Release Notes for Cisco IE3500 Series Switches, Release 26.1.x

© 2026 Cisco and/or its affiliates. All rights reserved.

Contents

Cisco IE3500 Series Switches, Release 26.1.x 3
New software features 3
New hardware features 5
Change in behavior 5
Resolved issues 7
Open issues 7
Known issues 8
Supported hardware 8
Supported software packages 10
Related resources 11
Legal information 12

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco IE3500 Series Switches, Release 26.1.x

This document provides Cisco IOS XE release information for the Cisco Industrial Ethernet (IE) switches.

Cisco IE3500/IE3505 Series Switches

Cisco IE3500 and IE3505 Series Switches are ruggedized switching platforms that provide high bandwidth and high-PoE power with Cisco IOS XE Software for industrial environments. These switches are designed to operate in harsh conditions, including temperatures from -40°C to +75°C (-40°F to 167°F), and can withstand severe shock and vibration.

These switches are designed for hardened deployments such as factory automation, smart cities, energy and process control, Intelligent Transportation Systems (ITS), energy production sites, and mining. They also provide improved scale, built-in security features, and simplified management. For more information, refer to the datasheet.

Cisco IE3500H/IE3505H Series Switches

Cisco IE3500H and IE3505H Series Switches are the next-generation managed IP67 switches powered by Cisco IOS XE. They are designed for deployment in harsh environments and are IP67-rated for water and dust resistance. These switches also operate in temperatures from -40°C to +75°C (-40°F to 167°F) and are built to withstand severe shock and vibration.

These switches are available with up to 24 ports. Fast Ethernet is supported through Fast Ethernet PIDs, and 1G PIDs can also operate at 100 Mbps. For a list of supported SFPs, refer to the datasheet. These switches can be wall-mounted and deployed without a housing cabinet. They offer a power budget of 240 W and support Power over Ethernet (PoE), PoE+, and Universal Power over Ethernet (UPoE) at 60 W.

These switches provide advanced security, segmentation, and visibility for demanding industrial IoT edge deployments such as mining, rail, and manufacturing. For more information, refer to the datasheet.

New software features

This section provides a brief description of the new software features introduced in Cisco IOS XE Release 26.1.x

IOS XE 26.1.2

There are no new software features 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 Cisco IOS XE 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. The identified insecure commands are categorized as: • Line transport: Updates to secure remote access methods. • Device server configuration: Hardening of server-side settings. • File transfer protocols: Transitioning to encrypted transfer methods. • SNMP: Enhancements to secure management traffic.

© 2026 Cisco and/or its affiliates. All rights reserved.

Product Impact	Feature	Description
		▪ Passwords: Strengthening authentication and credential management. ▪ Miscellaneous: General security improvements for various system functions. The **show system insecure configuration** command introduced in Cisco IOS XE release 17.18.2 lists all insecure commands configured on the device. For all detected insecure configurations during device boot or upgrade, error messages are displayed. In Cisco IOS XE release 26.1.1, 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. ▪ Recommendation: Do not use insecure mode. This mode is temporary and will be removed in a future Cisco IOS XE release. Identify and replace all insecure commands with their secure alternatives. ▪ Upgrade behavior: If you upgrade to Cisco IOS XE release 26.1.1 with insecure commands already present in the running configuration, the **system mode insecure** command is automatically added to your configuration to prevent service disruption. For more information, refer to Resilient Infrastructure IOS XE Security Warnings Reference
Upgrade	Frame Preemption with IEEE 802.1Qbu	This feature provides a low-latency mechanism for high-priority frames by allowing the suspension of non-critical frames for critical ones. It helps achieve low latency and low jitter for real-time control networks, effectively extending QoS capabilities. When high-priority frames are transmitted, the preempted non-critical frame resumes transmission for multiple splits.
	Media Redundancy Client	This feature enables configuring Cisco switches as Media Redundancy Clients (MRC) within an MRP ring, acting as regular ring participants that forward 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.
	PTP over MACsec	This feature allows highly accurate time synchronization between devices, even when MACsec encrypts Ethernet traffic for security. This ensures industrial, utility, or automation networks can maintain precise timing and robust data protection on the same infrastructure.
	HSR-HSR QuadBox	This feature enables you to interconnect two distinct High-availability Seamless Redundancy (HSR) rings, providing continuous, fault-tolerant communication between them. This capability is crucial in industrial and critical infrastructure environments where zero packet loss and high network availability are paramount. It allows for robust network segmentation and enhanced resilience on IE3505 and IE3505H platforms.
Ease of Use	Industrial Asset Discovery	Industrial Asset Discovery feature automatically identifies and catalogs directly connected industrial devices without impacting network performance. It also exports inventory data to a syslog server in JSON format, streamlining asset tracking and security enforcement.
	Migration to Meraki Managed Dashboard	Cisco IE3500 Series Switches support cloud management mode, enabling centralized control through the Meraki dashboard. This functionality supports zero-touch provisioning and cloud-based management for streamlined monitoring and configuration. Additionally,

