UCC 5G SMI Release Notes, Release 2025.01.1.14

First Published: 2025-01-30

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	31-Jan-2025
End of Life	EoL	31-Jan-2025
End of Software Maintenance	EoSM	1-Aug-2026
End of Vulnerability and Security Support	EoVSS	1-Aug-2026
Last Date of Support	LDoS	31-Aug-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.22.04.0-20250107.iso.SPA.tgz	22.04.0-20250107
cee-2025.01.1.14.SPA.tgz	2025.01.1.14
cluster-deployer-2025.01.1.14.SPA.tgz	2025.01.1.14
NED Package	ncs-6.1.14-cisco-cee-nc-1.1.2025.01.1.14.tar.gz ncs-6.1.14-cisco-smi-nc-1.1.2025.01.1.14.tar.gz
NSO	6.1.14

Descriptions for the various packages provided with this release are provided in the Release Package Descriptions, on page 9 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
CoreDNS Configuration	SMI allows configuration of CoreDNS parameters for policy and cache updates via the SMI Cluster Manager. This enhancement streamlines DNS management and improves network performance. Command Introduced: **clusters** *cluster_name* **configuration core-dns** *string*
Kubernetes Version Upgrade	With this release, you can upgrade the Kubernetes version from 1.30 to 1.31.

Feature	Description
Software Upgrade from 2024.03.1 to 2025.01.1	You can upgrade SMI directly from 2024.03.1 to the latest 2025.01.1 release, which includes a new base image and a security patch. This release also upgrades the K8s version from 1.29 to 1.31. **Note** As part of this upgrade, ensure that you also update the PCF from release 2024.03.0 to 2025.01.0. 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.
CPU Frequency Scaling	SMI provides configuration options to improve CPU performance by adjusting the CPU scaling governor settings. This feature allows the operator to switch between "powersave" and "performance" modes, with "powersave" as the default setting. The operator changes the governor setting to "performance" to increase system performance during demanding workloads. Commands Introduced: • **clusters** *cluster_name* **node-defaults os tuned base-profile { balanced | latency-performance }** • **clusters** *cluster_name* **nodes** *node_name* **os tuned base-profile { balanced | latency-performance }** • **clusters** *cluster_name* **node-type-defaults** *node_type* **os tuned base-profile { balanced | latency-performance }**
UPF HDD Size Customization for Enhanced Data Storage	SMI introduces the ability to customize the HDD size for UPF, ranging from the default 16GB up to a maximum of 999GB. This flexibility supports additional storage needs for EDRs, CDRs, and PCAP traces. Commands Introduced: **clusters** *cluster_name* **disk-size** *size_value*

Feature	Description
Updated Versions for Third-Party Software	SMI supports updated versions for the following third-party software in this release: • Calico—3.29.1 • Containerd—1.7.24 • Confd—7.7.16 • Docker—27.4.1 • Helm—3.16.2 • nginx-ingress—4.12.0
Upgrade of OS to Ubuntu 22.4	This release recommends upgrading the SMI base image and Cluster Manager to Ubuntu 22.04. Additionally, it is recommended to update the Inception Server to the latest SMI disk ISO and refresh the container images in smi-app, smi-library, smi-build, smi-shared, smi-incubator, and related components. **Important** You must upgrade the CEE to 2025.01.1 release along with base image upgrade.

Behavior Changes

This section covers a brief description of behavior changes introduced in this release.

Behavior Change	Description

Change in VPP Defaults for UPF Deployment on M6 and M7 Servers	**Previous Behavior**: The default VPP count was a third of the available cores for UPF.
	New Behavior: The VPP count is now hardcoded for UCS C220 M6 and M7 servers as follows:
	• **With Hyperthreading**:
	  • Full: 48
	  • Half: 24
	  • Quarter: 12
	• **Without Hyperthreading**:
	  • Full: 24
	  • Half: 12
	  • Quarter: 6
	Note that the VPP count can be configured in the Cluster Manager. If this configuration is available, the configured VPP values take precedence over the default values.
	Each host can reserve only one core if hyperthreading is enabled.
	Customer Impact: Existing deployments and upgrades will retain their current settings. These new values apply only to new deployments.

