



Release Notes for the Ultra Cloud Core User Plane Function

Version 2021.01.1

First Published: February 25, 2021

Last Updated: February 25, 2021

Introduction

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

Release Package Version Information

Software Packages	Version
qvpc-si-21.22.uj1.bin.SPA.tar.gz	21.22.uj1
qvpc-si_T-21.22.uj1.bin.SPA.tar.gz	21.22.uj1

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	2020.01.1.26
	2020.02.1.32
NSO-CFP	1.1.0
RCM	2021.01.0

Notes and Considerations for this Release

This UPF release is qualified with OSP and CNDP.

Recommended BIOS Settings

The following table provides the recommended BIOS settings for UPF.

BIOS Options	Preferred Value
Enhanced Intel SpeedStep Technology	Disabled
Intel Turbo Boost Technology	Disabled
Intel Hyper-Threading Technology	Disabled
CPU Performance	Enterprise
Execute Disable Bit feature	Enabled
Intel VT for Directed I/O	Enabled
Processor C1E	Disabled
Processor C6 report	Disabled
Energy performance	Performance
Power performance tuning	BIOS
Hardware P-States	HWPM Native Mode
Workload Configuration	I/O Sensitive
Non-uniform memory access (NUMA)	Enabled
Sub-NUMA Clustering	Disabled
Extended Partition Table prefetch	Enabled
Intel UltraPath Interconnect prefetch	Enabled
Patrol Scrub	Disabled
Fan Policy	Maximum Power

NOTE: Changing the Preferred Value/Configuration of “Intel Hyper-Threading Technology” requires a reboot. It is a Global configuration that affects all the CPU and VMs on a server.

To configure BIOS by using host profiles on Cisco UCS servers, refer the *SMI Cluster Manager Operations* chapter in the *UCC SMI Operations Guide*.

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-user-plane-function/tsd-products-support-series-home.html>

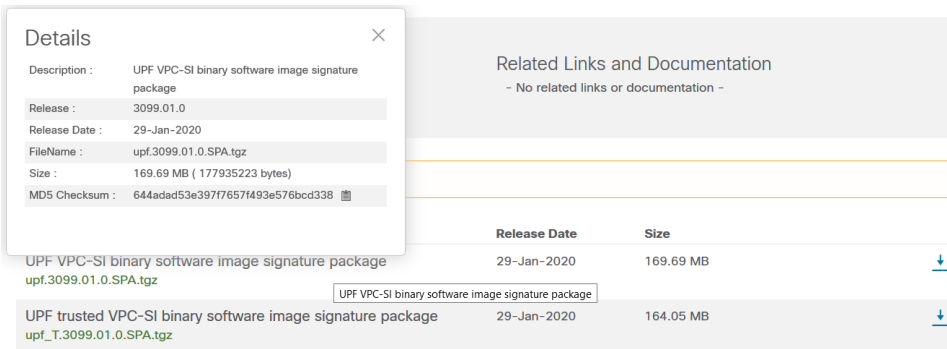
Installation and Upgrade Notes

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 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>

Operating System	SHA512 checksum calculation command examples
<p>NOTES:</p> <p><code><filename></code> is the name of the file.</p> <p><code><extension></code> 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

UPF 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
CSCvv92817	Change in EDR format for transaction end EDR is not getting applied for current as well as new call
CSCvw48604	[UPF-SVI] Active UPF is losing IP Chunks allocated by SMF after ICSR Switchover but recovering later
CSCvw56143	UPF cpu utilization at 100% with 230K calls and close to 8Gbps throughput
CSCvw58960	Crash is observed during 21.22.0 Regression - egtpu_process_tx_setup_req_evt()
CSCvw65922	[UPF-SVI] Negative case - Removing "ip vrf <vrf-name >" cli -- > huge no of continuous VPNMGR restarts
CSCvw72152	Task Resources - Session Manager and bulkstats in Warn Status on UPF.
CSCvw74614	[Combo-UPF]: Peer ID is not displayed correctly in show sx peers cli
CSCvx02862	[Combo-UPF]5G-4G handover , UE goes to Idle, D/L data , debuffering, after that all pkts to sessmgr.
CSCvx03805	UPF: continuous ip address range pool of same network on multiple SMF is not working
CSCvx08150	[UPF-SVI] Assertion at sn_memblock_memcache_alloc() while 5G call-model was running
CSCvx14614	[Combo-UPF]Per peer statistics are incorrect for combo calls, in multi smf topology.
CSCvx40996	[SVI_UPF] Continuous restarts at PC: [f66d8fdd/X] libc.so.6/malloc_usable_size()

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](#).

