Release Notes for Cisco Catalyst IE3x00, IE3400 Heavy Duty, and ESS3300 Series Switches, Release 26.1.x

Cisco Catalyst IE3x00, IE3400 Heavy Duty, and ESS3300 Series Switches, Release 26.1.x

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

- Cisco Catalyst IE3x00 Rugged Series
- Cisco Catalyst IE3400 Heavy-Duty Series
- Cisco Embedded Services 3300 Series

Cisco Catalyst IE3x00 Rugged Series Switches feature advanced, full Gigabit Ethernet speed for rich real-time data—and a modular, optimized design. These Cisco rugged switches bring simplicity, flexibility and security to the network edge, and are optimized for size, power, and performance.

From their end-to-end security architecture to delivering centralized automation and scale with Cisco

intent-based networking, the Cisco Catalyst IE3x00 family is the perfect solution to your switching needs in almost any use case.

Cisco Embedded Services 3300 Series Switches (ESS3300) revolutionize Cisco's embedded networking portfolio with 1G/10G capabilities. ESS3300 switches are optimized to meet specialized form-factor, ruggedization, port density, and power needs of many applications requiring customization. They complement Cisco's off-the-shelf Industrial Ethernet switching portfolio.

On ESS3300, the small form factor, board configuration options, and optimized power consumption provide Cisco partners and integrators the flexibility to design custom solutions for defense, oil and gas, transportation, mining, and other verticals. The ESS3300 runs the trusted and feature-rich Cisco IOS-XE Software, allowing Cisco partners and integrators to offer their customers the familiar Cisco IOS CLI and management experience on their ESS3300 solutions.

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. 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.

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 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. 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. ▪ 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. ▪ 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. For more information, refer this document Cisco C9000 Switching IOS XE – Resilient Infrastructure Playbook.
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 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.
Ease of use	Industrial Asset Discovery Completion	Industrial Asset Auto-Discovery feature automatically identifies, and catalogs directly connected industrial devices without impacting network performance. This feature exports inventory data to a syslog server in JSON format, streamlining asset tracking, security enforcement, and the detection of unauthorized hardware.

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 resolved issues for 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
CSCwo96008	PTP not processed/forwarded on ESS3300 running 17.12.04
CSCwp24973	Support for SFP 10G-SR-S in Profinet Module
CSCwq73986	connectivity issue between ccv-sensor-app and default gateway
CSCwr62046	ICMPv6 packets are duplicated when device tracking is enabled on the interface
CSCwr81607	IE3400 SNMP Multicast Counters not working - ifOutMulticastPkts
CSCwr90222	IE3400:Padding is not working correctly with vlan tag when PRP is enabled
CSCws17503	Broadcast traffic is leaking over a routed port
CSCwt13348	switchport block multicast not working after switch reload or shut/no shut on interface
CSCwp05951	IE3400 increments input/CRC/L2nat discards/Ethernet-controller stats unexpectedly with L2nat config.
CSCwp38345	DHCP snooping dropping DHCP discover message for non CDP devices
CSCwp38501	IE-3300-8T2S-E switch not forwarding STCN packet intermittently
CSCwp84508	Device with IPv6 ACL applied on 13 or more interfaces crashes on reload
CSCwq21589	IE3400H: FTP fails between port G1/1 and G1/2 with L2NAT
CSCwq80434	With " reload" command, switchports stay up for an extended time after the switch stops forwarding traffic.
CSCwr05475	IE3400 - 17.12.3 - Memory Leak observed in SNMP ENGINE
CSCwr42830	IE3300 - MKA session fails to come up after upgrade or power cycle

Bug ID	Description
CSCws18543	Rate limit is failing when there is L2 Loop
CSCws31153	Hardening of IP Default Gateway removal

Open issues

This table 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

Table 3. Open issues in release 26.1.1

Bug ID	Description
CSCwt38298	IE3200 Memory Leak in Pool Manager and Possible Crashes
CSCwt65703	IOS image corrupted on sdflash
CSCwt68784	[ESS-3300]: RADIUS packets routed via Mgmt-vrf when " ip vrf forwarding" and " source-interface" is configured in the server group

Known issues

This section lists the limitations.