Resolved Security Issues

This section contains information about resolved security issues including severity and description.

Severity	ID	Description
Critical	213189	GStreamer vulnerability (USN-7174-1)
Critical	148367	Python Unsupported Version Detection
Critical	209121	libarchive vulnerabilities (USN-7070-1)
Critical	211522	GLib vulnerability (USN-7114-1)
High	211884	Twisted vulnerability (USN-6988-2)
High	209164	Linux kernel vulnerabilities (USN-7073-1)
High	212270	Intel Microcode vulnerabilities (USN-7149-1)
High	212722	Linux kernel vulnerabilities (USN-7159-1)
High	213100	Linux kernel vulnerabilities (USN-7173-1)
High	209984	libarchive vulnerability (USN-7087-1)
High	210006	Linux kernel vulnerabilities (USN-7088-1)

Severity	ID	Description
High	211896	libsoup vulnerabilities (USN-7126-1)
Medium	212213	Expat vulnerability (USN-7145-1)
Medium	209876	urllib3 vulnerability (USN-7084-1)
Medium	207723	Intel Microcode vulnerabilities (USN-7033-1)
Medium	207823	ConfigObj vulnerability (USN-7040-1)
Medium	211586	Python vulnerability (USN-7116-1)
Medium	183592	NTP vulnerability (USN-5175-1)
Medium	209342	AMD Microcode vulnerability (USN-7077-1)
Medium	209028	nano vulnerability (USN-7064-1)
Medium	207996	Vim vulnerability (USN-7048-1)
Low	211920	Vim vulnerability (USN-7131-1)
Low	213082	curl vulnerability (USN-7162-1)

