



Cisco Nexus 3600 NX-OS Release Notes, Release 7.0(3)F3(5)

This document describes the features, caveats, and limitations for Cisco NX-OS Release 7.0(3)F3(5) software for use on Cisco Nexus C3636C-R and C36180YC-R switches. Use this document in combination with documents listed in [Related Documentation](#).

Note: Cisco NX-OS Release 7.0(3)F3(5) for use on the Cisco Nexus C3636C-R and C36180YC-R switches.

[Table 1](#) shows the online change history for this document.

Table 1. Online History Change

Date	Description
March 5, 2019	Created the release notes for Release 7.0(3)F3(5).

Contents

Introduction	3
Licensing Information	3
System Requirements	3
New and Changed Information	4
Resolved Caveats—Cisco NX-OS Release 7.0(3)F3(5)	4
Open Caveats—Cisco NX-OS Release 7.0(3)F3(5)	4
Limitations	5
Related Documentation	6
Obtaining Documentation and Submitting a Service Request	6

Introduction

Cisco NX-OS software is a data center-class operating system designed for performance, resiliency, scalability, manageability, and programmability at its foundation. The Cisco NX-OS software provides a robust and comprehensive feature set that meets the requirements of virtualization and automation in mission-critical data center environments. The modular design of the Cisco NX-OS operating system makes zero-impact operations a reality and enables exceptional operational flexibility.

The Cisco NX-OS 7.0(3)F3(5) image is specifically designed to support and bring up the N3K-**C3636C-R** and N3K-C36180YC-R switches of the Cisco Nexus 3600 platform switches.

Licensing Information

Temporary licenses with an expiry date are available for evaluation and lab use purposes. They are strictly not allowed to be used in production. Please use a permanent or subscription license that has been purchased through Cisco for production purposes.

For more information, see the [Cisco NX-OS Licensing Guide](#).

System Requirements

This section includes the following sections:

- Supported Device Hardware
- Supported Optics

Supported Device Hardware

[Table 2](#) lists the Cisco Nexus 3600 switch hardware that Cisco NX-OS Release 7.0(3)F3(5) supports. For additional information about the supported hardware, see the [Cisco Nexus 3600 NX-OS Mode Switch Hardware Installation Guide](#).

Table 2. Cisco Nexus 3600 Switch Hardware

Product ID	Hardware
N3K-C3636C-R	The Cisco Nexus 3636C-R (N3K-C3636C-R) is a 1 rack unit (RU) switch with 36 100-Gigabit QSFP28 ports, 2 management ports, 1 console port, and 1 USB port. The switch supports both port-side exhaust and port-side intake airflow schemes. The switch has two power supplies, one for operations and the other for redundancy. Both power supplies must be either AC power supplies or DC power supplies.
N3K-C36180YC-R	The Cisco Nexus 36180YC-R (N3K-C36180YC-R) is a 1 rack unit (RU) switch with 48 1/10/25-Gigabit SFP ports and 6 40-Gigabit QSFP/100-Gigabit QSFP28 ports, 1 management port, 1 console port, and 1 USB port. The switch supports both port-side exhaust and port-side intake airflow schemes. The switch has two power supplies, one for operations and the other for redundancy. Both power supplies must be either AC power supplies or DC power supplies.

Supported Optics

See the [Cisco Transceiver Modules Compatibility Information](#) for a list of supported optical components.

New and Changed Information

This section lists the following topic:

- New Software Features in Cisco NX-OS Release 7.0(3)F3(5)

New Hardware Features in Cisco NX-OS Release 7.0(3)F3(5)

Cisco NX-OS Release 7.0(3)F3(5) has no hardware features.

New Software Features in Cisco NX-OS Release 7.0(3)F3(5)

Cisco NX-OS Release 7.0(3)F3(5) has no software features.

Resolved Caveats—Cisco NX-OS Release 7.0(3)F3(5)

The following table lists the resolved bugs in Cisco NX-OS Release 7.0(3)F3(5). You can use the bug ID to access the [Cisco Bug Search Tool](#) and see additional information about the bug.

Bug ID	Description
CSCve51704	Cisco NX-OS Software CLI Arbitrary Command Execution Vulnerability
CSCvg04127	Cisco NX-OS System Software Interactive TCL Shell Escape Vulnerability
CSCvg34748	N9K USB not detected after OIR
CSCvh10089	copy running-config to startup-config failed due to Service "policyelem"
CSCvh24763	Vulnerable version of libxml2 present in line cards
CSCvh58592	No Syslog message for Login On-Success Event
CSCvj14692	Redirected IP packet not forwarded to destination
CSCvj23487	Account for cable type to choose FEC mode for 25G ports
CSCvj67977	Cisco NX-OS Authenticated SNMP Denial of Service Vulnerability
CSCvj70029	Cisco NXOS Software Authenticated Simple Network Management Protocol Denial of Service Vulnerability
CSCvk30831	BIOS upgrade may fail during install all
CSCvm45182	Nexus 9500-R, Nexus 3000-R // 7.0(3)F3(3) // slot 1 quoted "show hardware internal.." crashes box

Open Caveats—Cisco NX-OS Release 7.0(3)F3(5)

The following table lists the open caveats in Cisco NX-OS Release 7.0(3)F3(5). Click the bug ID to access the [Cisco Bug Search Tool](#) and see additional information about the bug.