© 2026 Cisco and/or its affiliates. All rights reserved.

Product Impact	Feature	Description
		it includes access to a Local Status Page (LSP) to facilitate troubleshooting and setup in environments without DHCP.
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-availability 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 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 protects the IP address, gateway, and device name from modification. It also helps prevent unexpected connectivity loss by preserving essential network settings. The feature remains compatible with LLDP, SNMP, and CDP, and still allows identification and basic network discovery.

New hardware features

This section provides a brief description of the new hardware features introduced in Cisco IOS XE Release 26.1.x

IOS XE 26.1.2

There are no new hardware features in this release.

IOS XE 26.1.1

There are no new hardware features in this release.

Change in behavior

To mitigate potential CRC errors on the Cisco IE3105 platform following a device reload, ensure that auto negotiation settings are consistent across both ends of the link (either enabled or disabled on both sides). We also recommend either replacing the **speed auto 100** command with **speed 100 duplex full** or configuring **speed auto 100** at both ends.

Syslog warning on reload for SSH Hostkeys

After a device reload, a syslog warning may appear indicating insufficient key length, even when a strong RSA or EC key is already configured.

Note:

- If the syslog warning message displays ***crypto key generate rsa modulus <modulus-size> label <label-name>,*** then 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 warnings:

© 2026 Cisco and/or its affiliates. All rights reserved.

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: Provision an SSH RSA hostkey with minimum modulus size of 3072 bits for enhanced security.

Sub mode: 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: Provision an SSH hostkey with minimum modulus size of 256 bits for enhanced security.

Sub mode: exec.

Parent CLI: Not Applicable.

If you have already configured a strong key and associated it using **ip ssh ec|rsa <keypair-name>**, you can ignore this warning during boot. The configured SSH keypair association is applied after the boot process, and SSH then uses the correct key for secure connections once the configuration is active.

FPGA profile

Starting with Cisco IOS XE Release 26.1.1, the switch uses updated FPGA profiles for different combinations of PRP, Redundancy, HSR-QuadBox, and DLR features. The DLR port assignments on the expansion module have also changed. For details, see the FPGA profile table in Configure FPGA Profile and the port-assignment information in Device Level Ring. The switch installs the default FPGA profile by default. During startup, the switch rejects any existing feature configurations that are not supported by the installed FPGA profile.

To retain existing feature configurations that are supported by the required FPGA profile, follow these steps:

1. After the switch starts, select the required FPGA profile. For more information about FPGA profiles, see the "Configure FPGA Profile" chapter of the Cisco IE3500 Series Switch Software Configuration Guide, Cisco IOS XE 26.1.x.

Important: Do not copy the running configuration to the startup configuration or enter the write memory command.

2. Reload the switch.

After the reload, the switch retains the existing feature configurations that are supported by the selected FPGA profile.

