# Release Notes for Cisco Catalyst IE9300 Rugged Series Switches, Release 26.1.x

# Cisco Catalyst IE9300 Rugged Series Switches, Release 26.1.x

This document provides release information for the following Cisco Catalyst IE switches.

- Cisco Catalyst IE9310 GE Fiber switch
- Cisco Catalyst IE9320 GE Fiber switch
- Cisco Catalyst IE9310 GE mixed port switch
- Cisco Catalyst IE9320 Fiber switch with 10 GE uplinks
- Cisco Catalyst IE9320 10 GE Copper Data switch
- Cisco Catalyst IE9320 10 GE PoE switch
- Cisco Catalyst IE9320 10 G mGig 4PPoE switch
- Cisco Catalyst IE9320 GE PoE switch

## Cisco Catalyst IE9300 Rugged Series Switch

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 fulfils the need for a high-density SFP, RJ-45, and Power over Ethernet (PoE) rack-, or wall-mount switch that can function as a Software-Defined-Access (SDA) fabric edge. It provides end-to-end architectural uniformity in the Cisco Catalyst Center 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.

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

- SD-cards socket
- Power input
- RJ-45 (RS-232) console
- Micro-USB console
- USB-A host port

# New software features

This section provides a brief description of the new software features introduced in this release.

## IOS-XE 26.1.1

**Table 1.** New software features in release 26.1.1

| Product Impact | Feature | Description |
|---|---|---|
| Security | Resilient Infrastructure | As part of the ongoing commitment to network security, this release introduces secure alternatives to legacy commands. These updates are designed to mitigate potential risks and assist in establishing a more robust and secure operational baseline.<br>The identified insecure commands are categorized as:<br>▪ Line transport: Updates to secure remote access methods.<br>▪ Device server configuration: Hardening of server-side settings.<br>▪ File transfer protocols: Transitioning to encrypted transfer methods.<br>▪ SNMP: Enhancements to secure management traffic.<br>▪ Passwords: Strengthening authentication and credential management.<br>▪ Miscellaneous: General security improvements for various system functions.<br>The show system insecure configuration command introduced in Cisco IOS XE 17.18.2 release lists all insecure commands configured on the device. For all detected insecure configurations during device boot or upgrade, error messages are displayed.<br>In Cisco IOS XE 26.1.1 release, all insecure CLI commands are blocked by default to strengthen your network infrastructure. If your environment requires the use of a legacy command, you must enable the system mode insecure command in global configuration mode.<br>▪ Recommendation: Do not use insecure mode. This mode is temporary and will be removed in a future release. Identify and replace all insecure commands with their secure alternatives.<br>▪ Upgrade behavior: If you upgrade to Cisco IOS XE 26.1.1 release with insecure commands already present in the running configuration, the system mode insecure command is automatically added to your configuration to prevent service disruption.<br>For more information, refer this document Cisco C9000 Switching IOS XE – Resilient Infrastructure Playbook. |
| Upgrade | PTP over stack | This feature enables PTP for your stacked Cisco IE9300 Rugged Series switches so they function as a unified network entity. You receive consistent, synchronized timing across the stack, making network management simpler and ensuring precise timekeeping for your critical applications. |
| | Media Redundancy Client | This feature enables configuring Cisco switches as Media Redundancy Clients (MRC) within an MRP ring, acting as regular ring participants that forwards traffic and continuously monitor link status, reporting any failures to the ring manager (MRM). This approach enhances network resiliency and simplifies deployment, supporting rapid failover and compliance with industrial certification requirements. |
| Ease of use and Ease of setup | REP Segment-ID auto-discovery | REP Segment ID Auto-Discovery automates the configuration of Resilient Ethernet Protocol (REP) Segment IDs using CDP. This feature reduces manual effort and prevents mismatches for both standard REP and REP Fast protocols, making it easier to add switches to existing segments or create new daisy-chain segments. |
| Upgrade | PROFINET system redundancy | This feature enables Cisco Industrial Ethernet (IE) switches to interoperate with existing high available systems by providing robust controller failover using PROFINET S2 controller redundancy mode. It aims to minimize potential issues and downtime in the event of network |

| Product Impact | Feature | Description |
|---|---|---|
| | | or controller failures. |
| Software Reliability | Read-only PROFINET | This feature enhances device security and network flexibility by setting Discovery and Configuration Protocol (DCP) operations to read-only mode. It safeguards the IP address, gateway, and device name from modifications, protects essential network settings to prevent unexpected connectivity loss, and remains compatible with LLDP, SNMP, and CDP. Additionally, it enables devices to carry out identification and basic network discovery. |

## New hardware features

This section provides a brief description of the new hardware features introduced in this release.