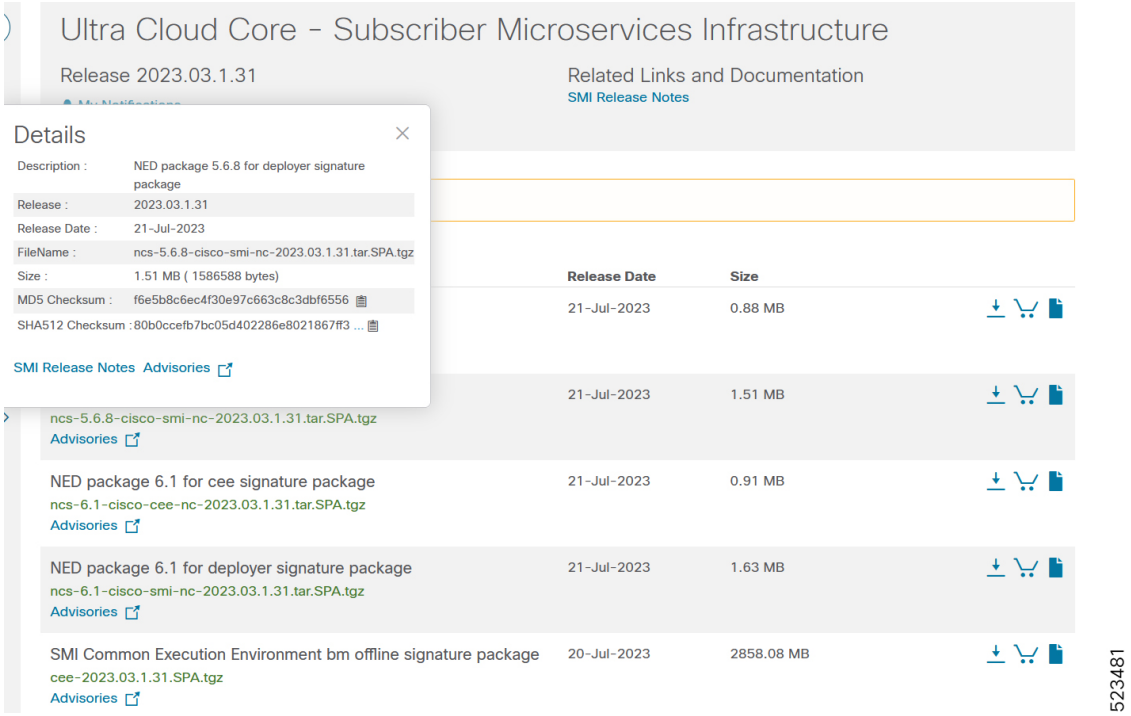
Installation and Upgrade Notes

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>`**
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
CSCwn53639	Intf name changed on Mellanox NIC after upgrading from Oct'24 to Jan'25
CSCwn61473	SNMP traps not sent when internal and external VIPs are on 2 different nodes

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 for this release are available in the Cisco Bug Search Tool.

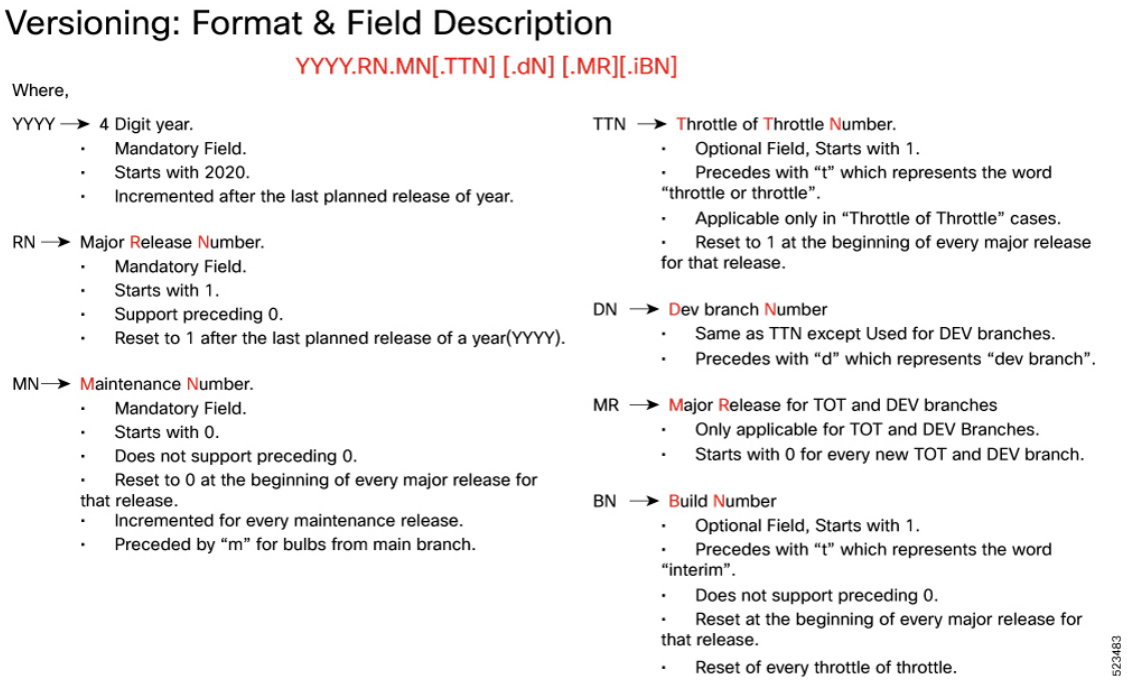
Bug ID	Headline	Behavior Change
CSCwn45697	M6 UPFs got redeployed on second cluster sync, configs wiped out	Yes

Bug ID	Headline	Behavior Change
CSCwn49207	Errors seen in BMC log exporter, SEL not reset after 2000 entries	No
CSCwn61626	Node isolation feature with tolerance not working as expected	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.