Release Notes for the 5G Converged Core Session Management Function Version 2022.04.0

First Published: October 20, 2022
Last Updated: October 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
ccg.2022.04.0.SPA.tgz	2022.04.0

NOTE: The *ccg.<version>.SPA.tgz* software package is common to both the cnSGW and SMF 5G Network Functions (NF). The deployment and configuration procedure determines the NF deployment.

Descriptions for the software 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
Ultra Cloud Core UPF	2022.04.0
Ultra Cloud cnSGWc	2022.04.0

Related Documentation

For a complete list of documentation available for this release, go to:

https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-session-management-function/tsd-products-support-series-home.html

Installation and Upgrade Notes

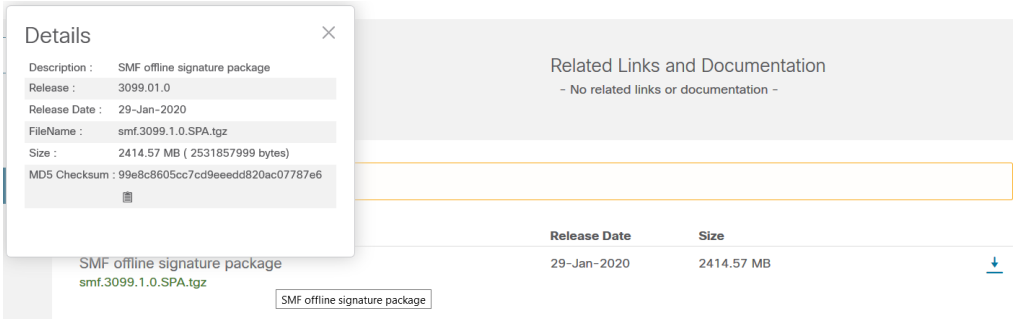
This Release Notes does not contain general installation and upgrade instructions. Refer to the existing installation documentation for specific installation and upgrade considerations.

NOTE: In this software release, you must deploy SMF in merged mode only. For more information on this mode, see the *UCC SMF Configuration and Administration Guide* and *UCC cnSGWc Configuration and Administration Guide*.

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>

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

NOTES: *<filename>* is the name of the file. *<extension>* is the file extension (e.g. .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.

Certificate Validation

SMF 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.

Open Bugs for this Release

There are no open bugs in this software release.

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
CSCvz46093	[SMF-SVI] modify_bearer_request , Attempted!=(Success+Failure) - Issue during N4 reload.	No
CSCwb68839	[SVI-CNSGW] li-ep panic at fileChangeMonitor configMgr ApplicationContext LiEpConfigListener	No

CSCwc32754	[SMF-SVI] : Rendering error with Regex support feature config	No
CSCwc43683	[SMF-IVT] Stats needed for cretificate (TLS/mTLS) feature support/debugging	No
CSCwc46621	[SMF-MTLS] 400 bad request seen post Client Hello msg on x1 interface during ADMF node creation	No
CSCwc57191	[SMF-IVT] SMF rest & li pods restart when certificates are added/removed from ops-centre config	No
CSCwc67128	F93395 : [SMF]:PFCP association Setup Fails in ipv6	No
CSCwc69753	[SMF-SVI]: Sxa tcp CISCO legacy tap not working for cnSGW content lawful Intercept for F97277	No
CSCwc78252	[IVT-F102224]: smf crashes while decoding GTP TEID TransportLayerAddress consisting ipv4 and ipv6	No
CSCwc99353	[IVT-SMF-Ipv6-Ph1-SBI-F93395]:N4 MOD Reject as outer header creation is not present in FAR with FWD	No
CSCwc99507	[SMF-IVT]:When TCP active LI tap is enabled, FORW and DUPL bits are not set in sx mod request.	No
CSCwd04403	[SMF-SVI] : Seen Panic for smf-service pod on build BUILD_2022.04.m0.i65	No
CSCwd15583	[5GaaS] SMF has only three running pods after install/upgrade using short-form ipv6 ipam addresses	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 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 provides descriptions for the software packages that are available with this release.

Table 2 - Release Package Information

Software Packages	Description
ccg.<version>.SPA.tgz	The SMF offline release signature package. This package contains the SMF deployment software as well as the release signature, certificate, and verification information.

NOTE: The *ccg.<version>.SPA.tgz* software package is common to both the cnSGW and SMF 5G Network Functions (NF). The deployment and configuration procedure determines the NF deployment.

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.

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 WITHTHE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSEOR 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.