Release Notes for NSO SMI AFP, Release 2026.04.0

© 2026 Cisco and/or its affiliates. All rights reserved.

Contents

NSO SMI Automation Function Pack, 2026.04.0 3
New software features 3
Changes in behavior 4
Resolved issues 5
Open issues 5
Compatibility 6
Supported software packages 7
Related resources 9
Legal information 10

© 2026 Cisco and/or its affiliates. All rights reserved.

NSO SMI Automation Function Pack, 2026.04.0

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:

- Centralized IP address management: Simplifies and standardizes IP address allocation across the cluster, ensuring consistent network configuration.
- Enhanced Mellanox Hardware Control: Simplifies the management of Mellanox network interfaces to ensure optimal performance and operational consistency.
- Automated energy efficiency: Reduces operational costs by enabling intelligent, automated power-saving configurations across the infrastructure.
- DLM (Data Layer Manager) Network Function support: This enhancement enables lifecycle and configuration management for DLM NFs within SMI AFP. It streamlines deployment using new parameters and existing automation to ensure operational consistency.
- NSO support for ULB (Unified Load Balancer) lifecycle and configuration management: This enhancement extends NSO support to include the lifecycle and configuration management of the ULB.
- Automated deployment verification: Increases system stability by automatically validating configuration changes before they are finalized, reducing the risk of manual errors.

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, 2026.04.0

Milestone	Date
First Customer Ship (FCS)	5-Nov-2026
End of Life (EoL)	5-Nov-2026
End of Software Maintenance (EoSM)	5-May-2028
End of Vulnerability and Security Support (EoVSS)	5-May-2028
Last Date of Support (LDoS)	31-May-2029

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.

© 2026 Cisco and/or its affiliates. All rights reserved.

Table 2. New software features for SMI AFP, 2026.04.0

Product impact	Feature	Description
Software Reliability	Support for Whereabouts CNI IPAM Plugin	Enables the configuration of the Whereabouts IPAM plugin within SMI AFP, providing centralized and consistent IP address management across the cluster.
Software Reliability	Support for Mellanox NIC firmware parameters	Enables native configuration of Mellanox NIC firmware parameters using key-value pairs, allowing for precise, hardware-level control directly through the AFP.
Software Reliability	Support for IPM power-saving	Enables Intelligent Power Management (IPM) and other power-saving parameters within the AFP by providing a direct mapping of configurations from the cluster manager.
Software Reliability	Lifecycle and configuration management of DLM Network Function	AFP supports lifecycle and configuration management for the DLM Network Function, introducing new function object parameters for deployment while utilizing existing mop-automation workflows for configuration.
Software Reliability	Lifecycle and configuration management of the ULB	AFP supports lifecycle and configuration management of the Unified Load Balancer (ULB), leveraging automated workflows to streamline deployment and ensure operational consistency.
Software Reliability	Post-checks for N:1 automated configuration push	Enables automated verification of configuration pushes via customizable "show" commands and regex patterns, ensuring instance readiness and operational integrity before completing the deployment process.

Changes in behavior

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

Table 3. Behavior changes for SMI AFP, Release 2026.04.0

Description	Behavior changes
Removal of default password for Keepalived authentication [CSCwx66107]	**Previous Behavior**: The keepalived-auth parameter within the smi deployment configuration included a pre-defined default password. If a user did not specify a password, the AFP would automatically push this default value to the Cluster Manager. **New Behavior**: The default value for the keepalived-auth parameter has been removed from the SMI AFP. The AFP no longer automatically provides or pushes a default password for this field during deployment or synchronization. **Customer Impact**: No functional impact on system operations is expected, as the underlying Cluster Manager currently maintains its own internal default for this value. However, the configuration data sent from the AFP to the Cluster Manager will no longer contain this specific default. If a custom authentication password is required, it must now be explicitly defined in the smi deployment settings.

© 2026 Cisco and/or its affiliates. All rights reserved.

Description	Behavior changes
Automated detection and abort of interrupted N:1 configuration pushes [CSCwx66135]	**Previous Behavior**: During an N:1 automated configuration push, the AFP did not detect if an MSUP or EPCGW instance reloaded while the process was underway. The system would attempt to continue the configuration transfer regardless of the reboot, potentially resulting in an incomplete configuration state while still incorrectly marking the instance as ready for its assigned role. **New Behavior**: The AFP now monitors the status of the MSUP or EPCGW instance during the configuration push. If a reload is detected mid-process, the AFP immediately aborts the current push. This prevents the instance from being certified as " ready" when it may only possess a partial or inconsistent configuration. **Customer Impact**: This enhancement improves system reliability and prevents service errors by ensuring that no instance enters an active or standby state with an incomplete configuration. In the event of a reboot during a push, the process is safely halted so it can be restarted or investigated, ensuring only fully configured instances handle traffic.

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 SMI AFP, Release 2026.04.0

Bug ID	Description
CSCwv71176	AFP 2026.03.0.i10 :mtu defined under the interface is not shown in internal configs, hence not pushed to Cluster Manager.
CSCwv87952	DLM deploy support on NSO AFP.

