Release Notes for Cisco Catalyst IE3x00 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches, Cisco IOS XE Bengaluru 17.5.x

First Published: 2021-04-01

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 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.

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.

New Features for Cisco Catalyst IE and ESS Switches in Cisco IOS XE 17.5.x

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

Feature Name	License Level	Description	Supported Platforms
Central Web Authentication (Redirection)	Network Essentials	Central web authentication offers the possibility to have a central device that acts as a web portal.	IE3200 IE3300 IE3300-10G IE3400/IE3400H ESS3300
IOx Load on EXT4 Filesystem Formatted File on a FAT32 SD Card	Network Essentials	Support for partitioning the SD Flash: filesystem into FAT32 for IOS-XE and EXT4 for IOx.	IE3300-10G IE3400/IE3400H ESS3300
Increased L2 MAC Scale - 16K	Network Essentials	With Release 17.5.x, IE3x00 switches increase support from 8K MAC addresses to 16K MAC addresses.	IE3200 IE3300 IE3300-10G IE3400/IE3400H ESS3300
Increased IPv4 Scale - 3K	Network Essentials	With Release 17.5.1, IPv4 routing scale in IE3x00 switches is increased from 2K to 3K.	IE3200 IE3300 IE3300-10G IE3400/IE3400H ESS3300
VRF Aware SGT for IPv4	Network Advantage	The Cisco TrustSec VRF-Aware SGT feature binds a Security Group Tag (SGT) Exchange Protoco (SXP) connection with a specific virtual routing and forwarding (VRF) instance.	IE3400/IE3400H
MAC Learning Optimization using ARP Snooping	Network Essentials	This feature minimizes the unknown unicast IP traffic flood, by learning the MAC address through ARP packet itself. As part of this feature a global CLI will be introduced to turn it on/off and by default it will be disabled. Enabling/disabling this feature will not have any impact on existing MAC learning mechanisms.	IE3200 IE3300 IE3300-10G IE3400/IE3400H ESS3300

Feature Name	License Level	Description	Supported Platforms
PRP Supervision Frame VLAN tagging with VLAN ID	Network Essentials	PRP VLAN tagging requires that PRP interfaces be configured in trunk mode. This feature allows you to specify a VLAN ID in the supervision frames for a PRP channel.	IE3400/IE3400H
SFP Support	Network Essentials	The following SFPs are supported from this release: CWDM-SFP-1610 CWDM-SFP-1530 CWDM-SFP-1490 DWDM-SFP-3033 DWDM-SFP-3112 SFP-10G-LR-S (Only supported on IE-3300-8T2X/IE-3300-8U2X and ESS3300) SFP-10G-LRM (Only supported on IE-3300-8T2X/IE-3300-8U2X) CWDM-SFP10G-1470 (Only supported on IE-3300-8T2X/IE-3300-8U2X and ESS3300) DWDM-SFP10G-3033 (Only supported on IE-3300-8T2X/IE-3300-8U2X)	IE3200 IE3300 IE3300-10G IE3400 ESS3300

Feature Name	License Level	Description	Supported Platforms
RFC4884 Support	Network Essentials	RFC 4884 redefines selected ICMP error messages to support multi-part operation. A multi-part ICMP message carries all of the information that ICMP messages carried previously, as well as additional information that applications may require. As part of RFC 4884 support, 'length' field will be added in ICMP data structure while sending ICMP error message packets and extension header will be added if required. This feature is applicable to ICMPv4 and ICMPv6 messages.	ESS3300
BFD echo mode	Network Advantage	Support BFD echo mode for OSPF/OSPFv3 clients. BFD (Bidirectional Forwarding Detection) is defined by IETF RFC 5880 and extended by other RFCs. The purpose of BFD is to provide a common, low-overhead mechanism for rapidly detecting the failure of next-hop link partners.	IE3300 IE3300-10G IE3400/IE3400H ESS3300

Important Notes

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.

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 and DLR 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.

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.

PoE Limitation on IE3x00

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 datasheet for your switch for more details.

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. Enter **power inline max** *max-wattage* to increase the PoE budget based on the power supplies used.

   max-wattage is the maximum available PoE power.

IE3200 and IE 3300 with 10Mbps or 100Mbps speed in Half-Duplex Mode

CRC errors were observed on the IE 3200 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.

Cisco Catalyst IE3x00 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches—Model Numbers (17.5.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-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

	Default License Level[1]	**Description**
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 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

	Default License Level[1]	Description
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 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-3300-8T2X-A	Network Advantage	8 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 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 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 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-3400-8T2S-E	Network Essentials	8 Gigabit Ethernet 10/100/1000 RJ45 ports, 2 fiber 100/1000 SFP-based ports, non-PoE

	Default License Level[1]	Description
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
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 .

	Default License Level[1]	Description
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-3300-4MU	4 copper 2.5Gigabit Ethernet ports. With IEEE 802.3bt type 4 PoE.
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	Font Size
233 MHz minimum[2]	512 MB[3]	256	1280 x 800 or higher	Small

[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.

Finding the Software Version

The package files for the Cisco IOS XE software can be found on the system board flash device flash (flash:) or external SDFlash (sdflash:).

