Release Notes for Cisco Catalyst IE3x00 Rugged, IE 3400 Heavy Duty, and ESS3300 Series Switches, Cisco IOS XE Amsterdam 17.2.x

First Published: 2020-03-14

Last Modified: 2024-04-04

Introduction

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 and complement Cisco's off-the-shelf Industrial Ethernet switching portfolio.

On the 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–based solutions.

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

Cisco IOS-XE Release Schedule

Cisco IOS-XE releases generally follow the schedule as follows:

- Standard Maintenance (SM) Release - Defect fixes for 6 months, and PSIRT fixes for 6 months.
- Extended Maintenance (EM) Release - Defect fixes for 24 months, and PSIRT fixes for 12 months.

There are typically 3 major releases each year:

- End of March - Standard Maintenance
- End of July - Extended Maintenance
- End of November - Standard Maintenance

New Features for Cisco Catalyst IE and ESS Switches in Cisco IOS XE 17.2.1

The following features apply to both the IE3x00 and ESS3300 switches unless specifically mentioned.

Feature Name	License Level	Description, and Documentation Link Information
Express setup and Day 0 co-existence	Network Essentials and Advantage	Express setup is a switch manageability feature used by IoT customers for configuring the factory default switch to make it ready to plug into connected factory architecture. Prerequisite for express setup is switch must not be running non-default configuration. Perform 'short press' from the push button as per the user instruction guide, switch is going to be configured in the background made ready for the installation. Day-0 is a feature used by enterprise switches to make factory default switch configuration ready for management and control. Prerequisite for day-0 is same as in express setup feature, with day-0 user can configure IP address, VLAN Id, NTP server and new user creation.

Feature Name	License Level	Description, and Documentation Link Information
HSRP (IPv4 and IPv6)	Network Advantage	HSRP (Hot Standby Router Protocol) is a redundancy protocol to provide gateway redundancy without any additional configuration on the end devices in the subnet. With HSRP configured between a set of routers (treated as HSRP group or a standby group), they work in concert to present the appearance of a single virtual router to the hosts on the LAN. A single router elected from the group is responsible for forwarding the packets that hosts send to the virtual router. This router is known as the Active router. Another router is elected as the Standby router. In the event that the Active router fails, the Standby assumes the packet-forwarding duties of the Active router. Although an arbitrary number of routers may run HSRP, only the Active router forwards the packets sent to the virtual router. To minimize network traffic, only the Active and Standby routers send periodic HSRP messages once the protocol has completed the election process. If the Active router fails, the Standby router takes over as the Active router. If the Standby router fails or becomes the ACTIVE router, then another router is elected as the Standby router.
Boot from USB (Not supported on IE 3400H)	Network Essentials and Advantage	Supporting USB flash drive in bootloader will enable the switch to be able to boot software images from the USB flash drive. In bootloader, the functional behaviour of USB flash drive will be similar to that of SD cards.

Feature Name	License Level	Description, and Documentation Link Information
VRRP (IPv4 and IPv6)	Network Advantage	The Virtual Router Redundancy Protocol (VRRP). VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router controlling the IP address(es) associated with a virtual router is called the Master, and forwards packets sent to these IP addresses. The election process provides dynamic fail over in the forwarding responsibility should the Master become unavailable. This allows any of the virtual router IP addresses on the LAN to be used as the default first hop router by end-hosts. The advantage gained from using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host.
PBR (Policy Based Routing)	Network Advantage	PBR (Policy Based Routing) is a technique used to make routing decisions based on policies configured. When a Router/Switch receives a packet, forwarding decision is based on the destination IP Address of a packet, which is used to look up an entry in a routing table However, in some cases, there may be a need to forward the packet based on other criteria. e.g., Source IP address, not the Destination IP Address. This permits routing of packets originating from different sources to different networks even when the destinations are the same and can be useful when interconnecting several private networks.

