



Release Notes for NSO SMI AFP, Release 2026.01.0

Contents

| | |
|---|---|
| NSO SMI Automation Function Pack, Release 2026.01.0 | 3 |
| New software features..... | 3 |
| Changes in behavior | 4 |
| Resolved issues | 4 |
| Open issues..... | 5 |
| Compatibility..... | 5 |
| Supported software packages | 6 |
| Related resources..... | 9 |
| Legal information | 9 |

NSO SMI Automation Function Pack, Release 2026.01.0

The NSO SMI Automation Function Pack is a collection of multiple packages including the cisco-smi-deployer (previously referred to as the SMI Core Function Pack).

The key highlights of this release include:

- **TACACS nodeport configuration support:** SMI AFP now supports configuring TACACS nodeport for CNDP Cluster Manager, requiring SSH and NETCONF parameters when enabled.
- **Supermicro server support for AMF and NRF:** This enhancement provides customers with greater hardware flexibility and investment protection by supporting AMF and NRF on Supermicro server platforms, enabling optimized resource utilization and broader infrastructure choices for network function deployments.
- **Balloons policy support:** This enhancement ensures optimized resource allocation and improved deployment efficiency for EPCGW and MSUP, helping customers achieve better performance and scalability through standardized and automated policy management.
- **Support for RCM HA configuration:** This feature simplifies HA deployments and operations by streamlining configuration management for RCM pairs, enhancing service reliability and operational efficiency.
- **MSUP and MSCP Support on UCS M8:** Extended lifecycle and configuration management support to UCS M8 servers without requiring additional software updates.

For more information on SMI AFP, see the [Related resources](#) section.

Release lifecycle milestones

The following table provides EoL milestones for NSO SMI AFP software:

Table 1. EoL milestone information for NSO SMI AFP, Release 2026.01.0

| Milestone | Date |
|---|--------------|
| First Customer Ship (FCS) | 30-Jan-2026 |
| End of Life (EoL) | 30-Jan-2026 |
| End of Software Maintenance (EoS) | 31-July-2027 |
| End of Vulnerability and Security Support (EoVSS) | 31-July-2027 |
| Last Date of Support (LDoS) | 31-July-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 SMI AFP, Release 2026.01.0

| Product impact | Feature | Description |
|----------------------|--|--|
| Software Reliability | TACACS nodeport configuration support | CNDP now supports TACACS nodeport configuration for Cluster Manager (CM) deployments, with SMI AFP pushing the configuration from NSO. When enable-nodeport is true, nodeport-ssh and nodeport-netconf parameters are required. |
| Software Reliability | Supermicro server support for AMF and NRF | SMI AFP now extends support for deploying AMF and NRF network functions on Supermicro servers. The deployment process and configuration steps remain consistent with existing NF deployments, and no additional configuration changes are required. |
| Software Reliability | Balloons policy support | SMI AFP now supports balloons policy configuration for EPCGW and MSUP deployments, enabling it to push balloons configurations to the CNDP resource manager. Balloons policy is now recommended as the NRI plugin policy for deploying EPCGW and MSUP, requiring configuration on the CNDP Kubernetes cluster before deployment. |
| Software Reliability | Support for RCM HA configuration | The MFP component of AFP now enables joint configuration and management of both instances in an RCM HA (High Availability) pair. With this enhancement, the same configuration can be pushed to both RCM instances using existing configuration commands, ensuring consistency across the HA pair. |
| Software Reliability | Lifecycle and configuration management of MSUP and MSCP on UCS M8 server | This release extends MSUP and MSCP lifecycle and configuration management support to include UCS M8 servers. As a result of successful validation, these features are available without needing new configuration or software updates. |

