UCC 5G SMI Release Notes, Release 2024.04.1.14

First Published: 2024-10-25

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-Oct-2024
End of Life	EoL	30-Oct-2024
End of Software Maintenance	EoSM	30-Apr-2026
End of Vulnerability and Security Support	EoVSS	30-Apr-2026
Last Date of Support	LDoS	30-Apr-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.20.04.0-20240922.iso.SPA.tgz	20.04.0-20240922
cee-2024.04.1.14.SPA.tgz	2024.04.1.14
cluster-deployer-2024.04.1.14.SPA.tgz	2024.04.1.14
image-patch-20.04.0-20240709-20240925.2024.04.1.14.tgz.SPA.tgz	20.04.0-20240709-20240925.2024.04.1.14
NED Package	ncs-6.1.12-cisco-cee-nc-2024.04.1.14 ncs-6.1.12-cisco-smi-nc-2024.04.1.14
NSO	6.1.12

Descriptions for the various packages provided with this release are provided in the Release Package Descriptions, on page 8 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 4.3.2.240009 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
Grafana Dashboard using ConfigMap	In the Cisco Common Execution Environment (CEE), you can now define and deploy Grafana dashboards using ConfigMap in the CNDP-managed Kubernetes cluster. A ConfigMap is an API object used to store non-confidential data in key-value pairs. It allows you to decouple environment-specific configuration from container images to port your applications easily. This support is added in addition to the existing mechanism of loading dashboards using Git server pods.
Kubernetes Version Upgrade	With this release, you can upgrade the Kubernetes version from 1.29 to 1.30.

Feature	Description
New Addons	SMI supports new addons that can be configured during cluster synchronization: • **Flux** is a tool for keeping Kubernetes clusters in sync with sources of configuration such as Git repositories. It automates updates to configuration whenever there is new code to deploy. **Command Introduced: clusters** *cluster_name* **addons flux { enabled | disabled }** • **Cert-manager** allows you to add certificates and certificate issuers as resource types in Kubernetes clusters. This simplifies the process of managing TLS certificates and tunnel termination for API endpoints. **Command Introduced: clusters** *cluster_name* **addons cert-manager { enabled | disabled }** • **External Secrets Operator (ESO)** is a Kubernetes operator that integrates external secret management systems such as Vault. The operator reads information from external APIs and automatically injects the values into a Kubernetes Secret. **Command Introduced: clusters** *cluster_name* **addons external-secrets-operator**
Prometheus Operator and Pushgateway Support	CEE is enhanced to install Prometheus using the Prometheus Operator with the support of Pushgateway. The Prometheus Operator allows you to manage and configure the Prometheus-based monitoring stack for Kubernetes clusters. The Pushgateway is an intermediary service that allows you to push metrics to Prometheus from batch jobs which cannot be scraped. **Commands Introduced:** • **prometheus prometheus-operator** • **prometheus pushgateway** • **prometheus pushgateway port**
Server Isolation	The server isolation feature allows you to set a threshold for worker node failures that the system can tolerate. This feature increases the success rates of cluster synchronization. **Command Introduced:** **clusters** *cluster_name* **actions sync run upgrade-strategy concurrent [isolate-on-hardware-failure { false | true } node-tolerance** *tolerance_value* **]**

Feature	Description
SMI Base Image Patch Without A/B Upgrade	The Base Image Patch feature enables the application of patches to the base image in a non-disruptive manner and avoids the need for a full A/B upgrade. This feature is useful when minor updates or security patches need to be applied to the base image for the following scenarios: • Third-party software and library updates • Kernel upgrades for security changes • Addition or upgrade of kernel modules **Note** This feature is applicable only to 2024.03.1 and 2024.04.1 releases. For support on versions older than 2024.03.1, you can contact your Cisco account representative. **Commands Introduced:** • **clusters** *cluster_name* **actions sync run disable-partition-upgrade { true | false }**—Apply the patch from cluster manager for full cluster synchronization • **clusters** *cluster_name* **actions sync run sync-phase patch**—Apply the patch using sync-phase • **clusters** *cluster_name* **actions patch pre-check**—Identify any issues before applying a patch • **clusters** *cluster_name* **actions patch status**—Provide the current patch level and status
Updated Versions for Third-Party Software	SMI supports updated versions for the following third-party software in this release: • Calico—3.28 • Containerd—1.7.18 • Confd—7.7.16 • Docker—26.1.4 • Helm—3.15.2 • nginx—4.10.1

