UCC 5G SMI Release Notes, Release 2024.03.1.12

First Published: 2024-07-31

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-Jul-2024
End of Life	EoL	31-Jul-2024
End of Software Maintenance	EoSM	29-Jan-2026
End of Vulnerability and Security Support	EoVSS	29-Jan-2026
Last Date of Support	LDoS	31-Jan-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.20.04.0-20240709.iso.SPA.tgz	20.04.0-20240709
cee-2024.03.1.12.SPA.tgz	2024.03.1.12
cluster-deployer-2024.03.1.12.SPA.tgz	2024.03.1.12
NED Package	ncs-6.1.3-cisco-cee-nc-2024.03.1.12 ncs-6.1.3-cisco-smi-nc-2024.03.1.12
NSO	6.1.3

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 Version 4.3.2.240009 is qualified 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
Cluster Synchronization Lock	In Cluster Manager HA deployment mode with multiple remote clusters, you can lock cluster synchronization to prevent operational errors on the undesired cluster. You can enable or disable cluster synchronization using the **clusters** *cluster_name* **sync-lock** CLI command. Once you enable the lock, cluster synchronization will be rejected and can be triggered only after disabling the lock. Default Setting: Disabled – Configuration Required to Enable
Kubernetes Version Upgrade	With this release, you can upgrade the Kubernetes version from 1.28 to 1.29.
Log Forwarding using Syslog	CEE provides the capability to forward logs to the Syslog server for internal centralized storage and debugging purposes. It sends Syslog messages using Fluent Bit over UDP, TCP, or TLS in RFC3164 or RFC5424 format. You can configure log forwarding to Syslog using the **logging syslog** command in the Config mode. Default Setting: Disabled – Configuration Required to Enable
SMI Software Optimization	The SMI software is optimized and stabilized to support the upgrade process. The Ansible tasks are enhanced to improve the resiliency and performance of cluster synchronization.

Feature	Description
Software Upgrade from 2023.03.1 to 2024.03.1	You can upgrade SMI directly from 2023.03.1 to the latest 2024.03.1 release, which includes a new base image and security patch. The K8s version will also be upgraded from 1.25 to 1.29. 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. **Note** You must not trigger rolling upgrade for this upgrade process.
UCS C220 M7 Server Qualification for SMF and UPF	The Cisco UCS C220 M7 server is qualified to enable SMF and four UPF VMs for on-premise deployments. For UPF, the server allows scaling up to four VMs per KVM node using the quarter flavor configuration. This feature enhances the throughput and session handling capacity.
Updated Versions for Third-Party Software	SMI supports updated versions for the following third-party software in this release: • Confd—7.7.16 • Docker—26.1.4 • Helm—3.14.4 • nginx—4.10.1

Installation and Upgrade Notes

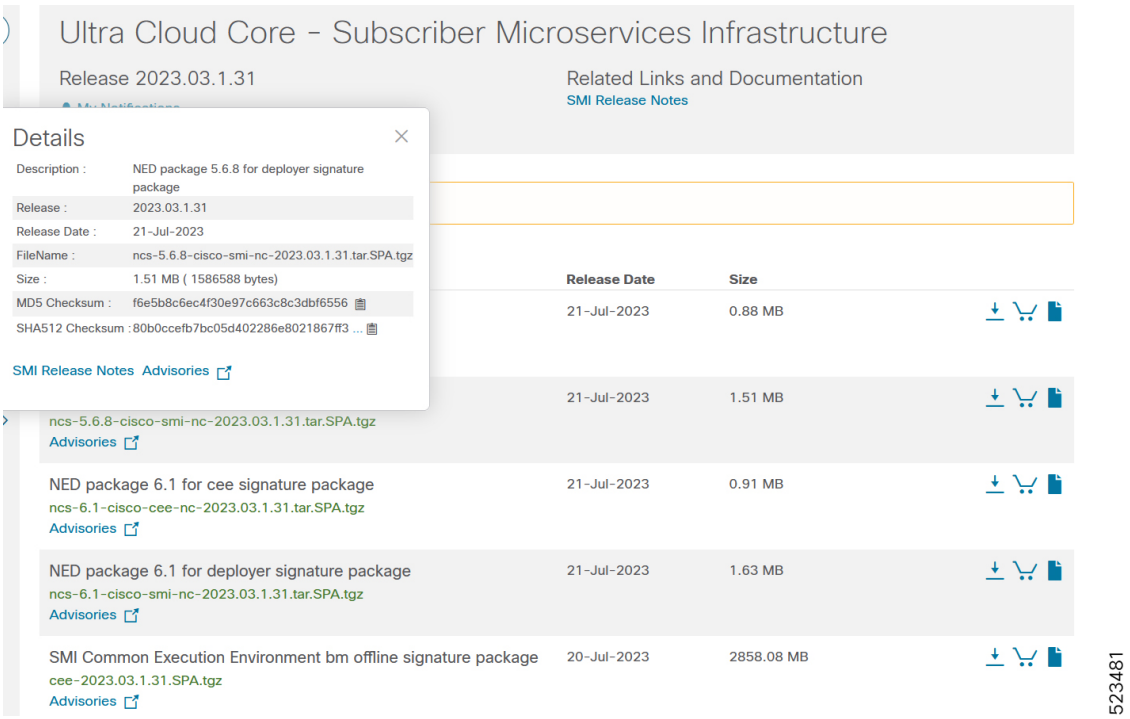
This Release Note does not contain general installation and upgrade instructions. Refer to the existing installation documentation for specific installation and upgrade considerations.

