Release Notes for Catalyst 3560-CX and 2960-CX Series Switches, Cisco IOS Release 15.2(7)Ex

First Published: March 27, 2019
Last Updated: September 26, 2024

This release note describes the features and caveats for the Cisco IOS Release 15.2(7)Ex software on the Catalyst 3560-CX and the Catalyst 2960-CX family of switches.

Verify that these release notes are correct for your switch:

- If you are installing a new switch, see the Cisco IOS release label on the rear panel of the switch.
- If your switch is on, use the **show version** privileged EXEC command. See the "Upgrading the Switch Software" section on page 4.
- If you are upgrading to a new release, see the software upgrade filename for the software version. See the "Software Image" section on page 5.

You can download the switch software from this site (registered Cisco.com users with a login password):

https://software.cisco.com/download/navigator.html

Contents

Cisco Systems, Inc.
www.cisco.com

- Related Documentation, page 13

Introduction

The Catalyst 3560-CX and Catalyst 2960-CX switches are compact Gigabit Ethernet (GE) switches that have features comparable to high-end Cisco switches but in smaller form factors. Some of the key features are:

- Up to 10 Gigabit uplinks for high-bandwidth applications and business growth
- Cisco Catalyst Instant Access mode (on 3560cx-12PD-S and 3560CX-8XPD-S switches) for management simplicity on switches with 10G uplink. See Instant Access FAQ here.
- Support for Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) for software-defined networking (SDN) and programmability
- Integration with Cisco TrustSec® for identity, segmentation, and security
- Up to 240W of available power for PoE+ per switch — twice the available power of previous generation switches — for supporting more PoE devices
- Switch Hibernation Mode and Energy Efficient Ethernet (EEE) for lower energy costs
- NetFlow Lite for end-to-end visibility to the flows in the network

Supported Hardware

Switch Models

Table 1 Catalyst 3560-CX Switch Models

Switch Model	Cisco IOS Image	Description
WS-C3560CX-8TC-S	IP Base IP Services	Non-PoE, 8 downlink ports, 8 access ports of 1G access ports, 2 SFP uplink ports of 1G, 2 uplink Cu ports of 1G[1]
WS-C3560CX-8PC-S	IP Base IP Services	240W PoE+, 8 downlink ports, 8 access ports of 1G access ports, 2 SFP uplink ports of 1G, 2 uplink Cu ports of 1G
WS-C3560CX-12TC-S	IP Base IP Services	Non-PoE, 12 downlink ports, 12 access ports of 1G, 2 SFP uplink ports of 1G, 2 uplink Cu ports of 1G
WS-C3560CX-12PC-S	IP Base IP Services	240W PoE+, 12 downlink ports, 12 access ports of 1G, 2 SFP uplink ports of 1G, 2 uplink Cu ports of 1G
WS-C3560CX-12PD-S	IP Base IP Services	240W PoE+, 12 downlink ports, 12 access ports of 1G, 2 SFP+ uplink ports of 10G, 2 uplink Cu ports of 1G

Table 1 Catalyst 3560-CX Switch Models (continued)

Switch Model	Cisco IOS Image	Description
WS-C3560CX-8PT-S	IP Base IP Services	146W PoE+, 8 downlink ports, 8 access ports of 1G, 2 uplink UPoE+ ports of 1G
WS-C3560CX-8XPD-S	IP Base IP Services	240W PoE+, 8 downlink ports, 6 access ports of 1G, 2 access ports of 100M/1G/2.5G/5G/10G, 2 SFP+ uplink ports of 10G

1. For all switch models, the SFP ports and Cu ports are usable concurrently.

Table 2 Catalyst 2960-CX Switch Models

Switch Model	Cisco IOS Image	Description
WS-C2960CX-8TC-L	LAN Base	Non-PoE, 8 downlink ports, 8 access ports of 1G, 2 SFP uplink ports of 1G, 2 uplink Cu ports of 1G[1]
WS-C2960CX-8PC-L	LAN Base	124W PoE+, 8 downlink ports, 8 access ports of 1G, 2 SFP uplink ports of 1G, 2 uplink Cu ports of 1G

1. For all switch models, the SFP ports and Cu ports are usable concurrently.

Optics Modules

The Catalyst 3560-CX and 2960-CX switches support a wide range of optics. Because the list of supported optics is updated on a regular basis, consult the tables at this URL for the latest SFP+ and SFP module compatibility information:

http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

Device Manager System Requirements

Hardware Requirements

Table 3 Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[1]	512 MB[2]	256	1024 x 768	Small

1. We recommend 1 GHz.
2. We recommend 1 GB DRAM.

Software Requirements

- Windows 2000, XP, Vista, Windows 7, and Windows Server 2003.
- Internet Explorer 6.0, 7.0, Firefox up to version 26.0 with JavaScript enabled.