© 2026 Cisco and/or its affiliates. All rights reserved.

Resolved issues

This section lists resolved issues in Cisco IOS XE Release 26.1.x

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

IOS XE 26.1.2

Table 2. Resolved issues in release 26.1.2

Bug ID	Description
CSCwt56767	Serial number printed on physical device does not match the serial number in software.
CSCwt94316	IE3505 L2NAT - inside/private communication failing
CSCwt45045	IE-3500:Observing assert and clear syslog alarms messages when contact alarm is triggered.The alarm is in not asserted state when the contact is closed.
CSCwt94165	Input Errors on Peer would not process packets from IE-3500

IOS XE 26.1.1

Table 3. Resolved issues in release 26.1.1

Bug ID	Description
CSCwr77016	Cisco IOS XE Software for Cisco Catalyst and Rugged Series Switches Secure Boot Bypass Vulnerability.

Open issues

This section lists open issues in Cisco IOS XE Release 26.1.x

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

IOS XE 26.1.2

No customer-impacting bugs were identified in this release.

IOS XE 26.1.1

Table 4. Open issues in release 26.1.1

Bug ID	Description
CSCwt56767	Serial number printed on physical device does not match the serial number in software
CSCwt94316	IE3505 L2NAT - inside/private communication failing

© 2026 Cisco and/or its affiliates. All rights reserved.

Known issues

This section lists known issues in Cisco IOS XE Release 26.1.x

IOS XE 26.1.2

There are no known issues in this release.

IOS XE 26.1.1

There are no known issues in this release.

Supported hardware

This section lists supported hardware information.

Table 5. Supported IE3500 SKUs

PID	Uplink Ports			Downlink Ports		
	Type	Ports	Interface name	Type	Ports	Interface name
IE-3500-8T3S	SFP/SFP+	3	Gigabit Ethernet 1/1-3	Copper	8	Gigabit Ethernet 1/4-11
IE-3500-8P3S						
IE-3505-8T3S						
IE-3505-8P3S						
IE-3500-8U3X			TenGigabit Ethernet 1/1-3			
IE-3500-8T3X						

Table 6. Supported IE3500H SKUs

System	PIDs	SW	Uplinks	Downlinks	Data Path FPGA	PoE	Alternate PIDs (TAA and COO)
All Gig Copper	IE-3500H-8T	Network Essentials or Network Advantage	4x1G Copper	4x1G Copper	No	No	none
	IE-3500H-16T			12x1G Copper			none
	IE-3500H-24T			20x1G Copper			
Mixed Gig/GE Copper	IE-3500H-12FT4T			12xFE Copper	No	No	none
	IE-3500H-20FT4T			20xFE Copper			

© 2026 Cisco and/or its affiliates. All rights reserved.

System	PIDs	SW	Uplinks	Downlinks	Data Path FPGA	PoE	Alternate PIDs (TAA and COO)
Advanced Copper	IE-3505H-16T			12x1G Copper	Yes	No	none
PoE	IE-3500H-14P2T		2x1G Copper	14x1G Copper	No	Yes	none
	IE-3500H-12P2MU2X		2x10G SFP	12x1G PoE and 2xMGig UPoE			

Supported expansion modules

Table 7. Supported expansion modules

PID	Downlink Ports		
	Type	Ports	Interface name
IEM-3500-16P	Copper RJ45	16 PoE	Gigabit Ethernet 2/1-16
IEM-3500-16T		16	Gigabit Ethernet 2/1-16
IEM-3500-8P		8 PoE	Gigabit Ethernet 2/1-8
IEM-3500-8T		8	Gigabit Ethernet 2/1-8
IEM-3500-4MU		4 PoE	Gigabit Ethernet 2/1-4
IEM-3500-8S	SFP	8	Gigabit Ethernet 2/1-8
IEM-3500-14T2S	Copper RJ45/ SFP	Copper RJ45: 14 SFP: 2	Gigabit Ethernet 2/1-16
IEM-3500-6T2S		Copper RJ45: 6 SFP: 2	Gigabit Ethernet 2/1-8

Web UI system requirements

The Web UI is a web browser-based switch management tool that runs on the switch.