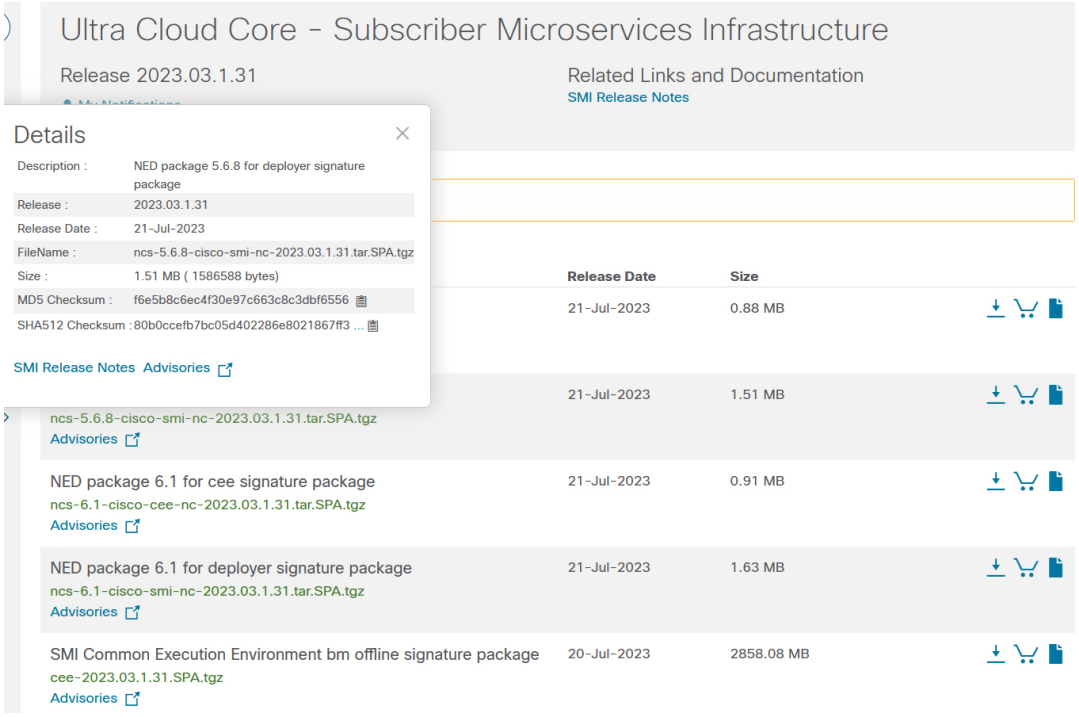
Installation and Upgrade Notes

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

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>`**

Operating System	SHA512 Checksum Calculation Command Examples
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
CSCwm59951	Grafana, ops-center access lost after shutting down Mgmt Vlan on M2 having the VIP
CSCwm87591	Cluster Sync is failing at Core-DNS pod check step
CSCwm92840	Cdl ep is not able to fetch the key from cdl index pod, and sending empty response to smf service
CSCwm94824	\buff/cache memory utilization going high on specific server in SMF cluster
CSCwm99119	SMI Opscenter pod crash and multiple coredump generated after 2024.04.1.i11 to 2024.04.1.i14 upgrade

Resolved Bugs for this Release

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

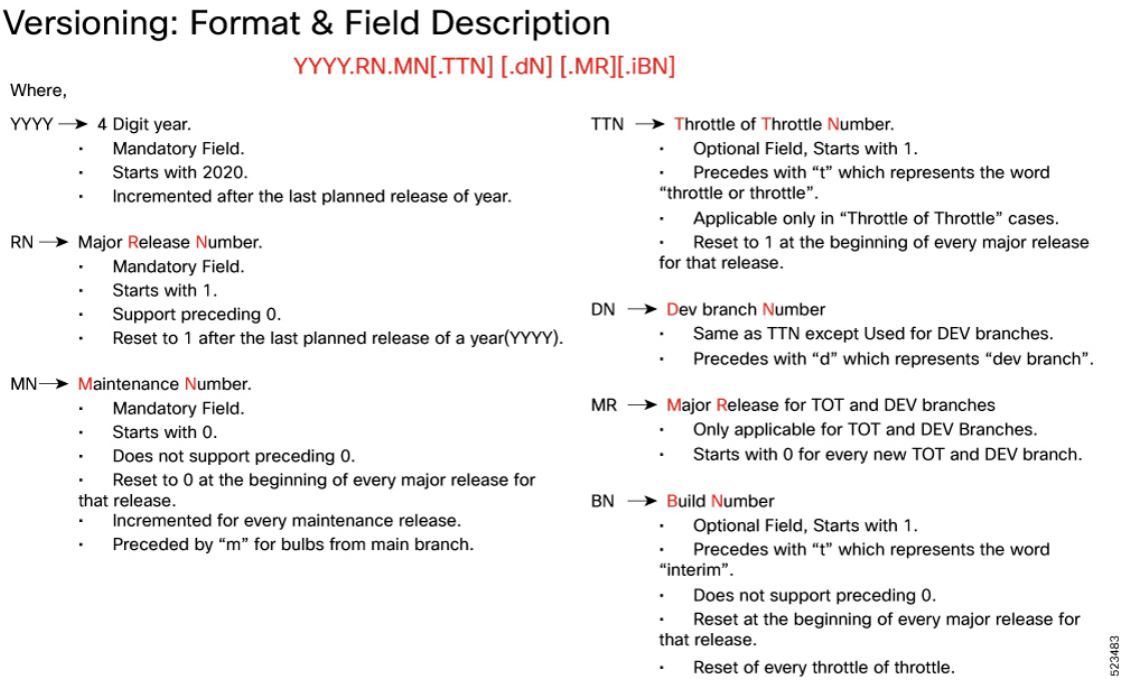
Note This software release may contain resolved bugs first identified in other releases. Additional information for all resolved bugs are available in the Cisco Bug Search Tool.

Bug ID	Headline	Behavior Change
CSCwm26664	M6 migrating vpp-cpu-worker-cnt from 24 to 14 from July'24 to Oct'24, cluster sync failure	No
CSCwm40916	PCF ops-center config wiped out after upgrading to i07	No
CSCwm78176	Post Upgrade from 2024.04.1.i10 to 2024.04.1.i11 not able to login to CM	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.