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

First Published: 2024-01-31

Ultra Cloud Clore 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
Configurable Cluster Access for OS Users	SMI supports the access of OS users to SMI cluster upon login using the **addons secure-access { enabled | disabled }** CLI command in the Cluster Configuration mode. By default, this command is disabled to reduce resource usage in the K8s cluster. 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. **Default Setting**: Disabled – Configuration required to enable
Inception Deployer Support using Ubuntu	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. **Default Setting**: Disabled – Configuration required to enable
Kubernetes Version Upgrade	With this release, the Kubernetes version is upgraded from 1.26 to 1.27. **Default Setting**: Enabled – Always On

Feature	Description
Optimizing Parallel Cluster Sync Time for Multiple Clusters	SMI supports parallel cluster sync triggered from the same inception deployer or cluster manager. **Note** This functionality is currently supported only on Bare Metal and not fully supported on VMware. The following enhancements optimize time while downloading artifacts: • Only the individual files will be locked to allow subsequent syncs parallely • Only the software required to be synced will be downloaded and verified • Each sync will perform SHA256 or SHA512 validation on each package • For clusters that require different packages, the downloads will happen concurrently **Note** 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.
Optimizing SMI Cluster Sync Time	During SMI base image upgrade, the sync time for KVM cluster is reduced to approximately 40 minutes per node. This is achieved by setting the other nodes in maintenance mode to **true**, desyncing the cluster for the active node, and repeating the same process for other nodes.
SNMP Trap Changes for Equipment Alarms	SMI supports the following SNMP trap changes in this release: • The **server-alert** trap will now send unique values for hardware alerts from CEE in the CISCO-CNEE-MIB::cneeFaultId field. The trap definition includes the **affectedDN** SNMP element. The MIB is also updated with **CISCO-CNEE-MIB::cneeAffectedDn** to provide a direct object reference. • The **server-not-reachable-alert** trap is updated to include the trap descriptions for the equipment faults.
Updated Versions for Third Party Software	SMI supports updated versions for the following third party software in this release: • Calico—3.26 • Docker—24.0.4 **Default Setting**: Enabled – Always On

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

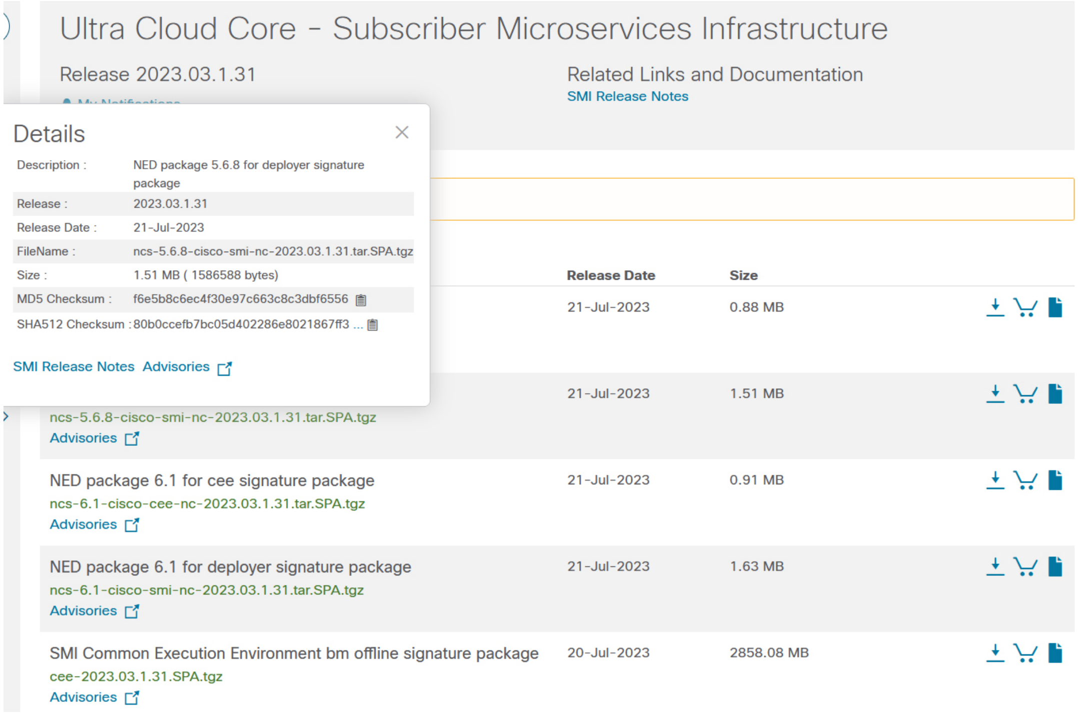
Installation and Upgrade Notes

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 :	80b0ccefb7bc05d402286e8021867ff3 ...

