



Release Notes for the Ultra Cloud Core Session Management Function

Version 2021.02.0

First Published: June 6, 2021

Last Updated: June 6, 2021

Introduction

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

Release Package Version Information

Software Packages	Version
csg.2021.02.0.SPA.tgz	2021.02.0

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	2020.02.2.25
Ultra Cloud Core UPF	2021.02.0

Notes and Considerations for this Release

The April FCS *csg.2021.02.0.i262* build includes all the fixes from Jan-21 TP as per *csg.2021.01.1.i208* (delivered 2021-05-14).

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>

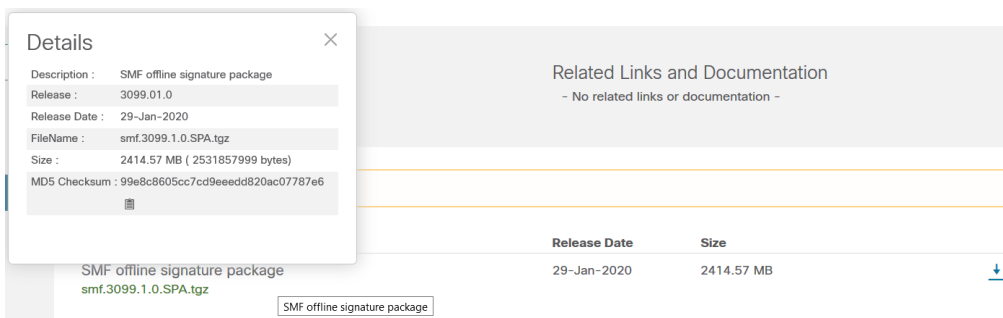
Installation and Upgrade Notes

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

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

The following table lists the known bugs that were found in this software release and which remain open.

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
CSCvx66258	[SMF-SVI] ngap.gTPTunnel_element not updated - Xn HO
CSCvx73884	[SMF-SVI] peerGtpuEpKey missing for SUPI performing 5G Make-Break events
CSCvy02677	[SMF-SVI] db_conflict_pdu_sess_rel seen during downgrade procedure.
CSCvy04190	[SMF-SVI] ~350K sessions mismatch between SMF and UPF during longevity system test run
CSCvy09346	[SMF-SVI] Stale peerGtpuEpKey entries in DB - Xn Hos
CSCvy27973	[cnSGW-C+SMF-SVI] ~30k Session loss was observed during 4G Performance Call model run
CSCvy35856	[SMF-SVI] Small number of duplicate IPs during longevity run
CSCvy44679	[SMF-SVI] SmPolicyUpdate issue for \"PDU 5G to UnTrusted WiFi Handover\"
CSCvy53307	[SVI-SOL-Test]:Rest-EP restart seen with traffic with Disc. failure due to huge go-routine numbers
CSCvy57463	[SMF-SVI] Error logs piling up during Performance run

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
CSCvx42555	[SMF-SVI] Observing 5G attach failures with pduimn26_ue_req_idle_to_active when run in scale.	No
CSCvx42661	[SMF] Bug to track WIFI Collision issues	No
CSCvx43109	[DR-IVT] SMF to allow routes as default behaviour when no BGP policy configured	No
CSCvx45374	[PERF-CNDP-CN5G] nodes + replica config to be replaced with only replica in cndp setup	Yes

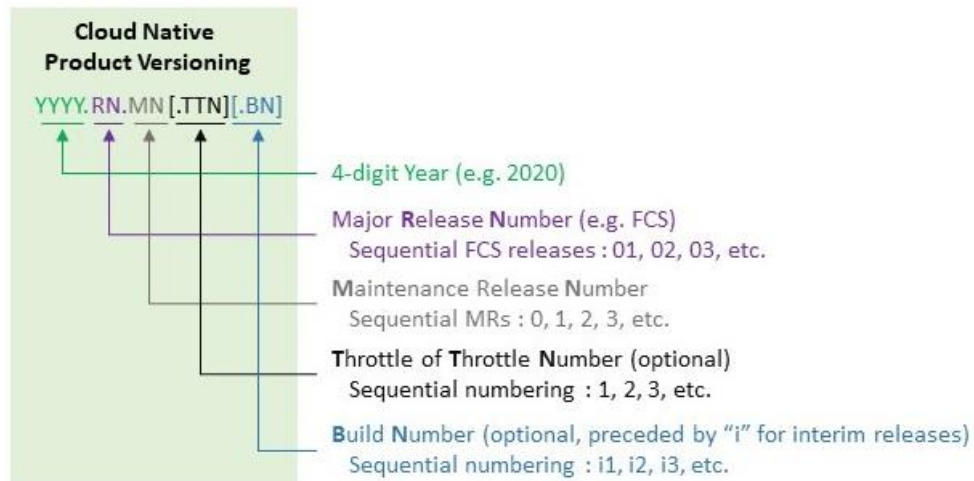
Operator Notes

CSCvx67368	[SMF-SVI] show peers doesn't show max-remote-restart-counter-change	No
CSCvx68018	[UPF-Parity] SMF is not updating Message Priority when wps session is updated as non-wps session	Yes
CSCvx70255	[SMF] During CBR MBR collision PDN modification procedure doesn't resume for 4G call	No
CSCvx74279	[SMF] Range value is missing for parameter in the gtp-p-profile	Yes
CSCvx78021	[SMF-SVI] nodemgr_gtpc_peer_status shows interface_type as \"None\"	No
CSCvx92817	[SMF-SVI] Huge number of IP leak issue seen during longevity run [April branch]	No
CSCvx97848	[SMF-SVI] Multiple smf-service pods restarted with OOM during CM run	No
CSCvx98286	PCF expedite is failing for IMS calls	No
CSCvy02596	[SMF-SVI] service restart at smf-service/subscriber.GetRoamerStatusString	Yes
CSCvy09346	[SMF-SVI] Stale peerGtpuEpKey entries in DB - Xn HOs	No
CSCvy09849	[SMF-SVI] service ERROR: (pk)]-CatchAllProcedure: Handling timer event-[0]	No
CSCvy14203	[SMF-SVI] 5G Calls are not getting successful when simulated PCF instance is paused intentionally	No
CSCvy17513	[SVI-SMF] panic observed at ApplicationContext writeSessionToDB dbUpdateThread Run	No
CSCvy17526	[SMF] SMF is not querying for usage during X2ho with location change trigger enabled from CHF	Yes
CSCvy18059	Need to update entitlement tag of cnSGW in Converged Core	No
CSCvy31552	Deferred Usage in SMF, Fail Open During Dynamic Rule Installation is failing	Yes

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.



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.

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 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)

© 2021 Cisco Systems, Inc. All rights reserved.