UCC 5G SMI Release Notes, Release 2025.02.1.20

First Published: 2025-06-05

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-2025.02.1.20.SPA.tgz	2025.02.1.20
cluster-deployer-2025.02.1.20.SPA.tgz	2025.02.1.20
NED Package	ncs-6.1.14-cisco-cee-nc-1.1.2025.02.1.20.tar.gz ncs-6.1.14-cisco-smi-nc-1.1.2025.02.1.20.tar.gz ncs-6.4.3-cisco-cee-nc-1.1.2025.02.1.20.tar.gz ncs-6.4.3-cisco-smi-nc-1.1.2025.02.1.20.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 5 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

There are no new features and enhancements in this release.

Behavior Changes

There are no behavior changes in this release.

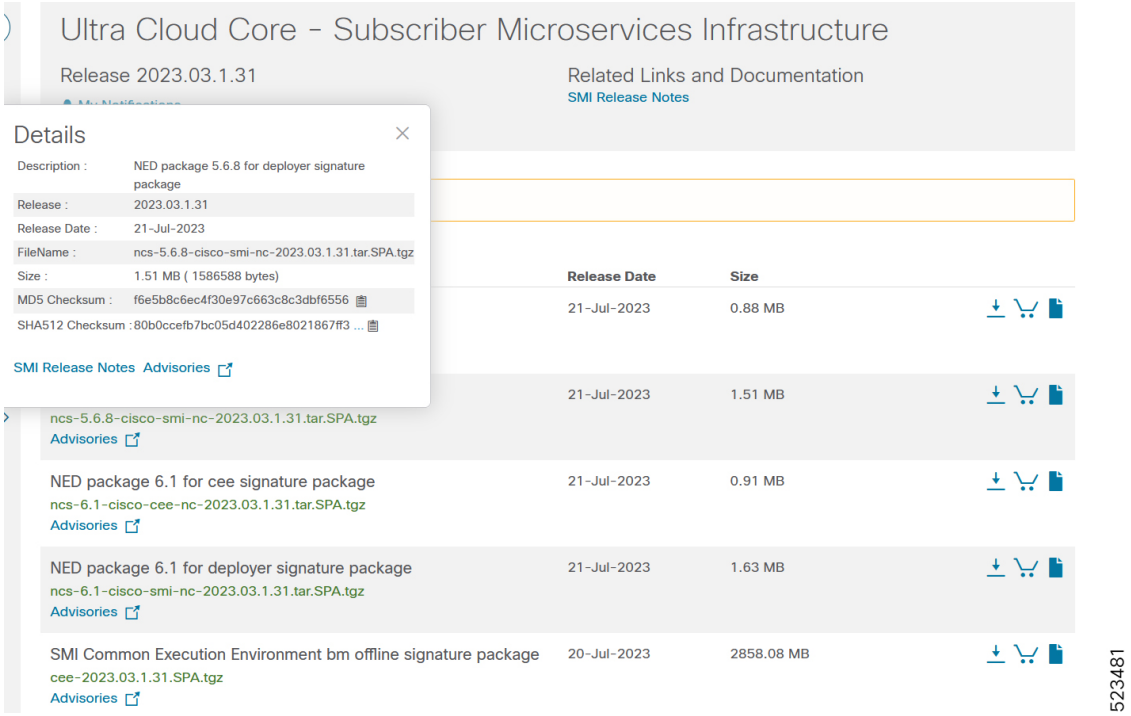
Installation and Upgrade Notes

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.



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

There are no open bugs in this software release.

Resolved Bugs for this Release

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

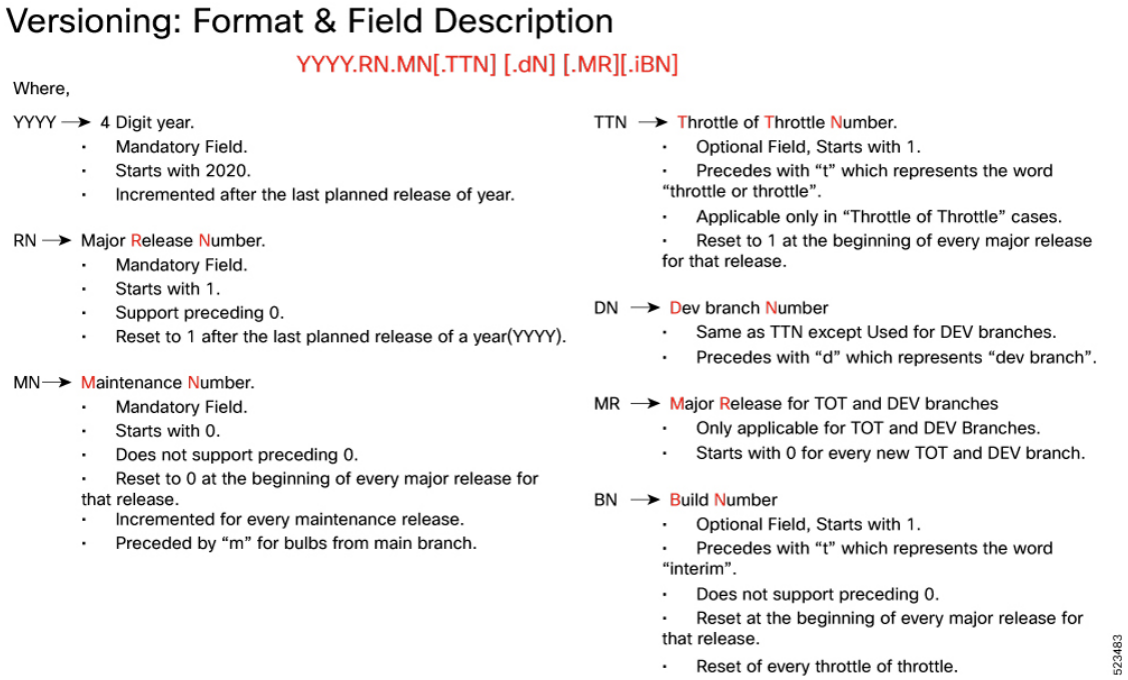
Note This software release may contain bug fixes first introduced in other releases. Additional information for all resolved bugs for this release are available in the Cisco Bug Search Tool.

Bug ID	Headline	Behavior Change
CSCwo83747	Evaluation of Ultra Cloud Core - Subscriber Microservices Infrastructure for Erlang-OTP SSH vulnerability	No
CSCwp03100	SMI - Cluster sync - FAILURE - TASK [bm-ucs : Fail when recovery/isolation not possible]	No
CSCwp07398	SMI - Cluster sync - FAILURE - TASK [os-base : Install Tuned] failed - KVM IMS/KVM Data / AIO	No
CSCwp11631	Host Profile is removed and default values are set for ARP_RP Filters during SMI Upgrade to Apr'25	No
CSCwp22952	Host profile with ADDDC disable and hugepages, one of the VMs didn't get deployed	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.

Software Packages	Description
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.