UCC 5G SMI Release Notes, Release 2025.02.1.17

First Published: 2025-04-30

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	30-Apr-2025
End of Life	EoL	30-Apr-2025
End of Software Maintenance	EoSM	29-Oct-2026
End of Vulnerability and Security Support	EoVSS	29-Oct-2026
Last Date of Support	LDoS	31-Oct-2027

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.22.04.0-20250328.iso.SPA.tgz	22.04.0-20250328
cee-2025.02.1.17.SPA.tgz	2025.02.1.17
cluster-deployer-2025.02.1.17.SPA.tgz	2025.02.1.17
NED Package	ncs-6.1.14-cisco-cee-nc-1.1.2025.02.1.17.tar.gz ncs-6.1.14-cisco-smi-nc-1.1.2025.02.1.17.tar.gz ncs-6.4.3-cisco-cee-nc-1.1.2025.02.1.17.tar.gz ncs-6.4.3-cisco-smi-nc-1.1.2025.02.1.17.tar.gz
NSO	6.1.14 6.4.3

Descriptions for the various packages provided with this release are provided in the Release Package Descriptions, on page 6 section.

Verified Compatibility

UCS Server	CIMC Firmware Version
Cisco UCS C220 M7	4.3(3.240022)
Cisco UCS C220 M6	4.2(2a) or later
Cisco UCS C220 M5	4.1(3f) or later It is recommended that you use version 4.3(2.250016) with this release.

- For deployment of C-Series M6 and M7 servers, it is mandatory to enable secure boot on the servers.
- For C-Series M5 servers, it is recommended to use UEFI boot mode and enable secure boot for more security. This will align the older hardware settings with the newer hardware requirements.

What's New in this Release

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
Audit logging for ops-center login attempts	To prevent brute-force attacks, the new audit log will identify which user attempted to authenticate to the OpsCenter.
Enhanced alert management with node manager integration	CEE allows you to configure the Node Manager's API endpoint directly to interact with Alert manager. This configuration ensures that alerts can be sent to or received from alert manager for appropriate processing and action.
Lifecycle management of VPC-DI	This release provides necessary support to deploy the VPC-DI VMs on SMI. This release offers new software types and VM configurations for KVM deployments, exposing VM sizing parameters. Command enhanced: **clusters vpc-di nodes** *node_name* **vms { cf | sf | upf }**
Kubernetes version upgrade	With this release, you can upgrade the Kubernetes version from 1.31 to 1.32.

Feature	Description
Software upgrade from 2023.03.1 to 2025.02.1	You can upgrade SMI directly from 2023.03.1 to the latest 2025.02.1 release, which includes a new base image and a security patch. This release also upgrades the K8s version from 1.25 to 1.32. **Note** As part of this upgrade, ensure that you also update the PCF from release 2024.03.1 to 2025.02.1. The following actions must be performed before upgrade: • Initiate complete cluster synchronization. • Trigger concurrent upgrade for cluster synchronization to upgrade the cluster and all nodes using the **upgrade-strategy concurrent** command. **Important** You must not trigger rolling upgrade for this upgrade process.
Support for Node Problem Detector	This feature supports onboarding of Node Problem Detector (NPD) through CEE Ops center. The NPD enhances hardware resiliency by detecting and addressing issues at the OS, hardware, and platform levels. It prevents the impact of node problems on Kubernetes pods, thereby maintaining application performance and reliability. Note that the NPD complements existing metrics, alerting, and log forwarding solutions. Commands introduced: **node-problem-detector agent enabled**
Upgrade of Prometheus to v3.0	Prometheus has been upgraded from version 2.55 to version 3.0 in this release.
Updated versions for third-party software	SMI supports updated versions for the following third-party software in this release: • Calico—3.29.3 • Containerd—1.7.27 • Confd—7.7.16 • Docker—27.5.1 • Helm—3.17.2 • nginx-ingress—4.12.1

Behavior Changes

There are no behavior changes in this release.