Note In this release, you must install a patch to use all SMI functionalities. For more information, contact your Cisco account representative.

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 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>**

Operating System	SHA512 Checksum Calculation Command Examples
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
CSCwk68073	CM ops-cent pod crashing after upgrade to 2024.03.1.i08 "Day0 passwrd is required" - already present
CSCwk88152	Upgrade from i10 to i12 got stuck at TASK [cleanup : Always restart pgpool pod]

Resolved Bugs for this Release

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

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

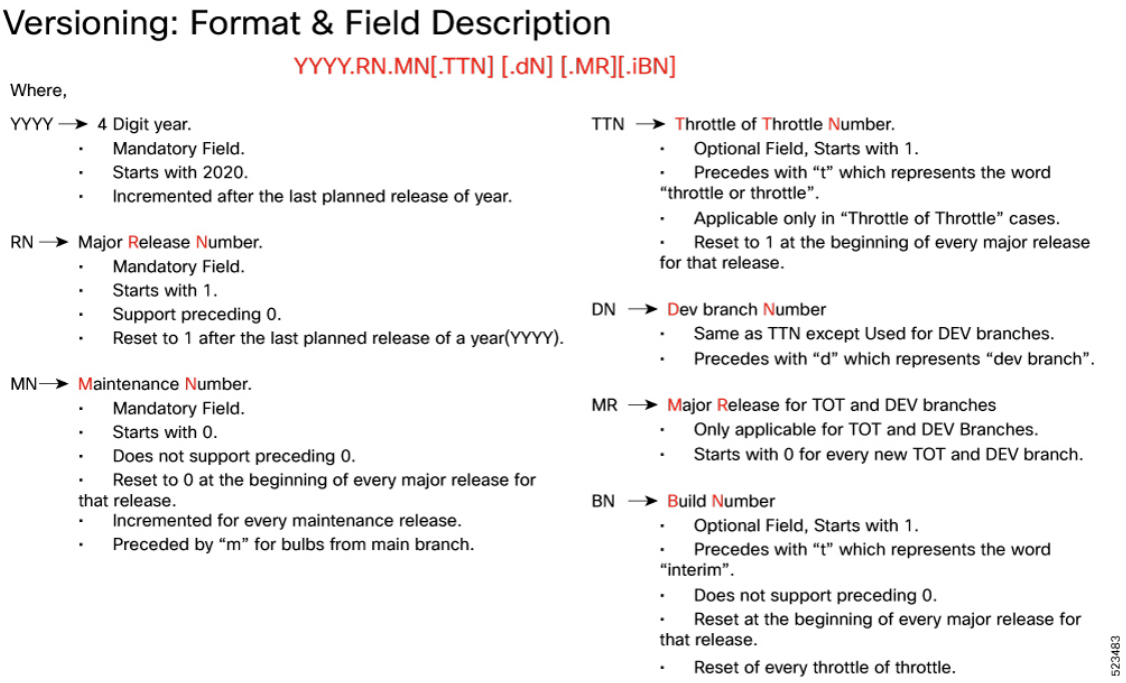
Bug ID	Headline	Behavior Change
CSCwk28616	CNDP-PCF: CEE OpsCenter Config Getting Deleted after CNDP Upgrade - 2024.03.1.i05	No

Bug ID	Headline	Behavior Change
CSCwk82724	CM HA FW upgrade cluster sync failed with upgrade strategy concurrent	No
CSCwk82773	Decouple opscenter sync phase from distributed registry	No
CSCwk89336	Increase ssh connection max in sshd_config	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

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.