PoE configuration on Cisco Catalyst IE3x00 Switch

Even when using power supplies that can provide up to a supported maximum (for example, 170W, 240W, or 480W) for the PoE budget, the PoE budget for the IE3x00 defaults to 125W regardless of the power supplies used. You can configure the power budget to use the maximum.

Note: Before changing the power budget, the minimum power requirements for the switch need to be considered as well. Please refer to the data sheet for your switch for more details.

The attached power supply powers the IE3x00 switch operation as well as PoE power. When increasing the maximum PoE budget, you must subtract the power draw of the IE3x00 switch from the capacity of the attached power supply. You do so to prevent the IE3x00 switch from overdrawing the capacity of the attached power supply. For example, the IE3400 switch with an expansion module supports a maximum PoE budget of 480W. The IE3400-8P2S with an attached IEM-3400-8P draws 67W. With a 480W capacity power supply, the maximum you should configure the PoE budget is (480W-67W) 413W.

To use the power supply's maximum supported wattage for the PoE budget, configure the power supply max wattage in global configuration mode as follows:

1. Verify the maximum amount that the power supplies support for the PoE budget.
2. Subtract the operating power of the IE3x00 switch according to its datasheet from the maximum capacity of the power supply. This is your max PoE budget.

3. Enter **power inline max** *max-wattage* to increase the PoE budget based on the power supplies used.
4. *max-wattage* is the maximum available PoE power.

IE3200 and IE3300 with 10Mbps or 100Mbps speed in Half-Duplex Mode

CRC errors were observed on the IE3200 and IE3300 platforms when the switch is configured with 10Mbps or 100Mbps speed in half-duplex mode.

As a workaround, configure no ptp enable on the half-duplex interface. This improves ingress and egress latencies considerably and ensures that there are no late collisions (and therefore, no CRC errors).

The issue and workaround apply to Cisco IOS-XE releases 17.3.5 and later.

L3 ACL limitation on usage of L4OP in ACLs

Layer 4 Operator (L4OP) in ACLs is limited by the hardware to a maximum of 8 L4OP (range and gt) for UDP and 8 L4OP for TCP, for a total of 16 global L4OP. Keep in mind that the **range** operator consumes 2 L4OP.

The L4OPs include: gt (greater than), lt (less than), neq (not equal), eq (equal), range (inclusive range).

Note: The eq does not consume L4OPs. For more information see QoS Configuration Guide.

Compatibility

Refer to Cisco IOS-XE Migration Guide for IIoT Switches for software upgrade and downgrade information for Cisco Catalyst IE3x00, IE3400 Heavy Duty, and ESS3300 Series Switches, Release 26.1.x.

Supported hardware

This section lists the hardware support information.

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:

