Release Notes for UCC SMI, Release 2025.04.1.16

Contents

Ultra Cloud Core - Subscriber Microservices Infrastructure, Release 2025.04.1.16

This Release Notes identifies changes and issues related to the release of Ultra Cloud Clore (UCC) Subscriber Management Infrastructure (SMI).

The key highlights of this release include:

- Central cluster manager scaling - Central CM now supports up to 9 clusters with 30 nodes per cluster, recommended for optimal performance.
- Containerized cnEPCGW deployment - cnEPCGW is now available for containerized deployment via ops-center installation.
- Declarative disablement of System Users/Groups - Safely disable system users/groups on cluster nodes using new model keys with built-in validation and auditing.
- LDAPS security for Ops Center - Secure directory authentication with new LDAPS (LDAP over TLS) support.
- Enhanced subscriber reporting - CDL now offers advanced filtering by creation and update time for improved session reporting.
- FQDN-compliant hostname support - Configure RFC4120-compliant FQDN hostnames per node for improved integration and standards compliance.
- Kubernetes version upgrade - Upgrade Kubernetes from v1.33 to v1.34.
- Streamlined add-on management - Add-on Manager reduces tar sizes, speeds up load times, and enables flexible add-on installation for SMI clusters.
- TLS for TACACS+ - Adds robust TLS 1.3/mTLS support for TACACS+ traffic security.
- Ubuntu 24.04 OS upgrade - Base image, Cluster Manager, and Inception Server now support Ubuntu 24.04; CEE upgrade to 2025.04.1 required.
- IPA integration - Seamless integration with Identity, Policy, Audit (IPA) servers for centralized identity management.
- Software RAID for CNDP - Software RAID support added for CNDP deployments on Supermicro servers, enhancing platform resilience.
- IPv6 dual-stack support - Full IPv6 dual-stack support for external interfaces across SMI and CNDP environments.

For more information on SMI, see the Related resources section.

Release lifecycle milestones

This table provides EoL milestones for Cisco UCC SMI software:

Table 1. EoL milestone information for UCC SMI, Release 2025.04.1.16

Milestone	Date
First Customer Ship (FCS)	31-Oct-2025
End of Life (EoL)	31-Oct-2025

Milestone	Date
End of Software Maintenance (EoSM)	01-May-2027
End of Vulnerability and Security Support (EoVSS)	01-May-2027
Last Date of Support (LDoS)	30-Apr-2028

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.

New software features

This section provides a brief description of the new software features introduced in this release.

Table 2. New software features for UCC SMI, Release 2025.04.1.16

Product impact	Feature	Description
Ease of Setup	Containerized deployment of cnEPCGW	This feature supports the containerized deployment of cnEPCGW through ops-center installation.
Software Reliability	Declarative disablement of system users and groups	This feature allows operators to declaratively and safely disable system users and groups on cluster nodes using the existing configuration model and Ansible. It introduces disable-system-users and disable-system-groups keys under OS: in the data model, along with validation to prevent accidental removal of protected accounts. Ansible tasks in the os-base role idempotently apply these specified changes, logging all actions and gracefully skipping non-existent users or groups. This ensures enhanced security, consistent configuration, and reliable system administration.
Software Reliability	Enhanced security with LDAPS for ops-center	The LDAPS (LDAP over TLS) support for ops-center provides a secure mechanism for all directory authentication and lookup traffic. This feature encrypts data in transit, addressing security concerns associated with plain LDAP and fulfilling requirements for secure communication with LDAP servers such as Active Directory or OpenLDAP.
Ease of Use	Enhanced subscriber reporting with CDL filtering options	CDL includes enhanced filtering capabilities with the addition of the "create-time" and "last-update-time" options in the commands "cdl show sessions summary" and "cdl show sessions detailed," enabling more precise and improved subscriber reporting.
Software Reliability	FQDN compliant hostname support	SMI introduces enhanced hostname management, allowing you to configure Fully Qualified Domain Names (FQDNs) compliant with RFC4120 for individual nodes within your cluster. This feature provides precise control over node-level hostnames, ensuring they meet specific networking and integration standards.
Ease of Setup	IPA integration	SMI offers seamless integration with IPA (Identity, Policy, Audit) servers.

