Release Notes for the Ultra Cloud Core Policy Control Function Version 2022.01.0

First Published: January 31, 2022
Last Updated: January 31, 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-Jan-2022
End of Life	EoL	31-Jan-2022
End of Software Maintenance	EoSM	1-Aug-2023
End of Vulnerability and Security Support	EoVSS	1-Aug-2023
Last Date of Support	LDoS	31-July-2024

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
pcf.2022.01.0.SPA.tgz	2022.01.0

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.i33
Ultra Cloud Core CDL	1.6

For information on the Ultra Cloud Core SMI release, refer to the corresponding SMI Release Notes available at:

https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-subscriber-microservices-infrastructure/products-release-notes-list.html.

Related Documentation

For the 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

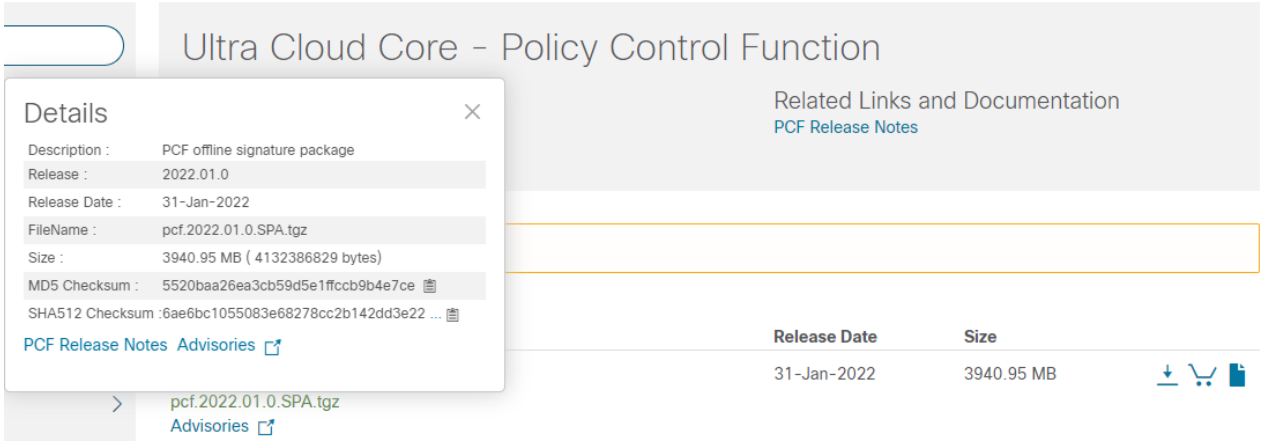
Installation and Upgrade Notes

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 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

PCF software images are signed via x509 certificates. For information and instructions on how to validate the certificates, refer to the .README file packaged with the software.

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	Product
CSCwa21225	Transaction log enhancement to include command sub type CHF_SUBSCRIPTION_TYPE detail	PCF
CSCvx25333	To make sure all critical logs, rest, diameter, cdl, ldap, engine pods are being forwarded to Splunk	SMI

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.

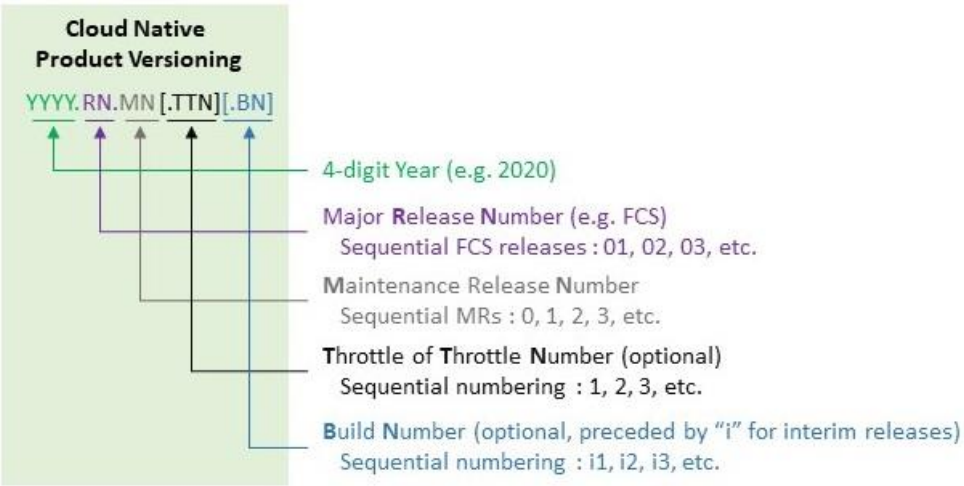
Bug ID	Headline	Product	Behavior Change
CSCvz83293	scanner issue with java and openjdk	PCF	No

Bug ID	Headline	Product	Behavior Change
CSCvz96874	PCF sends Two subsequent N28 subscribe with different session ID when Session is out of data occur	PCF	No
CSCwa33660	[PCF-CNDP-SVI] connection reset by peer error is coming on etcd pod log on i157 build	SMI	No
CSCwa51215	Evaluation for Log4j RCE (Log4Shell) Vulnerability - PCF	PCF	No
CSCwa54613	Evaluation of pcf for Log4j 2.x DoS vulnerability fixed in 2.17	PCF	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.



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 provide descriptions for the software 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.