



Release Notes for the Ultra Cloud Core Policy Control Function

Version 2020.02.2

First Published: August 04, 2020
Last Updated: August 04, 2020

Introduction

This Release Notes identifies changes and issues related to this software release. This release is the next release after 2020.02.1.65.

Release Package Version Information

Software Packages	Version
pcf.2020.02.2.SPA.tgz	2020.02.2

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	2020.01.1
Ultra Cloud Core SMF	2020.02.3
Ultra Cloud Core UPF	2020.02.4

Enhancements and Behavior Changes

Support for Configuring the Interface-level Request Timeout

The PCF now allows you to configure the inbound and outbound request timeout values for the REST endpoints. With this enhancement, you can add or modify the timeout period at the interface level.

Previous Behavior: In the earlier releases, the response timeout period was configured with the default value. As a result, PCF timed out while waiting for responses from SMF such as N7_notify request, which took longer than the default timeout period.

New Behavior: In this release, new timeout configuration options are provided in the existing REST endpoint configuration CLI.

To configure REST endpoint, use the following configuration in the Policy Ops Center console:

config

rest-endpoint

```
interface [ n7 | n15 | n25 | n28 | nnrf ]  
    ip interface_ip_address  
    port interface_port_number  
  
ips ip_address  
  
port port_number  
  
replicas replica_count  
  
inbound-request-timeout-ms inbound_timeout  
  
outbound-request-timeout-ms outbound_timeout  
  
repository repository_address  
  
tracing-service-name tracing_service  
  
uri-scheme uri_scheme  
  
end
```

NOTES:

- **inbound-request-timeout-ms** *inbound_timeout* – Configures the timeout period after which the inbound request expires. You can configure a single *inbound_timeout* value for all the configured interfaces or for a single interface.
- **outbound-request-timeout-ms** *outbound_timeout* – Configures the timeout period after which the outbound request expires. You can configure a single *outbound_timeout* value for all the configured interfaces or for a single interface.

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-policy-control-function/tsd-products-support-series-home.html>

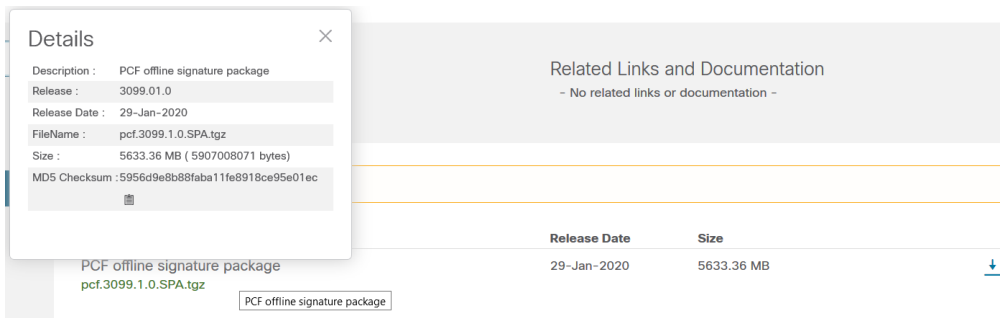
Installation and Upgrade Notes

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 <code>> certutil.exe -hashfile <filename>.<extension> SHA512</code>
Apple MAC	Open a terminal window and type the following command <code>\$ shasum -a 512 <filename>.<extension></code>
Linux	Open a terminal window and type the following command <code>\$ sha512sum <filename>.<extension></code> Or <code>\$ shasum -a 512 <filename>.<extension></code>
NOTES: <code><filename></code> is the name of the file. <code><extension></code> 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

PCF 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

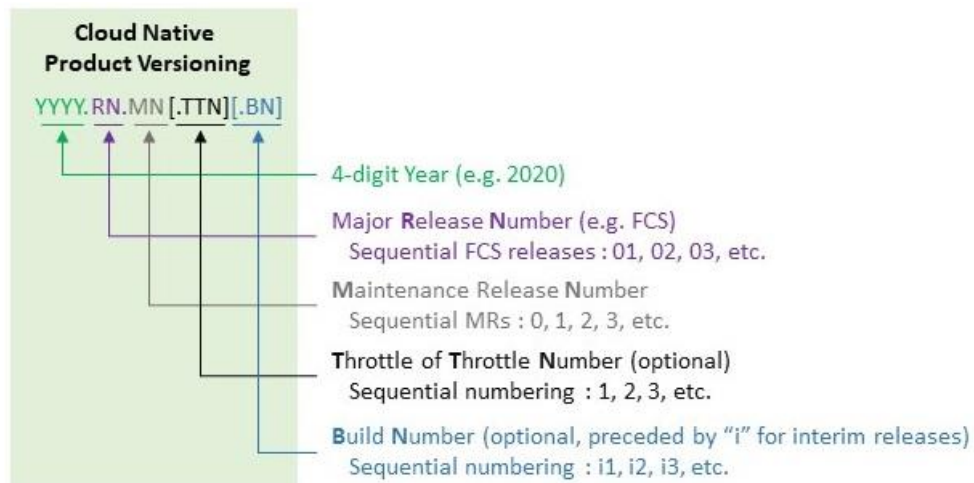
The following table lists the bugs that were resolved in this software release.

Bug ID	Headline
CSCvu40159	The SVN pods enter the evicted state on experiencing low resource and disk pressure.
CSCvu67160	Support for configuring interface-level timeout period for the outbound requests.

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](#) lists provides descriptions for the packages that are available with this release.

Table 2 - Release Package Information

Software Packages	Description
pcf.<version>.SPA.tgz	The PCF offline release signature package. This package contains the PCF 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 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)

© 2020 Cisco Systems, Inc. All rights reserved.