Release Notes for UCC 5G AMF, Release 2025.02.1

Contents

Ultra Cloud Core - Access and Mobility Management Function, Release 2025.02.1

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

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 2025.02.1

Milestone	Date
First Customer Ship (FCS)	30-Apr-2025
End of Life (EoL)	30-Apr-2025
End of Software Maintenance (EoSM)	29-Oct-2026
End of Vulnerability and Security Support (EoVSS)	29-Oct-2026
Last Date of Support (LDoS)	31-Oct-2027

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 2025.02.1

Feature	Description
Configuration control for managing RINMR flag	AMF provides CLI configuration to enable and manage features such as the handling of the RINMR flag within the additional 5G Security Information IE of the security mode command message. The Retransmission of Initial NAS Message Requested (RINMR) is a specific bit within the 5G security Information IE. When set, the RINMR bit instructs the UE to retransmit the entire initial Non-Access Stratum (NAS) message, such as registration request, if it fails the integrity check. Command introduced: **feature-support-ie rinmr-supported** – Configures the RINMR flag support at AMF in security mode command. **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 2025.02.1

Bug ID	Description
CSCwn53811	AMF does not send RINMR in SMC when NAS message container decoding fails

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 4. Open issues for Ultra Cloud Core – Access and Mobility Management Function, Release 2025.02.1

Bug ID	Description
CSCwo87202	Service pod memory leak seen after SCTP pod kill.

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 5. Compatibility information for Ultra Cloud Core – Access and Mobility Management Function, Release 2025.02.1

Product	Supported Release
Ultra Cloud Core SMI	2025.02.1.17
Ultra Cloud CDL	1.12.1

Supported software packages

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

Table 6. Software packages for Ultra Cloud Core – Access and Mobility Management Function, Release 2025.02.1

Software Package	Vesrion
amf.2025.02.1.SPA.tgz	2025.02.1
cdl-1.12.1-amf-2025.02.1.SPA.tgz	1.12.1

Software Package	Vesrion
NED package	ncs-6.4.3-amf-nc-2025.02.1
NSO	6.4.3

Cloud native product version numbering system

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

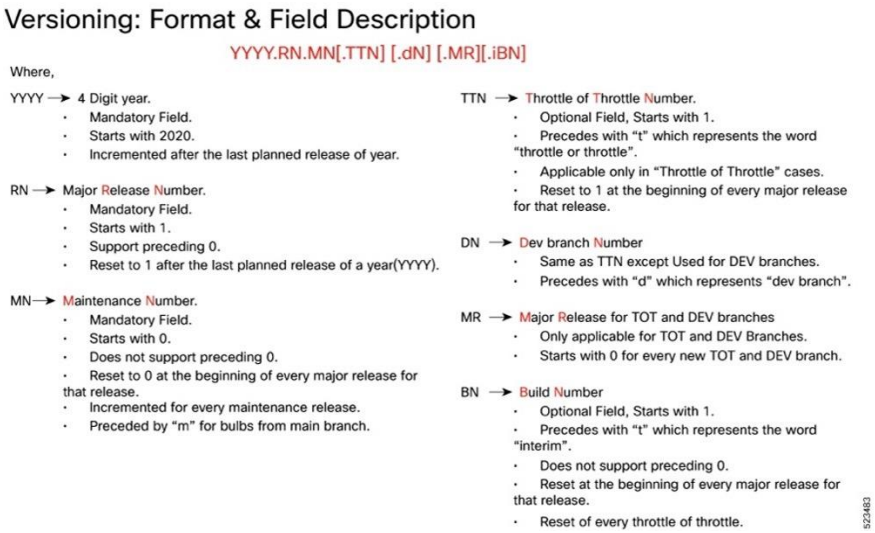


Figure 1. Cloud native product versioning format and description

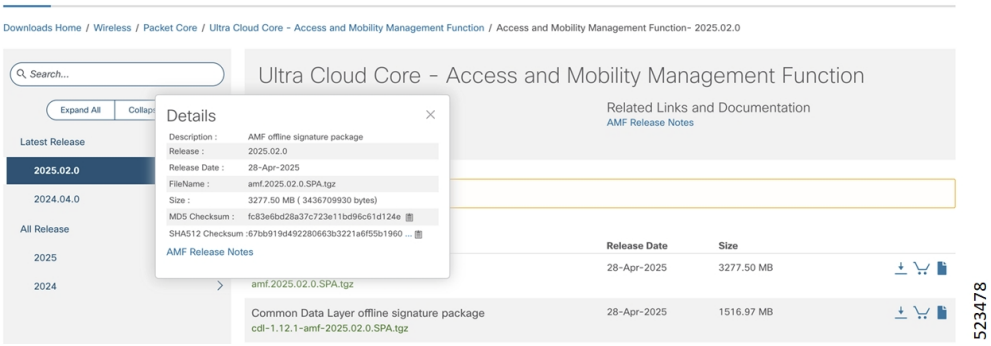
The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research 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 7. 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 8. 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