



Release Notes for the Ultra Cloud Core Access and Mobility Management Function Version 2022.04.2

First Published: December 20, 2022

Last Updated: December 20, 2022

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 | 31-Oct-2022 |
| End of Life | EoL | 31-Oct-2022 |
| End of Software Maintenance | EoSM | 30-Mar-2024 |
| End of Vulnerability and Security Support | EoVSS | 30-Mar-2024 |
| Last Date of Support | LDoS | 30-Mar-2025 |

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.2022.04.2.SPA.tgz | 2022.04.2 |
| cdl-1.10.1-amf-2022.04.1.SPA.tgz | 1.10.1 |

Descriptions for the various packages provided with this release are available in the [Release Package Descriptions](#) section.

Verified Compatibility

| Products | Version |
|----------------------|--------------|
| Ultra Cloud Core SMI | 2022.03.1.09 |
| Ultra Cloud CDL | 1.10.1 |

For information on the Ultra Cloud Core SMI release, refer to the SMI documents available at:
<https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-subscriber-microservices-infrastructure/series.html>

Related Documentation

For the complete list of documentation available for this release, go to: <https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-access-mobility-management-function/products-installation-and-configuration-guides-list.html>

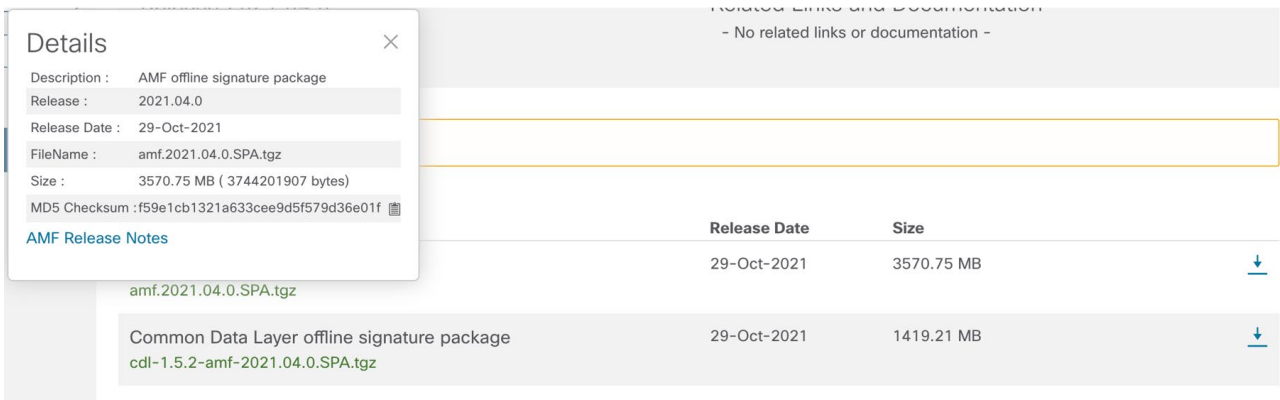
Installation and Upgrade Notes

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

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 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 [Table 1](#) and verify that it matches the one provided on the software download page.

To calculate a SHA512 checksum on your local desktop please see 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> |

Open Bugs for this Release

| | |
|---|--|
| Linux | <p>Open a terminal window and type the following command</p> <pre>\$ sha512sum <filename>.<extension></pre> <p>Or</p> <pre>\$ shasum -a 512 <filename>.<extension></pre> |
| <p>NOTES:</p> <p><i><filename></i> is the name of the file.</p> <p><i><extension></i> is the file extension (e.g. .zip or .tgz).</p> | |

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.

Certificate Validation

The software images are signed via x509 certificates. For information and instructions on how to validate the certificates, refer to the .README file packaged with the software.

Open Bugs for this Release

The following table lists the known bugs that remain open 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 are available in the [Cisco Bug Search Tool](#).

| Bug ID | Headline |
|----------------------------|--|
| CSCwc63377 | AMF does not reject mTLS handshake when PCF sends expired server certificate |
| CSCwd03811 | Callmodel impacted after rest ep pod forceful delete without mTLS as well as with mTLS |
| CSCwd20451 | AMF is sending UEContextReleaseCommand even after follow on bit is set in mobi reg. |
| CSCwd22513 | Rest-ep pod restart twice after ~99hrs during performance longevity |
| CSCwd27108 | Amf-Protocol crashes for IMEI Emergency Registration with "5g-ea0":0 in security mode |

Resolved Bugs for this Release

The following table lists the known bugs that are resolved 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 |
|----------------------------|---|-----------------|
| CSCwd74230 | 5G to 4g ho - idle mode - 2-Digit MNC, AMF initiates the CNTXT release, fails to find Session | No |

| Bug ID | Headline | Behavior Change |
|----------------------------|---|-----------------|
| CSCwd80829 | Length of UE Network Capability is 0 in Fwd Relocation Request after HandoverRequired from 5G to 4G | No |
| CSCwd84867 | AMF should not treat APN/DNN as Case Sensitive | Yes |

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 builds from main branch.

TTN → Throttle of Throttle Number.

- Optional Field, Starts with 1.
- Precedes with "t" which represents the word "throttle of 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 "i" which represents the word "interim".
- Does not support preceding 0.
- Reset at the beginning of every major release for that release
- Reset for every throttle of throttle.

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

[Table 2](#) lists provide 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 deployment software as well as the release signature, certificate, and verification information. |

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>.

Obtaining Documentation and Submitting a Service Request

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANYKIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright ©1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: <http://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. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.