

# Release Notes for Cisco Catalyst IE9300 Rugged Series Switches, Cisco IOS XE Cupertino 17.8.x

---

**First Published:** 2022-04-29

**Last Modified:** 2022-05-02

## Cisco Catalyst IE9300 Rugged Series Switches

This document provides release information for the following Catalyst IE switches:

- IE9310 GE Fiber
- IE9320 GE Fiber

Cisco Catalyst IE9300 Rugged Series Switches provide rugged and secure switching infrastructure for harsh environments. It is suitable for industrial Ethernet applications, including manufacturing, utility substations, intelligent transportation systems (ITSs), rail transportation, and other similar deployments.

The switch fulfills the need for a high-density SFP, rack-, or wall-mount switch that can function as a software-defined (SD)-Access fabric edge. It provides end-to-end architectural uniformity in the Cisco Digital Network Architecture (DNA) for Internet of Things (IoT) connected communities and extended enterprises.

In industrial environments, the switch can be connected to any Ethernet-enabled industrial communication devices. These devices include programmable logic controllers (PLCs), human-machine interfaces (HMIs), drives, sensors, and input and output (I/O) devices.



---

**Note** The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

---

## New Features in Cisco Catalyst IE9300 Rugged Series Switches

The following features apply to all versions of the IE9310 GE Fiber and IE9320 GE Fiber switches unless otherwise noted. The features are new in this release for the switches.

Feature Name	License Level	Description	Supported Switches
CIP support	Network Essentials	The Common Industrial Protocol (CIP) is an industrial protocol for industrial automation applications. CIP encompasses a comprehensive suite of messages and services for the collection of manufacturing automation applications	<ul style="list-style-type: none"> <li>• IE-9310-26S2C-A</li> <li>• IE-9310-26S2C-E</li> <li>• IE-9320-26S2C-A</li> <li>• IE-9320-26S2C-E</li> </ul>
Cisco IOx support	Network Essentials	The Cisco IOx application environment combines Cisco IOS and the Linux OS for highly secure networking. It enables you to execute IoT applications with secure connectivity with Cisco IOS software, and get powerful services for rapid, reliable integration with IoT sensors and the cloud.	<ul style="list-style-type: none"> <li>• IE-9310-26S2C-A</li> <li>• IE-9310-26S2C-E</li> <li>• IE-9320-26S2C-A</li> <li>• IE-9320-26S2C-E</li> </ul>
Enhanced Port Security	Network Essentials	<p>Enhanced Port Security restricts input to an interface by limiting and identifying MAC addresses allowed to access the port.</p> <p>When an illegal MAC address is detected, its presence is reported to the user. Depending on the settings you choose, traffic is allowed or blocked.</p>	<ul style="list-style-type: none"> <li>• IE-9310-26S2C-A</li> <li>• IE-9310-26S2C-E</li> <li>• IE-9320-26S2C-A</li> <li>• IE-9320-26S2C-E</li> </ul>

Feature Name	License Level	Description	Supported Switches
Media Access Control Security (MACsec)	<p>The MACsec 256-bit Cipher Suite is supported only on the Network Advantage License.</p> <p>The MACsec 128-bit Cipher Suite is supported on both Network Advantage and Network Essentials licenses.</p>	MACsec allows authorized systems to connect and then encrypt data that is transmitted across the wire. It prevents a man-in-the-middle from inserting frames on to the wire. MACsec enables authorized systems to encrypt traffic destined for the network. MACsec is for use on wired networks only.	<ul style="list-style-type: none"> <li>• IE-9310-26S2C-A</li> <li>• IE-9310-26S2C-E</li> <li>• IE-9320-26S2C-A</li> <li>• IE-9320-26S2C-E</li> </ul>
Network Edge Authentication Topology	Network Essentials	The NEAT feature enables extended secure access in areas outside the wiring closet (such as conference rooms). NEAT allows you to configure a switch to act as a supplicant to another switch. Thus, with NEAT enabled, the desktop switch can become a supplicant switch and authenticate itself to the access switch.	<ul style="list-style-type: none"> <li>• IE-9310-26S2C-A</li> <li>• IE-9310-26S2C-E</li> <li>• IE-9320-26S2C-A</li> <li>• IE-9320-26S2C-E</li> </ul>
Profinet support	Network Essentials	<p>PROFINET is the leading Industrial Ethernet Standard that uses TCP/IP and IT standards for automation control.</p> <p>PROFINET is particularly useful for industrial automation systems and process control networks in which motion control and precision control of instrumentation and test equipment are important.</p>	<ul style="list-style-type: none"> <li>• IE-9310-26S2C-A</li> <li>• IE-9310-26S2C-E</li> <li>• IE-9320-26S2C-A</li> <li>• IE-9320-26S2C-E</li> </ul>