Product impact	Feature	Description
		IPA is a comprehensive open-source solution for centralized identity management, providing robust authentication, authorization, and account management services across Linux/Unix environments.
Ease of Setup	IPv6 dual-stack support for external interfaces	SMI now fully supports IPv6 dual-stack capabilities across a wide range of its external communication interfaces. This enhancement ensures your CNDP environment is fully compatible with modern network infrastructures, offering increased flexibility and future-proofing your deployments.
Software Reliability	Kubernetes resource management with Balloons Policy NRI plugin	SMI introduces the NRI plugin with the Balloons Policy to enable support for multiple containers within a single pod, as well as multiple pods sharing the same CPU set. This enhancement delivers substantial improvements in resource management, network configuration, and diagnostic capabilities, providing users with enhanced control, flexibility, and performance for their critical workloads in the Mobility Services User Plane (MSUP) environment.
Upgrade	Kubernetes version upgrade	With this release, you can upgrade the Kubernetes version from 1.33 to 1.34.
Software Reliability	Optimize CNDP Cluster Networking with Cilium Netkit and BIGTCP	SMI enables activation of Cilium Netkit and BIG TCP features, resulting in significant enhancements in network throughput and efficiency for your containerized applications. NOTE: When the configuration for Netkit and BIG TCP features is enabled, you must manually restart all pods in the cluster for the changes to take effect, or alternatively, reboot all the nodes.
Software Reliability	Scalable cluster and node management with central Cluster Manager	The central Cluster Manager (CM) demonstrates significant scalability for managing numerous clusters and nodes. It supports up to 9 clusters with 30 nodes each, or any combination of clusters where the total number of nodes does not exceed 280, with a maximum of 30 nodes per cluster. The CM manages operations using Ansible fork batching. While system resources offer ample CPU capacity, concurrent cluster sync operations are primarily limited by network bandwidth during large downloads from external sources like artifactory.
Software Reliability	Software RAID support for CNDP deployments	This feature provides CNDP deployments on Supermicro servers with essential disk redundancy, enhancing the overall reliability and resilience of the platform.
Ease of Setup	Streamlined addon management in SMI clusters	The Add-on Manager significantly reduces cluster manager tar file size, shortens load times, and minimizes resource usage by allowing flexible installation and management of SMI cluster add-ons. It enables users to install only necessary add-ons, include basic images in offline tars, and configure custom add-ons via specific URLs. Dynamic Helm value configuration is also supported. Users deploy add-ons using the sync-phase add-ons command for synchronization.
Hardware Reliability	Support for UCS M8 server	SMI supports the deployment Cloud-Native Network Functions (CNFs) on UCS C225 M8 server.
Software Reliability	TLS support for TACACS+	This feature introduces robust Transport Layer Security (TLS) support for TACACS+ communications, enabling secure, encrypted transport of all TACACS+ traffic between clients and servers. It leverages industry-standard TLS 1.3 (with optional TLS 1.2 for

Product impact	Feature	Description
		interoperability) and supports mutual TLS (mTLS) for enhanced peer authentication.
Upgrade	Updated versions for third-party software	SMI supports updated versions for the following third-party software in this release: • Calico–3.29.5 • Containerd–1.7.28 • Confd–7.7.19.1 • Docker–28.4.0 • Helm–3.17.3 • nginx-ingress–4.12.1
Upgrade	Upgrade of OS to Ubuntu 24.04	This release recommends upgrading the SMI base image and Cluster Manager to Ubuntu 24.04. Additionally, it is recommended to update the Inception Server. **NOTE**: Container image OS is still on Ubuntu 22.

Changes in behavior

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

Table 3. Behavior changes for UCC SMI, Release 2025.04.1.16

Description	Behavior changes
Automatic cleanup of temporary installation files	**Previous behavior**: Temporary tar/tgz files (approximately 16GB) were retained indefinitely on each node after image installation. **New behavior**: When the parameter **disable-maintainer-pod** is set to **true** (for LAAS deployments), all tar/tgz files are automatically deleted after successful image loading. For standard deployments, these files continue to be retained for troubleshooting and debugging purposes. **Customer impact**: Substantial disk space savings per node; cleanup is automatic, seamless, and safe, as files are only removed after they are no longer needed post-installation.

Resolved issues

This table lists the resolved issues in this specific software release.

Note: This software release may contain bug fixes first introduced in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool. To search for a documented Cisco product issue, type in the browser: <bug_number> site:cisco.com

Table 4. Resolved issues for UCC SMI, Release 2025.04.1.16

Bug ID	Description
CSCwr29641	After base image upgrade from July'25 FCS to Oct'25, VPC-DI launch crashes

Bug ID	Description
CSCwr44029	UPF ends up in crash after upgrading to Oct'25 SMI build
CSCwr70364	NRF SBI VIP fails to initialize when cluster deployed with FQDN hostname feature
CSCwr96077	The multi-app software is configured but not used in the cluster, then it does not download the package
CSCwr84758	SMI upgrade failure for Remote NF at systemd-networkd-wait-online task

Open issues

This table lists the open issues in this specific software release.

Note: This software release may contain open bugs first identified in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool. To search for a documented Cisco product issue, type in the browser: <bug_number> site:cisco.com

Table 5. Open issues for UCC SMI, Release 2025.04.1.16

Bug ID	Description
CSCwr32206	Grafana URL login with IPv6 config experienced delayed response times

Known issues

This section provides the important guidelines in this specific software release.

To install the inception server in Ubuntu 22, the prerequisite is to add the following highlighted part in */etc/docker/daemon.json* file.

```
ubuntu@pyats-inception:~$ cat /etc/docker/daemon.json
{

        "default-address-pools": [{
                "base": "172.50.0.0/16",
                "size": 24
        },
                {
                        "base": "fd01::/80",
                        "size": 96
                }],
        "log-driver": "journald",
        "live-restore": true,
        "userland-proxy": false,
        "icc": false,
        "ipv6": true,
```

```
        "fixed-cidr-v6": "fd00::/80"
}
```

NOTE: Secure boot remains disabled in this release due to an update of the signing key in Cisco secured Linux.