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 17.5.x

Release	Image Type	File Name
Cisco IOS XE.17.5.1	Universal	ie3x00-universalk9.17.05.01.S
		ess3x00-universalk9.17.05.01.
	NPE	ie3x00-universalk9_npe.17.05.

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`

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 [10.106.224.22]?
Source username [xxxxx]?
Source filename []? $2/binos/linkfarm/iso1-petra/ie3x00-universalk9.17.05.01.SPA.bin

Destination filename [ie3x00-universalk9.17.05.01.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 344345038 ie3x00-universalk9.17.05.01.SPA.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
344345038 bytes copied in 637.684 secs (539993 bytes/sec)
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no boot system
Switch(config)#boot system sdflash:ie3x00-universalk9.17.0517.05.01.SPA.bin
Switch(config)#end
Switch#write memory
*May 27 14:49:55.121: %SYS-5-CONFIG_I: Configured from console by console
Building configuration...
[OK]
Switch#s
*May 27 14:50:01.341: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted private config
 file
Switch#sh boot
Current Boot Variables:
BOOT variable = sdflash:ie3x00-universalk9.17.05.01.SPA.bin;

Boot Variables on next reload:
BOOT variable = sdflash:ie3x00-universalk9.17.05.01.SPA.bin;
Config file = flash:/nvram_config
ENABLE_FLASH_PRIMARY_BOOT = no
MANUAL_BOOT variable = no
ENABLE_BREAK variable = yes

Switch#reload
Proceed with reload? [confirm]