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 SMI AFP, Release 2026.01.0

| Bug ID | Description |
|----------------------------|---|
| CSCwr43119 | MSG: software repo creation line by line is shows multiapp flag after ned. |
| CSCwr72907 | AFP 2025.04.00: prefer-ssh-ipv6 param value not pushed to device. |
| CSCwr87389 | AFP 2025.04.00: bind ip-address is mandatory for a pure ipv6 deployment on K8s cluster. |
| CSCwr94506 | Unable to add netplan-addtions when initial-netplan is configured under node level. |

| Bug ID | Description |
|----------------------------|---|
| CSCwr98327 | AFP 2025.04.00: When ssh-ip is not configured under node for a cluster it gets configured as "None". |
| CSCws14227 | AFP 2025.04.00: host-profile is rejected when environment is bm-server(supernmicro). |
| CSCws17184 | (additional-)master-vip-interface has dependency on IPv4 parameter (additional-)master-vip in pure IPv6 deployment. |
| CSCws37772 | AFP: Unconfig of bind-ip from existing K8s deployment throws errors. |
| CSCws76976 | Compatibility issues with SMI AFP 2026.01.0 Beta release. |

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 SMI AFP, Release 2026.01.0

| Bug ID | Description |
|----------------------------|--|
| CSCwq34560 | SMI AFP does not allow configuring functions without static NETCONF and SSH ports. |
| CSCws76472 | NED prompts for unnecessary string value for "node-defaults os ipa enabled". |
| CSCws76512 | NED shows IPA password in clear text under devices template (node-defaults os ipa password). |

Compatibility

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

Table 5. Compatibility information for SMI AFP, Release 2026.01.0

| Product | Supported release |
|------------|-------------------|
| CEE | 2026.01.1.08 |
| PCF | 2026.01.0.i29 |
| RCM | 2026.01.0.i43 |
| SMF+cnSGWc | 2026.01.0.i102 |

| Product | Supported release |
|---------|-------------------|
| UPF | 21.28.Mh34.99440 |

The NSO SMI AFP software is compatible with the following operating systems:

Table 6. Compatible operating systems for NSO SMI AFP software

| OS | Minimum server configuration | Version |
|---------|--|-------------|
| Ubuntu | CPU: 8 Cores RAM: 64 GB Disk: 250 GB | 18.04 LTS |
| Red Hat | CPU: 8 Cores RAM: 64 GB Disk: 250 GB | 7.3 (Maipo) |
| CentOS | CPU: 8 Cores RAM: 64 GB Disk: 250 GB | 7.4 (Core) |
| MacOS | CPU: 8 Cores RAM: 64 GB Disk: 250 GB | 10.12.6 |

Note the following product, platform, and runtime requirements for this release:

- NSO: 6.4.8.2
- SMI: 2026.01.1.08

Note: If upgrading from a beta version of NSO SMI AFP, the SMI cluster manager NED must be upgraded simultaneously. See resolved issues table, [CSCws76976](#).

- Python: 3.12.x

Supported software packages

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

Table 7. Software packages for SMI AFP, Release 2026.01.0

| Software package | Release |
|---|----------------------------|
| ncs-6.4.8.2-nso-smi-afp-2026.01.0.tar.SPA.tgz | SMI AFP version: 2026.01.0 |
| cisco-etsi-nfvo | 4.7.8 |

| Software package | Release |
|------------------------|------------------|
| cisco-smi-deployer | 2026.01.0 |
| cisco-smi-dvpc | 2026.01.0 |
| cisco-smi-nc-1.1 | 1.1.2026.01.1.08 |
| cisco-staros-cli-5.57 | 5.57.5 |
| esc | 5.3.0.94 |
| etsi-sol003-gen-1.13 | 1.13.19 |
| mobility-common | 2026.01.0 |
| mobility-rm-subscriber | 2026.01.0 |
| mop-automation | 2026.01.0 |
| mop-common | 2026.01.0 |
| openstack-cos-gen-4.2 | 4.2.34 |
| resource-manager | 4.2.10 |

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

Versioning: Format & Field Description

YYYY.RN.MN[.TTN] [.dN] [.MR][.iBN]

Where,

- YYYY → 4 Digit year.
 - Mandatory Field.
 - Starts with 2020.
 - Incremented after the last planned release of year.

- TTN → Throttle of Throttle Number.
 - Optional Field, Starts with 1.
 - Precedes with "t" which represents the word "throttle or throttle".
 - Applicable only in "Throttle of Throttle" cases.
 - Reset to 1 at the beginning of every major release for that release.