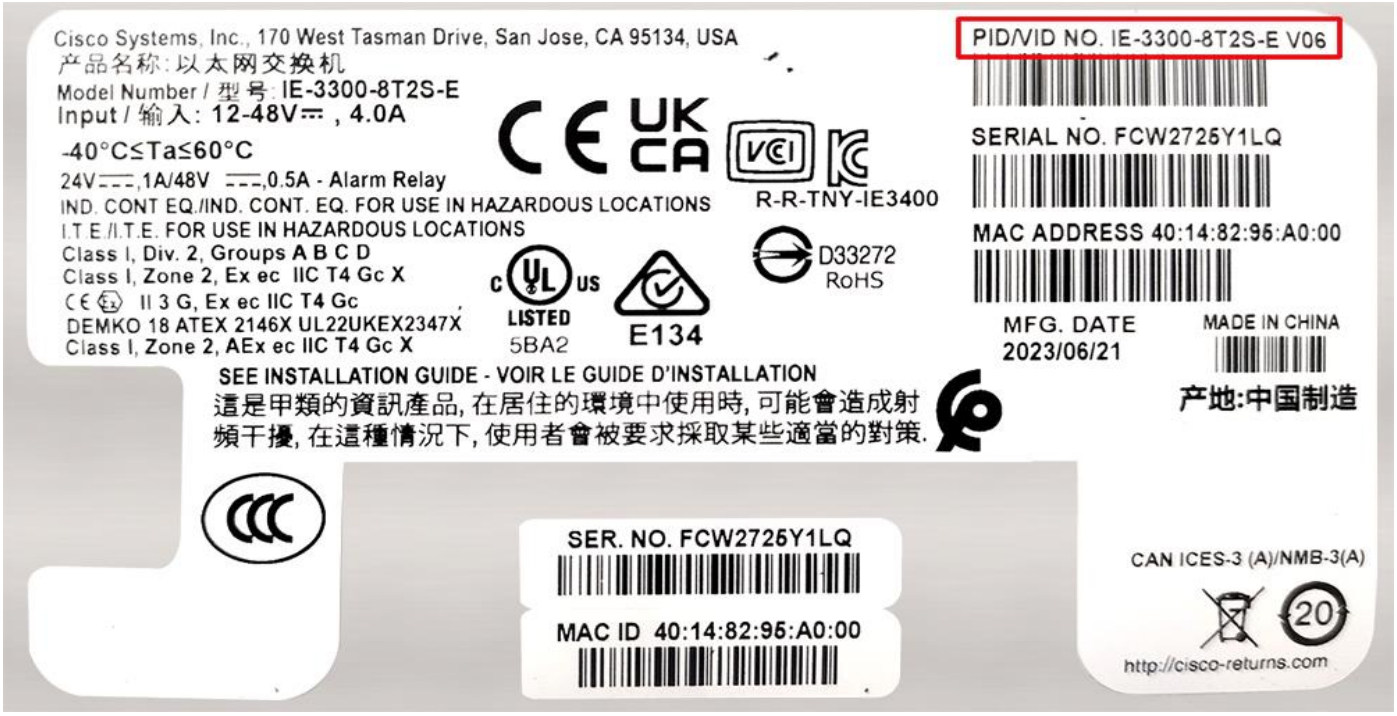
- Key Exchange algorithm:
  - diffie-hellman-group14-sha1
- MAC algorithms:
  - hmac-sha1
  - hmac-sha2-256
  - hmac-sha2-512

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.

IOx support for Cisco Catalyst IE3300 Switches

To see if the IE-3300-8P2S switch or IE-3300-8T2S switch supports IOx application environment, check the Hardware Version ID on the switch label. The Hardware Version ID is in the upper-right corner of the label, as shown in the following illustration. Support for the feature is available only with Hardware Version ID 06 or later. In the following

illustration, the Version ID appears as " V06" at the end of the string inside the red rectangle in the upper-right corner of the label.



You also can see the Version ID by entering the **show version** command and examining the output, as shown in the following example:

```
IE-3300# show version
Base Ethernet MAC Address : b0:c5:3c:99:c8:a0
Motherboard Assembly Number : 73-101289-11
Motherboard Serial Number : FOC27151WEZ
Model Revision Number : V06
Motherboard Revision Number : B
Model Number : IE-3300-8T2S
System Serial Number : FCW2507P4CV
Top Assembly Part Number : 68-102662-01
Top Assembly Revision Number : B0
System FPGA version : 0.89.2
CIP Serial Number : 0x1999C8A0
SKU Brand Name : Cisco
```

IE-3300-8U2X and IE-3300-8T2X switches have supported IOx since the Cisco IOS-XE 17.4.1 release.

Startup configuration is always read from Flash

From Cisco IOS-XE release 17.10.1, the startup configuration is always read from flash. The latest configuration is available only in flash when you save the running config, irrespective of the booted media (for example, flash, sdflash, or usbflash) and the boot mode (install or bundle). If a switch cannot find a configuration in flash, it will try to find one in sdflash.

Note: Starting from the Cisco IOS-XE release 17.10.1, you can configure Cisco Catalyst embedded switches to use USB Flash as the primary boot device.

SMU installation: Boot in Install mode

Software Maintenance Upgrade (SMU) installation is no longer supported in bundle mode. Previously, SMU installation was supported in both bundle boot and install mode. Beginning in Cisco IOS-XE 17.9.1, SMU supports patching using install mode only.

SMU installation stops if the device is booted up in bundle mode and syslog messages are displayed. You must boot the switch in install mode to support SMU installation.

If the device is booted up in install mode, SMU installation continues to work as before.

