UCC AMF Release Notes, Release 2024.04.0

First Published: 2024-10-25

Ultra Cloud Core Access and Mobility Management Function

Introduction

This Release Notes identifies changes and issues related to this software release.

Release Lifecycle Milestones

Release Lifecycle Milestone	Milestone	Date
First Customer Ship	FCS	30-Oct-2024
End of Life	EoL	30-Oct-2024
End of Software Maintenance	EoSM	30-Apr-2026
End of Vulnerability and Security Support	EoVSS	30-Apr-2026
Last Date of Support	LDoS	30-Apr-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.

Release Package Version Information

Software Packages	Version
amf.2024.04.0.SPA.tgz	2024.04.0
cdl-1.11.9.1-amf2024.04.0.SPA.tgz	1.11.9.1
NED package	ncs-6.1-amf-nc-2024.04.0
NSO	6.1.12

Descriptions for the various packages provided with this release are available in the Release Package Descriptions, on page 6 section.

Verified Compatibility

Products	Version
Ultra Cloud Core SMI	2024.04.1.14

Products	Version
Ultra Cloud CDL	1.11.9.1

For more information on the Ultra Cloud Core SMI, refer to the documents for this release available at:

https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-subscriber-microservices-infrastructure/series.html

What's New in this Release

Features and Enhancements

This section covers a brief description of the features and enhancements introduced in this release.

Feature	Description
NITZ Display	The Network Identity and Time Zone Display (NITZ) feature enables the AMF to deliver the network name and time zone information to the UE. This feature ensures that UE receives accurate network name and time zone data, crucial for network operations and user experience. Command introduced: **network-name { short** *short_network_name* **| full** *full_network_name* **}** — Used to configure short and full network name under TAI-group and TAI- list level. **Default Setting**: Disabled – Configuration Required
UE Location Reporting	The event exposure functionality enables the AMF to provide specific event notifications to peer Network Functions (NFs) or external clients, such as the Gateway Mobile Location Center (GMLC). This functionality allows the AMF to expose certain events related to UE to subscribed clients, enabling them to receive updates about these events. This feature provides location information of the UE to GMLC using AMF event exposure mechanism. GMLC subscribes for one time location event report from AMF through UDM. Command introduced: **enable ngran-location reporting** — Used in AMF global configuration mode to enable UE location reporting. **Default Setting**: Disabled – Configuration Required
3GPP LI	3GPP Lawful Interception (LI) enables legally sanctioned access to private communications by law enforcement agencies. For more information, contact your Cisco account representative.

Behavior Changes

There are no behavior changes in this release.

Installation and Upgrade Notes

This Release Note does not contain general installation and upgrade instructions. Refer to the existing installation documentation for specific installation and upgrade considerations.

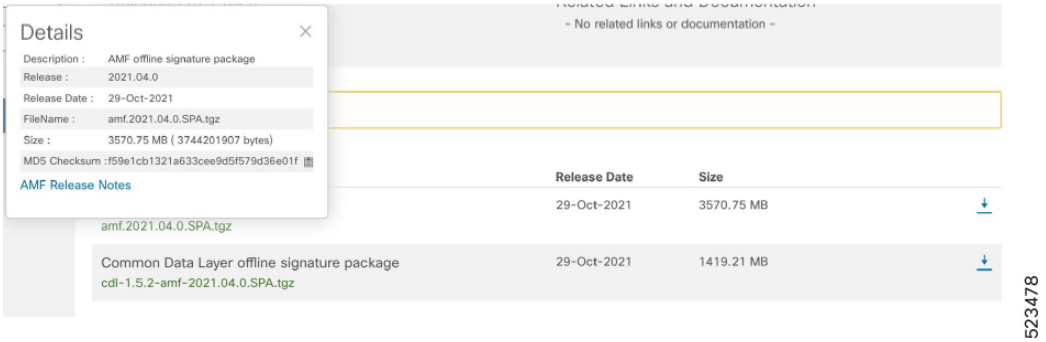
Certificate Validation

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.

