Cisco Nexus 9000 Series NX-OS Release Notes

Release 10.6(3s)F

Contents

Cisco Nexus 9000 Series NX-OS Release Notes, Release 10.6(3s)F 3
Software Features 4
Release Image 5
Open Issues 6
Resolved Issues 6
Known Issues 6
Optics 6
Upgrade and Downgrade 7
Related Content 7
Documentation Feedback 7
Legal Information 8

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

Cisco Nexus 9000 Series NX-OS Release Notes, Release 10.6(3s)F

This document describes the features, issues, and limitations of Cisco NX-OS software Release 10.6(3s)F for use on the Cisco Nexus 9000 Series switches.

Date	Description
October 26, 2026	Added CSCwx19159 to the Known Issues section.
August 23, 2026	Release 10.6(3s)F became available.

Cisco N9300 Series Smart Switches

The Cisco N9300 Series Smart Switches are integrated network devices designed for scalable, secure, and efficient data center operations. They combine advanced networking and security features with hardware acceleration and software flexibility, embedding stateful security powered by Cisco Hypershield directly into the network fabric.

Cisco N9300 Series Smart Switches utilize Cisco® Silicon One® E100 ASIC for high-performance switching and Data Processing Units (DPUs) for enhanced security and services. The family includes 100G and 25G switches with 800G DPU acceleration. Models such as the Cisco Nexus N9348Y2C6D-SE1U and N9324C-SE1U offer exceptional flexibility and performance, making them ideal Top of Rack (ToR) solutions for VXLAN-EVPN, BGP fabrics, and Multisite deployments. These switches can be deployed as leaf switches, border leaf, or border gateways, enabling customers to build adaptable and high-performing data center architectures.

The Cisco N9300 Series Smart Switches offer converged switching and routing services. The Cisco N9300 Series Smart Switches operate in network mode (NPU functions) and DPU security mode (DPU functions). Both the network and DPU security features are available in the DPU security mode.

For more information about product specifications, refer to the Cisco N9300 Series Smart Switch Data Sheet.

For more information about network mode feature set, refer to *Cisco Nexus 9000 Series NX-OS Release Notes, Release 10.6(2)F*, Cisco Nexus 9000 Series NX-OS Release Notes, Release 10.6(3)F, and 10.6(x) Documentation.

For more information about configuring the DPU security mode and troubleshooting, refer to the *Cisco Smart Switches Configuration Guide for DPU Security Mode* and *Cisco Smart Switches Troubleshooting Guide for DPU Security Mode*.

Cisco N9324C-SE1U switch

Beginning with Cisco NX-OS Release 10.6(2)F, the N9300 Series Smart Switches introduce the Cisco N9324C-SE1U switch, a 1-RU solution designed to deliver high-performance networking capabilities. Its features include:

- 24 x 100G ports
- Cisco Silicon One E100 ASIC offering high-speed connectivity and scalability
- 4 DPU offering software-defined stateful services

For hardware details, refer to the Cisco N9324C-SE1U NX-OS-Mode Switch Hardware Installation Guide.

Cisco N9348Y2C6D-SE1U switch

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

Beginning with Cisco NX-OS Release 10.6(2)F, the N9300 Series Smart Switches introduce the Cisco N9348Y2C6D-SE1U switch, a 1-RU solution designed to deliver high-performance. It features include:

- 48-port 25G + 2-port 100G + 6-port 400G switch
- Cisco Silicon One E100 ASIC offering high-speed connectivity and scalability
- 2 DPUs offering software-defined stateful services

For hardware details, refer to the Cisco N9348Y2C6D-SE1U NX-OS-Mode Switch Hardware Installation Guide.

Software Features

DPU security mode on Cisco N9300 Series Smart Switches is the main software feature in Cisco NX-OS Release 10.6(3s)F. Prior to this release, the N9300 Series Smart Switches operated only in the network mode.