Feature Name	License Level	Description, and Documentation Link Information
Routed Jumbo Frame Support	Network Essentials and Advantage	Jumbo frames are frames larger than the standard Ethernet frame size of 1518 bytes, which includes the Layer 2 header and Frame Check Sequence (FCS). In other words, jumbo frames refer to Ethernet packets of up to 9000 bytes in size. When the jumbo frame feature is enabled on a port, the port can switch large or jumbo frames. This feature optimizes server-to-server performance. The default Maximum Transmission Unit (MTU) frame size is 1548 bytes for all Ethernet ports. The jumbo frame MTU size is limited to 2000 for advanced SKUs(3400/3400H) and 8996 for other SKUs when jumbo frame feature is enabled on a port.
MSDP (Multicast Source Discovery Protocol)	Network Advantage	MSDP is often used between Anycast RP within a PIM domain to synchronize information about the active sources being served by each Anycast-RP peer (by virtue of IGP reachability). MSDP will be supported in inter domain deployments or in deployment where MSDP peering happens without BGP (MBGP). No claim for Intra domain deployments in this Phase as MBGP is not fully qualified for support.
Flow-based SPAN	Network Essentials and Advantage	FSPAN is used, in order to mirror the traffic based on filter cirteria. FSPAN supports three types of access control lists to the span session and filtering based on vlan.

Feature Name	License Level	Description, and Documentation Link Information
IPv4/IPv6 Multicast routing BSR	Network Advantage	BSR (Bootstrap) is a protocol that we use to automatically find RP in multicast network. BSR supports PIMv2 and its not cisco proprietary. From platform perspective infra is in place to handle control packets and BSR msg exchanges. Elected RP node info/address is not maintained at the PD level explicitly. RP election is a PI functionality and once after the RP election according to the populated S,G or *,G routes will be updated to elected RP. No specific configuration or show commands are in place from platform perspective
Auto RP (IPv4)	Network Advantage	A Rendezvous Point (RP) is a router in a multicast network domain that acts as a shared root for a multicast shared tree. Any number of routers can be configured to work as RPs and they can be configured to cover different group ranges. For correct operation, every multicast router within a Protocol Independent Multicast (PIM) domain must be able to map a particular multicast group address to the same RP. Auto-RP is a mechanism to automate distribution of RP information in a multicast network. The Auto-RP mechanism operates using two basic components, the candidate RPs and the RP mapping agents.

Feature Name	License Level	Description, and Documentation Link Information
IPv6 Multicast routing Embedded RP	Network Advantage	With this feature RP addresses are bound into Group addresses. No explicit configuration needs to be done to enable this feature. Initial Incoming Multicast data packets from source S to group G gets punted to CPU. When Flag field (4 bits) is set to 0111 (0x7) it indicates RP addresses is binded into Group address. Address with different Scope level (1,2,4,5,8,E) will be supported. No specific configuration or show commands are in place from platform perspective
IPv6 FHS RA Guard	Network Essentials and Advantage	Router advertisements can be used by hosts to automatically configure their own IPv6 address and set a default route using the information they see in the RA. Hosts automatically select a router advertisement and they don't care where it came from. This is how it was meant to be, but it does introduce a security risk since any device can send router advertisements and your hosts will happily accept it. An attacker can send rogue router advertisements to redirect the traffic, or you can send so many RAs that it causes a DOS since your hosts will be too busy configuring their IPv6 prefixes.
IPv6 FHS DHCPv6 Guard	Network Essentials and Advantage	IPv6 DHCPv6 Guard is one of the IPv6 FHS (First Hop Security) mechanisms and is very similar to IPv4 DHCP snooping. This feature inspects DHCPv6 messages between a DHCPv6 server and DHCPv6 client (or relay agent) and blocks DHCPv6 reply and advertisements from (rogue) DHCPv6 servers. DHCPv6 messages from clients or relay agents to a DHCPv6 server are not affected.

