Release Notes for Cisco Digital Building 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 Cisco Digital Building series 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 3.
- If you are upgrading to a new release, see the software upgrade filename for the software version. See the "Software Image" section on page 3.

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

http://www.cisco.com/download/navigator.html

Contents

Cisco Systems, Inc.
www.cisco.com

- Related Documentation, page 13

Introduction

The Cisco Digital Building series switches are Fast Ethernet switches to which you can directly connect various PoE endpoints (such as lighting endpoints).

Lighting endpoints can be controlled through the switch using a Web UI, a mobile app on your smartphone, or standard network PnP (plug-and-play) cable connected to the switch. You can also connect other devices such as Cisco IP Phones, Cisco Wireless Access Points, workstations, and other network devices such as servers, routers, and other switches.

Supported Hardware

Switch Models

Table 1 Cisco Digital Building Switch Models

Switch Model	Cisco IOS Image	Description
CDB-8U	LAN Lite	Switch with 8 10/100 Fast Ethernet Cisco UPOE ports and 2 Gigabit Ethernet uplink ports
CDB-8P	LAN Lite	Switch with 8 10/100 Fast Ethernet Cisco PoE+ ports and 2 Gigabit Ethernet uplink ports

Device Manager System Requirements

The following table lists the system requirements for a PC running Cisco Configuration Professional for Catalyst, including Web browser versions.

Table 2 System Requirements

System Component	Requirement
Operating System	Any of the following: • Mac OS 10.9.5 • Microsoft Windows Version 7
Browser	Cisco CPC can be used with the following browsers: • Google Chrome 52 and later • Mozilla Firefox 48 and later • Apple Safari 9 and later • Internet Explorer 11 and later
Screen Resolution	1280 X 800 pixels or higher

Table 2 System Requirements

System Component	Requirement
Cisco Management Tools	• Identity Services Engine (ISE) 2.1 • Cisco Prime 3.1 DP11 (to be released)
Mobile App	Supported OS for Cisco Digital Building app: • Android 4.4.2 and higher • iOS 9 and higher

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.

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.

Software Image

For information on installing or upgrading the switch's software image, refer to the *Working with the Cisco IOS File System, Configuration Files, and Software Images* section in the *Software Configuration Guide, Cisco IOS Release 15.2(7)E (Catalyst Digital Building Series Switches)*.

The software image can also be upgraded over bluetooth using the Cisco Digital Building smartphone app.

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

The Cisco Digital Building switch supports the LAN Lite feature set. This provides standard Layer 2 security, quality of service (QoS) features, and other features that are unique to Cisco Digital Building. The switch models have reduced functionality and scalability with entry level features in Layer 2, and provide no routing capability. They do not support stacking.

The feature sets are described in the following sections.

- Digital Building, page 4
- Ease of Operations, page 4
- Network Security, page 5
- Deployment and Control Features, page 6
- Quality of Service, page 7

Digital Building

- PoE+ or Cisco UPOE available on all 8 Fast Ethernet downlink ports. Each switch also contains 2 Gigabit Ethernet copper uplink ports.
- Depending on the switch model, a total of either 240 W or 480 W power is available for endpoints.
- Automatic device classification for various endpoints such as lights, IP phones, wireless access points, and cameras.
- Deep Sleep, where the switch goes into a low standby power mode and draws only 0.5 W per port, thus enhancing power efficiency.
- Constrained Application Protocol (CoAP) support, for use with constrained devices to enable Internet of Things (IoT).
- Perpetual UPOE, a first in the industry, that ensures uninterrupted power for endpoints during switch upgrade, reboot, and configuration changes.
- Smartphone-based management of the switch over bluetooth via mobile app.
- Plenum certification, that enhances safety by restricting the burning of cables when exposed to heat or fire.

Ease of Operations

- Cisco Catalyst Smart Operations is a comprehensive set of features that simplify LAN deployment, configuration, and troubleshooting. Catalyst Smart Operations enable zero touch installation and replacement of switches and fast upgrade, as well as ease of troubleshooting with reduced operational cost. Catalyst Smart Operations is a set of features that includes Smart Install, Auto Smartports, Smart Configuration, and Smart Troubleshooting to enhance operational excellence:
  - Cisco Smart Install is a transparent plug-and-play technology that can configure the Cisco IOS software image and switch configuration without user intervention. Smart Install uses dynamic IP address allocation and the assistance of other switches to facilitate installation.