Cisco Network Assistant Compatibility

For Cisco IOS Release 15.2(4)E, Cisco Network Assistant support is available on release Version 5.8.9 and later.

You can download Cisco Network Assistant from this URL:
http://www.cisco.com/pcgi-bin/tablebuild.pl/NetworkAssistant

For more information about Cisco Network Assistant, see the *Release Notes for Cisco Network Assistant* on Cisco.com.

Upgrading the Switch Software

Finding the Software Version and Feature Set

The Cisco IOS image is stored as a bin file in a directory that is named with the Cisco IOS release number. The files necessary for web management are contained in a subdirectory. The image is stored on the system board flash device (flash:).

You can use the **show version** privileged EXEC command to see the software version that is running on your switch.

Note Although the **show version** output always shows the software image running on the switch, the model name shown at the end of this display is the factory configuration and does not change if you upgrade the software license.

You can also use the **dir** *filesystem***:** privileged EXEC command to see the directory names of other software images that you might have stored in flash memory.

Viewing the Software Image Upgrade History

Starting Release 15.2(7)E3, you can view the history of software image upgrades performed on the Cisco Catalyst 3560-CX devices, using the **show archive sw-upgrade history** command. This command displays the image name, version, upgrade method and timeline for each upgrade that is done through Auto Install, PnP, archive CLI, or HTTP methods.

Manual upgrades done through TFTP of tar files or binary files are not displayed.

If you have booted the Cisco IOS software, wait for ten minutes before using this command. This is because the software takes time to initialize after a boot.

Note that the **show archive sw-upgrade history** command displays the records of only the first 100 successful upgrades or downgrades (performed through Auto Install, PnP, archive CLI, or HTTP methods).

Software Image

If you have a service support contract and order a software license or if you order a switch, you receive the universal software image and a specific software license.

Table 4 Software Image for Cisco Catalyst 3560-CX

Image	Filename	Description
Universal image	c3560cx-universalk9-mz.152-7.E.bin	IP Base and IP Services images.
Universal image	c3560cx-universalk9-tar.152-7.E.tar	IP Base and IP Services cryptographic images with Device Manager.

Table 5 Software Image for Cisco Catalyst 2960-CX

Image	Filename	Description
Universal image	c2960cx-universalk9-mz.152-7.E.bin	LAN Base image.
Universal image	c2960cx-universalk9-tar.152-7.E.tar	LAN Base cryptographic image with Device Manager.

Web UI

If the Web UI does not load or work properly after the software upgrade, perform the following steps:

Step 1 Specify the authentication method for HTTP server users as local.

Device(config)# **ip http authentication local**

Step 2 Configure the username and password with privilege 15.

Device(config)# **username** *user* **privilege 15 password** *password*

Step 3 Clear the browser cache and relaunch the Web UI.

Step 4 Login by entering the privilege 15 username and password.

Features of the Switch

Cisco Catalyst 3560-CX switches features:

- In Cisco IOS Release 15.2(7)E3 and later releases, SSH is enabled by default to connect to networks, and Telnet is disabled by default.
- PoE+ and non-PoE, 8 and 12 downlink ports, 1G SFP and 10G SFP+ uplink port models
- IPv4 and IPv6 routing, Multicast routing, advanced quality of service (QoS), and security features in hardware
- Cisco Catalyst Instant Access mode (on WS-C3560CX-12PD-S and WS-C3560CX-8XPD-S switches) for management simplicity on switches with 10G uplink
- Up to 240W of available power for PoE+ per switch
- Switch Hibernation Mode and Energy Efficient Ethernet (EEE) for lower energy costs
- Horizontal Stacking (on WS-C3560CX-12PD-S and WS-C3560CX-8XPD-S switches

- Enhanced Limited Lifetime Warranty (E-LLW) with next business day (NBD) advance hardware replacement and 90 day access to Cisco Technical Assistance Center (TAC) support
- Enhanced Cisco EnergyWise for operational cost optimization by measuring actual power consumption of the PoE devices, reporting, and reducing energy consumption across the network
- USB Type-A and Type-B ports for storage and console respectively
- Application visibility and capacity planning with integrated NetFlow Lite
- Hardware support for Secure Group Access Control lists (SGACL) and IEEE 802.1AE MACsec.
- Software support for IEEE 802.1AE MACsec from Cisco IOS Release 15.2(4)E.