Feature Name	License Level	Description, and Documentation Link Information
Web authentication (Flexible Authentication – 802.1x, dACL, customizable web auth)	Network Essentials and Advantage	With this feature, users can acquire network resource access by specifying their user credentials (viz. username, password, etc). When a host initiates an http session, web-based authentication intercepts ingress http packets from the host and sends an html login page to the user. The users enter their credentials, which the web-based authentication feature sends to the authentication, authorization, and accounting server for authentication. If authentication succeeds, web-based authentication sends a Login-Successful html page to the host and applies the access policies returned by the AAA server. If authentication fails, web-based authentication forwards a Login-Fail html page to the user, prompting the user to retry the login. If the user exceeds the maximum number of attempts, web-based authentication forwards a Login-Expired html page to the host.
IPv6 QoS	Network Essentials and Advantage	QoS features supported for IPv6 environments include packet classification, queuing, class-basedpacket marking, and policing of IPv6 packets. IPv6 packets are forwarded by paths that are differentfrom those for IPv4. All QoS features available for IPv6 environments are managed from the modular QoS command-lineinterface (MQC). The MQC allows you to define traffic classes, create and configure traffic policies(policy maps), and then attach those traffic policies to interfaces.

Feature Name	License Level	Description, and Documentation Link Information
IOx Container support - Native Docker Support (IE-3400/IE-3400H/ESS3300 only)	Network Essentials	Starting with 17.2.1, IOX images on IE3400 support native Docker. IOx executes the container image.
IOx - Support for FSPAN/ERSPAN of packets to the AppGig port (IE-3400/IE-3400H/ESS3300 only)	Network Essentials	Flow Based SPAN – allows for specific traffic flows to be redirected to AppGigabitEthernet 1/1 interface for input to IOx applications. SPAN Session can be configured for ERSPAN encapsulation preserving orginal ingress time, and ingress port.

Important Notes

Complete List of Supported Features

For the complete list of features supported on a platform, see the Cisco Feature Navigator at https://www.cisco.com/go/cfn.

Accessing Hidden Commands

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

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

Hidden commands are available under:

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

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

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

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

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

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

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

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

Catalyst IE3x00 Rugged and ESS3300 Supported Hardware

Cisco Catalyst IE3x00 Rugged, IE 3400 Heavy Duty and ESS3300 Series Switches—Model Numbers (17.1.x)

The following 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*.

	Default License Level[1]	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-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

	Default License Level[1]	Description
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-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
IE-3200-8T2S-E	Network Essentials	8 Gigabit Ethernet 10/100/1000 RJ45 ports, 2 fiber 100/1000 SFP-based ports, non-PoE
IE-3200-8P2S-E	Network Essentials	8 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 Gigabit Ethernet 10/100/1000 RJ45 ports, 2 fiber 100/1000 SFP-based ports, non-PoE
IE-3300-8P2S-E	Network Essentials	8 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 Gigabit Ethernet 10/100/1000 RJ45 ports, 2 fiber 100/1000 SFP-based ports, non-PoE
IE-3300-8P2S-A	Network Advantage	8 Gigabit Ethernet 10/100/1000 PoE/PoE+ ports, 2 fiber 100/1000 SFP-based ports; PoE power budget of 360W (including expansion module)
IE-3400-8T2S-E	Network Essentials	8 Gigabit Ethernet 10/100/1000 RJ45 ports, 2 fiber 100/1000 SFP-based ports, non-PoE
IE-3400-8T2S-A	Network Advantage	8 Gigabit Ethernet 10/100/1000 RJ45 ports, 2 fiber 100/1000 SFP-based ports, non-PoE
IE-3400-8P2S-E	Network Essentials	8 Gigabit Ethernet 10/100/1000 RJ45 ports, 2 fiber 100/1000 SFP-based ports with PoE

	Default License Level[1]	Description
IE-3400-8P2S-A	Network Advantage	8 Gigabit Ethernet 10/100/1000 RJ45 ports, 2 fiber 100/1000 SFP-based ports with PoE
IE-3400H-8T-E	Network Essentials	8x1-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	8x1-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	8 100-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	8 100-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	16x1-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	16x1-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	16 100-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	16 100-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	24x1-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	24x1-Gbps X-Coded ports, 1 Alarm input and 1 Alarm output, 1 Console port, mini-change input for Single power source
IE-3400H-24FT-E	Network Essentials	24 100-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	24 100-Mbps D-coded ports, 1 Alarm input and 1 Alarm output, 1 Console port, Mini-change input for Single Power Source .

