Release Notes for UCC 5G SMF, Release 2026.02.0

© 2026 Cisco and/or its affiliates. All rights reserved.

Contents

© 2026 Cisco and/or its affiliates. All rights reserved.

Ultra Cloud Core - Session Management Function, Release 2026.02.0

This Release Notes identifies changes and issues related to the software release of 5G Converged Core Session Management Function (SMF).

The key highlights of this release include:

- **Multi-server Control Plane (CP) scaling**: Enhances network scalability and high availability through a robust, multi-server redundancy model.
- **Enhanced subscriber filtering**: Improves operational efficiency by providing more precise and flexible options for managing subscriber sessions.
- **Intelligent IP conflict detection**: Prevents accidental session drops during inter-network transitions by accurately identifying connection-specific IP conflicts.
- **Resilient policy framework**: Ensures service continuity and consistent quality by maintaining policy enforcement even when primary policy servers are unreachable.
- **Simplified rule configuration**: Reduces administrative effort by allowing the system to automatically recognize predefined rules without requiring specific naming prefixes.
- **Automated N2 failure recovery**: Increases VoNR call rates by enabling the system to automatically resolve transient signaling failures.
- **Per-peer PFCP compression negotiation**: Enables the UPF to automatically negotiate data compression with individual control plane peers.
- **Discovery cache optimization for range-based query parameters**: Improves the efficiency of Network Function (NF) discovery by optimizing how range-based queries are cached, resulting in faster system response times and reduced signaling overhead.

For more information about Ultra Cloud Core - Session Management Function, see the Related resources section.

Release lifecycle milestones

The following table provides EoL milestones for Cisco UCC SMF software:

Table 1. EoL milestone information for UCC SMF, Release 2026.02.0

Milestone	Date
First Customer Ship (FCS)	23-Apr-2026
End of Life (EoL)	23-Apr-2026
End of Software Maintenance (EoSM)	22-Oct-2027
End of Vulnerability and Security Support (EoVSS)	22-Oct-2027
Last Date of Support (LDoS)	31-Oct-2028

These milestones and the intervals between them are defined in the Cisco Ultra Cloud Core (UCC) Software Release Lifecycle Product Bulletin available on cisco.com.

© 2026 Cisco and/or its affiliates. All rights reserved.

New software features

This section provides a brief description of the new software features introduced in this release.

Table 2. New software features for UCC SMF, Release 2026.02.0

Product impact	Feature	Description
Software Reliability	Multi-server Control Plane (CP) scaling	This feature implements a 1-active/2-standby pod model across master nodes to improve scalability. It simplifies configuration through centralized virtual IP management, separates Sx/N4 interfaces, and uses BGP for high availability.
Software Reliability	Enhanced clear subscriber filtering	The `clear subscriber` command now supports connected-duration, and max-count filters. These features require an updated CDL framework. Additionally, it extends non-VoLTE and non-emergency capabilities with bulk combination options. Commands introduced: • **clear subscriber connected-duration [greater-than | lesser-than | equals] <seconds>:** Enables clearing of sessions based on the time they have been connected. • **clear subscriber creation-time [before | after] <timestamp>:** Extends the existing creation-time filter to allow clearing of sessions created after a specific time. • **clear subscriber max-count lesser-than <value>:** Allows for the clearing of a specific number of random sessions.
Software Reliability	Duplicate static IP detection on Attach over Attach PDU sessions	This feature provides duplicate IP detection to be RAT-aware. The mechanism now restricts conflict detection to the same RAT type, preventing erroneous session rejection when users transition between 4G and 5G sessions. Command introduced: **rat no-match** and **attributes session-type all** – when both these commands are configured in the Event Management policy, the system rejects new session and releases the old session.
Software Reliability	Support for predefined rules without prefix identifiers	The SMF now automatically identifies rulebases by matching received names against internal configurations, allowing predefined rules to be processed without requiring specific prefix identifiers.
Software Reliability	Local N7 policy usage during PCF failovers	Enables the SMF to switch to locally configured policies providing minimum QoS guarantees during PCF create or update failures.