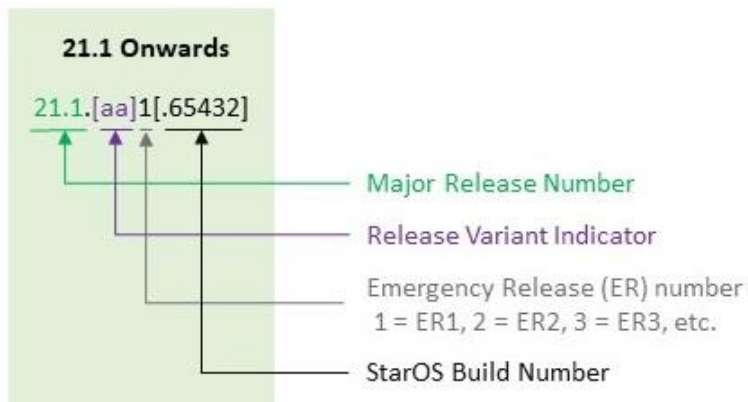
Bug ID	Headline
CSCvt30501	Potential memory leak issue at function sessmgr_uplane_alloc_simple_buffer for TCP OOO
CSCvu08963	[UPF-SVI]:multiple restarts@Function: sessmgr_uplane_process_sx_sess_modify_create_rulebase_pdr()
CSCvu21615	Fatal signal at uplane_handle_itc_processing() after push config from CP
CSCvu57146	UPF Dropping Data received on default flow after 4g to 5g idle mode
CSCvu58018	UPF is holding IP chunks, resulting in more number of chunks in UPFs
CSCvu62892	[UPF]: IP pool chunks not relased on UPF when path-failure detected in \"releasing\" state
CSCvu96441	[UPF-SVI]: Segmentation fault at acsmgr_process_show_cf_stats() during call model run
CSCvu99351	SGW-UP going down leading to outage
CSCvv61902	[SVI-UPF] VPP crash observed followed by continuous smgr resets.
CSCvw39909	UPF sending incorrect Time Reporting in Sx_Modifcation Response in Query URR case.

Operator Notes

StarOS Version Numbering System

The output of the **show version** command displays detailed information about the version of StarOS currently running on the ASR 5x00 or Cisco Virtualized Packet Core platform.

The Version Build Number for releases 21.1 and later include a major and emergency release number, for example, “21.1.1”.



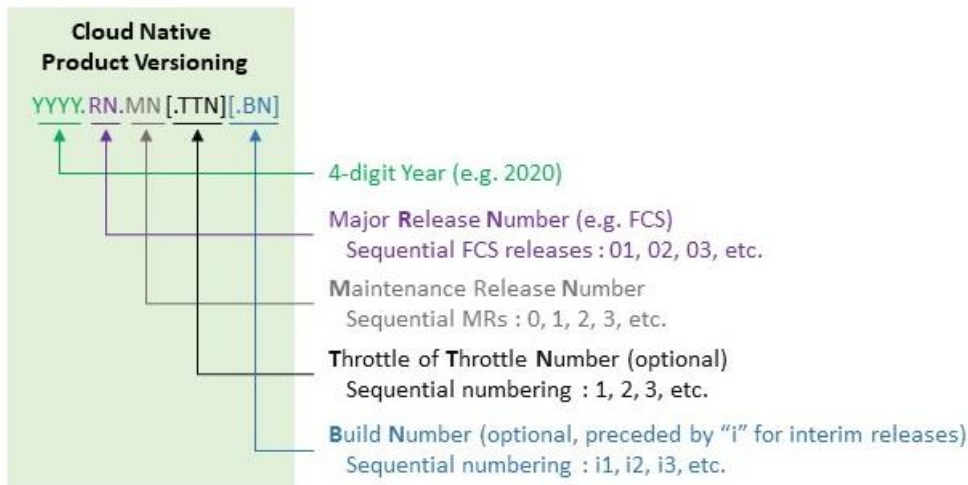
Operator Notes

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.

NOTE: The 5G UPF software is based on StarOS and implements the version numbering system described in this section. However, as a 5G network function (NF), it is posted to Cisco.com under the Cloud Native Product Numbering System as described in [Cloud Native Product Version Numbering System](#).

Cloud Native Product Version Numbering System

Though the packages that comprise the UPF use the StarOS version numbering system as described in the previous section, the UPF product leverages the cloud native version numbering system described below.



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
qvpc-si-<version>.bin.SPA.tar.gz	<p>The UPF release signature package. This package contains the VPC-SI deployment software for the UPF as well as the release signature, certificate, and verification information.</p> <p>Files within this package are nested under a top-level folder pertaining to the corresponding StarOS build.</p>
qvpc-si_T-<version>.bin.SPA.tar.gz	<p>The trusted UPF release signature package. This package contains the VPC-SI deployment software for the UPF as well as the release, signature, certificate, and verification information.</p> <p>Files within this package are nested under a top-level folder pertaining to the corresponding StarOS build.</p>

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 ANY KIND, 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.