



# Release Notes for Cisco Digital Building Series Switches, Cisco IOS Release 15.2(5)EX

---

## Cisco IOS Release 15.2(5)EX

This release note describes the features and caveats for the Cisco IOS Release 15.2(5)EX software on the Cisco Digital Building (CDB) 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

- [Introduction](#), page 2
- [Supported Hardware](#), page 2
- [Device Manager System Requirements](#), page 2
- [Upgrading the Switch Software](#), page 3
- [Features of the Switch](#), page 3
- [Limitations and Restrictions](#), page 6
- [Service and Support](#), page 7
- [Caveats](#), page 7
- [Related Documentation](#), page 8



# 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** CDB 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: <ul style="list-style-type: none"> <li>Mac OS 10.9.5</li> <li>Microsoft Windows Version 7</li> </ul>
Browser	Cisco CPC can be used with the following browsers: <ul style="list-style-type: none"> <li>Google Chrome 52 and later</li> <li>Mozilla Firefox 48 and later</li> <li>Apple Safari 9 and later</li> <li>Internet Explorer 11 and later</li> </ul>
Screen Resolution	1280 X 800 or higher

**Table 2**      **System Requirements**

System Component	Requirement
Cisco Management Tools	<ul style="list-style-type: none"> <li>Identity Services Engine (ISE) 2.1</li> <li>Cisco Prime 3.1 DP11 (to be released)</li> </ul>
Mobile App	Supported OS for Cisco Digital Building app: <ul style="list-style-type: none"> <li>Android 4.4.2 and higher</li> <li>iOS 9 and higher</li> </ul>

## 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 switch's configuration guide at

[https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst\\_digital\\_building\\_series\\_switches/software/15-2\\_5\\_ex/configuration\\_guide/b\\_1525ex\\_consolidated\\_cdb\\_cg.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst_digital_building_series_switches/software/15-2_5_ex/configuration_guide/b_1525ex_consolidated_cdb_cg.html).

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

## 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 CDB. 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 6

## 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.

## 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, page 7](#)
- [Open Caveats, page 8](#)
- [Caveats Resolved in Cisco IOS Release 15.2\(5\)EX, page 8](#)

## 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

Bug ID	Headline
CSCvc31736	CDB: Storm-control false counters on spanning-tree blocked port
CSCvd49160	CDB: Wrong storm-control counters and the functionality
CSCvd49350	CDB: UDLD error-disable/LOOP Guard / BA with/without data/control traffic

## Caveats Resolved in Cisco IOS Release 15.2(5)EX

Bug ID	Headline
CSCvb83954	CDB: MAC learning not happening in software when storm-control enabled
CSCvd47317	CDB: ping failure between two authenticated clients
CSCvc25038	CDB: MAC and IPv6 ACL allowing denied traffic if IPV4 ACL exists

## 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>

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see [What's New in Cisco Product Documentation](#).

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the [What's New in Cisco Product Documentation RSS feed](#). The RSS feeds are a free service.

---

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

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](http://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.

© 2017 Cisco Systems, Inc. All rights reserved