*May 27 14:50:08.989: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload
Command.
watchdog: watchdog0: watchdog did not stop!
reboot: Restarting system
```

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`**`]`

Summary of Software Installation Commands for Install Mode	
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

This section provides information about the licensing packages for features available on Cisco Catalyst IE3x00 Rugged, and ESS3300 Series Switches.

License Types

The following license types are available:

- Permanent: for a license level, and without an expiration date.
- Evaluation: a license that is not registered.

Note Evaluation licenses are only used in Cisco IOS XE Release 17.3.1. Starting with Cisco IOS XE Release 17.3.2, Evaluation licenses are no longer used by Smart Licensing.

- Term: a time-based license for a three, five, or seven year period.

License Levels - Usage Guidelines

- Base licenses (Network Advantage) are ordered and fulfilled only with a permanent license type.
- Add-on licenses (DNA Essentials, DNA Advantage) are ordered and fulfilled only with a term license type.
- An add-on license level is included when you choose a network license level. If you use DNA features, renew the license before term expiry, to continue using it, or deactivate the add-on license and then reload the switch to continue operating with the base license capabilities.
- Evaluation licenses cannot be ordered. They are not tracked via Cisco Smart Software Manager and expire after a 90-day period. Evaluation licenses can be used only once on the switch and cannot be regenerated. Warning system messages about an evaluation license expiry are generated only 275 days after expiration and every week thereafter. An expired evaluation license cannot be reactivated after reload.

Note Evaluation licenses are only used in Cisco IOS XE Release 17.3.1. Starting with Cisco IOS XE Release 17.3.2, Evaluation licenses are no longer used by Smart Licensing.

- Network Essentials license is the default license. It is permanent. A connection to the Smart Licensing server is not required if the IE switch will be deployed with a Network Essentials license.

Smart Licensing

Cisco Smart Licensing is a unified license management system that manages all the software licenses across Cisco products.

It enables you to purchase, deploy, manage, track, and renew Cisco Software. It provides information about license ownership and consumption through a single user interface.

The solution is composed of Smart Accounts and Cisco Smart Software Manager. The former is an online account of your Cisco software assets and is required to use the latter. Cisco Smart Software Manager is where you can perform all your licensing management-related tasks such as establishing trust, checking license usage, transferring licenses, removing devices, and so forth. Users can be added and given access and permissions to the smart account and specific virtual accounts.

Important Cisco Smart Licensing is the default and the only available method to manage licenses on IE3x00 products.

Deploying Smart Licensing

The following provides a process overview of a day 0 to day *N* deployment directly initiated from a device. Links to the configuration guide provide detailed information to help you complete each one of the smaller tasks.

Procedure

Step 1 Begin by establishing a connection from your network to Cisco Smart Software Manager on cisco.com.

Step 2 Create and activate your Smart Account, or login if you already have one.

To create and activate Smart Account, go to Cisco Software Central → Create Smart Accounts. Only authorized users can activate the Smart Account.

Step 3 Complete the Cisco Smart Software Manager set up.

a) Accept the Smart Software Licensing Agreement.

b) Set up the required number of Virtual Accounts, users and access rights for the virtual account users.

Virtual accounts help you organize licenses by business unit, product type, IT group, and so on.

With this,

- The device is now in an authorized state and ready to use.
- The licenses that you have purchased are displayed in your Smart Account.

What to do next

Register and convert traditional licenses to Smart Licenses.

Using Smart Licensing on an Out-of-the-Box Device

If an out-of-the-box device has the software version factory-provisioned, all licenses on such a device remain in evaluation mode until registered in Cisco Smart Software Manager.

How Upgrading or Downgrading Software Affects Smart Licensing

Note how upgrading to a release that supports Smart Licensing or moving to a release that does not support Smart Licensing affects licenses on a device:

- **When you upgrade from an earlier release to one that supports Smart Licensing**—all existing licenses remain in evaluation mode until registered in Cisco Smart Software Manager. After registration, they are made available in your Smart Account.
- **When you downgrade to a release where Smart Licensing is not supported**—all smart licenses on the device are converted to traditional licenses and all smart licensing information on the device is removed.

Smart Licensing Using Policy

An enhanced version of Smart Licensing is available, with the overarching objective of providing a licensing solution that does not interrupt the operations of your network, rather, one that enables a compliance relationship to account for the hardware and software licenses you purchase and use.

With this licensing model, you do not have to complete any licensing-specific operations, such as registering or generating keys before you start using the software and the licenses that are tied to it. Only export-controlled and enforced licenses require Cisco authorization *before* use. License usage is recorded on your device with timestamps, and the required workflows can be completed at a later date.

Multiple options are available for license usage reporting – this depends on the topology you implement. You can use the Cisco Smart Licensing Utility (CSLU) Windows application, or report usage information directly to Cisco Smart Software Manager (CSSM). A provision for offline reporting for air-gapped networks, where you download usage information and upload to CSSM, is also available.

Starting with this release, Smart Licensing Using Policy is automatically enabled on the device. This is also the case when you upgrade to this release.

By default, your Smart Account and Virtual Account in CSSM is enabled for Smart Licensing Using Policy.

Note Starting with Cisco IOS XE Amsterdam 17.3.2, with the introduction of Smart Licensing Using Policy, even if you configure a hostname for a product instance or device, only the Unique Device Identifier (UDI) is displayed.

This change in the display can be observed in all licensing utilities and user interfaces where the hostname was displayed in earlier releases. It does not affect any licensing functionality. There is no workaround for this limitation.

The licensing utilities and user interfaces that are affected by this limitation include only the following: Cisco Smart Software Manager (CSSM), Cisco Smart License Utility (CSLU), and Smart Software Manager On-Prem (SSM On-Prem).

Important Note

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

Known Issues

This section contains the known issues in this release.

Failure to Learn MAC Addresses

Problem: Failed to learn MAC addresses due to hardware hash collision. This limitation is applicable to all the IE3x00 SKUs having Marvell Poncat3 as switch ASIC.

Conditions: Hash collision is a condition in the hardware where there is no more empty space in the MAC table for the new MAC address to be learned. Underneath switch ASIC implements hash table to store MAC addresses using (mac_addr+vlan) as the hash key. There are four buckets in a chain at each hash index. If all four buckets are full and there is a new fifth entry to be stored at the same hash index, the new MAC address is not learned in the hardware MAC table. This is the ASIC limitation. If this condition occurs, hardware drops the new MAC address learning request. Flooding occurs for such MAC addresses that were not learned on the switch due to the hash collision condition.

Workaround: One workaround is to make space for the new MAC addresses by making at least one hash bucket available either by explicit MAC removal of old MAC at that hash index or aging. The other option is to use more random pattern of MAC address and VLAN to avoid hash collision condition in the hardware. Hash collision has no direct relation to MAC address scale. It can occur even with low scale with more than four MAC addresses hitting the same hash index.

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.

Open Caveats in Cisco IOS XE Bengaluru 17.5.x

Identifier	Description
CSCvw53326	IE3400 and IE3300 10Gig only: Docker Apps gets less throughput on Appgig when SSS enabled.
CSCvx52870	IE3400H - Dying gasp signal is not generated.
CSCvw69183	FNF entries created for the traffic received at Spanning tree BLOCKED port.
CSCvw89264	Radius pac request always sent via non default vrf.
CSCvw93228	Ipv6 SSM multicast packets choke TM queue, resulting in loss of SM mode traffic.
CSCvx82341	IE-3200: no vlan tag in dying-gasp trap packet
CSCvw67744	IE3x00: Dante PTP devices fail to synchronize clocks.
CSCvx66354	IE-3300/IE-3400: L4 ACLs not summarised properly causing some entries to not take effect.

Resolved Caveats in Cisco IOS XE Bengaluru 17.5.1

Identifier	Description
CSCvv53350	Host to switch MACSEC session is not stable when access-session closed enabled on interface.
CSCvv91077	FNF: Restricting the minimum timeout value in configurations.
CSCvw79787	IE3400H port is up but no ingress traffic is registered.
CSCvw87310	IE3300 Critical software exception reload during collect show tech output.
CSCvw97442	IE3400H Auto medium is not disabled for Copper ports for 1/1 and 1/2.
CSCvx12483	WebUI: Unable to access the GUI on some IE3x00 using HTTPS.
CSCvx25216	IE3400/H: CTS credentials are not synced with swap drive commands.
CSCvx32737	IE3400H - Packet duplication observed for DHCP unicast packets with IPDT enabled.
CSCvx37011	Port flip/flap seen in peer or IXIA ports during the switch bootup.

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

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.