[1] See section *Licensing → Table: Permitted Combinations*, in this document for information about the add-on licenses that you can order.

Expansion Modules

The following table lists the optional expansion modules for the IE3300 and IE3400 base systems. Modules with IEM-3400-xx are only supported on IE3400 base systems. IEM expansion modules that support POE are only supported on Base systems that support POE.

Expansion Module	Description
IEM-3300-8T	8 copper Gigabit Ethernet ports. Non PoE.
IEM-3300-8P	8 copper Gigabit Ethernet ports. With PoE
IEM-3300-8S	8 SFP Gigabit Ethernet ports. Non PoE.
IEM-3300-16T	16 copper Gigabit Ethernet ports. Non PoE.
IEM-3300-16P	16 copper Gigabit Ethernet ports. With PoE.
IEM-3300-6T2S	6 copper Gigabit Ethernet ports and 2 SFP Gigabit ports. Non PoE.
IEM-3300-14T2S	14 copper Gigabit Ethernet ports, and 2 SFP Gigabit ports. Non PoE.
IEM-3400-8T	8 copper Gigabit Ethernet ports with Advanced features. Non PoE.
IEM-3400-8S	8 SFP Gigabit Ethernet ports with Advanced features. Non PoE.
IEM-3400-8P	8 copper Gigabit Ethernet ports with Advanced features with PoE.

Optics Modules

Cisco Catalyst Series Switches support a wide range of optics and the list of supported optics is updated on a regular basis. Use the Transceiver Module Group (TMG) Compatibility Matrix tool, or consult the tables at this URL for the latest transceiver module compatibility information: https://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

The Cisco Catalyst IE3x00 Rugged, IE3400 Heavy Duty and ESS3300 Series Switches datasheets contain the current list of supported SFP and optics.

WebUI System Requirements

The WebUI 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 WebUI.

Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution
233 MHz minimum[2]	512 MB[3]	256	1280 x 800 or higher

[2] We recommend 1 GHz
[3] We recommend 1 GB DRAM

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)

Upgrading the Switch Software

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

Note See the Cisco IOS XE Migration Guide for IIoT Switches for the latest information about upgrading and downgrading switch software.

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.

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 17.2x

Release	Image Type	File Name
Cisco IOS XE.17.2.1	Universal	ie3x00-universalk9.17.02.0
		ess3x00-universalk9.17.02.
	NPE	ie3x00-universalk9_npe.17

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 "4.1.3" for IE3x00 and ESS-3300.
	`Checking Bootloader upgrade...`
	`…`
	`Bootloader upgrade successful`

Bundle Mode Upgrade

To upgrade the Cisco IOS XE software when the switch is running in bundle mode, follow these steps:

Procedure

Step 1 Download the bundle file to local storage media.

Step 2 Configure the **boot system** global configuration command to point to the bundle file.

Step 3 Reload the switch.

Example

Upgrading Cisco IOS XE Software Bundle Mode

This example shows the steps to upgrade the Cisco IOS XE software on a switch that is running in bundle mode. It shows using the **copy** command to copy the bundle file to flash:, configuring the boot system variable to point to the bundle file, saving a copy of the running configuration, and finally, reloading the switch.

```
Switch# copy scp: sdflash:
Address or name of remote host [10.1.1.54]?
Source username [xxxxxx]?
Source filename? ie3x00-universalk9.16.12.05.SPA.bin
Destination filename [ie3x00-universalk9.16.12.05.SPA.bin]?
This is a Cisco managed device to be used only for authorized purposes.
Your use is monitored for security, asset protection, and policy compliance.


Password:
Sending file modes: C0644 269211776 ie3x00-universalk9.16.12.05.SPA.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
269211776 bytes copied in 408.784 secs (658567 bytes/sec)
SWITCH#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no boot system
Switch (config)#no boot manual
Switch (config)#boot system sdflash:ie3x00-universalk9.16.12.05.SPA.bin
Switch (config)#end
Switch #reload

System configuration has been modified. Save? [yes/no]:
*Feb 2 16:12:04.780: %SYS-5-CONFIG_I: Configured from console by console
yes
Building configuration...
[OK]
Proceed with reload? [confirm]
```

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.