SMI Release Notes Advisories

	Release Date	Size
	21-Jul-2023	0.88 MB
ncs-5.6.8-cisco-smi-nc-2023.03.1.31.tar.SPA.tgz Advisories	21-Jul-2023	1.51 MB
NED package 6.1 for cee signature package ncs-6.1-cisco-cee-nc-2023.03.1.31.tar.SPA.tgz Advisories	21-Jul-2023	0.91 MB
NED package 6.1 for deployer signature package ncs-6.1-cisco-smi-nc-2023.03.1.31.tar.SPA.tgz Advisories	21-Jul-2023	1.63 MB
SMI Common Execution Environment bm offline signature package cee-2023.03.1.31.SPA.tgz Advisories	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: **`> 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

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
CSCwi79394	Postgres coredump seen on Cluster Manager during SMI Upgrade
CSCwi79409	Python coredump seen on Cluster Manager during upgrade

Bug ID	Headline
CSCwi79646	Fluentd coredump seen on remote NF clusters during SMI upgrade

Resolved Bugs for this Release

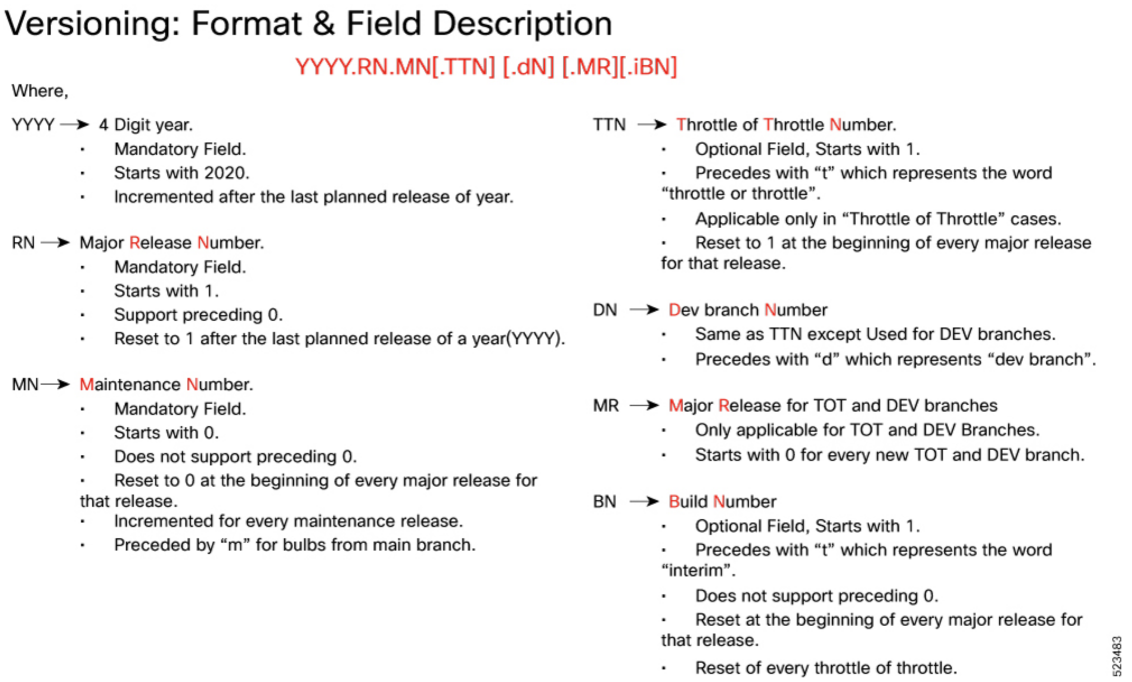
The following table lists the resolved bugs in this specific software release.

Bug ID	Headline	Behavior Change
CSCwi15801	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.
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.