Release Notes for the Ultra Cloud Core Session Management Function Version 2020.02.1

First Published: May 13, 2020
Last Updated: May 13, 2020

Introduction

This Release Notes identifies changes and issues related to this software release. This release is the next release after 2020.02.0.

Release Package Version Information

Software Packages	Version
smf.2020.02.1.SPA.tgz	2020.02.1

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	2020.02.1
Ultra Cloud Core PCF	2020.02.1.65
Ultra Cloud Core UPF	2020.02.1

Enhancements

N10 failure handling: “retry-and-terminate” on N10 error codes

Config	Messages	Error Code
Two endpoints each with different priority and capacity; and a primary UDM configured.	• UDM Registration • UDM Fetch Subscription	• 504 • 400 • 404 • 413 • 426 • 431 • 500 • 501 • 503 • 508

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

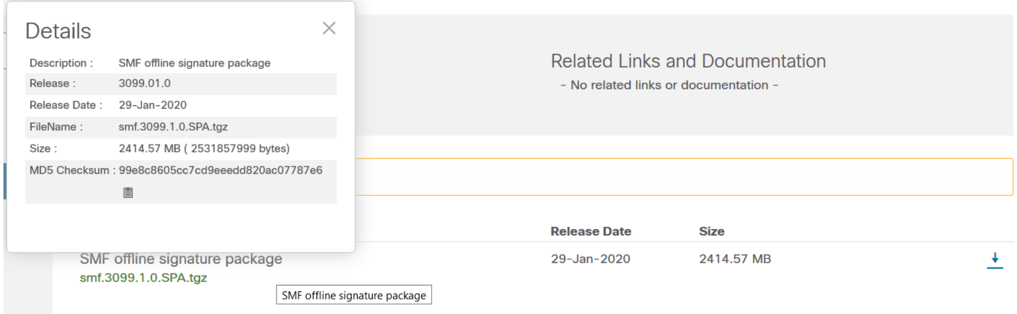
Installation and Upgrade Notes

This Release Note 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.



Details

Description : SMF offline signature package
Release : 3099.01.0
Release Date : 29-Jan-2020
FileName : smf.3099.1.0.SPA.tgz
Size : 2414.57 MB (2531857999 bytes)
MD5 Checksum : 99e8c8605cc7cd9eeedd820ac07787e6

Related Links and Documentation
- No related links or documentation -

	Release Date	Size
SMF offline signature package smf.3099.1.0.SPA.tgz	29-Jan-2020	2414.57 MB

SMF offline signature package

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 either 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
CSCvt62316	SMF-REGRESSION : SMF Rejecting PreDefined activation for 4G calls
CSCvt62771	[SMF-SVI] IPAM is not releasing all subs even though Calls are cleared and no subs in the system
CSCvt69765	[SMF-SVI]Proto ERROR, scheduled BG transaction;Unsupported REQ Message received, MsgType 26 seqNum 0
CSCvt71688	SMF not sending Remove URRs for all deleted ded brr in N4 modify post 5G to 4G HO during Wifi epsfb
CSCvt79335	UDM de registration is happening during 4G detach during Idle mode EPS FB.
CSCvt81417	[SMF] [Charging] RemoveURR is not sending in N4 Mod Req incase of change in ChrgDesc
CSCvt90037	SMF not sending Remove URR & it is including Urrid in QueryURR for gNB rejected flow during WIFepsfb
CSCvt99683	SMF not removing PDR/FAR/QER/URR when PccRule deleted & FailedQFI received from NR during WIFItoNRHO
CSCvu00590	[SVI-SMF] smf-service [ERROR] [TftUtils.go:129] [smf-service11.smf-app.gen] tft list full
CSCvu04411	[SMF-IVT] Partially accepted bearers in CBRes from EPDG to be handled in 5G to WIFI HO
CSCvu10103	[SMF-SVI] SMF Service Pod Restart @ infra.(*affinityCacheClient).delRemoteEntry
CSCvu15939	[SMF-SVI] LI Intercept ID/imsi mismatch observed on UPF CLIs
CSCvu17277	[SMF-SVI] Multiple Procedure Failures with BV run
CSCvu21673	[SMF-SVI] Service pod restarted at (*UpfServData).ProcessSessionModificationResponse on TP

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.

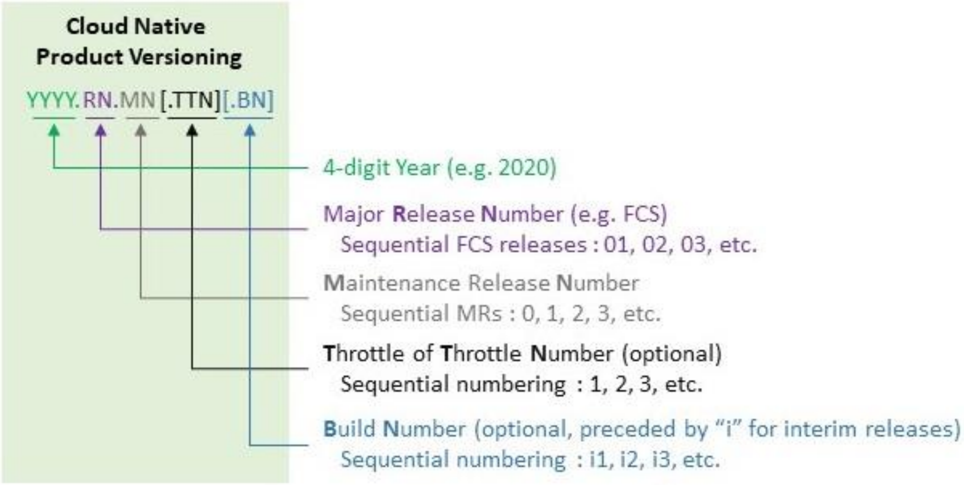
Bug ID	Headline
CSCvq16989	[SMF-SVI] NRF Heart-beat procedure is not handled as expected
CSCvt40217	CLI to reject 4G-only devices
CSCvt64995	N4 Userplane inactivity timer support
CSCvt81885	[SMF] N4 Userplane inactivity request (UPIR) handling

Bug ID	Headline
CSCvt95054	[SVI-SMF] Wifi-5G-EPSFB "PDU UnTrusted WiFi to 5G to EPS Fallback" stats support
CSCvt97943	[SVI SMF] small num of 404 not found errors on n2ho with partial fail for PDU session mod complete
CSCvu00921	[SMF-IOT] SMF is not handling AN-release procedure when received after Handover during EPSFB
CSCvu00941	[SMF-IVT] DL FARs are not removed in N4 during 5G to 4G HO for failed bearers in MBReq
CSCvu13936	PGW-C is using TEID as 000 in PFCP delete session request.
CSCvu15973	ControlPlane inactivity timer support
CSCvu19134	[SMF-IOT] SMF has to prioritise RA procedure over PDU session modification when there is a collision

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.


Cloud Native
Product Versioning
YYYY.RN.MN[.TTN][.BN]
4-digit Year (e.g. 2020)
Major Release Number (e.g. FCS)
Sequential FCS releases : 01, 02, 03, etc.
Maintenance Release Number
Sequential MRs : 0, 1, 2, 3, etc.
Throttle of Throttle Number (optional)
Sequential numbering : 1, 2, 3, etc.
Build Number (optional, preceded by "i" for interim releases)
Sequential numbering : i1, i2, i3, etc.

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

Table 2 - Release Package Information

Software Packages	Description
smf.<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 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.