# Release Notes for the Ultra Cloud Core Subscriber Management Infrastructure Version 2020.02.1.42

**First Published:** March 09, 2021
**Last Updated:** March 09, 2021

## Introduction

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

## Release Package Version Information

| Software Packages | Version |
|---|---|
| smi-install-disk.20210204.iso.SPA.tgz | 20210204 |
| cee-2020.02.1.42.SPA.tgz | 2020.02.1.42 |
| cluster-deployer-2020.02.1.42.SPA.tgz | 2020.02.1.42 |
| **NOTE:** In the event bugs need to be opened against this product, please reference the Package Component Version information in this table. | |

Descriptions for the various packages provided with this release are available in the Release Package Descriptions section.

## Enhancements

### Include kubelet.crt in cert-maintainer renew

The functionality previously introduced to auto-renew K8s certificates has been updated to include the auto-renewal of kubelet.crt. This change addresses a known limitation with K8s not renewing self-signed kubelet server certificates.

With this feature, the *kubelet.crt* and *kubelet.key* files are automatically deleted upon the restart of the K8s master and worker nodes. This forces *kubelet.service* to renew the *kubelet.crt* cert upon restart.

## 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-subscriber-microservices-infrastructure/series.html

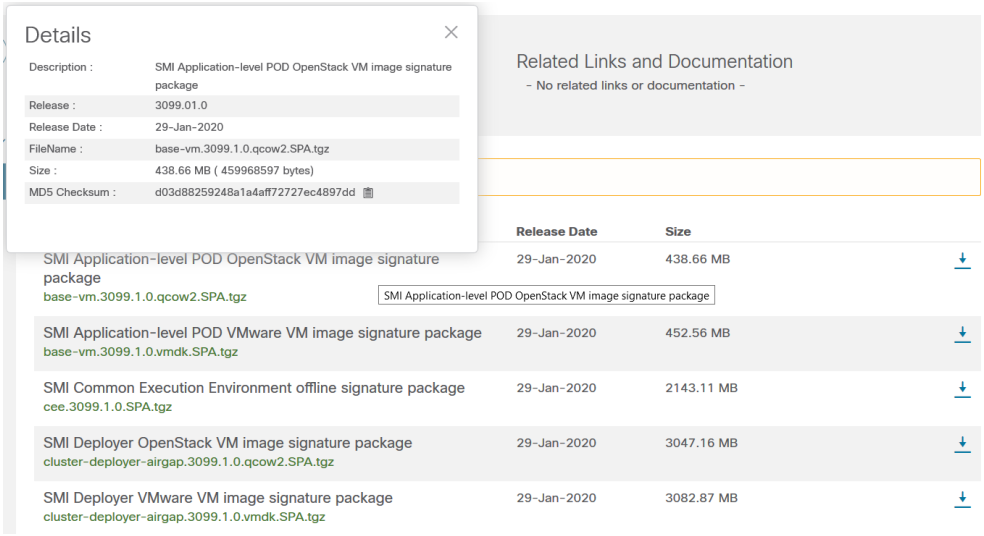
# Installation and Upgrade Notes

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.




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<br><br>> certutil.exe -hashfile *<filename>.<extension>* SHA512 |
| Apple MAC | Open a terminal window and type the following command<br><br>$ shasum -a 512 *<filename>.<extension>* |
| Linux | Open a terminal window and type the following command<br><br>$ sha512sum *<filename>.<extension>*<br><br>Or<br><br>$ 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

SMI 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

None for this release.

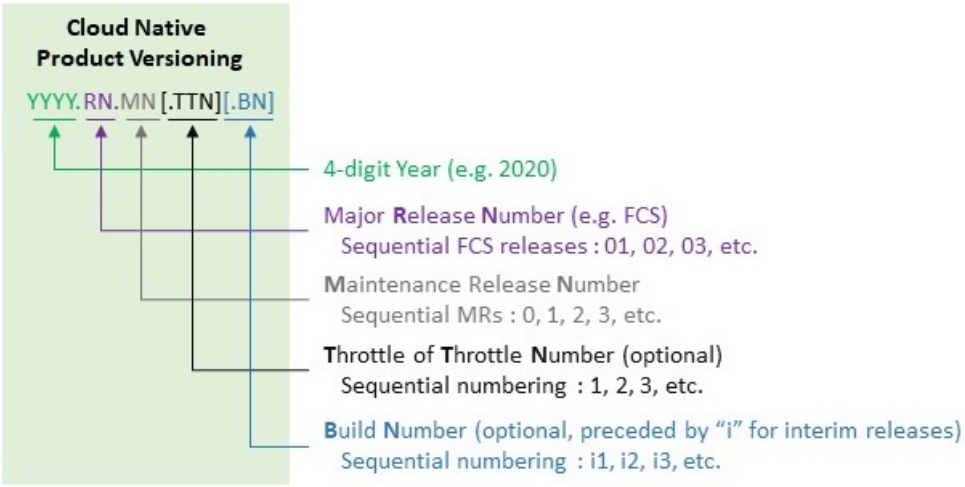
# Resolved Bugs for this Release

None for this release.

# 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 |
|---|---|
| base-vm.<version>.qcow2.SPA.tgz | The application-level POD OpenStack VM image signature package. This package contains the base qcow2 VM image as well as the release signature, certificate, and verification information. |
| base-vm.<version>.vmdk.SPA.tgz | The application-level POD VMware VM image signature package. This package contains the base vmdk VM image as well as the release signature, certificate, and verification information. |
| cee.<version>SPA.tgz | The SMI Common Execution Environment (CEE) offline release signature package. This package contains the CEE deployment package as well as the release signature, certificate, and verification information. |
| cluster-deployer-airgap.<version>.qcow2.SPA.tgz | The SMI Deployer OpenStack VM image signature package. This package contains the Deployer qcow2 VM image as well as the release signature, certificate, and verification information. |
| cluster-deployer-airgap.<version>.vmdk.SPA.tgz | The SMI Deployer VMware VM image signature package. This package contains the Deployer vmdk VM image 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.