • Handling RADIUS Disconnect and CoA Requests • RADIUS Accounting on SMF • New attributes in the RADIUS Access Response message	2020.02.5.t1
First introduced.	Pre-2020.02.0

Feature Description

SMF supports the RADIUS NAS-IP address functionality for accounting and authentication requests. The selected NAS-IP is encoded in authentication or accounting requests as per RFC2865 and is also used in the source IP address of outbound UDP packets.

In releases prior to 2021.01.0, only one common RADIUS NAS-IP address was used for all requests. This enhancement supports multiple RADIUS NAS-IP source addresses.

Important This functionality supports only the IPv4 NAS-IP address.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > RADIUS Client for SMF chapter.

Randomization of P-CSCF Addresses

Feature Summary and Revision History

Summary Data

Table 42: 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 43: Revision History

Revision Details	Release
Added support for randomization of P-CSCF addresses from DNS.	2021.01.0
First introduced.	Pre-2020.02.0

Feature Description

The SMF service supports random selection of resolved hosts. If a DNS resolution yielded a set of IP addresses for a host and if the **randomize-answers** CLI is enabled, the DNS lookup selects the IP addresses randomly.

The selection method is either round-robin or randomized for the DNS Proxy profile.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > DNS Proxy Integration chapter.

RAT Type Configuration for UDM Failure Handling

Feature Summary and Revision History

Summary Data

Table 44: Summary Data

Applicable Products 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 45: Revision History

Revision Details	Release
RAT type FHT support and graceful timeout handling and its related statistics introduced.	2021.01.0
First introduced.	Pre-2020.02.0

Feature Description

RAT type FHT support over UDM interface and graceful timeout handling and its related statistics introduced.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > Peer NF Failure Handling Support chapter.

Restoration of Old Deployment CLI for Grafana Dashboard—CSCvx73885

Behavior Change Summary and Revision History

Summary Data

Table 46: 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 47: Revision History

Revision Details	Release
First introduced. CDETS ID: CSCvx73885	2021.01.1

Behavior Change

Previous Behavior: Earlier deployment CLI caused Grafana dashboard queries to fail.

The earlier deployment used the following CLI commands:

- K8s name laucs504-cnat
- K8s namespace smf-data
- K8s nf-name smf

New Behavior: In this release, the old deployment CLI is restored to maintain the same behaviour as existed in the SMF Release 2020.02.0. With this deployment CLI, you can configure the app-name, cluster-name, and dc-name that is required for the Grafana dashboard queries.

The new deployment uses the following CLI commands:

- app-name LASMF106
- cluster-name LAUCS504-SMF-DATA

- dc-name LAUCS504

SBI Message Priority Mechanism

Feature Summary and Revision History

Summary Data

Table 48: 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 49: Revision History

Revision Details	Release
SBI Message Priority Mechanism and Message-Prioritization based on Procedures are introduced.	2021.01.0
The Wireless Priority Services feature is fully qualified in this release.	2020.03.0
First introduced. This feature is not fully qualified in this release. For more information, contact your Cisco Account representative.	2020.02.0

Feature Description

The primary usage of SBI Message Priority (SMP) is to provide guidance to 5GC NF acting as HTTP/2 clients or servers while making throttling decisions related to overload control. The priority information may also be used for routing in the proxies.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > Wireless Priority Services chapter.

Session-level URR Limitation

Feature Summary and Revision History

Summary Data

Table 50: 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 51: Revision History

Revision Details	Release
Introduced support for the following: • Zero Usage Report Suppression • Dynamic ACS Configuration Change	2021.01.0
First introduced.	Pre-2020.02.0

Feature Description

The SMF Charging feature includes the following limitations on the N4 interface:

- If the session-level URR (CDR-i) is created once, it will remain through the session. It will not get deleted in the subsequent session (CDR-u).
- If the session-level URR is not created, then it will not be created in the subsequent CDR-u even if session limits are available.

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

SMF Deployment on Bare Metal Server

Feature Summary and Revision History

Summary Data

Table 52: 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 53: Revision History

Revision Details	Release
SMF deployment on bare metal server is supported and fully qualified in this release.	2021.01.0
First introduced.	Pre-2020.02.0

Feature Description

This release supports deployment of SMF on bare metal server. For information on how to deploy SMF Ops Center on bare metal servers (currently Cisco UCS-C servers) environment, see *Operating the SMI Cluster Manager on Bare Metal* section in *Ultra Cloud Core Subscriber Microservices Infrastructure — Operations Guide*.

This release further supports pod level labelling using the CLI configuration. Note that the pod level configuration takes precedence over the layered node level configuration, that is, at the protocol, service, or session level configuration.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > Deploying and Configuring SMF through Ops Center chapter.

Support for Dynamic Change in ACS Configuration

Feature Summary and Revision History

Summary Data

Table 54: 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 55: Revision History

Revision Details	Release
Introduced support for the following: • Zero Usage Report Suppression • Dynamic ACS Configuration Change	2021.01.0
First introduced.	Pre-2020.02.0

Feature Description

The SMF supports dynamic change in the ACS configuration during the run time. The ACS Profile configuration defines various parameters for the ACS profile.

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

TAI Selection From AMF

Feature Summary and Revision History

Summary Data

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

Revision History

Table 56: Revision History

Revision Details	Release
First introduced.	2021.01.0

Feature Description

SMF supports TAI selection from AMF with this release. SMF is added with a new priority attribute in the SmfInfo data type. Which enables the discovery and the selection of SMF based on the relative priorities registered by candidate SMFs in different smfInfo entries with different TAI lists. New SmfInfoList map is supported.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > TAI Selection From AMF chapter.

TFT Handling for Wi-Fi Handovers

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	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 58: Revision History

Revision Details	Release
TFT Handling for Wi-Fi Handovers is supported.	2021.01.0
The Wi-Fi to 5GS Handover with EPS Fallback feature is fully qualified in this release.	2020.02.2
The Wi-Fi to 5GS Handover with EPS Fallback feature is not fully qualified in this release. For more information, contact your Cisco Account representative.	2020.02.1
First introduced.	Pre-2020.02.0

Feature Description

The Cloud Native based SMF+PGW-C product supports the Wi-Fi handover. The cloud-based architecture supports Wi-Fi handovers in 5GS or EPS and non-3GPP untrusted access.

For more information, refer to the UCC 5G SMF Configuration and Administration Guide > Wi-Fi Handovers chapter.

VRF Support

Feature Summary and Revision History

Summary Data

Table 59: Summary Data

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

Revision History

Table 60: Revision History

Revision Details	Release
VRF Support introduced.	2020.02.5
First introduced.	Pre-2020.02.0

Feature Description

It's possible for different MVNOs to have same IP address range in the deployment, this is supported through Virtual Routing and Forwarding(VRF) configuration, where same IP address range can exist in different VRFs.

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

Zero Usage Report Suppression

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	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 62: Revision History

Revision Details	Release
Introduced support for the following: • Zero Usage Report Suppression • Dynamic ACS Configuration Change	2021.01.0

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

The SMF leverages new configuration to control the offline charging records with zero byte data count.

When the **offline zero-usage** CLI command is configured in the Charging Profile configuration mode, the SMF relays the usage to the CHF without any overload of UUC or CDR-U.

The customers can select the UUC or CDRs they want to suppress based on the CLI configuration.

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