Bug ID	Description
CSCvc04860	On SVI interfaces, post routed packets may be dropped momentarily (till MAC is learnt)
CSCvc27054	Queue-limit Sum more than 100%

Limitations

Bug ID	Description
CSCvd47812	breakout priority drops when 3 streams comes from same soc under oversubscription
CSCve80686	N3K-C36180YC-R can't mix 1/10G and 25G in the same port group.
CSCvf24078	Mcast RPF Nbr IP showing local switch intf IP when /16 bit mask used on PIM intfs
CSCvf29905	N9K-X9636C-RX:: L2 SSM look up failure affecting IGMPv3 functionality
CSCvf49975	port range not working properly
CSCvf58154	L2GW : Outer IP TOS value to set as 0x00
CSCvf75978	Storm control counters not incrementing
CSCvf90062	packet is flooded to the port which has no receiver
CSCvg19938	Unshut of One of the ECMP links causes 1 minute + traffic drop due to high CPU for u6rib
CSCvg21203	1G copper GLC-TE XCVR LED state is GREEN when link is not connected
CSCvg30015	vpc secondary comes back up as oper primary after reload
CSCvg46829	QoS with " match protocol apr" on L3/SVI returning 'Failed to add acl in hardware'
CSCvg94936	Level 2 priority is not honored, which policy applied on per port level
CSCvh02489	N3K-C36180YC-R 1G port, priority traffic is not honored
CSCvh15029	"VLAN dot1q tag native" config/unconfig takes effect only after trunk port flap
CSCvh67600	Console hung after executing default interface command
CSCvh70200	7.0(3)F - snmp-server host informs config corruption - also DME conflict
CSCvh81352	fragments permit-all and deny-all
CSCvh83010	Ports for module N9K-X9636C-RX in error disable state after upgrade from MR2 to MR3 image
CSCvh85972	Traffic drop for low priority unicast traffic on the egress port
CSCvh96055	Multicast traffic in L2 range 0100.5e00.xxxx - 0100.5e7f.xxxx not denied by access-list
CSCvi06058	sflow sample packets not taking correct copp class
CSCvi12965	L3 routed port rewriting dst macs to 0000.0000.0000
CSCvi36673	Intermediate link failure on some ports of N3K-C36180YC-R/N3K-C3636C-R/N9K-X96160YC-R

Limitations

This section lists limitations related to Cisco NX-OS Release 7.0(3)F3(5).

- The PTP process restart and system switchover accumulates high corrections for a few seconds. For more information, see [CSCvg49023](#).
- The LDP neighbor might flap on switchover in a scaled setup with many interfaces. Increase the discovery hello hold time for MPLS under the MPLS LDP configuration. For more information, see [CSCvg71349](#).
- CoPP (Control Plane Policing) cannot be disabled. If you attempt to disable it, an error message appears. For more information, see [CSCvi09329](#).
- The skip CoPP policy option has been removed from the Cisco NX-OS initial setup utility because using it can impact the control plane of the network. For more information, see [CSCvc44819](#).
- IPv4 traffic might drop when only IPv6 uRPF is enabled on the interface. For more information, see [CSCvh99632](#).

Related Documentation

The entire Cisco Nexus 3600 NX-OS documentation set is available at the following URL:

<https://www.cisco.com/c/en/us/support/switches/nexus-3000-series-switches/tsd-products-support-series-home.html>

The *Cisco Nexus 3600 NX-OS Hardware Installation Guide* is available at the following URL:

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3600/hw/installation/guide/b_n3600_hardware_install_guide.html

The *Cisco Nexus 3600 NX-OS Verified Scalability Guide, Release 7.0(3)F3(5)* is available at the following URL:

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3600/sw/7x/scalability/guide/b_Cisco_Nexus_3600_NX-OS_Verified_Scalability_Guide_703F31.html

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus3k-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Open a service request online at:

<https://tools.cisco.com/ServiceRequestTool/create/launch.do>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

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)

Cisco Nexus 3600 Series NX-OS Release Notes, Release 7.0(3)F3(5)

© 2019 Cisco Systems, Inc. All rights reserved.