Release Notes for UCC SMI, Release 2025.03.1.10

Contents

Ultra Cloud Core - Subscriber Microservices Infrastructure, Release 2025.03.1.10

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:

- Hybrid deployment of containerized and virtualized VMs: Enables a single UCS M7 server to run both Kubernetes workloads and KVM virtual machines simultaneously, ensuring optimal performance isolation.
- Preserving client IPs in TACACS+ via NodePort configuration: Allows administrators to track original client IP addresses in TACACS+ logs for improved security auditing and traceability.
- Flexible configuration of VPC boot parameters: Users can now modify default values of VPC boot parameters (requires VM redeploy).
- UCS server status check: Introduces a single show_CLI command to simplify UCS hardware status summary, reducing the need for multiple API calls.
- Configurable TACACS server timeout: Allows network administrators to set both global and server-specific authentication timeouts via CLI, improving login reliability and user experience, especially in MFA-enabled environments.
- IPv6 dual-stack support for all external interfaces: Enables seamless communication using both IPv4 and IPv6 addresses across all CNDP components, supporting modern network environments and simplifying dual-stack management.
- Data encryption at REST: Ensures all data on the CNDP cluster is encrypted by default and automatically unlocked at boot using the Trusted Platform Module (TPM), enhancing security and compliance while reducing operational overhead.
- Delay rolling restart of keepalived pods: Introduces a configurable time interval for rolling restarts of keepalived pods during cluster upgrades, ensuring controlled VIP switchovers and greater service reliability.

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 2025.03.1.10

Milestone	Date
First Customer Ship (FCS)	14-Aug-2025
End of Life (EoL)	14-Aug-2025
End of Software Maintenance (EoSM)	12-Feb-2027
End of Vulnerability and Security Support (EoVSS)	12-Feb-2027

Milestone	Date
Last Date of Support (LDoS)	29-Feb-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 2025.03.1.10

Product impact	Feature	Description
Ease of setup	Hybrid deployment of containerized and virtualized VMs	This feature enables hybrid mode processing to allow a single UCS M7 server to run both Kubernetes workloads and KVM virtual machines simultaneously. This approach ensures optimal performance isolation between containerized SMF components and virtualized UPF instances.
Ease of use	Preserving client IPs in TACACS+ via NodePort configuration	This feature allows the configuration of NodePort in Ops-Centers to preserve the actual client IP addresses during TACACS+ authentication. By enabling this, administrators can: • Track the original client IP addresses in TACACS+ logs. • Improve security auditing and traceability for authentication attempts. • Ensure IP transparency for better operational security.
Ease of setup	Flexible configuration of VPC boot parameters	This feature allows users to modify the default values of VPC boot parameters. Note that the boot parameter update requires a VM redeploy.
Upgrade	Kubernetes version upgrade	With this release, you can upgrade the Kubernetes version from 1.32 to 1.33.
Upgrade	Updated versions for third-party software	SMI supports updated versions for the following third-party software in this release: • Calico—3.29.3 • Containerd—1.7.27 • Confd—7.7.19.1 • Docker—27.5.1 • Helm—3.17.3 • nginx-ingress—4.12.1
Ease of use	UCS server status check	This feature introduces a single show_CLI command to summarize the UCS hardware status, simplifying the workflow by reducing the need for multiple API calls and parsing.

Product impact	Feature	Description
Ease of setup	IPv6 dual-stack support for all external interfaces	You can now enable IPv6 dual-stack support across all external interfaces of the Cloud Native Deployment Platform (CNDP), allowing seamless communication using both IPv4 and IPv6 addresses. This update ensures all CNDP components—such as management, authentication, monitoring, and ingress—work with IPv6 without needing special configuration or feature-gates. The platform automatically applies IPv6 settings in deployment and operational workflows, ensuring compatibility with modern networks while continuing to support IPv4. This feature helps you future-proof your environment and simplifies managing dual-stack cloud deployments. **IMPORTANT**: Please note that Prometheus federation has not yet been fully tested end to end and is expected to be supported by July 31st.
Software Reliability	Delay rolling restart of keepalived pods	This feature introduces a configurable time interval (min-ready-seconds) between the rolling restarts of keepalived pods during cluster upgrades. By allowing administrators to specify the minimum time interval before each pod is considered available, the solution ensures that VIP (Virtual IP) switchovers are staggered and controlled. With the configurable time interval for keepalived pod rolling restarts, you can gain precise control over VIP switchovers during upgrades—delivering greater service stability, reliability, and continuity for mission-critical deployments.
Software Reliability	Configurable TACACS server timeout	This feature introduces configurable timeout settings for TACACS server authentication within the ops-center, allowing network administrators to set both global and server-specific connection timeouts directly via CLI. By enabling precise control over login timeout durations, especially in environments using multi-factor authentication (MFA), organizations can significantly reduce failed login attempts caused by premature timeouts. This ensures seamless and secure access on the first login attempt, improving operational efficiency and user experience. Administrators benefit from greater flexibility and reliability when adapting to network delays or MFA requirements, which aligns with best practices for network security and access management.
Ease of setup	Turn off spook check on SR-IOV interfaces - UCS M6 and M7 servers with UPF1.0 deployment	Users can now configure the spook check for SR-IOV VF interfaces, enabling or disabling it for UPF 1.0 deployments. For backward compatibility, the spook check is enabled by default on SR-IOV VF interfaces.