IE3400: Hardware changes may require action

Some hardware components on the Cisco Catalyst IE3400 Rugged Series and Cisco Catalyst IE3400 Heavy Duty Series switches have changed. The changes, which are automatically handled by the IOS-XE software, do not affect switch functionality or the ordering process. New units shipped after May 31, 2022 have the hardware change.
However, you may need to upgrade the software, depending on which base switch and expansions module you have, as shown in the following table.

Note: For detailed information about affected hardware versions, supported software releases, and instructions for different scenarios, see Field Notices on Cisco.com.

If you have...	then...
Older versions (shipped before May 31, 2022) of the base switch and expansion module	No action is required.
Newer versions (shipped after May 31, 2022) of the base switch and expansion module	Deploy one of the supported releases of IOS-XE. Refer to Field Notices on Cisco.com for details that are appropriate to your deployment.
Newer version of the base switch with an older version of the expansion module	Deploy one of the supported releases of IOS-XE. Refer to Field Notices on Cisco.com for details that are appropriate to your deployment.
Older version of the base switch with a newer version of the expansion module	Deploy one of the supported releases of IOS-XE. Refer to Field Notices on Cisco.com for details that are appropriate to your deployment.

FPGA profile

FPGA Profile is supported in Cisco IOS-XE release 17.8 and later. In a Cisco IOS-XE upgrade from an earlier release that does not support FPGA Profile, for example, an upgrade from Cisco IOS-XE 17.7.1 to 17.8.1, the default FPGA Profile is installed. Any features controlled by FPGA Profile that are configured in the switch running the earlier release and that are not included in the default profile will be rejected.

Note: This feature is supported for Cisco Catalyst IE3400 Rugged Series Switches and Cisco Catalyst IE3400 Heavy-Duty Series Switches.

For example, CTS IPv6 is not supported in the default profile, so CTS IPv6 configurations are rejected during bootup after the upgrade. Similarly, after a Cisco IOS-XE upgrade where the cts-ipv6 profile is loaded, existing PRP configurations are rejected upon bootup.

To keep the existing profile and feature configurations after an upgrade:

1. After booting the switch, selected the required FPGA Profile as described in " Changing the FPGA Profile" , in System Management Configuration Guide, Cisco Catalyst IE3x00 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches, chapter " Configuring FPGA Profile" .

   Do not copy running-config to startup-config or write memory.

2. Reload the switch.

The required feature configurations will not be discarded because they are supported by the selected profile.

Cisco Catalyst IE and ESS Switches: Model numbers

This table lists the supported hardware models and the default license levels they are delivered with. For information about the available license levels, see section *License Levels.*

Table 4. Hardware models and their default license levels

Model Number	Default License Level	Description
ESS-3300-NCP-E	Network Essentials	Main Board without a cooling plate 2 ports of 10 GE fiber, 8 ports of GE copper. 4 of the 8 GE copper ports can also be combo ports. Terminal Power: 16W
ESS-3300-NCP-A	Network Advantage	Main Board without a cooling plate 2 ports of 10 GE fiber, 8 ports of GE copper. 4 of the 8 GE copper ports can also be combo ports. Terminal Power: 16W
ESS-3300-CON-E	Network Essentials	Main Board conduction cooled 2 ports of 10 GE fiber, 8 ports of GE copper. 4 of the 8 GE copper ports can also be combo ports Terminal Power: 16W
ESS-3300-CON-A	Network Advantage	Main Board conduction cooled 2 ports of 10 GE fiber, 8 ports of GE copper. 4 of the 8 GE copper ports can also be combo ports Terminal Power: 16W
ESS-3300-24T-NCP-E	Network Essentials	Main Board with a 16p Expansion Board without a cooling plate 2 ports of 10 GE fiber, 24 ports of GE copper 4 of 8 GE ports can be combo ports on mainboard 4 of 16 GE ports can be combo ports on expansion board Terminal Power: 24W
ESS-3300-24T-NCP-A	Network Advantage	Main Board with a 16p Expansion Board without a cooling plate 2 ports of 10 GE fiber, 24 ports of GE copper 4 of 8 GE ports can be combo ports on mainboard 4 of 16 GE ports can be combo ports on expansion board

