Release Notes for UCC 5G AMF, Release 2025.04.0

Contents

Ultra Cloud Core – Access and Mobility Management Function, Release 2025.04.0 3
New software features 3
Changes in behavior 4
Resolved issues 4
Open issues 5
Compatibility 5
Supported software packages 5
Related resources 7
Legal information 7

Ultra Cloud Core - Access and Mobility Management Function, Release 2025.04.0

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 Network Reliability and Session Continuity**: Introduction of AMF Sets, allowing multiple AMF instances to share user context and provide seamless service, even during failures. This feature ensures uninterrupted service by enabling quick takeover by another AMF in the set and supports spanning across different Kubernetes clusters and regions.

  Note: This feature is not fully qualified in this release and is available only for testing purposes. For more information, contact your Cisco account representative.

- **Enhanced Routing and High Availability**: Introduction of Border Gateway Protocol (BGP) to enable dynamic, loop-free inter-domain routing between autonomous systems, allowing prioritization of service IP addresses and ensuring high availability through efficient traffic flow management and support for pod failovers.

- **IPv6 Support for N26 Interface**: Enhanced N26 interface to support IPv6 protocol, enabling the AMF to handle existing N26 message interactions with MME over IPv6, complementing the existing IPv4 support.

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 2025.04.0

Milestone	Date
First Customer Ship (FCS)	30-Oct-2025
End of Life (EoL)	30-Oct-2025
End of Software Maintenance (EoSM)	30-Apr-2027
End of Vulnerability and Security Support (EoVSS)	30-Apr-2027
Last Date of Support (LDoS)	30-Apr-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 2025.04.0

Product impact	Feature	Description
Upgrade	AMF Set Deployment in Different Cluster	AMF Sets improve network reliability and session continuity by allowing multiple AMF instances to share user context and provide seamless service, even during failures. Multiple AMFs in an AMF Set share UE context using a centralized data lake (CDL) for synchronization. If one AMF fails, another in the set quickly takes over, ensuring uninterrupted service. AMF Sets can span different Kubernetes clusters and regions, with unique identifiers for each set and region. The system supports context sharing and subscriber migration across AMFs, with secure data stored and synchronized in the CDL. Command introduced: `amf-services amf_services_name { guamis { mcc mcc_value | mnc mnc_value | region-id region_id | set-id set_id | pointer pointer_value { amf-name amf_name | backup-amf-name backup_amf_name | offline-mode } } }` – Used to configure the amf-name and backup-amf-name for specific GUAMIs under AMF services. **Default Setting**: Disabled – Configuration Required **Note**: This feature is not fully qualified in this release and is available only for testing purposes. For more information, contact your Cisco account representative.
Software Reliability	Border Gateway Protocol (BGP)	BGP feature enables dynamic, loop-free inter-domain routing between autonomous systems, allowing you to prioritize service IP addresses and ensure high availability. It works by using BGP speaker pods to advertise service IP addresses for incoming traffic and learn routes for outgoing traffic. BGP peers establish TCP connections and exchange routing information, with preference values determining traffic flow, especially in active-standby configurations. This feature also supports handling pod failovers and offers various commands for configuration and monitoring. Command introduced: `router bgp local_as_number` – Used to configure the autonomous systems (AS) and IP address for the BGP router. **Default Setting**: Disabled – Configuration Required
Upgrade	IPv6 Enablement on N26 Interface	AMF already supporting the N26 interface messages over IPv4 protocol is now enhanced to support the existing N26 message interaction with MME over IPv6 protocol. Command introduced: `interface n26 { instancetype { dual | ipv4 | ipv6 } }` – Used to set the IP stack type for the N26 interface. **Default Setting**: Disabled – Configuration Required

Changes in behavior

There are no behavior changes in this release

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 3. Resolved issues for Ultra Cloud Core – Access and Mobility Management Function, Release 2025.04.0

Bug ID	Description
CSCwn53811	AMF does not send RINMR in SMC when NAS message container decoding fails
CSCwq35018	Collision b/w UE context Rel & Service Req is not handled properly

Open issues

There are no open issues in this release.

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 4. Compatibility information for Ultra Cloud Core – Access and Mobility Management Function, Release 2025.04.0

Product	Supported Release
Ultra Cloud Core SMI	2025.04.1.15
Ultra Cloud CDL	1.12.3

Supported software packages

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

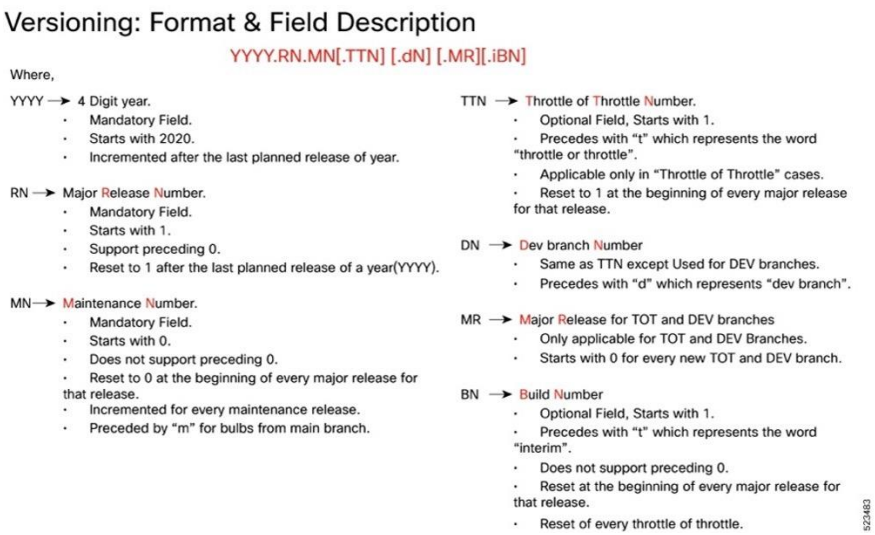
Table 5. Software packages for Ultra Cloud Core – Access and Mobility Management Function, Release 2025.04.0

Software Package	Vesrion
amf.2025.04.0.SPA.tgz	2025.04.0
cdl-1.12.3-amf-2025.04.0.SPA.tgz	1.12.3
NED package	ncs-6.4.8-amf-nc-2025.04.0
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**



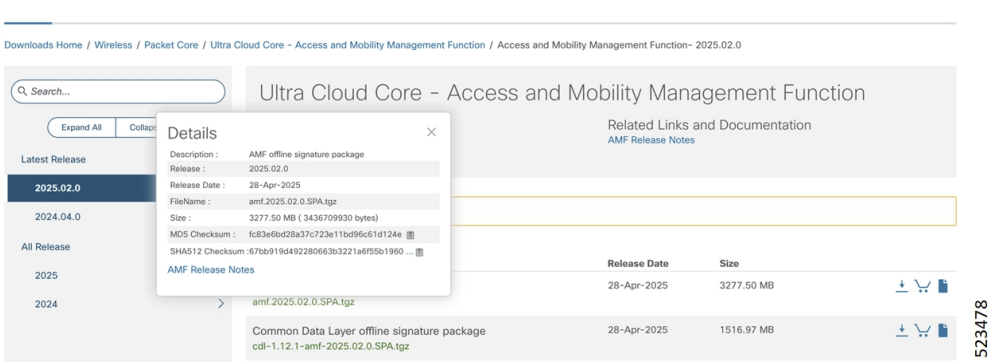
The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research 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 6. 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 7. 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

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 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.