Changes in behavior

There are no behavior changes in this release.

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 3. Resolved issues for UCC SMI, Release 2025.03.1.10

Bug ID	Description
CSCwo69633	VPC-DI, default di-net and service port mapping is incorrect
CSCwp39268	VM redeploy with forwarder type IFTASK fails

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 4. Open issues for UCC SMI, Release 2025.03.1.10

Bug ID	Description
CSCwn55187	CEE not sending syslogs to a remote rsyslog server
CSCwp60114	Postgres pods in crashloopback state after power outage due to image corruption
CSCwq56161	CEE fluent proxy in crash loop after adding syslog host with message key
CSCwq66421	Postgres0 Crash Post Apr25 FCS to July25 FCS SMI Upgrade

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 5. Compatibility information for UCC SMI, Release 2025.03.1.10

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.

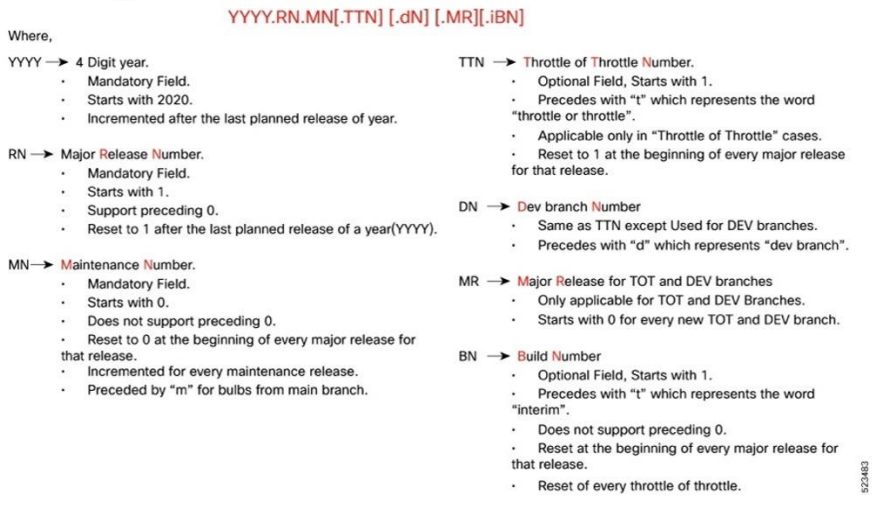
Table 6. Software packages for UCC SMI, Release 2025.03.1.10

Software Package	Description	Release
smi-install-disk.22.04.0-20250702.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.	22.04.0-20250702
cee-2025.03.1.10.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.	2025.03.1.10
cluster-deployer-2025.03.1.10.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.	2025.03.1.10
NED package	The NETCONF NED package. This package includes all the yang files that are used for configuration.	ncs-6.1.14-cisco-cee-nc-1.1.2025.03.1.10.tar.gz ncs-6.1.14-cisco-smi-nc-1.1.2025.03.1.10.tar.gz ncs-6.4.5-cisco-cee-nc-1.1.2025.03.1.10.tar.gz ncs-6.4.5-cisco-smi-nc-1.1.2025.03.1.10.tar.gz
NSO		6.1.14 6.4.5

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



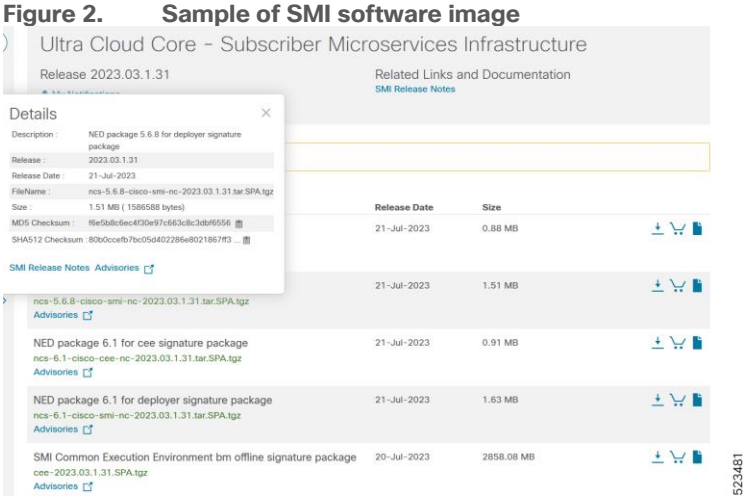
The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research 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 7. 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 8. Related resources and additional information

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

Legal information