Release Notes for UCC SMI, Release 2026.02.1.07

Contents

Ultra Cloud Core – Subscriber Microservices Infrastructure, Release 2026.02.1.07 3
New software features 4
Changes in behavior 5
Resolved issues 5
Open issues 5
Known issues 5
Compatibility 7
Supported software packages 7
Related resources 10
Legal information 10

Ultra Cloud Core - Subscriber Microservices Infrastructure, Release 2026.02.1.07

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:

- Critical updates
    - ConfD engine upgrade (7.7 to 8.6): This major upgrade introduces stricter configuration validation.
    - Kubernetes version upgrade: Support for upgrading Kubernetes from 1.34.3 to 1.35 is now available.
- Operational efficiency
    - Automated firmware and network management:
        - SMC firmware automation: Automate BMC, BIOS, and NIC upgrades via the Redfish API.
        - Common interface naming: Standardize network interface naming (for example, enc1, enc2) across UCS and SMC hardware for consistent configurations.
    - Simplified certificate and credential management:
        - CNI cluster issuer support: Automated certificate management via Cisco’s private ACME server.
        - Password rotation: Rotate initial-boot default passwords via sync command without redeploying nodes.
    - Workload stability: The new Reloader addon automatically restarts workloads when ConfigMaps or Secrets change, ensuring applications always use the latest configurations.
- Platform security and reliability
    - Enhanced access control: New 'nologin' user option for service accounts (for example, Prometheus) to perform automated tasks without SSH access.
    - Performance guardrails:
        - Added count capacity to FindAllNotify to prevent system overload.
        - Enforced equal CPU allocation for UPF " quarter flavor" deployments to prevent session manager imbalances.

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 2026.02.1.07

Milestone	Date
First Customer Ship (FCS)	23-Apr-2026

Milestone	Date
End of Life (EoL)	23-Apr-2026
End of Software Maintenance (EoSM)	22-Oct-2027
End of Vulnerability and Security Support (EoVSS)	22-Oct-2027
Last Date of Support (LDoS)	31-Oct-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 2026.02.1.07

Product impact	Feature	Description₹
Ease of Use	'nologin' user option	You can now create users in the OpsCenter with a nologin shell. This is a security feature that allows a user account to be used for automated tasks (like Prometheus scraping) while explicitly preventing that account from logging into the system via SSH.
Ease of Setup	Default user password rotation	You can now rotate the initial-boot default user password on existing nodes using a sync command, without needing to redeploy the node or regenerate cloud-init configurations.
Software Reliability	Reloader addon	This controller automatically monitors Kubernetes ConfigMaps and Secrets. When these change, it triggers a rolling restart of the associated workloads. This ensures applications (like Vault or MinIO) always use the latest configuration without requiring manual intervention.
Ease of Setup	SMC firmware upgrade support	Users can now automate firmware upgrades (BMC, BIOS, NIC) for Supermicro servers directly through the SMI cluster deployer using the Redfish API.
Software Reliability	FindAllNotify count capacity	An optional Count field has been added to the FindAllNotify filter. This allows users to limit the number of notifications sent during a request, preventing system overload when a large volume of records matches a query.
Ease of Setup	Common interface naming	To simplify managing different hardware environments (like UCS vs. SMC), you can now enable a common naming convention (e.g., enc1, enc2) for network interfaces. This makes network configurations consistent across different hardware platforms. **NOTE**: This functionality is currently supported only in fresh deployments.
Ease of Setup	Cluster issuer support	Cert-manager is now configurable to use Cisco's private ACME server. This allows for automated certificate management for Cisco Network Insight (CNI), removing the need for manual cluster issuer creation.

Product impact	Feature	Description₹
Software Reliability	Equal CPU allocation	For UPF deployments using the " quarter flavor," the system now ensures equal CPU distribution across all instances. This prevents session manager imbalances that could lead to call loss during recovery.
Upgrade	Kubernetes version upgrade	With this release, you can upgrade the Kubernetes version from 1.34.3 to 1.35.
Upgrade	Confd upgrade	This release includes an upgrade of ConfD configuration engine from version 7.7 to 8.6. Please be aware that this version enforces stricter configuration validation rules. Users with long-lived clusters should review their existing configurations for deprecated leaves (such as check-port) prior to upgrading to ensure a smooth transition. Refer to the Known issues section for more details.
Upgrade	Adopt gateway API for scalable ingress	To keep pace with evolving Kubernetes standards, CNDP is migrating to NGINX Gateway Fabric (NGF). This transition replaces our legacy Ingress implementation with the Gateway API. This migration modernizes our ingress traffic management, providing a more robust, standardized, and extensible architecture.

Changes in behavior

There are no behavior changes introduced 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 2026.02.1.i05

Bug ID	Description
CSCws41277	bm-alerts does not work on ipv6

Open issues

There are no open bugs in this specific software release.

