UCC 5G SMI Release Notes, Release 2024.02.1.14

First Published: 2024-04-30

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-2024
End of Life	EoL	30-Apr-2024
End of Software Maintenance	EoSM	29-Oct-2025
End of Vulnerability and Security Support	EoVSS	31-Oct-2025
Last Date of Support	LDoS	31-Oct-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.20.04.0-20240406.iso.SPA.tgz	20.04.0-20240406
cee.2024.02.1.14.SPA.tgz	2024.02.1.14
cluster-deployer-2024.02.1.14.SPA.tgz	2024.02.1.14
NED Package	ncs-5.6.8-cisco-cee-nc-2024.02.1.14 ncs-5.6.8-cisco-smi-nc-2024.02.1.14 ncs-6.1.3-cisco-cee-nc-2024.02.1.14 ncs-6.1.3-cisco-smi-nc-2024.02.1.14
NSO	5.6.8 6.1.3

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

- 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
CEE Log Forwarding on Fluent Worker Pods	When you enable CEE log forwarding, all logs are transferred to the configured nodes unless the filters do not match. CEE already supports the filters to drop logs from selected namespaces, pods, and pod annotations. The new filters on Fluent worker pods that intake the logs from each node reduce the volume of logs being forwarded. CEE supports the following new filters for log forwarding that are configurable in Logging Config mode: • Retain logs by namespaces using the **logging worker keep-namespace-logs** CLI • Retain logs by pods using the **logging worker keep-pod-logs** CLI • Drop logs by Linux OS services using the **logging worker drop-os-service-logs** CLI • Remove log metadata keys using the **logging worker remove-keys [keys]** CLI

Feature	Description
Cilium Configuration	The Cilium open-source project provides networking and security capabilities for Kubernetes clusters. It is used as a networking and security addon for Kubernetes, replacing or augmenting the default Kubernetes networking components. When you install or uninstall Cilium on the existing cluster without force-vm redeployment, each node is rebooted so that the pods will be controlled by Cilium. You can enable Cilium in chaining mode with Calico using the following CLI command in Cluster Configuration mode: **`clusters` *`cluster_name`* `configuration cilium { enabled | disabled }`** The following CLI command is deprecated in this release: **`clusters` *`cluster_name`* `addons cilium { enabled | disabled }`**
Cluster Synchronization using Netplan	You can trigger an additional cluster synchronization phase on the SMI cluster manager for Netplan updates. The Netplan sync phase helps with optimizing cluster sync and minimizing the time taken for route additions or updates from the complete cluster sync. You can configure the Netplan sync phase using the following CLI command in Cluster Configuration mode: **`clusters` *`cluster_name`* `actions sync run sync-phase netplan`**
Error Handling Logs in Cluster Deployer	The cluster deployer is enhanced to support debug logging in kubeadm init for errors such as cluster synchronization failure due to misconfiguration. A debug message captures the error logs in */var/tmp/kubeadm_out.log* to access the setup and retrieve the kubeadm init logs. You can view the error messages during cluster sync.
Kubernetes Version Upgrade	With this release, you can upgrade the Kubernetes version from 1.27 to 1.28. **Default Setting**: Enabled – Always On
Managing Custom Grafana Dashboards	The custom Grafana dashboards in CEE Ops Center are made persistent in this release. This enhancement ensures that the dashboards are not lost during pod restart, node shutdown, or any upgrade. The Grafana dashboards are stored in the */mnt/stateful_partition/data/cee-global/data-postgres-x* directory. The valid users of the dashboards are either local users or TACACS users who have access to CEE Ops Center. You can configure the **grafana enable-basic-auth { true | false }** CLI to enable or disable basic authentication. When enabled, you can perform all CRUD operations on the dashboards with the existing Grafana HTTP API.