Software Integrity Verification

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.



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

To validate the information, calculate a SHA512 checksum using the information in Table 1 and verify that it matches either the one provided on the software download page.

To calculate a SHA512 checksum on your local desktop, refer to the table below.

Table 1: Checksum Calculations per 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`

Operating System	SHA512 checksum calculation command examples

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 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 to not 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.

Open Bugs for this Release

The following table lists the open bugs in this specific software release.

Note This software release may contain open bugs first identified in other releases. Additional information for all open bugs for this release is available in the Cisco Bug Search Tool.

Bug ID	Headline
CSCwm53459	Active proto-ep pod heap memory leak observed during perf longevity of Oct'24 release.
CSCwm53488	Stand-by Protocol-ep heap memory increased by 1.5GB within 24hrs of performance run.
CSCwm82203	LI taps clear functionality not working.
CSCwm86766	3GPP LI TLS with ipv6: standby LI ep pod is in CrashLoopBackOff state after switchover.
CSCwm94328	Memory leak observed during ST longveity of 3gpp LI with MTLR enabled.

Resolved Bugs for this Release

The following table lists the resolved bugs in this specific software release.

Note This software release may contain bug fixes first introduced in other releases. Additional information for all resolved bugs for this release are available in the Cisco Bug Search Tool.

Bug ID	Headline	Behavior Change
CSCwk45189	Rest ep pod restarted with error at infra.(*RestRouter).populateHttpResponse.	No
CSCwk63875	AMF does NRF discovery of SMF instead of using the same SMF as before N2HO handover.	No
CSCwk72821	Rest ep pod crash at nrfnfdproto.(*PlmnId).MarshalToSizedBufferVT	No
CSCwm73804	AMF does not decode NAS Message container in monitor subscriber.	No
CSCwm77067	Continous memory increase trend on service pod observed on Oct24 TP build amf.2024.04.0.i136	No

Operator Notes

Cloud Native Product Version Numbering System

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

Versioning: Format & Field Description

YYYY.RN.MN[.TTN] [.dN] [.MR][.iBN]

Where,

YYYY → 4 Digit year.
- Mandatory Field.
- Starts with 2020.
- Incremented after the last planned release of year.

RN → Major Release Number.
- Mandatory Field.
- Starts with 1.
- Support preceding 0.
- Reset to 1 after the last planned release of a year(YYYY).

MN → Maintenance Number.
- Mandatory Field.
- Starts with 0.
- Does not support preceding 0.
- Reset to 0 at the beginning of every major release for that release.
- Incremented for every maintenance release.
- Preceded by “m” for bulbs from main branch.

TTN → Throttle of Throttle Number.
- Optional Field, Starts with 1.
- Precedes with “t” which represents the word “throttle or throttle”.
- Applicable only in “Throttle of Throttle” cases.
- Reset to 1 at the beginning of every major release for that release.

DN → Dev branch Number
- Same as TTN except Used for DEV branches.
- Precedes with “d” which represents “dev branch”.

MR → Major Release for TOT and DEV branches
- Only applicable for TOT and DEV Branches.
- Starts with 0 for every new TOT and DEV branch.

BN → Build Number
- Optional Field, Starts with 1.
- Precedes with “t” which represents the word “interim”.
- Does not support preceding 0.
- Reset at the beginning of every major release for that release.
- Reset of every throttle of throttle.

523483

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.

Release Package Descriptions

The following table provides descriptions for the packages that are available with this release.

Table 2: Release Package Information

Software Packages	Description
amf.<version>.SPA.tgz	The offline release signature package. This package contains the AMF deployment software, NED package, as well as the release signature, certificate, and verification information.
ncs-<nso_version>-amf-<version>.tar.gz	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.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, refer to https://www.cisco.com/c/en/us/support/index.html.