Compatibility

This section lists compatibility information of the Cisco UCC software products that are verified to work with this version of the UCC SMI software.

Table 6. Compatibility information for UCC SMI, Release 2025.04.1.16

Product	Supported Release
Cisco UCS C220 M7	4.3(3.240022) 4.3(5.250001)
Cisco UCS C220 M6	4.3(3.240022) 4.3(5.250001)
Cisco UCS C220 M5	4.3(2.250016)

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.

Supported software packages

This section provides information about the release packages associated with SMI.

Table 7. Software packages for UCC SMI, Release 2025.04.1.16

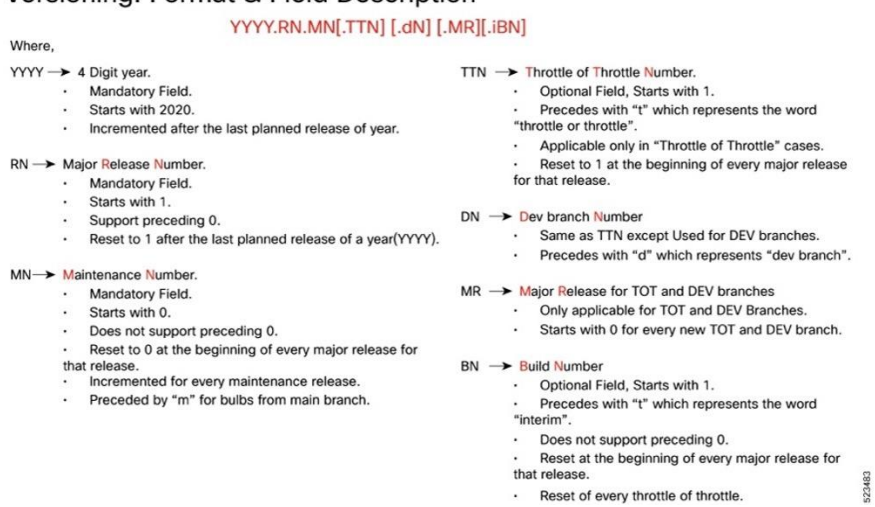
Software Package	Description	Release
smi-install-disk.24.04.0-20251025.iso.SPA.tgz	The application-level POD ISO image signature package for use with bare metal deployments. This package contains the base ISO image as well as the release signature, certificate, and verification information.	24.04.0-20251025
cee-2025.04.1.16.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.	2025.04.1.16
cluster-deployer-2025.04.1.16.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.	2025.04.1.16
NED package	The NETCONF NED package. This package includes all the yang files that are used for configuration.	ncs-6.4.8.1-cisco-cee-nc-1.1.2025.04.1.16.tar.gz ncs-6.4.8.1-cisco-smi-nc-1.1.2025.04.1.16.tar.gz ncs-6.1.14-cisco-cee-nc-1.1.2025.04.1.16.tar.gz ncs-6.1.14-cisco-smi-nc-

Software Package	Description	Release
		1.1.2025.04.1.16.tar.gz
NSO		6.4.8.1 6.1.14

Cloud native product version numbering system

The show helm list command displays detailed information about the version of the cloud native product currently deployed.

Figure 1. Cloud native product versioning format and description



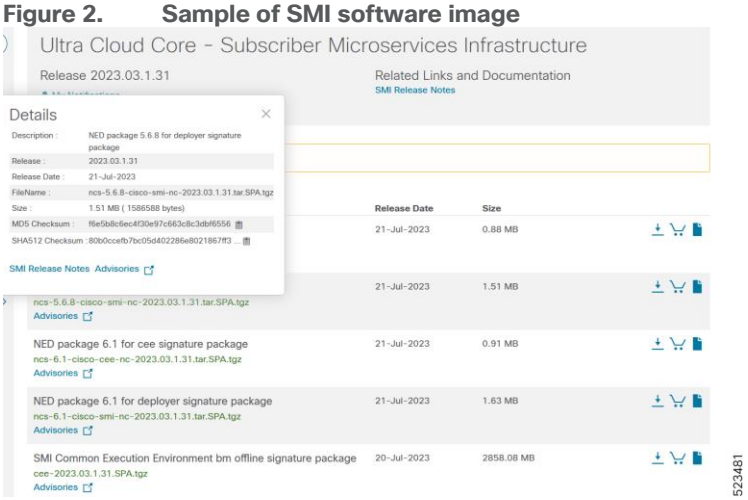
The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research software releases.

Software integrity version

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.

Figure 2. Sample of SMI software image



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 the one provided on the software download page.

To calculate a SHA512 checksum on your local desktop, see this table.

Table 8. 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>`

Note: <filename> is the name of the file. <extension> is the file type extension (for example, .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.

Related resources

This table provides key resources and links to the support information and essential documentation for SMI.

Table 9. Related resources and additional information

Resource	Link
SMI documentation	Subscriber Microservices Infrastructure
Service request and additional information	Cisco Support

Legal information