Model Number	Default License Level	Description
		Terminal Power: 24W
ESS-3300-24T-CON-E	Network Essentials	Main Board with a 16p Expansion Board conduction cooled 2 ports of 10 GE fiber, 24 ports of GE copper 4 of 8 GE ports can be combo ports on mainboard 4 of 16 GE ports can be combo ports on expansion board Terminal Power: 24W
ESS-3300-24T-CON-A	Network Advantage	Main Board with a 16p Expansion Board conduction cooled 2 ports of 10 GE fiber, 24 ports of GE copper 4 of 8 GE ports can be combo ports on mainboard 4 of 16 GE ports can be combo ports on expansion board Terminal Power: 24W
IE-3200-8T2S-E	Network Essentials	8 x Gigabit Ethernet 10/100/1000 RJ45 ports, 2 fiber 100/1000 SFP-based ports, non-PoE
IE-3200-8P2S-E	Network Essentials	8 x Gigabit Ethernet 10/100/1000 PoE/PoE+ ports, 2 fiber 100/1000 SFP-based ports; PoE power budget of 240W
IE-3300-8T2S-E	Network Essentials	8 x Gigabit Ethernet 10/100/1000 RJ45 ports, 2 fiber 100/1000 SFP-based ports, non-PoE
IE-3300-8P2S-E	Network Essentials	8 x Gigabit Ethernet 10/100/1000 PoE/PoE+ ports, 2 fiber 100/1000 SFP-based ports; PoE power budget of 360W (including expansion module)
IE-3300-8T2S-A	Network Advantage	8 x Gigabit Ethernet 10/100/1000 RJ45 ports, 2 fiber 100/1000 SFP-based ports, non-PoE
IE-3300-8P2S-A	Network Advantage	8 x Gigabit Ethernet 10/100/1000 PoE/PoE+ ports, 2 fiber 100/1000 SFP-based ports; PoE power budget of 360W (including expansion module)
IE-3300-8T2X-A	Network Advantage	8 x Gigabit Ethernet 10/100/1000 RJ45 ports, 2 fiber 1/10 Gigabit Ethernet SFP-based ports, non-PoE
IE-3300-8T2X-E	Network Essentials	8 x Gigabit Ethernet 10/100/1000 RJ45 ports, 2 fiber 1/10 Gigabit Ethernet SFP-based ports, non-PoE
IE-3300-8U2X-E	Network Essentials	8 x Gigabit Ethernet 10/100/1000 4PPoE (802.3bt type 3) ports, 2 fiber 1/10 Gigabit Ethernet SFP-based ports; PoE power budget of 480W
IE-3300-8U2X-A	Network Advantage	8 x Gigabit Ethernet 10/100/1000 4PPoE (802.3bt type 3) ports, 2 fiber 1/10 Gigabit Ethernet SFP-based ports; PoE power budget of 480W (requires and expansion module to deliver 480W)
IE-3400-8T2S-E	Network Essentials	8 x Gigabit Ethernet 10/100/1000 RJ45 ports, 2 fiber 100/1000 SFP-based ports, non-PoE