© 2026 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
Software Reliability	Configuration based N2 failure handling	You can now improve VoNR call success rates by configuring the Session Management Function (SMF) to automatically retry N2 modify procedures after specific failure causes. This feature introduces a new CLI configuration under the access profile. You specify the N2 message type, the failure cause codes, and the retry parameters, including the delay interval and maximum number of retry attempts. When the SMF receives a configured failure, it suspends the current procedure, initiates a timer based on your settings, and automatically retransmits the N2 message upon timer expiry. Command introduced: The following command structure is added to the profile access configuration mode: **n2 message-handling message-type [pdu-sess-rsrc-mod-resp] condition** *condition_id* **cause** *cause_list* **action retry attributes retry-after** *retry_interval* **max-retry** *max_retry* **Default Setting**: Disabled – Configuration required
Software Reliability	Traffic monitoring in Intra-rack geo redundancy	This feature enables pod monitoring of all the app-infra pods, enabling enhanced failure detection and automatic failover. When the configured threshold percentage of pod replicas fail, the Geo pod initiates a switchover to the mated pair site to maintain service continuity. The traffic monitoring capability prevents the service outages during the failure scenarios. This feature allows the geo-replication pod to monitor the traffic on the STANDBY instance.
Software Reliability	Uniformity in Compression at N4 and Sx Interfaces	Introduced per-peer PFCP compression negotiation between UPF and control plane using capability exchange during association setup. This enhancement allows UPF to dynamically select compressed or uncompressed PFCP messaging based on peer support, enabling coexistence of CUPS and converged core (cnSGW/SMF) peers on the same UPF while maintaining backward compatibility.
Ease of Use	Discovery cache optimization for range-based query parameters	With this release, SMF supports discovery cache optimization for range-based query parameters. An intelligent caching mechanism is introduced that allows the system to store and reuse NF profiles based on ranges of identifiers (such as SUPI ranges) rather than individual identity entries. This feature improves the efficiency of Network Function (NF) discovery within the Cisco NF environment.

Changes in behavior

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

© 2026 Cisco and/or its affiliates. All rights reserved.

Table 3. Behavior changes for UCC SMF, Release 2026.02.0

Description	Behavior changes
Inclusion of Serving Network MCC and MNC in N4 Modification Requests [CSCws84012]	**Previous Behavior**: The SMF did not transmit the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the serving network within N4 modification requests. **New Behavior**: Starting from the April 2026 release, the SMF now consistently transmits the MCC and MNC of the serving network within the N4 modification request. **Customer Impact**: This change ensures that the User Plane Function (UPF) receives accurate serving network metadata during session modifications, which may be required for specific charging, reporting, or policy enforcement functions.
Updated APN AMBR capping and rounding logic [CSCwt07758]	**Previous Behavior**: For devices with Dual Connectivity with New Radio (DCNR) disabled, APN Aggregate Maximum Bit Rate (AMBR) values were capped at 4.2 Gbps across all sessions. **New Behavior**: APN AMBR capping at 4.2 Gbps is now restricted to sessions where the Gx interface is enabled. For all other sessions, this cap has been removed. Additionally, if the corresponding CLI is enabled, APN AMBR values will now be rounded up to the nearest supported value. **Customer Impact**: Customers will see uncapped APN AMBR values in GTPv2-C messages for non-Gx sessions.
Migration from Kubernetes Ingress NGINX controller to gateway API (HTTPRoute) with NGF [CSCwt33517]	**Previous Behavior**: • Used Kubernetes Ingress (networking.k8s.io/v1), always deployed • Managed by nginx-ingress-controller • URL rewrite and headers via nginx annotations • TLS configured in Ingress **New Behavior**: • Supports HTTPRoute (gateway.networking.k8s.io/v1), conditionally deployed • Managed by NGINX Gateway Fabric (NGF) • URL rewrite and headers via Gateway API filters • TLS handled by shared Gateway **Customer Impact**: • No disruption; Ingress and HTTPRoute coexist • Traffic switch at platform level • No changes to hostname, routing, backend, or access model
Improved N2 retry timer management during PDU modification [CSCwt84705]	**Previous Behavior**: During a PDU modification procedure, if an N2 failure triggered a retry timer, the timer would continue to run even if an N1 response was received. This prevented the SMF from properly terminating the failed modification procedure. **New Behavior**: The SMF now immediately stops the N2 retry delay timer upon receiving an N1 response. The system then proceeds to clean up resources and correctly marks the PDU modification procedure as a failure. **Customer Impact**: This fix ensures that PDU modification procedures are terminated correctly and resources are cleaned up promptly when a failure occurs, preventing hung sessions or unnecessary delays.