The DPU security mode refers to the capability of the switch to provide distributed, stateful Layer-4 segmentation and DPU security enforcement directly within the switch using embedded Data Processing Units (DPUs).

Smart Switches integrate the Hypershield technology to enforce security policies at line rate, effectively embedding DPU security functions into the network infrastructure without requiring additional hardware.

From the licensing point of view, the DPU security mode requires the Premier license tier. For more information, refer to Cisco NX-OS Licensing Options Guide.

The below table contains the list of software features that are supported as part of the DPU security mode and the guides in which these features are documented.

Feature Type	Description
DPU security mode enablement	Allows you to power up the DPUs on the N9300 Smart Switches by enabling feature service acceleration. For more information, refer to *Cisco Smart Switches Configuration Guide for DPU Security Mode, Release 10.6(x).*
Network security operations	An exclusive admin role for the security mode on N9300 Smart Switches. For more information, refer to *Cisco Smart Switches Configuration Guide for DPU Security Mode, Release 10.6(x).*
VRF redirection and VLAN redirection	Supports VLAN-based bridged traffic redirection and VRF-based routed traffic redirection to the DPU providing Layer 3 and Layer 4 inspection. For more information, refer to: • *Cisco Smart Switches Configuration Guide for DPU Security Mode, Release 10.6(x)* • *Cisco Smart Switches Troubleshooting Guide for DPU Security Mode, Release 10.6(x)*

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

Feature Type	Description
Traffic inspection and integration with VXLAN	Integrates traffic inspection seamlessly with VXLAN overlays and traditional VLAN/VRF configurations, leveraging DPUs for hardware-accelerated security within the switch. For more information, refer to: • *Cisco Smart Switches Configuration Guide for DPU Security Mode, Release 10.6(x)* • *Cisco Smart Switches Troubleshooting Guide for DPU Security Mode, Release 10.6(x)*
Inter-VRF Traffic Inspection	Inspects traffic in the DPU between sources and destinations in different VRFs; supported by symmetric hashing mode only. For more information, refer to: • *Cisco Smart Switches Configuration Guide for DPU Security Mode, Release 10.6(x)* • *Cisco Smart Switches Troubleshooting Guide for DPU Security Mode, Release 10.6(x)*
High Availability	Ensures that the services remain available for both bridged and routed traffic during switch or DPU failure or outage. For more information, refer to: • *Cisco Smart Switches Configuration Guide for DPU Security Mode, Release 10.6(x)* • *Cisco Smart Switches Troubleshooting Guide for DPU Security Mode, Release 10.6(x)*
Layer 2 isolation for microsegmentation	Allows routing of the same-subnet IPv4 traffic through security inspection using receive-only VLAN mapping, Layer 2 isolation on a service VLAN, and enhanced local Proxy ARP. For more information, refer to *Cisco Smart Switches Configuration Guide for DPU Security Mode, Release 10.6(x).*
Packet tracer for the DPU interfaces	Provides visibility into forwarding path tracing between NPU and DPU.
Hypershield integration	Allows Hypershield to program security rules into DPU. For more information, refer to Cisco *Hypershield User Documentation.* and Cisco Hypershield Reference Documentation.
Support for Hypershield on-premise controller and Cisco Cloud Control	For more information, refer to Cisco Hypershield Release Notes and Cisco Hypershield User Documentation and Cisco Cloud Control documentation.
DPU Security Mode Scale updates	For more information, refer to Cisco Nexus 9000 Series NX-OS Verified Scalability Guide, Release 10.6(3s)F.

Release Image

In Cisco NX-OS Release 10.6(3s)F, the following 64-bit image is supported:

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

- The 64-bit Cisco NX-OS image filename with “nxos64-s1-dpu” as the prefix (for example, nxos64-s1-dpu.10.6.3s.F.bin) is supported and it is mandatory on Cisco N9300 Series Smart Switches. For more information, refer to Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide, Release 10.6(x).