Model Number	Default License Level	Description
IE-3400-8T2S-A	Network Advantage	8 x Gigabit Ethernet 10/100/1000 RJ45 ports, 2 fiber 100/1000 SFP-based ports, non-PoE
IE-3400-8P2S-E	Network Essentials	8 x Gigabit Ethernet 10/100/1000 RJ45 ports, 2 fiber 100/1000 SFP-based ports with PoE
IE-3400-8P2S-A	Network Advantage	8 x Gigabit Ethernet 10/100/1000 RJ45 ports, 2 fiber 100/1000 SFP-based ports with PoE
IE-3400H-8T-E	Network Essentials	8 x 1-Gbps X-Coded ports, 1 Alarm input and 1 Alarm output, 1 Console port, mini-change input for Single power source
IE-3400H-8T-A	Network Advantage	8 x 1-Gbps X-Coded ports, 1 Alarm input and 1 Alarm output, 1 Console port, mini-change input for Single power source
IE-3400H-8FT-E	Network Essentials	8 x 100-Mbps D-coded ports, 1 Alarm input and 1 Alarm output, 1 Console port, Mini-change input for Single Power Source
IE-3400H-8FT-A	Network Advantage	8 x 100-Mbps D-coded ports, 1 Alarm input and 1 Alarm output, 1 Console port, Mini-change input for Single Power Source
IE-3400H-16T-E	Network Essentials	16 x 1-Gbps X-Coded ports, 1 Alarm input and 1 Alarm output, 1 Console port, mini-change input for Single power source
IE-3400H-16T-A	Network Advantage	16 x 1-Gbps X-Coded ports, 1 Alarm input and 1 Alarm output, 1 Console port, mini-change input for Single power source
IE-3400H-16FT-E	Network Essentials	16 x 100-Mbps D-coded ports, 1 Alarm input and 1 Alarm output, 1 Console port, Mini-change input for Single Power Source
IE-3400H-16FT-A	Network Advantage	16 x 100-Mbps D-coded ports, 1 Alarm input and 1 Alarm output, 1 Console port, Mini-change input for Single Power Source
IE-3400H-24T-E	Network Essentials	24 x 1-Gbps X-Coded ports, 1 Alarm input and 1 Alarm output, 1 Console port, mini-change input for Single power source
IE-3400H-24T-A	Network Advantage	24 x 1-Gbps X-Coded ports, 1 Alarm input and 1 Alarm output, 1 Console port, mini-change input for Single power source
IE-3400H24FT-E	Network Essentials	24 x 100-Mbps D-coded ports, 1 Alarm input and 1 Alarm output, 1 Console port, Mini-change input for Single Power Source
IE-3400H-24FT-A	Network Advantage	24 x100-Mbps D-coded ports, 1 Alarm input and 1 Alarm output, 1 Console port, Mini-change input for Single Power Source

WebUI system requirements

The WebUI is a web browser-based switch management tool that runs on the switch. These subsections list the hardware and software required to access the WebUI.

Minimum hardware requirements

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

Software requirements

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

This section provides information about the release packages associated with Cisco Catalyst IE3x00, IE3400 Heavy Duty, and ESS3300 Series Switches.

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:)
- 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 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 5. Software packages for release 26.1.x

Release	Image Type	Platform	File Name
Cisco IOS-XE.26.1.x	Universal	IE3x00 (IE3200, IE3300, IE3400, and IE3400H)	ie3x00-universalk9.26.01.01.SPA.bin
		ESS3300	ess3x00-universalk9.26.01.01.SPA.bin

Automatic boot loader upgrade

When you upgrade from the existing release on your switch to a later or newer release for the first time, the boot loader may be automatically upgraded, based on the hardware version of the switch. If the boot loader 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.

Scenario	Automatic Boot Loader Response
If you boot Cisco IOS-XE the first time	Boot loader may be upgraded to version "8.1.2" for IE3x00 and ESS-3300. `Checking Bootloader upgrade... … Bootloader upgrade successful`

Software installation options

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

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.

This table lists the options for the install command for the Cisco Catalyst IE3x00, IE3400 Heavy Duty, and ESS3300 Series Switches.

Table 6. Summary of software installation commands for install mode

Option	Description
activate[auto-abort-timer]	Activates the file and reloads the device. The auto-abort-timer keyword automatically rolls back image activation.
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.
commit	Commit the changes to the load path.
remove	Remove installed packages.

Related resources

Table 7. Additional references for Cisco Catalyst IE3x00, IE3400 Heavy Duty, and ESS3300 Series Switches

Document	Description
Cisco IOS-XE	Provides information about Cisco IOS-XE.
Cisco Catalyst IE3200 Rugged Series Switches	Provides information about Cisco Catalyst IE3200 Rugged Series Switches.

Document	Description
Cisco Catalyst IE3300 Rugged Series Switches	Provides information about Cisco Catalyst IE3300 Rugged Series Switches.
Cisco Catalyst IE3400 Rugged Series Switches	Provides information about Cisco Catalyst IE3400 Rugged Series Switches.
Cisco Catalyst IE3400H Heavy Duty Series Switches	Provides information about Cisco Catalyst IE3400H Heavy Duty Series Switches.
Cisco Catalyst ESS3300 Series Switches	Provides information about Cisco Catalyst ESS9300 Series Switches.
Cisco Validated Designs	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.
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 Feature Navigator	You can browse Cisco products and find relevant features. It also allows you to compare platforms, determine common features between products, and identify unique product features. The CFN also has a tab that provides a MIB Locator
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