© 2026 Cisco and/or its affiliates. All rights reserved.

Description	Behavior changes
Sequence number handling for MBC-triggered UBR [CSCwt13922]	**Previous Behavior**: When SMF received an MBC without AMBR or Default QoS changes, the resulting UBR was sent directly to sgw-service and did not reuse the MBC's sequence number. **New Behavior**: The MBC-triggered UBR now always uses the same sequence number as the original MBC, regardless of AMBR or Default QoS changes. **Customer Impact**: Ensures consistent sequence number handling, resolving issues where UBR did not reuse the MBC sequence number in certain scenarios.
qosFlowDescription IE handling in EPCO/PCO within bearer context of CBR message [CSCwt09790]	**Previous Behavior**: qosFlowDescription IE in EPCO/PCO within Bearer-Context of a CBR message included EPS Bearer Identity (EBI) IE containing the previous call's dedicated bearer EBI. **New Behavior**: qosFlowDescription IE in EPCO/PCO within Bearer-Context of a CBR message no longer includes EBI IE. **Customer Impact**: Prevents semantic errors on the UE caused by EBI IE.
NRF subscription request - subscriptionId field handling [CSCwt26067]	**Previous Behavior:** SMF included the subscriptionId field with an empty value (" subscriptionId" : " ") in the NRF subscription creation request (POST/nnrf-nfm/v1/subscriptions). As per 3GPP TS 29.510, subscriptionId is a read-only attribute generated by NRF in the response and must not be present in the request. **New Behavior**: SMF omits the subscriptionId field from the NRF subscription creation request when it is not set. NRF generates and returns the subscriptionId only in the response, in accordance with 3GPP TS 29.510. **Customer Impact**: This change aligns the implementation with 3GPP TS 29.510 and ensures standards compliance.
Handling of conditional or optional IEs and Supportedfeatures in N11/N16 messages [CSCwt28379]	**Previous Behavior**: Conditional or optional IEs were sent with null/empty values in compliance with specification for nsmf-pdusession v.16. Supportedfeatures with 0 value were sent in nsmf-pdusession specification v.15, and mandatory feature flags HOFAIL, ES3XX, and AASN were included in Supportedfeatures in nsmf-pdusession specification v.16. **New Behavior**: To optimize N11 and N16 messaging, the SMF now omits null or empty conditional and optional IEs. • nsmf-pdusession specification v.15: SupportedFeatures are omitted if the value is empty. • Following the nsmf-pdusession v16 specification, the HOFAIL, ES3XX, and AASN flags are now excluded by default. A new CLI parameter has been added to the SMF profile to enable these flags if required: profile smf > instances > supported-features [hofail, es3xx, aasn] • By default, only the VQOS bit is included; DTSSA and ACSCR bits are sent only when explicitly enabled. **Customer Impact**: Null or empty conditional/optional IEs and supportedfeatures with empty values are skipped on N11/N16 messages, and mandatory feature flags are excluded unless explicitly enabled using a new CLI parameter.
Handling PDU session failure due to missing mandatory feature flags in supportedFeatures IE [CSCwt39026]	**Previous behavior**: In the release 16, the SMF is not sending the mandatory feature flags (HOFAIL, ES3XX and AASN) in supportedFeatures IE in the N11 and N16 messages. Due to this, the PDU session establishment is failing. **New behavior**: In order to handle this error, SMF does not include the mandatory feature flags (HOFAIL, ES3XX and AASN) in the supportedFeatures IE in the N11 and N16 messages. SMF allows to configure these flags using a CLI under supported-features.

© 2026 Cisco and/or its affiliates. All rights reserved.