### IOS-XE 26.1.1

There are no new hardware features introduced in this release.

## Change in behavior

**Syslog Warning on Reload for SSH Hostkeys:** After a device reload, you may observe a syslog warning indicating insufficient key length for SSH hostkeys, even if a strong RSA or EC key is configured.

**Note:**

- In the syslog warning message "*crypto key generate rsa modulus <modulus-size> label <label-name>",* the *<modulus-size>* and *<label-name>* represent the actual modulus size and label configured on the device.
- The SSH keypair association configuration is done using the command: **ip ssh ec|rsa <**keypair-name**>**, where *<keypair-name>* corresponds to the keypair name configured on the device.

**Example:**

- RSA

  Warning Observed : INSECURE DYNAMIC WARNING - Module: SSH,

  Command: crypto key generate rsa modulus <modulus-size> label <label-name>,

  Reason: An SSH hostkey has been provisioned on the device with insufficient key length,

  Remediation: Please provision an SSH RSA hostkey with minimum modulus size of 3072 bits for enhanced security,

  Submode: exec,

  Parent CLI: Not Applicable.

- EC

  Warning Observed : INSECURE DYNAMIC WARNING - Module: SSH,

  Command: crypto key generate ec keysize <modulus-size> label <label-name>,

  Reason: An SSH hostkey has been provisioned on the device with insufficient key length,

Remediation: Please provision an SSH RSA hostkey with minimum modulus size of 384 bits for enhanced security,

Submode: exec,

Parent CLI: Not Applicable.

Ignore these warnings if you have already configured a strong key. The system applies the SSH keypair association (**ip ssh ec/rsa** *keypair-name*) after the boot process.

Once this configuration is active, SSH will use the correct key for secure connections.

## Notice of changes introduced in the Cisco IOS-XE 17.18.2 release and beyond

Cisco is committed to safeguarding our products and customer networks against increasingly sophisticated threat actors. As computing power and the threat landscape have evolved, some features and protocols currently in use have become vulnerable to attack. While more secure alternatives are now available, legacy protocols may still be in use in some environments.

To improve network security, reduce the attack surface, and protect sensitive data, Cisco will begin phasing out legacy and insecure features and protocols, encouraging customers to transition to more secure alternatives. This process will be gradual and designed to minimize operational impact. The first phase began with the Cisco IOS-XE 17.18 release train. This is part of a broader initiative to make Cisco products more secure by default and secure by design.

Starting with the Cisco IOS-XE 17.18.2 release and in future releases, Cisco software displays warning messages when configuring features or protocols that do not provide sufficient security such as those transmitting sensitive data without encryption or using outdated encryption mechanisms. Warnings also appear when security best practices are not followed, along with suggestions for secure alternatives.

This list is subject to change, but the following is a list of features and protocols that generates warnings in releases beyond the version Cisco IOS-XE 17.18.1. Release notes for each release describes the exact changes for that release.

- **Plain-text and weak credential storage:** Type 0 (plain text), 5 (MD5), or 7 (Vigenère cipher) in configuration files.
  *Recommendation***:** Use Type 6 (AES) for reversible credentials, and Type 8 (PBKDF2-SHA-256) or Type 9 (Scrypt) for non-reversible credentials.
- **SSHv1**
  *Recommendation*: Use SSHv2.
- **SNMPv1 and SNMPv2, or SNMPv3 without authentication and encryption**
  *Recommendation*: Use SNMPv3 with authentication and encryption (authPriv).
- **MD5 (authentication) and 3DES (encryption) in SNMPv3**
  *Recommendation*: Use SHA1 or, preferably, SHA2 for authentication, and AES for encryption.
- **IP source routing based on IP header options**
  *Recommendation*: Do not use this legacy feature.
- **TLS 1.0 and TLS 1.1**
  *Recommendation*: Use TLS 1.2 or later.
- **TLS ciphers using SHA1 for digital signatures**
  *Recommendation*: Use ciphers with SHA256 or stronger digital signatures.

