Release Notes for Cisco IE3500 Series Switches, Release 17.18.x

Contents

Cisco Catalyst IE3500 Series Switches, Release 17.18.x 3
New software features 3
New hardware features 4
Change in behavior 4
Resolved issues 6
Open issues 6
Known issues 7
Supported hardware 7
Supported software packages 9
Related resources 10
Legal information 10

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Catalyst IE3500 Series Switches, Release 17.18.x

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

Cisco IE3500/IE3505 Series Switches

These ruggedized switching platforms provide superior bandwidth and high PoE power for industrial environments. They are hardened to withstand temperatures ranging from freezing cold to extreme heat (-40°C to +75°C or -40°F to 167°F), as well as severe shock and vibration.

The IE3500 switch is designed for hardened deployments, including factory automation, smart cities, energy and process control, transportation systems, and mining. They bring improved scale performance, built-in security feature set, and simplified management options for the switch. For more information, refer to the Datasheet.

Cisco IE3500H/IE3505H Series Switches

These are the next-generation managed IP67 switches powered by Cisco IOS XE and are ideal for deployment in the harshest environments. They are IP67-rated for water and dust resistance and are hardened to withstand temperatures ranging from freezing cold to extreme heat (-40°C to +75°C or -40°F to 167°F), as well as 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 be configured to operate at 100M speed. 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 240 W power budget and support PoE, PoE+, and Universal Power over Ethernet at 60 W.

These switches are equipped with advanced network-based security, segmentation, and visibility features for the most demanding industrial environments. They extend the power of intent-based networking to the harshest Internet of Things (IoT) edge, with use cases in industries such as mining, railways, and manufacturing. The switches can be wall mounted and deployed without a housing cabinet. For more information, refer to the Datasheet.

New software features

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

IOS XE 17.18.4

There are no new software features in this release.

IOS XE 17.18.3

There are no new software features in this release.

IOS XE 17.18.2

There are no new software features in this release.

IOS XE 17.18.1

Table 1. New software features in release 17.18.1

© 2025 Cisco and/or its affiliates. All rights reserved.

Product Impact	Feature	Description
Ease of Use	VLAN 0 priority tagging	This feature enables prioritization of critical traffic using 802.1Q frames with a VLAN ID of zero, ensuring higher processing priority without VLAN assignment.
	Product Analytics	Cisco IOS XE Product Analytics collects device Systems Information for the purposes of understanding product usage, enabling product improvements and product development, and assisting in product adoption and sales support. Only summarized data of feature usage and statistical counters of configuration are collected. No personally identifiable information, such as MAC/IP addresses, usernames, custom configuration names, or user-provided strings, are collected as part of Cisco IOS XE Product Analytics. Cisco processes this data following the General Terms, the Cisco Privacy Statement, and any other applicable agreement with Cisco. See Cisco Enterprise Networking Product Analytics Frequently Asked Questions.
	BGP EVPN over VXLAN	This feature allows you to simplify network management and scale easily with VXLAN overlays on your existing infrastructure. BGP EVPN as the control plane ensures efficient MAC and IP distribution.

New hardware features

IOS XE 17.18.4

There are no new hardware features in this release.

IOS XE 17.18.3

There are no new hardware features in this release.

IOS XE 17.18.2

There are no new hardware features in this release.

IOS XE 17.18.1

There are no new hardware features in this release.

Change in behavior

Notice of upcoming changes 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 begins 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.

© 2025 Cisco and/or its affiliates. All rights reserved.

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 generate warnings in releases beyond the version Cisco IOS XE 17.18.1. The release notes for each release describe 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.

© 2025 Cisco and/or its affiliates. All rights reserved.

- **TACACS+ using pre-shared keys and MD5**
  Recommendation: Use TACACS+ over TLS 1.3, introduced in 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 continue to support these features but display warnings if they are used. Future release trains may impose additional restrictions on these features which will be communicated through release notes. For more information, see Resilient Infrastructure IOS XE Security Warnings Reference.

Resolved issues

IOS XE 17.18.4

There are no resolved issues in this release.

