Release Notes for UCC 5G AMF, Release 2025.03.0

Contents

Ultra Cloud Core - Access and Mobility Management Function, Release 2025.03.0

This Release Notes identifies changes and issues related to the software release of Access and Mobility Management Function (AMF).

The key highlights of this release include:

- **Enhanced Traffic Management**: Introduction of Differentiated Services Code Point (DSCP) marking capabilities on N2/SCTP and N26/GTPC interfaces, allowing AMF to apply DSCP values to outgoing packets for appropriate traffic handling and Quality of Service (QoS) prioritization.
- **Improved Scalability and Resilience**: Support for Stateless Next-Generation Application Protocol (NGAP) Protocol Endpoint (EP) Deployment, enabling the horizontal scaling of AMF NGAP protocol pods and facilitating a transition from an Active-Standby to an Active-Active deployment model for enhanced performance and high availability.

For more information on the AMF software products, see the Related resources section.

Release Lifecycle Milestones

This table provides EoL milestones for Cisco UCC AMF software:

Table 1. EoL milestone information for Ultra Cloud Core - Access and Mobility Management Function, Release 2025.03.0

Milestone	Date
First Customer Ship (FCS)	14-Aug-2025
End of Life (EoL)	14-Aug-2025
End of Software Maintenance (EoSM)	12-Feb-2027
End of Vulnerability and Security Support (EoVSS)	12-Feb-2027
Last Date of Support (LDoS)	29-Feb-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.

New software features

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

Table 2. New software features for Ultra Cloud Core - Access and Mobility Management Function, Release 2025.03.0

Product impact	Feature	Description
Software Reliability	DSCP marking	AMF applies DSCP marking to outgoing packets on the N2/SCTP and N26/GTPC interfaces, ensuring that traffic is handled appropriately. Command introduced: • **config { instance instance-id** *instance_id* **{ endpoint sctp { dscp** *dscp_value* **} }**

Product impact	Feature	Description
		} – Used to configure the DSCP value for N2-SCTP interface. • **config { instance instance-id** *instance_id* **{ endpoint gtp { dscp** *dscp_value* **} } }** – Used to configure the DSCP value for N26-GTPC interface. **Default Setting**: Disabled – Configuration Required
Upgrade	Stateless NGAP protocol EP deployment	You can now enable horizontal scaling of AMF NGAP protocol pods by transitioning from an existing Active-Standby mode of deployment to an Active-Active deployment model. Command introduced: **amf-services** *amf_service_name* **{ stateless-proto-ep enabled }** – Used to enable the stateless protocol EP deployment. **Default Setting**: Disabled – Configuration Required

Changes in behavior

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

Table 3. Behavior changes for Ultra Cloud Core – Access and Mobility Management Function, Release 2025.03.0

Description	Behavior changes
HTTP header " 3gpp-Sbi-discovery-service-names" in SCP Model D indirect communication	**Previous Behavior**: The AMF used to send the " 3gpp-Sbi-Discovery-service-names" HTTP header to the SCP in an array format for all messages. Example: 3gpp-sbi-discovery-service-names : [" nsmf-pdusession"] **New Behavior**: The " 3gpp-Sbi-Discovery-service-names" HTTP header is now sent as a plain string to the SCP, but only when you configure the discovery-params [service-names] within the SCP network element profile. Example: 3gpp-sbi-discovery-service-names : nsmf-pdusession
Enhancement to Commercial Mobile Alert System (CMAS) send RAN response indication cache validity	**Previous Behavior:** For storing the send RAN response indication for CMAS broadcast messages, a hardcoded validity of 24 hours was used. This could lead to a continuous memory increase in ETCD pods during CMAS longevity overnight, potentially causing stability issues and impacting call models during upgrades and restarts. **New Behavior:** A new configuration is now available to adjust the cache validity for the CMAS send RAN response indication, allowing for improved memory management and system stability. The default cache validity is 2 hours. To configure the validity timer value, use the timers **cmas-send-response value** CLI command in the Call Control Policy configuration mode. **Note**: If no timer value is explicitly configured, the default cache timer value is 2 hours.

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 Ultra Cloud Core – Access and Mobility Management Function, Release 2025.03.0

Bug ID	Description
CSCwi71509	Memory consumption of Stand-by Protocol-ep pod is high during performance run
CSCwk45189	rest ep pod restarted with error at infra.(*RestRouter).populateHttpResponse.
CSCwq35018	Collision b/w UE context Rel & Service Req is not handled properly

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 Ultra Cloud Core – Access and Mobility Management Function, Release 2025.03.0

Bug ID	Description
CSCwq73943	Service pod leak observed during AMF ST 7K longevity.