Feature	Description
Sequential Deployment of Helm Charts in Ops-Center	This feature provides NF users the flexibility to manage the deployment of helm charts by introducing chart priority groups. It allows users to control the order in which the helm charts are deployed, ensuring that pods related to high-priority charts are available before deploying the lower-priority charts. This feature introduces the following new CLI commands: • **helm ordered_deployment enable true**—Use this command to enable sequential deployment. • **helm ordered_deployment chart** *chart_name* **priority_group** *priority_id*—Use this command to order the helm charts. Prior to executing this command, you must enable sequential deployment. **Important** When you configure this feature through NSO, you will observe that helm charts are removed from the device. This issue happens as the chart names that are loaded in Ops-center are not synced to NSO, thereby causing an illegal reference error. It is recommended that you sync the configuration from the device (using **sync-from** CLI) before initiating the ordered deployment configuration.
SMI Cluster Deployer on RHEL 8.9	You can install the inception deployer on Red Hat Enterprise Linux (RHEL) to enable Linux agnostic deployment. The supported RHEL version is 8.9. This feature is an extension of the inception server installation using Ubuntu 20.04 LTS.
Updated Default Value for Pod Eviction Toleration Time	The default value for **default-unreachable-toleration** and **default-not-ready-toleration** CLI commands is updated from 300 seconds to 30 seconds. This change will enable pods to move faster to other nodes during K8s pod rescheduling when the node is unreachable or not ready.
Updated Versions for Third Party Software	SMI supports updated versions for the following third party software in this release: • Calico—3.27.0 • Confd—7.7.14 • Containerd—1.7.13 • Docker—24.0.9 • Helm—3.14.1 • Prometheus—2.48.1 **Default Setting**: Enabled – Always On

Feature	Description
UCS M7 Server Support	SMI Bare Metal supports the UCS C220 M7 server with dual socket for On-Premise and Private 5G deployments. The Cisco UCS C220 M7 Rack Server is a versatile general-purpose infrastructure and application server. This high-density, 1RU, 2-socket rack server delivers industry-leading performance and efficiency for a wide range of workloads, including virtualization and bare-metal applications. **Note** It is recommended to use the UEFI secure boot mode only on UCS M7 server. For more information, see the *UCC SMI Deployment Guide*.
UCS Server Health Check	SMI allows you to perform extended heath check and monitoring of the deployed UCS C-series servers. The existing health reporting system within the REST (Redfish) API of the UCS servers is leveraged to obtain information from multiple hardware platforms. The server health check is a steadfast method to check and report the server health before executing a cluster-sync operation. This check reduces the disruptions caused by cluster-sync failures. This feature supports the following new CLI commands: • To force quit the cluster sync, you can override the health check sync failure using the following command: **clusters** *cluster_name* **nodes** *node_name* **ucs-server ignore-health { false | true }** • To review the condition of the servers anytime, you can run the server-check synchronization phase using the following command: **clusters** *cluster_name* **actions sync run sync-phase server-check**

