



# Release Notes for the Ultra Cloud Core Subscriber Management Infrastructure Version 2024.01.1.13

First Published: 2024-01-31

## Ultra Cloud Core Subscriber Management Infrastructure

### 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-2024 |
| End of Life                               | EoL       | 31-Jan-2024 |
| End of Software Maintenance               | EoSM      | 31-Jul-2025 |
| End of Vulnerability and Security Support | EoVSS     | 31-Jul-2025 |
| Last Date of Support                      | LDoS      | 31-Jul-2026 |

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          |
|---|------------------|
| smi-install-disk.20.04.0-20240120.iso.SPA.tgz | 20.04.0-20240120 |
| cee.2024.01.1.13.SPA.tgz                      | 2024.01.1.13     |
| cluster-deployer-2024.01.1.13.SPA.tgz         | 2024.01.1.13     |

Descriptions for the various packages provided with this release are provided in the [Release Package Descriptions, on page 7](#) section.

## Verified Compatibility

| UCS Server        | CIMC Firmware Version |
|-------------------|-----------------------|
| Cisco UCS C220 M6 | 4.2(2a) or later      |
| Cisco UCS C220 M5 | 4.1(3f) or later      |



**Note** For UCS C220 M6 deployment, it is mandatory to use secure boot for installing only Cisco signed firmware images on the servers.

## What's New in this Release

### New in Documentation

This version of Release Notes includes a new section titled **What's New in this Release** comprising all new features, enhancements, and behavior changes applicable for the release.

This section will be available in all the 5G release notes and will supersede content in the Release Change Reference (RCR) document. Effective release 2024.01, the RCR document will be deprecated.

### Features and Enhancements

This section covers a brief description of the features and enhancements introduced in this release. It also includes links to detailed documentation, where available.

| Feature  | Description  |
|--|--|
| Ansible Version Upgrade                                  | The cluster manager supports version 2.15 of the third-party Ansible software.   |
| <a href="#">Configurable Cluster Access for OS Users</a> | SMI supports the access of OS users to SMI cluster upon login using the <b>addons secure-access { enabled   disabled }</b> CLI command in the Cluster Configuration mode. By default, this command is disabled to reduce resource usage in the K8s cluster.<br><br>The helm chart is created to deploy Daemonsets onto master nodes. Only the access controller pod on the active master will run and manage user access.<br><br><b>Default Setting:</b> Disabled – Configuration required to enable |
| <a href="#">Inception Deployer Support using Ubuntu</a>  | To simplify the maintenance of the host server running the Inception Deployer, Ubuntu 20.04 LTS can be used as a replacement for the smi-install-disk.iso image. The users are allowed to install their own Ubuntu servers to manage security updates and install new releases of the cluster-deployer as required.<br><br><b>Default Setting:</b> Disabled – Configuration required to enable   |

| Feature   | Description  |
|---|--|
| Kubernetes Version Upgrade  | <p>With this release, the Kubernetes version is upgraded from 1.26 to 1.27.</p> <p><b>Default Setting:</b> Enabled – Always On</p>   |
| <a href="#">Optimizing Parallel Cluster Sync Time for Multiple Clusters</a> | <p>SMI supports parallel cluster sync triggered from the same inception deployer or cluster manager.</p> <p><b>Note</b> This functionality is currently supported only on Bare Metal and not fully supported on VMware.</p> <p>The following enhancements optimize time while downloading artifacts:</p> <ul style="list-style-type: none"> <li>• Only the individual files will be locked to allow subsequent syncs parallelly</li> <li>• Only the software required to be synced will be downloaded and verified</li> <li>• Each sync will perform SHA256 or SHA512 validation on each package</li> <li>• For clusters that require different packages, the downloads will happen concurrently</li> </ul> <p><b>Note</b> The download process creates file locks that must be persisted for the life of the file. You must not delete or modify the files under any conditions.</p> <p><b>Default Setting:</b> Enabled – Always On</p> |
| <a href="#">Optimizing SMI Cluster Sync Time</a>                            | <p>During SMI base image upgrade, the sync time for KVM cluster is reduced to approximately 40 minutes per node.</p> <p>This is achieved by setting the other nodes in maintenance mode to <b>true</b>, syncing the cluster for the active node, and repeating the same process for other nodes.</p> <p><b>Default Setting:</b> Enabled – Always On</p>  |
| <a href="#">SNMP Trap Changes for Equipment Alarms</a>                      | <p>SMI supports the following SNMP trap changes in this release:</p> <ul style="list-style-type: none"> <li>• The <b>server-alert</b> trap will now send unique values for hardware alerts from CEE in the CISCO-CNEE-MIB::cneeFaultId field.</li> </ul> <p>The trap definition includes the <b>affectedDN</b> SNMP element. The MIB is also updated with <b>CISCO-CNEE-MIB::cneeAffectedDn</b> to provide a direct object reference.</p> <ul style="list-style-type: none"> <li>• The <b>server-not-reachable-alert</b> trap is updated to include the trap descriptions for the equipment faults.</li> </ul> <p><b>Default Setting:</b> Enabled – Always On</p>  |

| Feature                                   | Description   |
|---|---|
| Updated Versions for Third Party Software | SMI supports updated versions for the following third party software in this release: <ul style="list-style-type: none"> <li>• Calico—3.26</li> <li>• Docker—24.0.4</li> </ul> <p><b>Default Setting:</b> Enabled – Always On</p> |