- RN → Major Release Number.
 - Mandatory Field.
 - Starts with 1.
 - Support preceding 0.
 - Reset to 1 after the last planned release of a year(YYYY).

- DN → Dev branch Number
 - Same as TTN except Used for DEV branches.
 - Precedes with "d" which represents "dev branch".

- MN → Maintenance Number.
 - Mandatory Field.
 - Starts with 0.
 - Does not support preceding 0.
 - Reset to 0 at the beginning of every major release for that release.
 - Incremented for every maintenance release.
 - Preceded by "m" for bulbs from main branch.

- MR → Major Release for TOT and DEV branches
 - Only applicable for TOT and DEV Branches.
 - Starts with 0 for every new TOT and DEV branch.

- BN → Build Number
 - Optional Field, Starts with 1.
 - Precedes with "t" which represents the word "interim".
 - Does not support preceding 0.
 - Reset at the beginning of every major release for that release.
 - Reset of every throttle of throttle.

523483

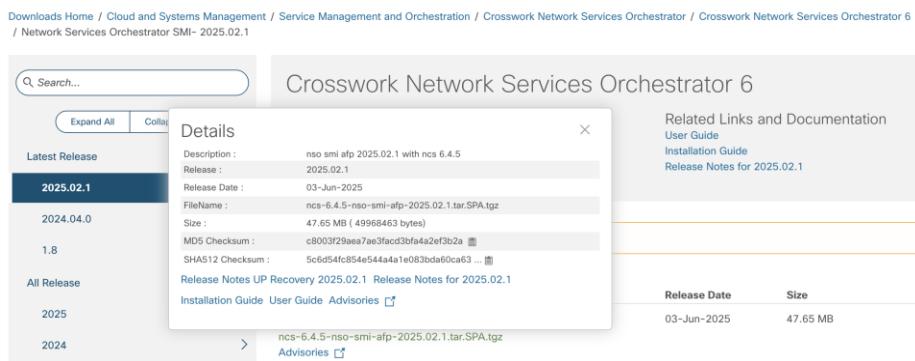
The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research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



Downloads Home / Cloud and Systems Management / Service Management and Orchestration / Crosswork Network Services Orchestrator / Crosswork Network Services Orchestrator / Network Services Orchestrator SMI - 2025.02.1

Search... Expand All Collapse

Crosswork Network Services Orchestrator 6

Details X

Latest Release 2025.02.1

2024.04.0

1.8

All Release 2025

2024

Description : nso smi afp 2025.02.1 with ncs 6.4.5

Release : 2025.02.1

Release Date : 03-Jun-2025

File Name : ncs-6.4.5-ns0-smi-afp-2025.02.1.tar.SPA.tgz

Size : 47.65 MB (4 49968463 bytes)

MD5 Checksum : c8003f29aea7ea73f3ccdf3fb4a42ef3b2a...

SHA512 Checksum : 5c6d84fc854e5444a1e0b3bda00ca63...

Release Notes UP Recovery 2025.02.1 Release Notes for 2025.02.1

Installation Guide User Guide Advisories

Related Links and Documentation

User Guide

Installation Guide

Release Notes for 2025.02.1

Release Date Size

03-Jun-2025 47.65 MB

ncs-6.4.5-ns0-smi-afp-2025.02.1.tar.SPA.tgz

Advisories

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: <code>> certutil.exe -hashfile <filename.extension> SHA512</code> |
| Apple MAC | Open a terminal window and type the following command: <code>\$ shasum -a 512 <filename.extension></code> |
| Linux | Open a terminal window and type the following command: <code>\$ sha512sum <filename.extension></code> OR <code>\$ shasum -a 512 <filename.extension></code> |

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 not to 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

NSO SMI AFP 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 AFP.

Table 9. Related resources and additional information

| Resource | Link |
|--|-------------------------------|
| NSO SMI AFP documentation | NSO SMI AFP |
| Service request and additional information | Cisco Support |

Legal information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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 included 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.

© 2026 Cisco Systems, Inc. All rights reserved.