Open issues

This table lists the open 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 5. Open issues for SMI AFP, Release 2026.04.0

Bug ID	Description
CSCwq34560	SMI AFP does not allow configuring functions without static NETCONF and SSH ports.
CSCwv10032	SMI AFP needs simultaneous support for regular and nodeport based SSH/NETCONF ports.
CSCwv96722	Enhance smi-deployer log to capture more info.
CSCwx65887	Few CLIs not unconfigured on EPCGW/MSUP during rollback from NSO.

© 2026 Cisco and/or its affiliates. All rights reserved.

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 6. Compatibility information for SMI AFP, 2026.04.0

Product	Supported release
CEE	1.1.2026.04.1.i10
SMF+cnSGWc	2026.04.0
UPF	2026.04.0

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

Table 7. 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: 6.4.15
- SMI: 2026.04.1.10
- Python: 3.12.x

© 2026 Cisco and/or its affiliates. All rights reserved.

Supported software packages

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

Table 8. Software packages for SMI AFP, 2026.04.0

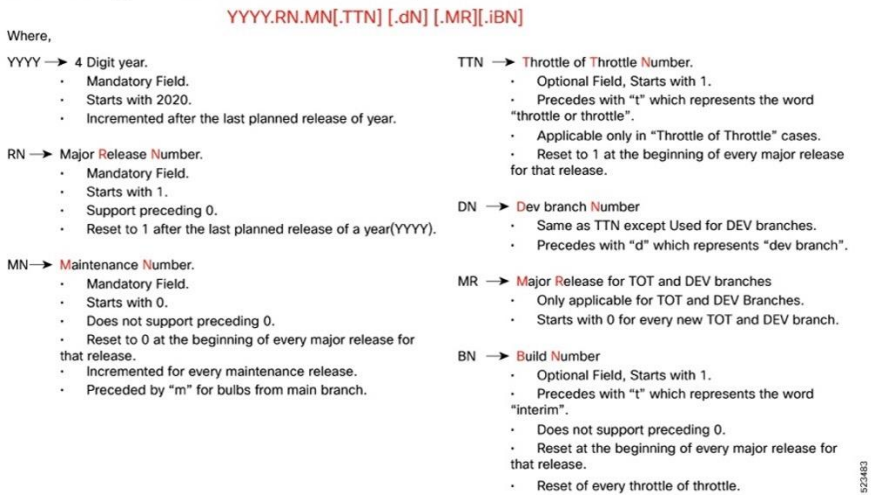
Software package	Release
ncs-6.4.15-nso-smi-afp-2026.04.0.tar.SPA.tgz	SMI AFP version: 2026.04.0
cisco-amf-nc-1.1	1.1.2026.04.0.i88
cisco-ccg-nc-1.1	1.1.2026.04.0.i118
cisco-cee-nc-1.1	1.1.2026.04.1.i10
cisco-etsi-nfvo	4.7.8
cisco-dlm-nc-1.1	1.1.2026.04.1.i10
cisco-nrf-nc-1.1	1.1.2026.02.0.i54
cisco-rcm-nc-1.1	1.1.2026.04.0.i61
cisco-smi-deployer	2026.04.0.i20
cisco-smi-dvpc	2026.04.0.i20
cisco-smi-nc-1.1	1.1.2026.04.1.i10
cisco-ulb-nc-1.1	1.1.2026.04.m0.i22
cisco-staros-cli-5.55	5.55
cisco-staros-cli-5.57	5.57.5
cisco-staros-cli-5.59	5.59.7
esc	5.3.0.94
etsi-sol003-gen-1.13	1.13.19
mobility-common	2026.04.0
mobility-ha-subscriber	2026.04.0
mop-automation	2026.04.0
mop-common	2026.04.0
openstack-cos-gen-4.2	4.2.34
resource-manager	4.2.10

© 2026 Cisco and/or its affiliates. All rights reserved.

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



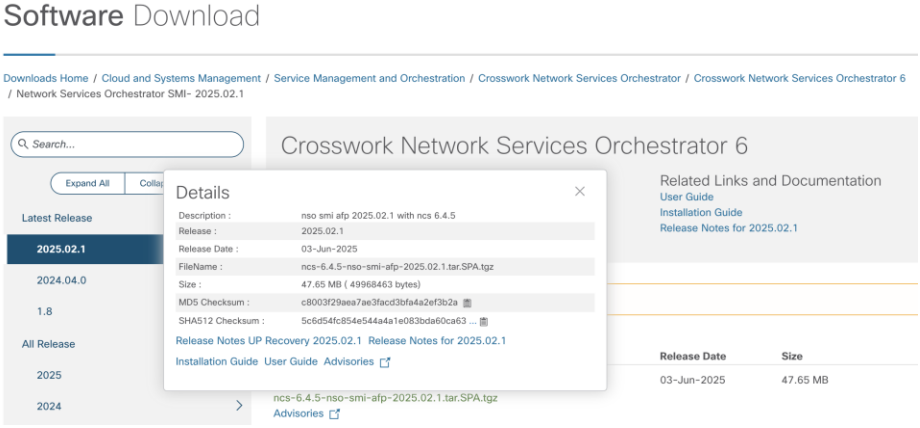
The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research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

© 2026 Cisco and/or its affiliates. All rights reserved.

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 9. 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 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 10. Related resources and additional information

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

© 2026 Cisco and/or its affiliates. All rights reserved.

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.