- **HTTP**
  *Recommendation*: Use HTTPS.
- **Telnet**
  *Recommendation*: Use SSH for remote access.
- **FTP and TFTP**
  *Recommendation*: Use SFTP or HTTPS for file transfers.
- **On-Demand Routing (ODR)**
  *Recommendation*: Use a standard routing protocol in place of CDP-based routing information exchange.
- **BootP server**
  *Recommendation*: Use DHCP or secure boot features such as Secure ZTP.
- **TCP and UDP small servers (echo, chargen, discard, daytime)**
  *Recommendation*: Do not use these services on network devices.
- **IP finger**
  *Recommendation*: Do not use this protocol on network devices.
- **NTP control messages**
  *Recommendation*: Do not use this feature.
- **TACACS+ using pre-shared keys and MD5**
  *Recommendation*: Use TACACS+ over TLS 1.3, introduced in release Cisco IOS-XE 17.18.1.

Cisco is committed to supporting customers through this transition. Subsequent releases in the Cisco IOS-XE 17.18 train continues to support these features but displays warnings if they are used. Future release trains may impose additional restrictions on these features which will be communicated through release notes.

The changes introduced in 17.18 persist in 26.1.x and later versions.

## Resolved issues

This section lists the issues resolved in this release.

**Note**: This software release may contain bug fixes first introduced in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool.

### IOS-XE 26.1.1

**Table 2.** Resolved issues in release 26.1.1

| Bug ID | Description |
|---|---|
| CSCwo44673 | Taggged traffic getting dropped in IE9k and IE3500 if more than 50 Extended Vlans enabled. |
| CSCwp22300 | IE-9320-22S2C4X: show ptp lan clock is not updating with gnss time clock |
| CSCwp24892 | IE9320 PTP BC invalid currentOffset |
| CSCwp65194 | Incomplete SNMPWALK of entSensorValue data retrieval for SFP modules on IE-9320- |

| Bug ID | Description |
|---|---|
| | 26S2C-A switches |
| CSCwq85911 | REP Interface broadcast unicast traffic to all the interface in the same vlan |
| CSCwr78633 | 100mb SFP not in sync with 1g SFP |
| CSCws05823 | Port VlanID is missing from show ptp lan port on changing native vlan configuration |
| CSCws48556 | Follow-up meessage stops transmitting from IE93xx |
| CSCwr60436 | On IE9k switches, the Dying-Gasp SNMP trap is not sent over loopback interface after a reboot. |
| CSCwr72487 | SFP status behaviour change from SNMP_ADMIN_NOT_PRESENT to SNMP_ADMIN_DOWN when Profinet disabl |
| CSCws18675 | IE-9310-26S2C: Express setup LED glows amber |
| CSCwr77016 | Cisco IOS-XE Software for Cisco Catalyst and Rugged Series Switches Secure Boot Bypass Vulnerability |

## Open issues

This section lists the open issues in this specific software release.

**Note**: This software release may contain open bugs first identified in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool.

### IOS-XE 26.1.1

There are no open issues in this release.

## Known issues

This section lists the known issues in this specific software release.

### IOS-XE 26.1.1

There are no known issues in this release.

## Compatibility

Refer to Cisco IOS-XE Migration Guide for IIoT Switches for the latest information about upgrading and downgrading switch software for Cisco Catalyst IE9300 Series Switches, release 26.1.x

**SSH Algorithms for Common Criteria Certification Limitation**

Starting from Cisco IOS-XE release 17.10, the following Key Exchange and MAC algorithms are removed from the default list:

- Key Exchange algorithm:
  - diffie-hellman-group14-sha1
- MAC algorithms:
  - hmac-sha1

- hmac-sha2-256
- hmac-sha2-512

Note: You can use **the ip ssh server algorithm kex** command to configure the Key Exchange algorithm and the **ip ssh server algorithm mac** command to configure the MAC algorithms.

## Supported hardware

This section lists the hardware support information.

This table lists the supported Cisco Catalyst IE9300 Rugged Series Switches hardware models and the default license levels that they are delivered with.