Note:

- The 32-bit image is no longer supported.
- The EPLD image is bundled with all NX-OS images and so the image sizes are correspondingly larger.

Open Issues

There are no open issues in this release. For more information about open issues for Hypershield, refer to Cisco Hypershield Release Notes.

Resolved Issues

There are no resolved issues in this release.

Known Issues

This table lists the limitations for this release. Click the bug ID to access the Cisco Bug Search Tool and see additional information.

Bug ID	Headline
CSCwx19159	Changing timezone configurations or clock summer-time on the Smart Switch after the service-redirect configuration is in place removes traffic redirection to the DPU. Avoid changing clock timezone / clock summer-time after enabling service firewall.

Optics

For information about transceivers and cables supported on a switch, refer to the Transceiver Module (TMG) Compatibility Matrix. For the transceiver specifications and installation information, refer to the Install and Upgrade Guides.

For information about upgrading firmware on ZR optics, refer to the Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 10.6(x).

Refer to Transceiver Firmware for more information about:

- firmware upgrades for all Command Data Block (CDB) supported transceivers or optical transceivers across multiple hardware platforms.
- upgrading transceiver firmware faster by processing multiple downloads simultaneously.

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

Upgrade and Downgrade

To perform a software upgrade or downgrade, follow the instructions in the Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide, Release 10.6(x).

Note: Only Disruptive Upgrade is supported. Refer to the disruptive upgrade option in the Cisco Nexus 9000 and 3000 Upgrade and ISSU Matrix.

Related Content

Document Title	Description
Cisco Nexus 9000 Series Switches	Cisco Nexus 9000 Series Switches documentation
Cisco NX-OS Software Strategy and Lifecycle Guide	Cisco NX-OS Software Release and Image-naming Convention
Cisco Nexus 3000 and 9000 Series NX-API REST SDK User Guide and API Reference	Cisco Nexus 3000 and 9000 Series NX-API REST SDK User Guide and API Reference
Cisco N9300 Series Smart Switch Data Sheet	Data sheet for Cisco N9300 Series Smart Switch
Licensing documentation: • Cisco NX-OS Licensing Options Guide • Cisco NX-OS Licensing • Cisco Nexus Smart Licensing Using Policy User Guide	Information about Smart Licensing Using Policy: • Licenses • Collection page on Cisco NX-OS Licensing to help you learn, deploy, and *troubleshoot* Smart Licensing Using Policy (SLP) • Smart Licensing Using Policy (SLP) User Guide for N9000 and 3000 Series Switches
Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide	Software upgrade and downgrade information for Cisco N9000 Series switches, Release 10.6(x)
Cisco Nexus 9000 and 3000 Upgrade and ISSU Matrix	Upgrade matrix for both disruptive and non-disruptive upgrades for N9000 and 3000 Series Switches
Nexus 9000 MIBs Supported upto Cisco NX-OS 10.6(3)F	Cisco NX-OS Supported MIBs
Cisco N9324C-SE1U NX-OS-Mode Switch Hardware Installation Guide	Hardware installation information for Cisco N9324C-SE1U NX-OS-Mode Switch
Cisco Nexus N9348Y2C6D-SE1U NX-OS-Mode Switch Hardware Installation Guide	Hardware installation information for Cisco N9348Y2C6D-SE1U NX-OS-Mode Switch
Cisco Nexus 9000 Series NX-OS Verified Scalability Guide, Release 10.6(3)F	Verified scalability information on Cisco N9000 Series switches for Release 10.6(3)F
Cisco Nexus 9000 Series FPGA/EPLD Upgrade Release Notes, Release 10.6(3s)F	Cisco Nexus 9000 Series FPGA/EPLD Upgrade Release Notes for Release 10.6(3s)F

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus9k-docfeedback@cisco.com. We appreciate your feedback.

© 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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

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.

© 2026 Cisco Systems, Inc. All rights reserved.