Minimum hardware requirements

Table 8. Minimum hardware requirements

Processor Speed	DRAM	Number of colors	Resolution
233 MHz minimum 1 GHz recommended	512 MB 1 GB recommended	256	1280 x 800 or higher

© 2026 Cisco and/or its affiliates. All rights reserved.

Operating systems

- Windows 10 or later
- Mac OS X 10.9.5 or later

Browsers

- Google Chrome: Version 59 or later (On Windows and Mac)
- Microsoft Edge
- Mozilla Firefox: Version 54 or later (On Windows and Mac)
- Safari: Version 10 or later (On Mac)

Supported software packages

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 platform configuration.
- Use the **show version** privileged EXEC command to display the software version running on the switch. The model name displayed at the end of the output reflects the factory configuration and does not change after software license upgrades.
- Use the **dir filesystem:** privileged EXEC command to view the names and versions of software images stored in flash memory.

Software images for Cisco IOS XE 26.1.x

This table provides the file names for the Cisco IOS XE 26.1.x software images for Cisco IE3500 Series Switches.

Table 9. Software package for Cisco IOS XE Release 26.1.x

Release	Image Type	Platform	File Name
Cisco IOS XE 26.1.2	Universal	IE3500, IE3505, IE3500H and IE3505H	ie35xx-universalk9.26.01.02.SPA.bin
Cisco IOS XE 26.1.1	Universal	IE3500, IE3505, IE3500H and IE3505H	ie35xx-universalk9.26.01.01.SPA.bin

Automatic boot loader upgrade

When you upgrade from the existing Cisco IOS XE release on your switch to a later or newer Cisco IOS XE release for the first time, the boot loader may be automatically upgraded based on the hardware version of the switch. If a boot loader upgrade occurs, it takes effect on the next reload.
For later Cisco IOS XE releases, if a new boot loader is included, it may also be automatically upgraded when the new image is booted for the first time.

Caution: Do not power cycle your switch during the upgrade.

Software installation commands

For a successful install, Cisco recommends having free space in flash equal to at least twice the image size. If insufficient space is available, remove inactive packages with **install remove inactive** command or

© 2026 Cisco and/or its affiliates. All rights reserved.

manually delete unnecessary files such as old core files or any other files that occupy a large amount of space in flash.

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

Table 10. Summary of software installation commands for install mode

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

Related resources

Table 11. Additional references for Cisco IE3500 Rugged and IE3500 Heavy Duty Series Switches

Document	Description
Cisco IOS XE	Provides information about Cisco IOS XE.
Cisco Warranty Finder	Provides warranty information for a specific product or product family.
Cisco IE3500 Rugged Series Switches	Provides information about Cisco IE3500 Rugged Series Switches.
Cisco IE3500H Heavy Duty Series Switches.	Provides information about Cisco IE3500 Heavy Duty Series Switches.
Cisco Validated Designs	Provides information about Cisco Validated Designs.
Cisco Profile Manager	Provides timely and relevant information from Cisco.
Cisco Services	Provides the business outcomes and technical support services needed to maximize the value of your Cisco technologies.
Cisco Support	You can submit a service request here.
Cisco DevNet	Enables you to discover and browse secure, validated, enterprise-class applications, products, solutions, and services.
Cisco Press	Provides general networking, training, and certification titles.
Cisco Support Community	You can ask and answer questions, share suggestions, and collaborate with your peers.
Cisco TAC	Provides the 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.

© 2026 Cisco and/or its affiliates. All rights reserved.

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

Legal information

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. 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.

© 2026 Cisco Systems, Inc. All rights reserved.