Compatibility

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

Table 6. Compatibility information for Ultra Cloud Core – Access and Mobility Management Function, Release 2025.03.0

Product	Supported Release
Ultra Cloud Core SMI	2025.03.1.10
Ultra Cloud CDL	1.12.2

Supported software packages

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

Table 7. Software packages for Ultra Cloud Core – Access and Mobility Management Function, Release 2025.03.0

Software Package	Vesrion
amf.2025.03.0.SPA.tgz	2025.03.0
cdl-1.12.2-amf-2025.03.0.SPA.tgz	1.12.2
NED package	ncs-6.4.5-amf-nc-2025.03.0
NSO	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.

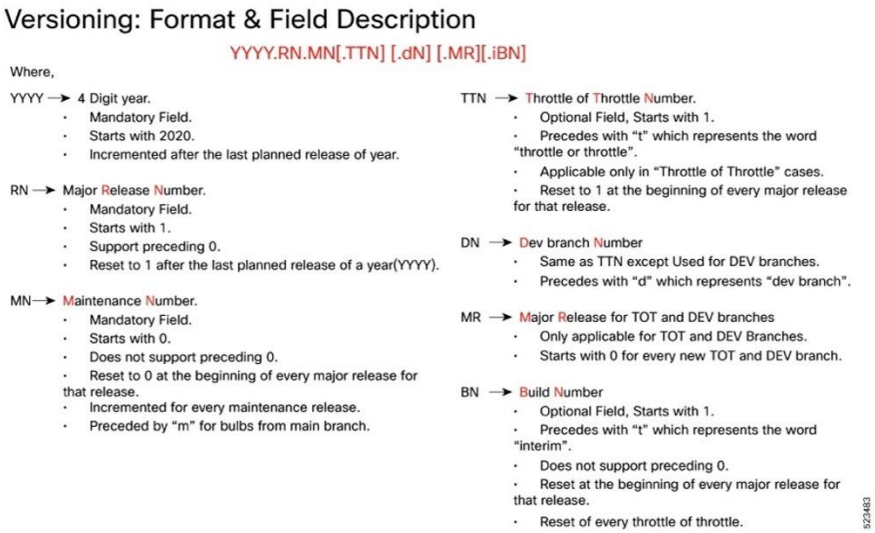


Figure 1. Cloud native product versioning format and description

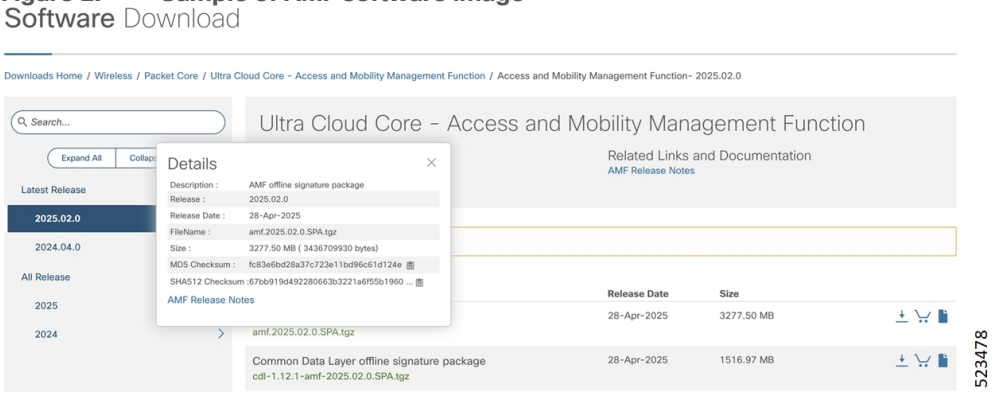
The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research 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 AMF 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. SHA512 checksum calculation commands by operating system

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

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

<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

AMF 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

The following table provides key resources and links to the essential documentation and support information for the Ultra Cloud Core AMF and Subscriber Microservices Infrastructure (SMI).

Table 9. Related resources and additional information

Resource	Link
AMF documentation	Access and Mobility Management Function
SMI documentation	Subscriber Microservices Infrastructure
Service Request and Additional information	Cisco Support

Legal information