Description	Behavior changes
SNSSAI encoding in N1 accept message during roaming [CSCwt33699]	**Previous Behavior**: SNSSAI was not encoded properly in N1 accept when both visitor SNSSAI (SST only) and mapped SNSSAI (SST and SD) were sent during roaming scenarios. **New Behavior**: SNSSAI is now encoded correctly in N1 accept with both visitor SNSSAI (SST with or without SD) and mapped SNSSAI (SST with or without SD) during roaming scenarios.
Compliance for Bidirectional Forwarding Detection. (BFD) source port allocation [CSCwt53390]	**Previous Behavior**: BFD sessions used fixed or sequential source ports for UDP connections. If a port was already in use, the system waited five seconds before retrying the same port. This caused delays in session establishment and risked infinite retry loops, failing to meet RFC 5881 standards. **New Behavior**: BFD now follows RFC 5881 by randomly selecting source ports from the IANA range (49152-65535). If a port is in use, the system immediately tries a new random port (up to five times) before falling back to a sequential scan. The previous five-second delay has been removed for port conflicts. The session terminates gracefully if all available ports are exhausted or after 10 non-port-related errors. **Customer Impact**: This change improves interoperability with third-party BFD implementations and ensures faster, more robust session establishment in environments with high port contention.
DSCP marking for HTTP2/ping messages [CSCwt66609]	**Previous Behavior**: Even when DSCP marking was enabled, outgoing HTTP2/Ping messages sent by the NF were transmitted without the DSCP value in the packet header, unlike other outgoing packets. **New Behavior**: When DSCP marking is enabled for a specific remote host or RPC, the outgoing HTTP/2 Ping messages sent to that host now include the configured DSCP value in the packet header, ensuring consistency with other outgoing traffic.
Incorrect PLMN_CH trigger in CHF update during inter-RAT HO [CSCwt35295]	**Previous Behavior**: During an inter-RAT handover (HO), the SMF was incorrectly sending a CHF Update with a PLMN_CH trigger to the CHF, even when no actual PLMN change had occurred. **New Behavior**: The PLMN change detection logic has been corrected. The SMF now sends a CHF Update with a PLMN_CH trigger to the CHF only when a verified PLMN change is detected during an inter-RAT HO. **Customer Impact**: This correction eliminates unnecessary signaling to the CHF, leading to improved system efficiency and reduced load on the CHF.
PDU session rejection for invalid SD values [CSCws68075]	**Previous behavior**: SMF accepted PDU session establishment requests even if the subscription data received from the Unified Data Management (UDM) contained an invalid Slice Differentiator (SD) value. **New behavior**: SMF now validates the SD value provided by the UDM. If the SD value is found to be invalid, the SMF now rejects the PDU session establishment request. **Customer Impact**: Customers may observe PDU session rejections if the UDM provides non-compliant SD values.
Corrected handling of ModifyBearerCommand received from invalid source [CSCwt98274]	**Previous Behavior**: When SMF received a ModifyBearerCommand from an unauthorized or invalid source, it incorrectly accepted the message and returned a success response. **New Behavior**: SMF now validates the source of ModifyBearerCommand message. If a request is received from an invalid source, SMF rejects the command and returns a failure indication with the cause code EGTP_CAUSE_CONTEXT_NOT_FOUND. **Customer Impact**: This change improves network security and session integrity by ensuring that only valid, authorized sources can modify bearer contexts.

© 2026 Cisco and/or its affiliates. All rights reserved.

Description	Behavior changes
Asynchronous 5G Cleanup for create-over-create scenarios (5G attach followed by 4G attach) [CSCwt64198]	**Previous Behavior**: In " create-over-create" scenarios (specifically a 5G attach immediately followed by a 4G attach), the SMF performed cleanup procedures for 5G interfaces synchronously. This required each interface to finish its teardown before the subsequent 4G attach could proceed, potentially slowing down the transition. **New Behavior**: The SMF now performs 5G interface cleanups asynchronously (with the exception of N4 and N10 interfaces). This allows the 5G release procedure to conclude significantly faster, enabling the 4G attach to begin immediately. **Customer Impact**: This change results in faster and more seamless transitions between 5G and 4G.

Resolved issues

This table lists the resolved issues in this specific software release.

Note: This software release may contain bug fixes first introduced in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool. To search for a documented Cisco product issue, type in the browser: <bug_number> site:cisco.com.