## 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/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.

Ultra Cloud Core - Subscriber Microservices Infrastructure

Release 2023.03.1.31

Related Links and Documentation  
[SMI Release Notes](#)

**Details** ✕

Description : NED package 5.6.8 for deployer signature package

Release : 2023.03.1.31

Release Date : 21-Jul-2023

FileName : ncs-5.6.8-cisco-smi-nc-2023.03.1.31.tar.SPA.tgz

Size : 1.51 MB ( 1586588 bytes)

MD5 Checksum : f6e5b8c6ec4f30e97c663c8c3dbf6556

SHA512 Checksum : 80b0ccef7bc05d402286e8021867f3 ...

[SMI Release Notes](#) [Advisories](#)

| Release Date | Size       |  |
|--------------|------------|--|
| 21-Jul-2023  | 0.88 MB    |  |
| 21-Jul-2023  | 1.51 MB    |  |
| 21-Jul-2023  | 0.91 MB    |  |
| 21-Jul-2023  | 1.63 MB    |  |
| 20-Jul-2023  | 2858.08 MB |  |

523481

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 the following table and verify that it matches with the one provided on the software download page.

To calculate a SHA512 checksum on your local desktop, refer to the following table please.

**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><pre>&gt; certutil.exe -hashfile &lt;filename&gt;.&lt;extension&gt; SHA512</pre>  |
| Apple MAC         | Open a terminal window and type the following command:<br><br><pre>\$ shasum -a 512 &lt;filename&gt;.&lt;extension&gt;</pre>  |
| Linux             | Open a terminal window and type the following command:<br><br><pre>\$ sha512sum &lt;filename&gt;.&lt;extension&gt;</pre> <p>Or</p> <pre>\$ shasum -a 512 &lt;filename&gt;.&lt;extension&gt;</pre> |

| Operating System   | SHA512 Checksum Calculation Command Examples |
|--|--|
| <b>NOTES:</b><br><filename> is the name of the file.<br><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

The following table lists the open bugs in this specific software release.



**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   |
|----------------------------|--|
| <a href="#">CSCwi79394</a> | Postgres coredump seen on Cluster Manager during SMI Upgrade   |
| <a href="#">CSCwi79409</a> | Python coredump seen on Cluster Manager during upgrade         |
| <a href="#">CSCwi79646</a> | Fluentd coredump seen on remote NF clusters during SMI upgrade |

## Resolved Bugs for this Release

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



**Note** This software release may contain bugs first identified in other releases. Additional information for all resolved bugs for this release are available in the [Cisco Bug Search Tool](#).

| Bug ID                     | Headline  | Behavior Change |
|----------------------------|---|-----------------|
| <a href="#">CSCwi15801</a> | After fluentd memory issue NF ops centers failed to recover | 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.

### Versioning: Format & Field Description

YYYY.RN.MN[.TTN] [.dN] [.MR][.iBN]

Where,

YYYY → 4 Digit year.

- Mandatory Field.
- Starts with 2020.
- Incremented after the last planned release of year.

RN → Major Release Number.

- Mandatory Field.
- Starts with 1.
- Support preceding 0.
- Reset to 1 after the last planned release of a year(YYYY).

MN → Maintenance Number.

- Mandatory Field.
- Starts with 0.
- Does not support preceding 0.
- Reset to 0 at the beginning of every major release for that release.
- Incremented for every maintenance release.
- Preceded by "m" for bulbs from main branch.

TTN → Throttle of Throttle Number.

- Optional Field, Starts with 1.
- Precedes with "t" which represents the word "throttle or throttle".
- Applicable only in "Throttle of Throttle" cases.
- Reset to 1 at the beginning of every major release for that release.

DN → Dev branch Number

- Same as TTN except Used for DEV branches.
- Precedes with "d" which represents "dev branch".

MR → Major Release for TOT and DEV branches

- Only applicable for TOT and DEV Branches.
- Starts with 0 for every new TOT and DEV branch.

BN → Build Number

- Optional Field, Starts with 1.
- Precedes with "t" which represents the word "interim".
- Does not support preceding 0.
- Reset at the beginning of every major release for that release.
- Reset of every throttle of throttle.

523483

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

The following table lists the descriptions for packages that are available with this release.

**Table 2: Release Package Information**

| Software Packages          | Description  |
|----------------------------|--|
| base.<version>.iso.SPA.tgz | The application-level POD ISO image signature package for use with bare metal deployments. This package contains the base ISO 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.      |

| Software Packages                  | Description   |
|------------------------------------|---|
| cluster-deployer-<version>.SPA.tgz | The SMI Deployer image signature package for use with bare metal deployments. This package contains the Deployer v 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>.