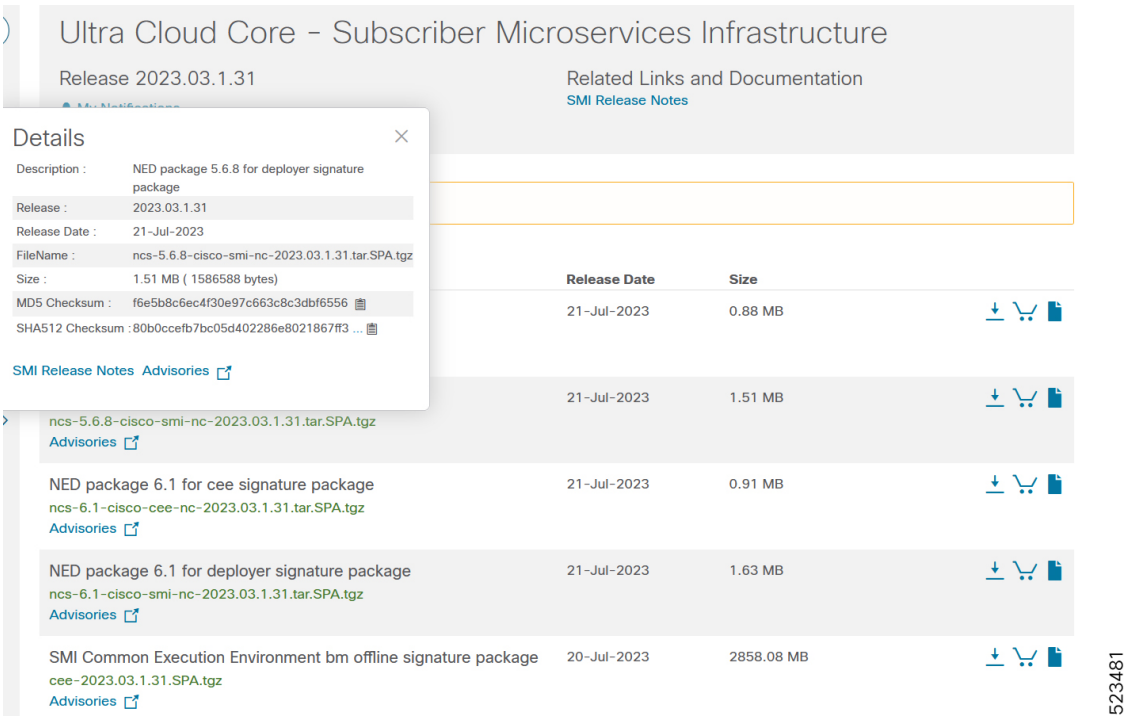
Installation and Upgrade Notes

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>`**
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
CSCwj67777	CM-HA primary reboot followed by Power off, CM-HA will not recover
CSCwj83959	RPC error towards CEE device: operation_failed: application communication failure for CEE Commits

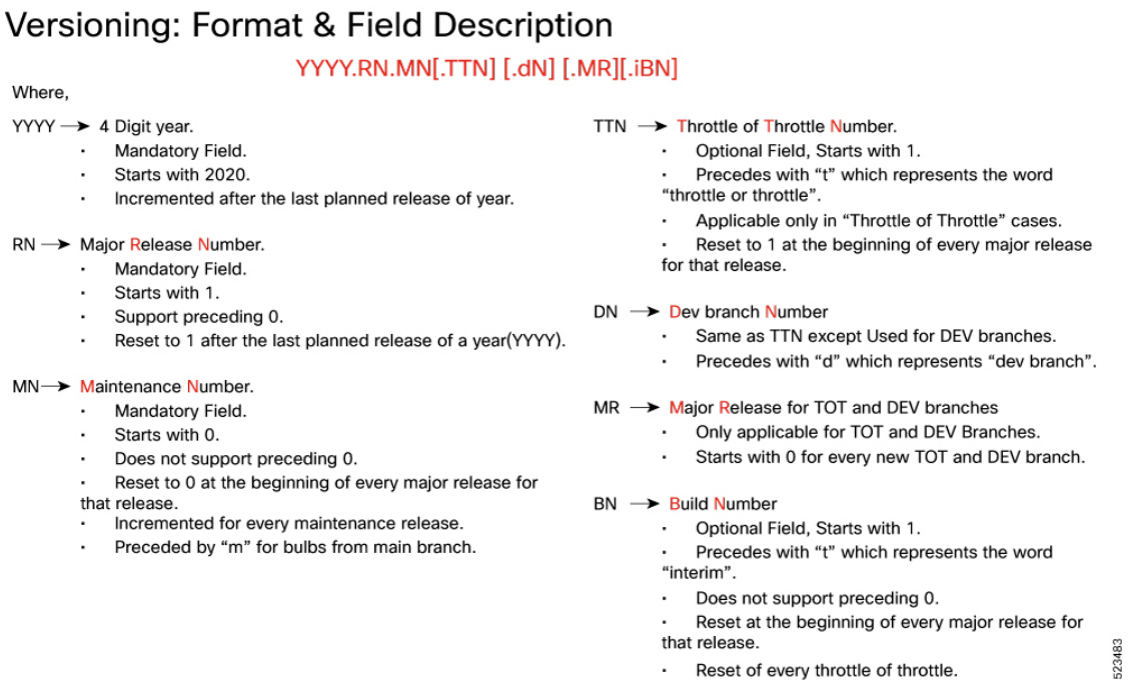
Resolved Bugs for this Release

There are no resolved bugs in this specific software release.

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.