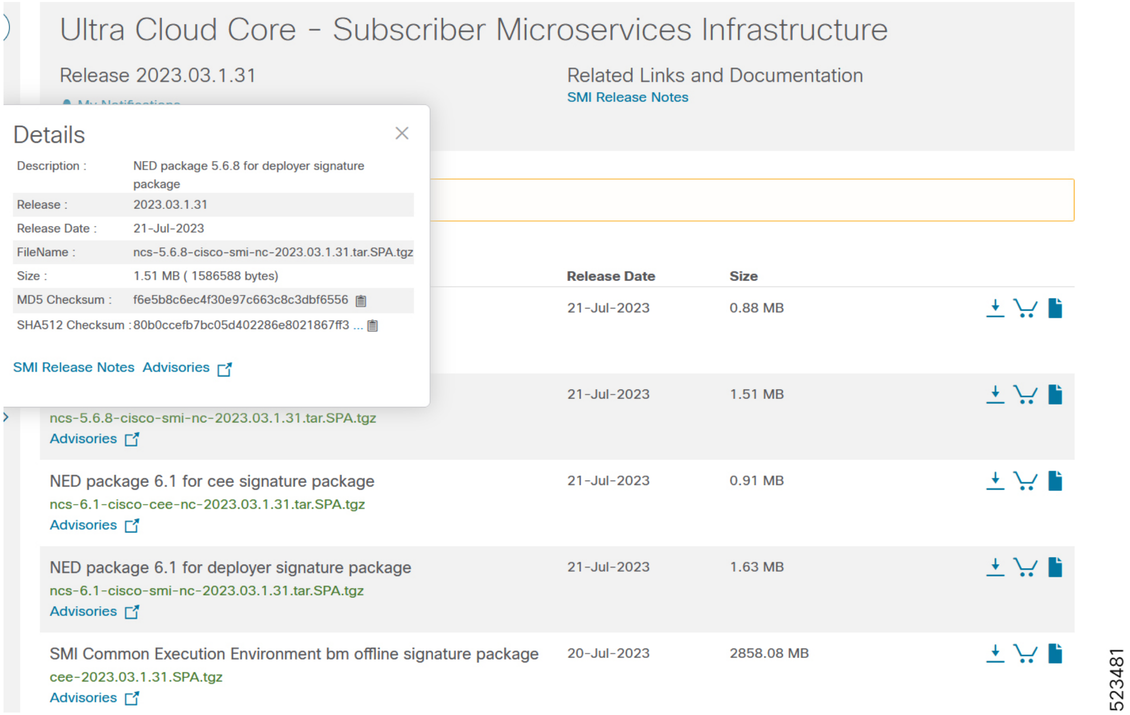
Installation and Upgrade Notes

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

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`

Operating System	SHA512 Checksum Calculation Command Examples
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
CSCwn81020	gtpc-ep, protocol, udp-proxy pods do not come up after CNDP upgrade to i13
CSCwo43517	VPC-DI, configuration of multiple vm per node shouldn't be allowed
CSCwo69633	VPC-DI, default di-net and service port mapping is incorrect

Resolved Bugs for this Release

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

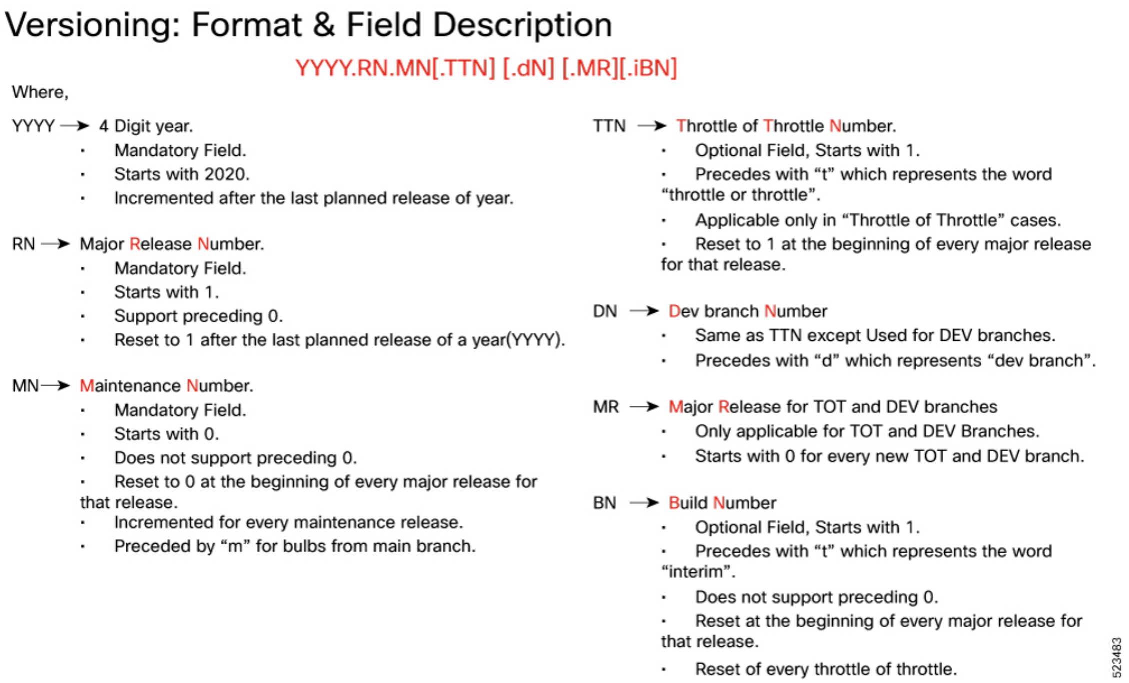
Note This software release may contain bug fixes first introduced in other releases. Additional information for all resolved bugs for this release are available in the Cisco Bug Search Tool.

Bug ID	Headline
CSCwo69661	VPC-DI, boot params always has 4 service port config
CSCwo73736	SMI Upgrade Failed from Jul'23 to Apr'25

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.

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 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.