| Model Number | Default License Level | Stacking Support | Description |
|---|---|---|---|
| IE-9310-26S2C-A | Network Advantage | No | • Total ports: 28<br>• SFP uplinks: 4x 1 Gb SFP<br>• SFP downlinks: 22x 100M/1000M SFP, 2x 100M/1000M dual-media<br>• Power supplies: Support for field-replaceable, redundant AC or DC power supplies |
| IE-9310-26S2C-E | Network Essentials | No | • Total ports: 28<br>• SFP uplinks: 4x 1 Gb SFP<br>• SFP downlinks: 22x 100M/1000M SFP, 2x 100M/1000M dual-media<br>• Power supplies: Support for field-replaceable, redundant AC or DC power supplies |
| IE-9310-16P8S4X-E | Network Essentials | No | • Total ports: 28<br>• PoE+ ports: 16 ports 10/100/1000M<br>• SFP downlinks: 8 ports 100/1000M<br>• SFP uplinks: 4 ports 1/10G<br>• Power supplies: Support for field-replaceable, redundant AC or DC power supplies |
| IE-9310-16P8S4X-A | Network Advantage | No | • Total ports: 28<br>• PoE+ ports: 16 ports 10/100/1000M<br>• SFP downlinks: 8 ports 100/1000M<br>• SFP uplinks: 4 ports 1/10G<br>• Power supplies: Support for field-replaceable, redundant AC or DC power supplies |
| IE-9320-26S2C-A | Network Advantage | Yes | • Total ports: 28<br>• SFP uplinks: 4x 1 Gb SFP<br>• SFP downlinks: 22x 100M/1000M SFP, 2x 100M/1000M dual-media<br>• Power supplies: Support for field-replaceable, redundant AC or DC power supplies |
| IE-9320-26S2C-E | Network Essentials | Yes | • Total ports: 28<br>• SFP uplinks: 4x 1 Gb SFP<br>• SFP downlinks: 22x 100M/1000M SFP, 2x 100M/1000M dual-media<br>• Power supplies: Support for field-replaceable, redundant AC or DC power supplies |
| IE-9320-22S2C4X-A | Network Advantage | Yes | • Total ports: 28<br>• SFP uplinks: 4x 10 Gb SFP+<br>• SFP downlinks:<br>• 22x 1 Gb SFP, 2x 1-Gb Dual-media ports |

| Model Number | Default License Level | Stacking Support | Description |
|---|---|---|---|
| | | | • Power supplies: Support for field-replaceable, redundant AC or DC power supplies |
| IE-9320-22S2C4X-E | Network Essentials | Yes | • Total ports: 28<br>• SFP uplinks: 4x 10 Gb SFP+<br>• SFP downlinks:<br>• 22x 1 Gb SFP, 2x 1-Gb Dual-media ports<br>• Power supplies: Support for field-replaceable, redundant AC or DC power supplies |
| IE-9320-24T4X-A | Network Advantage | Yes | • Total ports: 28<br>• SFP uplinks: 4x 10 Gb SFP+<br>• Copper downlinks: 24x 1 Gb RJ45<br>• Power supplies: Support for field-replaceable, redundant AC or DC power supplies. |
| IE-9320-24T4X-E | Network Essentials | Yes | • Total ports: 28<br>• SFP uplinks: 4x 10 Gb SFP+<br>• Copper downlinks: 24x 1 Gb RJ45<br>• Power supplies: Support for field-replaceable, redundant AC or DC power supplies. |
| IE-9320-24P4X-A | Network Advantage | Yes | • Total ports: 28<br>• SFP uplinks: 4x 10 Gb SFP+<br>• Copper downlinks: 24x 1 Gb RJ45 PoE+<br>• Power supplies: Support for field-replaceable, redundant AC or DC power supplies |
| IE-9320-24P4X-E | Network Essentials | Yes | • Total ports: 28<br>• SFP uplinks: 4x 10 Gb SFP+<br>• Copper downlinks: 24x 1 Gb RJ45 PoE+<br>• Power supplies: Support for field-replaceable, redundant AC or DC power supplies |
| IE-9320-16P8U4X-A | Network Advantage | Yes | • Total ports: 28<br>• SFP uplinks: 4x 10 Gb SFP<br>• Copper downlinks: 16 ports 1 Gb RJ45 PoE+, 8 ports 2.5 Gb RJ45 4PPoE (90W/port)<br>• Power supplies: Support for field-replaceable, redundant AC or DC power supplies |
| IE-9320-16P8U4X-E | Network Essentials | Yes | • Total ports: 28<br>• SFP uplinks: 4x 10 Gb SFP<br>• Copper downlinks: 16 ports 1 Gb RJ45 PoE+, 8 ports 2.5 Gb RJ45 4PPoE (90W/port)<br>• Power supplies: Support for field-replaceable, redundant AC or DC power supplies |
| IE-9320-24P4S-A | Network Advantage | Yes | • Total ports: 28<br>• SFP uplinks: 4x 1Gb SFP<br>• Copper downlinks: 24 ports 1 Gb RJ45 PoE+<br>• Power supplies: Support for field-replaceable, redundant AC or DC power supplies |
| IE-9320-24P4S-E | Network Essentials | Yes | • Total ports: 28<br>• SFP uplinks: 4x 1Gb SFP<br>• Copper downlinks: 24 ports 1 Gb RJ45 PoE+<br>• Power supplies: Support for field- |

| Model Number | Default License Level | Stacking Support | Description |
|---|---|---|---|
| | | | replaceable, redundant AC or DC power supplies |