Table 4. Resolved issues for UCC SMF, Release 2026.02.0

Bug ID	Description
SMF	
CSCwt01329	GeoPod TriggerGR takes more time when multiple etcd get operation timed-out
CSCwt07758	SMF - bitrates rounded-up UBR sent with wrong values.
CSCwt09790	SMF - EBI in PCO CBR sent wrongly post EPSFB.
CSCwt13922	CC Enable-bypass UBR sent with wrong sequence number.
CSCwt16067	SMF sends TIME_LIMIT & `FINAL` in the same `UsedUnitContainer` when preemptive charging is enabled and SOT is not received.
CSCwt16290	Static IP allocation fails after GR switchover when new static IP pools and dnn added multiple times
CSCwt26067	SubscriptionId is empty in request to NRF.
CSCwt28379	Suppressing IE with null values on N16.
CSCwt29933	Add Retry mechanism to etcd Grant during setTTL.
CSCwt31579	PAPN SMF is not allocating IPAM from Dynamic Pool and unable to recover the same as well.
CSCwt33061	Roaming-Flow - AMF-N11 Released EBI Error log.
CSCwt33699	vSMF does not send correct value of mapped Slice SST and SD in PDU Session establishment accept.
CSCwt35295	PLMN_CH trigger getting armed for inter-RAT HO.

© 2026 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwt39953	Debug message required when N16 update is suppressed.
CSCwt47973	Redirect URL sent from PCF is observed only in the FAR of the access side for 5G calls.
CSCwt51430	ConfigMap with null values seen as <no value> with scale config.
CSCwt53190	Upon session report with zero usage for online RG, CDR drop is not happening.
CSCwt55728	Incorrect BCM in Create PDP Context Response in SMF.
CSCwt64196	Collision -WPS : DLDR and N7 notify, SMF sending default qos for paging.
CSCwt64198	SMF-Release over Release collision - Further attaches have impact.
CSCwt68370	SMF does not handle create over create from different RAT (4G to wifi/5G).
CSCwt76651	callhold and unhold results in multiple create QERs towards UPF.
CSCwt79999	SMF sets IPv4 flag in IPv6-only F-TEID (0.0.0.0 sent).
CSCwt81933	2026.02.0 SMF NED requires package reload "force" parameter to load.
CSCwt81979	SMF not updating RAT-TYPE when changed inbetween HO.
CSCwt85627	Unnecessary EBI Assignment during VoNR Flow multiparty calls.
CSCwt90003	Rest-ep pod got restarted in a 5G Cloud Core SMF environment.
IoT	
CSCws95725	UDM is not able to process supportedfeatures value sent by SMF.

Open issues

This table lists the open issues in this specific software release.

Note: This software release may contain open bugs first identified in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool. To search for a documented Cisco product issue, type in the browser: <bug_number> site:cisco.com.

Table 5. Open issues for UCC SMF, Release 2026.02.0

Bug ID	Description
SMF	
CSCwt63140	Sync between racks lost after a scale run of more than 1500 3GPP LI provisions.
CSCwt98424	SMF-monsub - session rule deletion not displayed.
CSCwt80012	Clear subscriber `non-volte` filter combined with `max-count` does not honor requested session count.

© 2026 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
IoT	
CSCwt91302	SMF N40 update and terminate message failure.
CSCws83533	Rest Ep pod go routine and memory spike observed during SCP C call model run with mTLS enabled.

Compatibility

This section lists compatibility information of the Cisco UCC software products that are verified to work with this version of the UCC SMF software.

Table 6. Compatibility information for UCC SMF, Release 2026.02.0

Product	Supported Release
Ultra Cloud Core SMI	2026.02.1.07
Ultra Cloud CDL	2.2.0
Ultra Cloud Core UPF	2026.02.0
Ultra Cloud cnSGWc	2026.02.0

Supported software packages

This section provides information about the release packages associated with UCC SMF software.