Feature Name	License Level	Description	Supported Switches
PTP power profile 2017	Network Essentials	This release supports the power profile standard power-2017 in 17.8.1 - IEEE Std C37.238™-2017 (Revision of IEEE Std C37.238-2011).  Only transparent clock mode is supported with this profile.	<ul style="list-style-type: none"> <li>• IE-9310-26S2C-A</li> <li>• IE-9310-26S2C-E</li> <li>• IE-9320-26S2C-A</li> <li>• IE-9320-26S2C-E</li> </ul>
SDA support	Network Advantage with DNA Advantage	Cisco Software-Defined (SD) Access helps organizations enable policy-based automation from the edge to the cloud.  Beginning in this release Cisco Catalyst IE9300 Rugged Series Switches are supported as fabric edges in SD-Access deployments. In that role, the switches support up to 32 virtual networks.	<ul style="list-style-type: none"> <li>• IE-9310-26S2C-A</li> <li>• IE-9310-26S2C-E</li> <li>• IE-9320-26S2C-A</li> <li>• IE-9320-26S2C-E</li> </ul>

## Important Notes

### Accessing Hidden Commands

Hidden commands have always been present in Cisco IOS XE, but were not equipped with CLI help. This means that entering enter a question mark (?) at the system prompt did not display the list of available commands. Such hidden commands are only meant to assist Cisco TAC in advanced troubleshooting and are therefore not documented. For more information about CLI help, see the *Using the Command-Line Interface* → *Understanding the Help System* chapter of the Command Reference document.

This section provides information about hidden commands in Cisco IOS XE and the security measures in place, when they are accessed. Hidden commands are meant to assist Cisco TAC in advanced troubleshooting and are therefore not documented. For more information about CLI help, see the *Using the Command-Line Interface* → *Understanding the Help System* chapter of the Command Reference document.

Hidden commands are available under:

- Category 1—Hidden commands in privileged or User EXEC mode. Begin by entering the **service internal** command to access these commands.
- Category 2—Hidden commands in one of the configuration modes (global, interface and so on). These commands do not require the **service internal** command.

Further, the following applies to hidden commands under Category 1 and 2:

- The commands have CLI help. Entering a question mark (?) at the system prompt displays the list of available commands.



**Note** For Category 1, enter the **service internal** command before you enter the question mark; you do not have to do this for Category 2.

- The system generates a %PARSER-5-HIDDEN syslog message when the command is used. For example:

```
*Feb 14 10:44:37.917: %PARSER-5-HIDDEN: Warning!!! 'show processes memory old-header '
is a hidden command.
Use of this command is not recommended/supported and will be removed in future.
```

Apart from category 1 and 2, there remain internal commands displayed on the CLI, for which the system does NOT generate the %PARSER-5-HIDDEN syslog message.



**Important** We recommend that you use any hidden command only under TAC supervision. If you find that you are using a hidden command, open a TAC case for help with finding another way of collecting the same information as the hidden command (for a hidden EXEC mode command), or to configure the same functionality (for a hidden configuration mode command) using non-hidden commands.

## Cisco Catalyst IE9300 Rugged Series Switch Model Numbers

The following table lists the supported hardware models and the default license levels they are delivered with.

Model Number	Default License Level	Stacking Support	Description
IE-9310-26S2C-A	Network Advantage	No	<ul style="list-style-type: none"> <li>• <i>Total ports:</i> 28</li> <li>• <i>SFP uplinks :</i> 4x 1 Gb SFP</li> <li><i>SFP downlinks:</i> 22x 1 Gb SFP, 2x 1 Gb dual-media ports</li> <li>• <i>Power supplies:</i> Support for field-replaceable, redundant AC or DC power supplies.</li> </ul>
IE-9310-26S2C-E	Network Essentials		
IE-9320-26S2C-A	Network Advantage	Yes	
IE-9320-26S2C-E	Network Essentials		

All Cisco Catalyst IE9300 Rugged Series Switches have 4 GB of DRAM, four alarm inputs, and one alarm output. Additional I/O include the following:

- SD-cards socket
- Power input

- RJ-45 (RS-232) console
- Micro-USB console
- USB-A host port



**Note** This document uses the term IE9310 GE Fiber when referring to both IE-9310-26S2C-A and IE-9310-26S2C-E switches. This document uses the term IE9320 GE Fiber when referring to both IE-9320-26S2C-A and IE-9320-26S2C-E switches.

## Upgrading the Switch Software

This section covers the various aspects of upgrading or downgrading the device software.

### Finding the Software Version

The package files for the Cisco IOS XE software can be found on the system board flash device flash (flash:) or external SDFlash (sdflash:).

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.

### Software Images for Cisco IOS XE Cupertino 17.8.x

The following table provides the filenames for the IOS XE 17.8.x software image for Cisco Catalyst IE9300 Rugged Series Switches.