  - Cisco Auto Smartports provide automatic configuration as devices connect to the switch port, allowing auto detection and plug and play of the device onto the network.
  - Cisco Smart Configuration provides a single point of management for a group of switches and in addition adds the ability to archive and back up configuration files to a file server or switch allowing seamless zero touch switch replacement.
  - Cisco Smart Troubleshooting is an extensive array of debug diagnostic commands and system health checks within the switch, including Generic Online Diagnostics (GOLD) and Onboard Failure Logging (OBFL).
  - Auto Configuration determines the level of network access provided to an endpoint based on the type of the endpoint device.
- Cisco Prime Infrastructure is a set of tools that enables you to automate much of the management of your Cisco network.
- Interface templates provide a mechanism to configure multiple commands at the same time and associate it with a target (such as an interface). An interface template is a container of configurations or policies that can be applied to specific ports.

Network Security

The Cisco Digital Building series switches provide a range of security features to limit access to the network and mitigate threats.

- Port security secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding.
- DHCP snooping to filter untrusted DHCP messages between untrusted hosts and DHCP servers.
- Dynamic ARP inspection (DAI) to prevent malicious attacks on the switch by not relaying invalid ARP requests and responses to other ports in the same VLAN.
- Flexible authentication via 802.1x and MAC Authentication Bypass using a single, consistent configuration.
- Open mode that creates a user friendly environment for 802.1X operations.
- Comprehensive RADIUS Change of Authorization capability for asynchronous policy management.
- ACLs define security policies on interfaces for control-plane and data-plane traffic. IPv6 ACLs can be applied to filter IPv6 traffic. Port-based ACLs for Layer 2 interfaces allow security policies to be applied on individual switch ports.
- Secure Shell (SSH) Protocol and Simple Network Management Protocol Version 3.
- (SNMPv3) provide network security by encrypting administrator traffic during Telnet and SNMP sessions. SSH Protocol, Kerberos, and the cryptographic version of SNMPv3 require a special cryptographic software image because of U.S. export restrictions.
- Bidirectional data support on the Switched Port Analyzer (SPAN) port allows Cisco Intrusion Detection.
- TACACS+ and RADIUS authentication facilitates centralized control of the switch and restricts unauthorized users from altering the configuration.
- MAC address notification allows administrators to be notified of users added to or removed from the network.
- Multilevel security on console access prevents unauthorized users from altering the switch configuration.

- Bridge protocol data unit (BPDU) Guard shuts down Spanning Tree PortFast-enabled interfaces when BPDUs are received to avoid accidental topology loops.
- IGMP filtering provides multicast authentication by filtering out non-subscribers and limits the number of concurrent multicast streams available per port.
- 802.1x monitor mode allows companies to enable authentication across the wired infrastructure in an audit mode without affecting wired users or devices. It helps IT administrators smoothly manage 802.1x transitions by allowing access and logging system messages when a device requires reconfiguration or is missing an 802.1x supplicant.