Cisco Catalyst 2960-CX switches features:

- In Cisco IOS Release 15.2(7)E3 and later releases, SSH is enabled by default to connect to networks, and Telnet is disabled by default.
- PoE+ and non-PoE models, 8 downlink ports, 1G SFP uplink port models
- Reduced power consumption and advanced energy management features
- USB Type-A and Type-B ports for storage and console respectively
- Application visibility and capacity planning with integrated NetFlow Lite
- Switch Hibernation Mode and Energy Efficient Ethernet (EEE) for lower energy costs
- Enhanced Limited Lifetime Warranty (E-LLW) with next business day (NBD) advance hardware replacement and 90 day access to Cisco Technical Assistance Center (TAC) support
- Enhanced Cisco EnergyWise for operational cost optimization by measuring actual power consumption of the PoE devices, reporting, and reducing energy consumption across the network

New Software Features

Features Introduced in Cisco IOS Release 15.2(7)E11

None

Features Introduced in Cisco IOS Release 15.2(7)E10

None

Features Introduced in Cisco IOS Release 15.2(7)E9

None

Features Introduced in Cisco IOS Release 15.2(7)E8

None

Features Introduced in Cisco IOS Release 15.2(7)E7

Data Sanitization: Supports the use of the National Institute of Standards and Technology (NIST) purge method that renders data unrecoverable through simple, non-invasive data recovery techniques or through state-of-the-art laboratory techniques.

For more information, see the Data Sanitization chapter of the System Management Configuration Guide.

Features Introduced in Cisco IOS Release 15.2(7)E6

None

Features Introduced in Cisco IOS Release 15.2(7)E5

None.

Features Introduced in Cisco IOS Release 15.2(7)E4

None.

Features Introduced in Cisco IOS Release 15.2(7)E3

- Support for enabling the secret masking functionality using the **username masked-secret** command.
- Support for viewing the history of software image upgrades using the **show archive sw-upgrade history** command.

Features Introduced in Cisco IOS Release 15.2(7)E2

None.

Features Introduced in Cisco IOS Release 15.2(7)E1a

None.

Features Introduced in Cisco IOS Release 15.2(7)E1

None.

Features Introduced in Cisco IOS Release 15.2(7)E0a

SFTP: The device supports SSH File Transfer Protocol (SFTP). The SFTP client functionality is provided as part of the SSH component and is always enabled on the corresponding device. Therefore, any SFTP server user with the appropriate permission can copy files to and from the device.

Service and Support

Information About Caveats

If you need information about a specific caveat that does not appear in these release notes, you can use the Cisco Bug Toolkit to find caveats of any severity. Click this URL to browse to the Bug Toolkit:

http://tools.cisco.com/Support/BugToolKit/

If you request a defect that cannot be displayed, the defect number might not exist, the defect might not yet have a customer-visible description, or the defect might be marked Cisco Confidential.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at this URL:

http://www.cisco.com/en/US/support/index.html

Click **Product Support** > **Switches**. Choose your product and click **Troubleshooting** to find information on the problem you are experiencing.

Limitations and Restrictions

No known limitations or restrictions.

Caveats

Cisco Bug Search Tool

The Bug Search Tool (BST), which is the online successor to Bug Toolkit, is designed to improve the effectiveness in network risk management and device troubleshooting. The BST allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of a caveat listed in this document:

1. Access the BST (use your Cisco user ID and password) at https://tools.cisco.com/bugsearch/.
2. Enter the bug ID in the **Search For:** field.

Open Caveats

Caveats Resolved in Cisco IOS Release 15.2(7)Ex

None.

Resolved Caveats

Caveats Resolved in Cisco IOS Release 15.2(7)E11

Table 6 Caveats Resolved in Cisco IOS Release 15.2(7)E11

Bug ID	Headline
CSCvv54811	17.4:ASR1K:RP crashed while runnint ISAKMP codenomicon suite
CSCwh66334	Cisco IOS and IOS XE Software IKEv1 Fragmentation Denial of Service Vulnerabilities

Table 6 Caveats Resolved in Cisco IOS Release 15.2(7)E11

Bug ID	Headline
CSCwi59625	Cisco IOS and IOS XE Software Web UI Cross-Site Request Forgery Vulnerability
CSCwj05481	Cisco IOS and IOS XE Software Resource Reservation Protocol Denial of Service Vulnerability

Caveats Resolved in Cisco IOS Release 15.2(7)E10

None.