Known issues

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

- For dual stack cluster deployments, it is strongly recommended to explicitly configure both node-ipv6 and ssh-ipv6. If you enable node-ipv6 on an existing deployment where it was not previously set up, be sure to redeploy the clusters to apply the changes.
- 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"
}
```

When installing the Inception server on Red Hat Enterprise Linux (RHEL), ensure that the Jinja2 Python package is installed as a prerequisite. You can do this by running the following command:

```
python3 -m pip install Jinja2
```

NOTE: Secure boot remains disabled in this release due to the UCS bug (CSCwt30472).

Cluster manager upgrade failure due to legacy configuration

Issue description:

Upgrading to Cluster Manager 2026.02.1.07 may fail if the existing cluster configuration contains both the deprecated check-port and the newer check-ports leaves within the same virtual-ips entry. During the upgrade, the transition to ConfD 8.6+ triggers a CDB validation check that rejects this mixed configuration, causing the confd container to enter a CrashLoopBackOff state.

Impact:

The Cluster Manager will remain unhealthy, and the upgrade process will not complete until the invalid configuration is removed.

Resolution:

Before initiating the upgrade to 2026.02.1.07, inspect your cluster configuration for the presence of both check-port and check-ports under virtual-ips.

Step 1. Identify the conflict:

```
virtual-ips <name>
  check-port     <value>  <-- Deprecated
  check-ports    [ <value> ]
```

Step 2. Remove the check-port entry, retaining only the check-ports configuration:

```
virtual-ips <name>
  check-ports [ <value> ]
```

Recovery steps (If upgrade has already failed):

If the upgrade has already been initiated and confd is in a crash loop:

Step 1. Roll back or downgrade the Cluster Manager to the previous 2026.01.x release to restore service.

Step 2. Run the synchronization command:

```
clusters <cluster-name> actions sync run sync-phase cluster-manager debug true
```

Step 3. Remove the deprecated check-port configuration as noted earlier.

Step 4. Retry the upgrade to 2026.02.1.07.

Step 5. Run the synchronization command again after the upgrade completes.

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 4. Compatibility information for UCC SMI, Release 2026.02.1.07

Product	Supported Release
Cisco UCS M8	4.3(6.250053) 6.0(1.250130)
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(2.260007)

Supported software packages

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

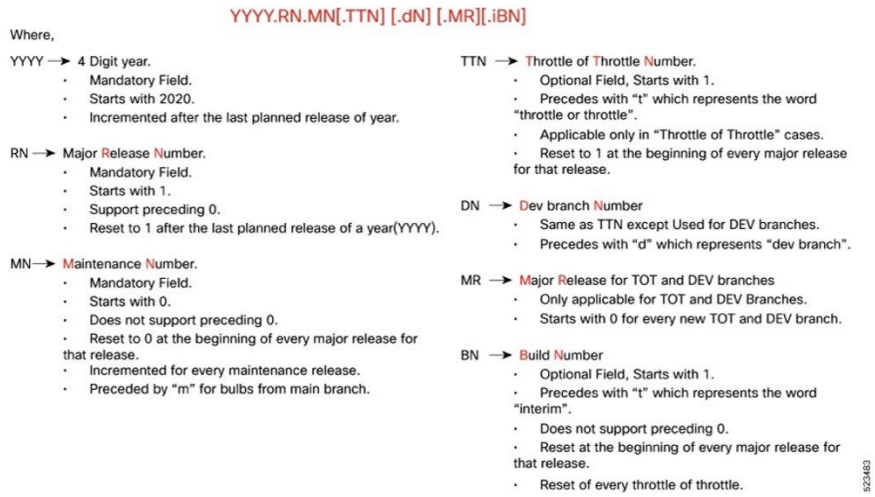
Table 5. Software packages for UCC SMI, Release 2026.02.1.07

Software Package	Description	Release
smi-install-disk.24.04.0-20260408.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.	24.04.0-20260408
smi-install-disk.24.04.0-20260408.qcow2.SPA.tgz	The application-level POD QCOW image signature package for use with bare metal deployments. This package contains the QCOW image as well as the release signature, certificate, and verification information.	24.04.0-20260408
cee-2026.02.1.07.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.	2026.02.1.07
cluster-deployer-2026.02.1.07.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.	2026.02.1.07
NED package	The NETCONF NED package. This package includes all the yang files that are used for configuration.	ncs-6.4.8.2-cisco-cee-nc-1.1.2026.02.1.07.tar.gz ncs-6.4.8.2-cisco-smi-nc-1.1.2026.02.1.07.tar.gz ncs-6.1.14-cisco-cee-nc-1.1.2026.02.1.07.tar.gz ncs-6.1.14-cisco-smi-nc-1.1.2026.02.1.07.tar.gz
NSO		6.4.8.2 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



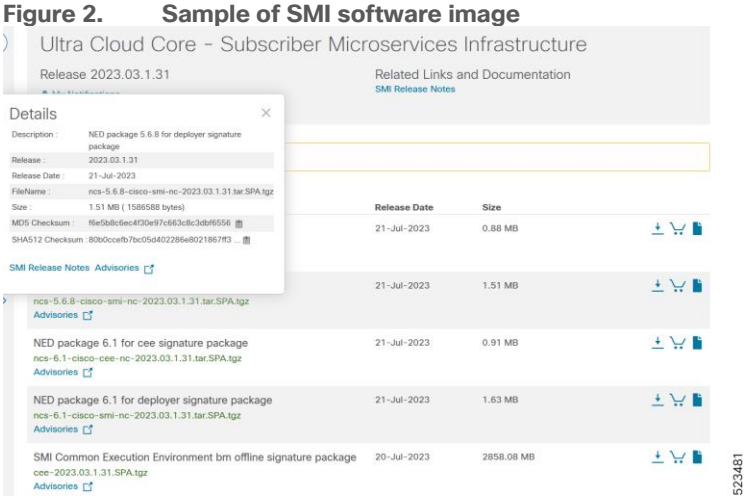
The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research 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 6. 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 7. Related resources and additional information

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

Legal information

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.