Deployment and Control Features

- Dynamic Host Configuration Protocol (DHCP) Auto-configuration of multiple switches through a boot server eases switch deployment.
- Auto-negotiation on all ports automatically selects half- or full-duplex transmission mode to optimize bandwidth.
- Dynamic Trunking Protocol (DTP) facilitates dynamic trunk configuration across all switch ports.
- Port Aggregation Protocol (PAgP) automates the creation of Cisco Fast EtherChannel groups and Gigabit groups.
- Link Aggregation Control Protocol (LACP) allows the creation of Ethernet channeling with devices that conform to IEEE 802.3ad.
- Unidirectional Link Detection Protocol (UDLD) and Aggressive UDLD allow unidirectional links caused by incorrect wiring. Also, port faults can be detected and disabled on the interfaces.
- Internet Group Management Protocol (IGMP) v1, v2, v3 Snooping for IPv4. MLD v1 and v2 Snooping provide fast client joins and leaves of multicast streams and limit bandwidth-intensive video traffic to only the requestors.
- Voice VLAN simplifies telephony installations by keeping voice traffic on a separate VLAN for easier administration and troubleshooting.
- The Embedded Remote Monitoring (RMON) software agent supports four RMON groups (history, statistics, alarms, and events) for enhanced traffic management, monitoring, and analysis.
- Layer 2 traceroute eases troubleshooting by identifying the physical path that a packet takes from source to destination.
- Trivial File Transfer Protocol (TFTP) reduces the cost of administering software upgrades by downloading from a centralized location.
- Network Timing Protocol (NTP) provides an accurate and consistent timestamp to all intranet switches.
- Storm control for unicast, broadcast and multicast traffic to prevent disruption in the network due to packet flooding on the LAN.
- Switch-port auto-recovery (error-disable) automatically attempts to reactivate a link that is disabled because of a network error.
- Auto-LAG and etherchannel min-link support.

Quality of Service

- Up to 4 egress queues per port and strict priority queuing, and finer flow segregation using 2 threshold markers for non-strict-priority queues.
- Strict priority queuing to ensure that the highest-priority packets are serviced ahead of all other traffic.

Limitations and Restrictions

- The switch does not support routing protocols.
- The switch has 180 free TCAM entries, which are allocated between MAC ACE, IPv4 ACE and IPv6 ACE entries.
- Extension header match options for IPv6 PACLs are not supported on the switch. Also, PACLs not supported in the out direction.
- The switch does not support jumbo frames.
- IPv4 access-list supports only the **eq** layer-4 operator.

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)E4

None.

Features Introduced in Cisco IOS Release 15.2(7)E3

None.

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)E

- 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.
- The Password Strength and Management for Common Criteria feature is introduced to specify password policies and security mechanisms for storing, retrieving, and providing rules to specify user passwords for local and remote users.

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.

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

None.

Resolved Caveats

Caveats Resolved in Cisco IOS Release 15.2(7)E11

Table 3 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
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

Table 4 Caveats Resolved in Cisco IOS Release 15.2(7)E10

Bug ID	Headline
CSCwf54007	Cisco IOS and IOS XE Software IS-IS Denial of Service Vulnerability
CSCwh96519	For PoE used and remaining power on 3560, the SNMP walk result is showing inaccurate data.

Caveats Resolved in Cisco IOS Release 15.2(7)E9

None.

Caveats Resolved in Cisco IOS Release 15.2(7)E8

None.

Caveats Resolved in Cisco IOS Release 15.2(7)E7

Table 5 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)E6

Table 6 Caveats Resolved in Cisco IOS Release 15.2(7)E6

Bug ID	Headline
CSCvy72006	DHCP Release is sent during the on-boarding IE4000 with the IP address in use in Cisco DNA IE4000.
CSCwa24812	PnP does not work with PnP startup VLAN and native VLAN configured on the trunk.

Caveats Resolved in Cisco IOS Release 15.2(7)E4

Table 7 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 8 Caveats Resolved in Cisco IOS Release 15.2(7)E3

Bug ID	Headline
CSCvt23089	IPv6 ping does not work on 15.2(7.0)E1a for CDB switch.
CSCvu58749	CDB silent reload caused by I2C bus hung due to insufficient time delay.
CSCvt62275	MAC learning issue on peer when CDB egress is configured as trunk port and native vlan allowed.
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 9 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.
CSCvh90127	Cisco Digital Building switches going for a silent reload on production boxes.

Caveats Resolved in Cisco IOS Release 15.2(7)E1a

Table 10 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, cannot be created after that time.
CSCvh90127	Cisco Digital Building switches going for a silent reload on production boxes.

Caveats Resolved in Cisco IOS Release 15.2(7)E1

None.

Caveats Resolved in Cisco IOS Release 15.2(7)E

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

Bug ID	Headline
CSCvn65197	Switch crashes after applying Auto SmartPort Macro configuration on the device.

Related Documentation

- Cisco Digital Building switch documentation at these URLs:

  http://www.cisco.com/go/digitalbuilding
- 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.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.