Summary of Software Installation Commands for Install Mode	
To install and activate the specified file, and to commit changes to be persistent across reloads—**`install add file`** *`filename`* [**`activate commit`**]	
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.

Licensing

The information about the licensing packages for features available on Cisco Catalyst IE3x00 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches and Cisco Catalyst IE3100 Rugged Series Switches are available at: https://www.cisco.com/c/en/us/td/docs/iot/collections/cisco-iiot-licensing.html.

Important Note

Multicast traffic not registered with the switch will be distributed to every port.

Caveats

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

Cisco Bug Search Tool

Cisco Bug Search Tool is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Click the link for the caveat in the sections below to view details for the caveat in Bug Search Tool.

Cisco Bug Search Tool

The Cisco Bug Search Tool (BST) allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The BST is designed to improve the effectiveness in network risk management and device troubleshooting. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of a caveat, click on the identifier.

Open Caveats in Cisco IOS XE 17.2.1

Identifier	Description
CSCvs04837	Webauth : Login page is not coming when virtual-IP is configured in the switch.
CSCvs30801	dACL download is failing when number of ACEs are 30 with both webauth and dot1x session.
CSCvs40032	TCAM entries create/update/modify is not happening properly with both IPv4 and IPv6 dACL
CSCvt02699	DHCPV6 clients unable to recieve ip address with Petra as V6DHCP server
CSCvt03350	QinQ: mac-learning disabled on dot1q-tunnel port after port-sec and storm-control
CSCvt16054	WEBAUTH: on reaching 255aces/port, new incoming http connections are allowed without auth
CSCvt20731	[RSPAN]: Remote-Span issues with Port-Channel
CSCvt30079	External alarm relay does not truly clear a fault from the system
CSCvt06469	Undesirable Autosave of Running Config to eMMC flash
CSCvt71855	IE3x00 does not see the mrouter interfaces

Troubleshooting

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

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

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

Related Documentation

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

All support documentation for Cisco Catalyst IE3100 Rugged Series Switches is at this URL: https://www.cisco.com/c/en/us/support/switches/catalyst-ie3100-rugged-series/series.html

Allsupport documentation for Cisco Catalyst IE3100H Heavy Duty Series Switches is at this URL: https://www.cisco.com/c/en/us/support/switches/catalyst-ie3100-heavy-duty-series/series.html

All support documentation for Cisco Catalyst IE3200 Rugged Series Switches is at this URL: https://www.cisco.com/c/en/us/support/switches/catalyst-ie3200-rugged-series/tsd-products-support-series-home.html

All support documentation for Cisco Catalyst IE3300 Rugged Series Switches is at this URL: https://www.cisco.com/c/en/us/support/switches/catalyst-ie3300-rugged-series/tsd-products-support-series-home.html

All support documentation for Cisco Catalyst IE3400 Rugged Series Switches is at this URL: https://www.cisco.com/c/en/us/support/switches/catalyst-ie3400-rugged-series/tsd-products-support-series-home.html

All support documentation for Cisco Catalyst IE3400H Heavy Duty Series Switches is at this URL: https://www.cisco.com/c/en/us/support/switches/catalyst-ie3400-heavy-duty-series/tsd-products-support-series-home.html

All support documentation for Cisco ESS3300 Series Switches is at this URL: https://www.cisco.com/c/en/us/support/switches/embedded-service-3000-series-switches/tsd-products-support-series-home.html

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

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

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Customer Experience.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Solution Partner Program.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

© 2020–2024 Cisco Systems, Inc. All rights reserved.