Release	Image Type	Filename
Cisco IOS XE.17.8.1	Universal	ie9k_iosxe.17.08.01a.SPA.bin
	NPE	ie9k_iosxe_npe.17.08.01a.SPA.bin

### Software Installation Commands

#### Summary of Software Installation Commands

To install and activate the specified file, and to commit changes to be persistent across reloads—**install add file filename [activate commit]**

Summary of Software Installation Commands	
<b>add file tftp:</b> <i>filename</i>	Copies the install file package from a remote location to the device and performs a compatibility check for the platform and image versions.
<b>activate</b> [ <b>auto-abort-timer</b> ]	Activates the file, and reloads the device. The <b>auto-abort-timer</b> keyword automatically rolls back image activation.
<b>commit</b>	Makes changes persistent over reloads.
<b>remove</b>	Deletes all unused and inactive software installation files.

## Licensing

This section provides information about the licensing packages for features available on Cisco Catalyst IE9300 Rugged Series Switches.

### License Levels

The software features available on Cisco Catalyst IE9300 Rugged Series Switches fall under these base or add-on license levels.

#### Base Licenses

- Network Essentials
- Network Advantage: Includes features available with the Network Essentials license and more.

#### Add-on Licenses

Add-on licenses require a Network Essentials or Network Advantage as a prerequisite. The features available with add-on license levels provide Cisco innovations on the switch, and on the Cisco Digital Network Architecture Center (Cisco DNA Center).

- DNA Essentials
- DNA Advantage: Includes features available with the DNA Essentials license and more.

To find information about platform support and to know which license levels a feature is available with, use Cisco Feature Navigator. To access Cisco Feature Navigator, go to <https://cfng.cisco.com>. An account on Cisco.com is not required.

### Smart Licensing Using Policy

Smart Licensing Using Policy, which is an enhanced version of Smart Licensing, is the default and the only supported method to manage licenses.

An enhanced version of Smart Licensing is available, with the overarching objective of providing a licensing solution that does not interrupt the operations of your network, rather, one that enables a compliance relationship to account for the hardware and software licenses you purchase and use.

With this licensing model, you do not have to complete any licensing-specific operations, such as registering or generating keys before you start using the software and the licenses that are tied to it. Only export-controlled and enforced licenses require Cisco authorization *before* use. License usage is recorded on your device with timestamps, and the required workflows can be completed at a later date.

Multiple options are available for license usage reporting – this depends on the topology you implement. You can use the Cisco Smart Licensing Utility (CSLU) Windows application, or report usage information directly to Cisco Smart Software Manager (CSSM). A provision for offline reporting for air-gapped networks, where you download usage information and upload to CSSM, is also available.

Starting with this release, Smart Licensing Using Policy is automatically enabled on the device. This is also the case when you upgrade to this release.

By default, your Smart Account and Virtual Account in CSSM is enabled for Smart Licensing Using Policy.

## Caveats

Caveats describe unexpected behavior in Cisco IOS XE releases. Caveats listed as open in a prior release are carried forward to the next release as either open or resolved.

### Open Caveats

Identifier	Description
<a href="#">CSCwa48106</a>	IE9300: High mean path delay observed for 100M SFP, RJ45 intfs and negative mean path delay on some intfs
<a href="#">CSCwb12681</a>	IE9300 17.8.x: REP convergence high for node failure

### Resolved Caveats

Identifier	Description
<a href="#">CSCvz79250</a>	FCS errors with sync/pdel req/resp packets with PTP power profile when spanned on rx
<a href="#">CSCwa00379</a>	PTP: Pdelay_Req messages are missing after PTP enable/disable in TC mode
<a href="#">CSCwa20424</a>	PTP time synchronization init fails when the port is moved between L2 and L3 and reloaded
<a href="#">CSCwa27652</a>	Clock syntonized shows FALSE when moving between GMs
<a href="#">CSCwa34430</a>	CDP neighbors not shown when removing an 100m SFP and inserting a 1Gig SFP on same port
<a href="#">CSCwa39943</a>	"speed 10 or speed 100" config is not shown in combo ports after device reload
<a href="#">CSCwa31367</a>	NTP source is not removing from clock data set when we shut the NTP interface



## Troubleshooting

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

<https://www.cisco.com/en/US/support/index.html>

Go to **Product Support** and select your product from the list or enter the name of your product. Look under Troubleshoot and Alerts, to find information for the problem that you are experiencing.

## Related Documentation

Information about Cisco IOS XE at this URL: <https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-xe/index.html>.

Information about Cisco Catalyst IE9300 Rugged Series Switches is at this URL: <https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-xe/index.html>

All support documentation for Cisco Catalyst IE9300 Rugged Series Switches is at this URL: <https://www.cisco.com/go/designzone>

Cisco Validated Designs documents at this URL: <https://www.cisco.com/go/designzone>

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <http://www.cisco.com/go/mibs>

## 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 DevNet](#).
- 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 gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

## Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