IOS XE 17.18.3

There are no resolved issues in this release.

IOS XE 17.18.2

There are no resolved issues in this release.

IOS XE 17.18.1

There are no resolved issues in this release.

Open issues

IOS XE 17.18.4

Table 2. Open issues in release 17.18.4

Bug ID	Description
CSCwt64311	IE9K/IE3505: Padding is not working correctly with vlan tag when PRP is enabled
CSCwt56767	Serial number printed on physical device does not match the serial number in software
CSCwt94316	IE3505 L2NAT - inside/private communication failing
CSCwt94165	Input Errors on Peer would not process packets from IE-3500
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.

IOS XE 17.18.3

Table 3. Open issues in release 17.18.3

Bug ID	Description
CSCwt56767	Serial number printed on physical device does not match the serial number in software

IOS XE 17.18.2

There are no open issues in this release.

© 2025 Cisco and/or its affiliates. All rights reserved.

IOS XE 17.18.1

There are no open issues in this release.

Known issues

There are no known issues in this release.

Supported hardware

Table 4. 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 5. Supported IE3500H SKUs

System	PIDs	Software	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			
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			

© 2025 Cisco and/or its affiliates. All rights reserved.

Supported expansion modules

Table 6. 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/ SFP+	8	Gigabit Ethernet 2/1-8
IEM-3500-14T2S	Copper RJ45/ SFP/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. The following subsections list the hardware and software required to access the Web UI.

Minimum hardware requirements

Table 7. Minimum hardware requirements

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

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)

© 2025 Cisco and/or its affiliates. All rights reserved.

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 device configuration.
- You can use the show version privileged EXEC command to see the software version that is running on your switch.

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 17.18.x

The following table provides the file names for the IOS XE 17.18.x software images for Cisco Catalyst IE3500 Series Switches.

Table 8. Software package for Cisco Catalyst IE3500 Series Switches, Release 17.18.x

Release	Image Type	Platform	File Name
Cisco IOS XE 17.18.1	Universal	IE3500, IE3505, IE3500H and IE3505H	ie35xx-universalk9.17.18.01.SPA.bin
Cisco IOS XE 17.18.2	Universal	IE3500, IE3505, IE3500H and IE3505H	ie35xx-universalk9.17.18.02.SPA.bin
Cisco IOS XE 17.18.3	Universal	IE3500, IE3505, IE3500H and IE3505H	ie35xx-universalk9.17.18.03.SPA.bin
Cisco IOS XE 17.18.4	Universal	IE3500, IE3505, IE3500H and IE3505H	ie35xx-universalk9.17.18.04.SPA.bin

Automatic bootloader upgrade

When you upgrade from the existing release on your switch to a later or newer release for the first time, the bootloader may be automatically upgraded, based on the hardware version of the switch. If the bootloader is automatically upgraded, it will take effect on the next reload.

For subsequent Cisco IOS XE Releases, if there is a new bootloader in that release, it may be automatically upgraded based on the hardware version of the switch when you boot up your switch with the new image for the first time.

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

Software installation commands

Note: For the **install** command to be successful, it is recommended to have a minimum of free space that is twice the size of the image in flash. If there is not enough space available in flash, you are advised to free up space in flash either by issuing the **install remove inactive** command or to manually clean up the flash by removing unwanted 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—
install add file *filename* [**activate commit**]

© 2025 Cisco and/or its affiliates. All rights reserved.

Table 9. 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 10. Additional content for Cisco Catalyst IE3500 Rugged Series Switch

Document	Description
Cisco Warranty Finder	Provides warranty information for a specific product or product family.
Cisco Validated Designs	Provides Cisco-validated designs for deploying reliable and tested solutions.
Cisco Profile Manager	To receive timely, relevant information from Cisco, sign up here.
Cisco Services	Provides services that help you deploy, manage, optimize, and secure Cisco technologies to achieve your business outcomes.
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 Cisco-authorized books, e-books, and digital learning resources for Cisco products and technologies.
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.
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.

© 2025 Cisco Systems, Inc. All rights reserved.