Note: Documentation sometimes uses these terms:

- IE9310 GE Fiber switch when referring to both IE-9310-26S2C-A and IE-9310-26S2C-E switches
- IE9320 GE Fiber switch when referring to both IE-9320-26S2C-A and IE-9320-26S2C-E switches
- IE9320 Fiber switch with 10 GE uplinks when referring to both IE-9320-22S2C4X-A and IE-9320-22S2C4X-E switches
- IE9320 10 GE Copper Data switch when referring to both IE-9320-24T4X-A and IE-9320-24T4X-E switches
- IE9320 10 GE PoE switch when referring to both IE-9320-24P4X-A and IE-9320-24P4X-E
- IE9320 10 G mGig 4PPoE switch when referring to both IE-9320-16P8U4X-A and IE-9320-16P8U4X-E
- IE9320 GE PoE switch when referring to both IE-9320-24P4S-A and IE-9320-24P4S-E
- IE9310 GE mixed port when referring to 9310-16P8S4x

Network Essentials and Network Advantage licenses are available for Cisco Catalyst IE9300 Rugged Series Switch starting with release 17.10.1. The features available in the two licenses follow the IE9300 series, except for MACsec-256.

| Network advantage license | Description |
|---|---|
| Security | MACsec-256 |
| Routing | Layer 3 routing support. |

## Supported software packages

This section provides information about the release packages associated with <product>

### Finding the software version

- The package files for Cisco IOS-XE software can be found on the system board's internal flash memory device (flash:) or an external USB, depending on the device configuration.
- 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 names and versions of other software images that you might have stored in flash memory.

## Software images for Cisco IOS-XE 26.1.x

This table provides the filename for the IOS-XE 26.1.x software image for Cisco Catalyst IE9300 Rugged Series Switches.

**Table 3.** Software packages for release 26.1.x

| Release | Image type | Filename | Switch Models |
|---|---|---|---|
| Cisco IOS-XE.26.1.1 | Universal | ie9k_iosxe.26.01.01.SPA.bin | Cisco Catalyst IE9300 Rugged Series Switches |

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

This table lists the options for the **install** command for the Cisco Catalyst IE9300 Rugged Series Switches.

**Table 4.** Summary of software installation commands for install mode

| Option | Description |
|---|---|
| abort | Abort the current install operation. |
| activate | Activate an installed package. |
| add | Install a package file to the system. |
| auto-abort-timer | Install auto-abort-timer. |
| autoupgrade | Initiate software auto-upgrade on all incompatible switches. |
| commit | Commit the changes to the load path. |
| deactivate | Deactivate an install package. |
| label | Add a label name to any installation point. |
| remove | Remove installed packages. |
| rollback | Rollback to a previous installation point. |

# Related resources

**Table 5.** Additional references for Cisco Catalyst IE9300 Rugged Series Switches

| Document | Description |
|---|---|
| Cisco IOS-XE | Provides information about Cisco IOS-XE. |
| Cisco Validated Design documents | Provides Cisco validated designs |
| Cisco MIB Locator | Provides locating and downloading MIBs. |
| Cisco Profile Manager | To receive timely, relevant information from Cisco, sign up here. |

| Document | Description |
| --- | --- |
| Cisco Services | Provides the business impact you're looking for with the technologies |
| Cisco Support | You can submit a service request here. |
| Cisco DevNet | To discover and browse secure, validated enterprise-class apps, products, solutions, and services. |
| Cisco Press | To obtain general networking, training, and certification titles visit here. |
| Cisco Warranty Finder | Provides warranty information for a specific product or product family. |
| Cisco support community | You can ask and answer questions, share suggestions, and collaborate with your peers. |
| Cisco TAC | Provides most up-to-date detailed troubleshooting information. |
| Cisco Feature Navigator | Provides platform support details and license level information for features. |
| Cisco TAC | Provides most up-to-date, detailed troubleshooting information. 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. |
| Documentation Feedback | To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document. |
| Licenses | You can find information about the licensing packages for features here. |

## Legal information