Table 7. Software packages for UCC SMF, Release 2026.02.0

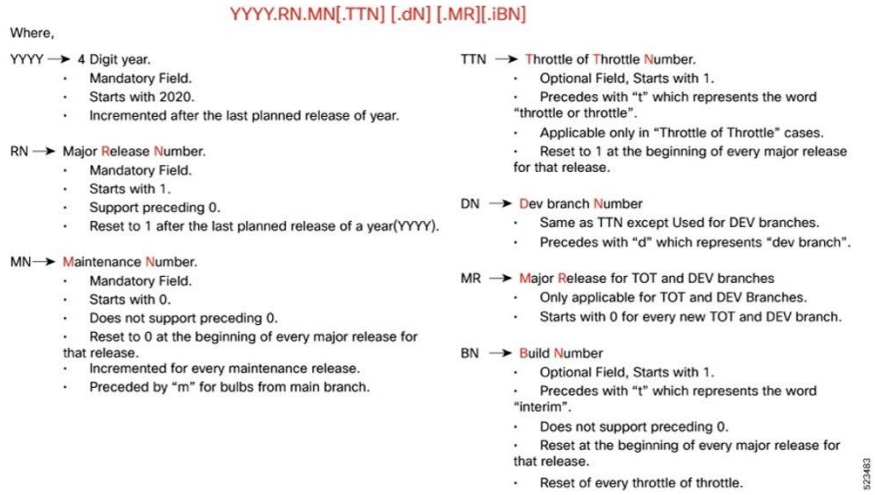
Software Package	Description	Release
ccg-2026.02.0.SPA.tgz	The SMF offline release signature package. This package contains the SMF deployment software, NED package, as well as the release signature, certificate, and verification information.	2026.02.0
ncs-6.4.8.2-ccg-nc-1.1.2026.02.0.tar.SPA.tgz	The NETCONF NED package. This package includes all the yang files that are used for NF configuration. Note that NSO is used for the NED file creation.	6.4.8.2
ncs-6.1.14-ccg-nc-1.1.2026.02.0.tar.SPA.tgz		6.1.14

Cloud native product version numbering system

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

© 2026 Cisco and/or its affiliates. All rights reserved.

Figure 1. Cloud native product versioning format and description



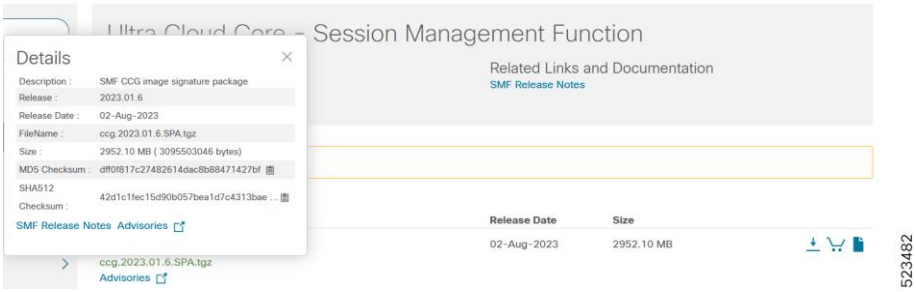
The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research software releases.

Software integrity version

To verify the integrity of the software image you have from Cisco, you can validate the SHA512 checksum information against the checksum identified by Cisco for the software.

Image checksum information is available through **Cisco.com Software Download Details**. To find the checksum, hover the mouse pointer over the software image you have downloaded.

Figure 2. Sample of converged core gateway software image



At the bottom you find the SHA512 checksum, if you do not see the whole checksum you can expand it by pressing the " ..." at the end.

To validate the information, calculate a SHA512 checksum using the information in the following table and verify that it matches the one provided on the software download page.

To calculate a SHA512 checksum on your local desktop, see this table.

Table 8. Checksum calculations per operating system

Operating System	SHA512 checksum calculation command examples
Microsoft Windows	Open a command line window and type the following command:

© 2026 Cisco and/or its affiliates. All rights reserved.

Operating System	SHA512 checksum calculation command examples
	`> certutil.exe -hashfile <filename.extension> SHA512`
Apple MAC	Open a terminal window and type the following command: `$ shasum -a 512 <filename.extension>`

Linux	Open a terminal window and type the following command:
	`$ sha512sum <filename.extension>`
	OR
	`$ shasum -a 512 <filename.extension>`

Note: <filename> is the name of the file. <extension> is the file type extension (for example, .zip or .tgz).	

If the SHA512 checksum matches, you can be sure that no one has tampered with the software image or the image has not been corrupted during download.

If the SHA512 checksum does not match, we advise you not to attempt upgrading any systems with the corrupted software image. Download the software again and verify the SHA512 checksum again. If there is a constant mismatch, please open a case with the Cisco Technical Assistance Center.

Certificate validation

SMF software images are signed via x509 certificates. Please view the.README file packaged with the software for information and instructions on how to validate the certificates.

Related resources

This table provides key resources and links to the support information and essential documentation for cnSGWc and other Ultra Cloud Core (UCC) products.

Table 9. Related resources and additional information

Resource	Link
SMF documentation	Session Management Function
cnSGWc documentation	Serving Gateway Function
SMI documentation	Subscriber Microservices Infrastructure
UPF documentation	User Plane Function
Service request and additional information	Cisco Support

Legal information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2026 Cisco Systems, Inc. All rights reserved.