Caveats Resolved in Cisco IOS Release 15.2(7)E9

Table 7 Caveats Resolved in Cisco IOS Release 15.2(7)E9

Bug ID	Headline
CSCwe53798	PnP for 2960cx fails with error "PKI signing failed”.
CSCwe81286	AAA not including cts-pac-opaque in RADIUS requests when reloading and using Dynamic IP.
CSCwf06443	AAA configuration non persisting across reloads for VTY line 0-4 on IOS platform.

Caveats Resolved in Cisco IOS Release 15.2(7)E8

None.

Caveats Resolved in Cisco IOS Release 15.2(7)E7

Table 8 Caveats Resolved in Cisco IOS Release 15.2(7)E7

Bug ID	Headline
CSCvw60355	DHCPv6: Memory allocation of DHCPv6 relay option results in crash.
CSCvx63027	Cisco IOS and IOS XE Software SSH Denial of Service Vulnerability.
CSCwa96810	Cisco IOS and IOS XE Software Common Industrial Protocol Request Denial of Service Vulnerability.

Caveats Resolved in Cisco IOS Release 15.2(7)E5

Table 9 Caveats Resolved in Cisco IOS Release 15.2(7)E5

Bug ID	Headline
CSCvx76066	Switch crashes due to "HTTP Core".
CSCvx90769	C2960cx-8PC-L || 15.2.7 E3 || Switch Crash after adding multi-domain host mode in interface level.
CSCvy40917	Username <username> privilege command is not accepted without specifying a password.
CSCvz13185	CISCO-INNOLIGHT vendor SFP-10G-ER-S is not showing DOM data on WS-C3560CX-12PD-S.
CSCvx66699	Cisco IOS and IOS XE Software TrustSec CLI Parser Denial of Service Vulnerability.

Caveats Resolved in Cisco IOS Release 15.2(7)E4

Table 10 Caveats Resolved in Cisco IOS Release 15.2(7)E4

Bug ID	Headline
CSCvv86851	TACACS not working if TACACS group server has "server-private <ip> key <passw>" in 15.2(7)E3/3.11.3E.
CSCvv93417	Stack Member Switch fails wired dot1x; MasterSwitch passes dot1x using the same configs

Caveats Resolved in Cisco IOS Release 15.2(7)E3

Table 11 Caveats Resolved in Cisco IOS Release 15.2(7)E3

Bug ID	Headline
CSCvt95011	Connection to MGIG port causing loop in the interface itself.
CSCvg86228	File "day0.cfg" generated on C2960CX when upgraded
CSCvu10399	Cisco IOS and IOS XE Software Information Disclosure Vulnerability.
CSCvv00134	VTY telnet disable, enable ssh based on platform request.

Caveats Resolved in Cisco IOS Release 15.2(7)E2

Table 12 Caveats Resolved in Cisco IOS Release 15.2(7)E2

Bug ID	Headline
CSCvt19077	AAA configurations are missing after reload.
CSCvq91578	IPDT doesn't trigger the inactivity timer.
CSCvs58516	LWAPP header corrupted by 3560cx.

Caveats Resolved in Cisco IOS Release 15.2(7)E1a

Table 13 Caveats Resolved in Cisco IOS Release 15.2(7)E1a

Bug ID	Headline
CSCvi48253	Self-signed certificates expire on 00:00 1 Jan 2020 UTC, can't be created after that time.

Caveats Resolved in Cisco IOS Release 15.2(7)E1

Table 14 Resolved Caveats in Cisco IOS Release 15.2(7)E1

Bug ID	Headline
CSCvq16632	command that activate right-to-use license was different after upgrade to 15.2(6)E.
CSCvr57005	2960XR Flow-based SPAN(FSPAN) not work when mutilple session configured.

Caveats Resolved in Cisco IOS Release 15.2(7)E0a

Table 15 Resolved Caveats in Cisco IOS Release 15.2(7)E0a

Bug ID	Headline
CSCvh80999	IP Phone not placed in critical voice VLAN when AAA server is not reachable.
CSCvn65197	Switch crashes after applying Auto SmartPort Macro configuration on the device.
CSCvn73382	2960-plus QoS \"police rate-bps burst-byte exceed-action drop\" police Not worked expected.

Related Documentation

- Catalyst 3560-CX and Catalyst 2960-CX switch documentation at these URLs:

  http://www.cisco.com/c/en/us/support/switches/catalyst-2960-cx-series-switches/tsd-products-support-series-home.html

  http://www.cisco.com/c/en/us/support/switches/catalyst-3560-cx-series-switches/tsd-products-support-series-home.html
- Cisco SFP and SFP+ modules documentation, including compatibility matrices at this URL:

  http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html
- Cisco Validated Designs documents at this URL:

  http://www.cisco.com/go/designzone

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.