

# Release Notes for Cisco Catalyst IE3x00 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches, Cisco IOS XE Amsterdam 17.3.x

---

**First Published:** 2020-07-06

**Last Modified:** 2024-05-04

## 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.

---

## Smart Licensing Using Policy in Cisco IOS XE Release 17.3.2

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).

---

## New Features for Cisco Catalyst IE and ESS Switches in Cisco IOS XE 17.3.x

There are no new features in the Cisco IOS XE 17.3.8 release as it is a PSIRT only release.




---

**Note** The Cisco IOS XE 17.3.8 release provides the fix for CSCwh87343, Cisco IOS XE Software Web UI Privilege Escalation Vulnerability.

For more information, see [Cisco Security Advisory](#).

---

The following features apply to both the IE3x00 and ESS3300 switches in Cisco IOS XE 17.3.x unless specifically mentioned.

Feature Name	License Level	Description, and Documentation Link Information
MRP 500ms Profile Support	Network Essentials (Must have MRP Ring Manager or Client License)	<p>In today's Ethernet based Industrial Automation applications, one of the critical features is the availability of the communication network. This availability of the network will influence directly the availability of control system of the manufactory plant. The important characteristic of a plant is how long it can run when the control system in a fault state. This recovery time, namely grace time, has different values depending on the type of application.</p> <p>Media Redundancy Protocol (MRP) is one of the ring protocols supported by Cisco for such applications. With this release, IE3x00 will now support 200ms and 500ms profiles. With support of 500ms profile, the IE3x00 is now in compliance with IEC62439-2.</p>

Feature Name	License Level	Description, and Documentation Link Information
Media Redundancy Auto-Manager (MRA)	Network Essentials (Must have MRP Ring Manager License)	<p>An MRP compliant network shall have a ring topology with multiple nodes. The nodes consist of two different types, i.e. Media Redundancy Manager (MRM) and Media Redundancy Clients (MRC). MRM periodically sends frames on one of the ring ports and receives on the other one, in order to monitor the status of the ring topology; MRC reacts on received reconfiguration frames from the MRM.</p> <p>Certain nodes or all nodes in the ring topology may also start as a Media Redundancy Auto-manager (MRA). MRAs exchange frames to elect one MRM among themselves, and the rest will transition into MRCs. The MRA role is not an operational MRP role like MRM or MRC. It is only an administrative, temporary role at device start-up, and a node must transition to the MRM role or the MRC role after start-up and the MRM is selected through the manager voting process.</p>

Feature Name	License Level	Description, and Documentation Link Information
QinQ Support	Network Essentials	<p>Traditional 802.1Q tunneling (QinQ) performs all-to-one bundling of C-VLAN IDs to a single S-VLAN ID for the port. The S-VLAN is added to the incoming unmodified C-VLAN. You can configure the UNI as an 802.1Q tunnel port for traditional QinQ, or you can configure selective QinQ on trunk ports for a more flexible implementation. Mapping takes place at ingress and egress of the port. All packets on the port are bundled into the specified S-VLAN.</p> <p>Selective QinQ maps the specified customer VLANs entering the UNI to the specified S-VLAN ID. The S-VLAN is added to the incoming unmodified C-VLAN. You can also specify that traffic carrying all other customer VLAN IDs is dropped.</p> <p>For quality of service (QoS), the switch supports flexible mapping between C-CoS or C-DSCP and S-CoS, and maps the inner CoS to the outer CoS for traffic with traditional QinQ or selective QinQ VLAN mapping.</p>

Feature Name	License Level	Description, and Documentation Link Information
HSR Support	Network Essentials	<p>HSR achieves the same result as PRP but designed to work in a ring topology. Instead of two parallel independent networks of any topology in PRP (LAN-A and LAN-B), HSR defines a ring with traffic in opposite directions. Port-A sends traffic counterclockwise in Ring, and Port-B sends traffic clockwise in Ring. The packet format is different from PRP, instead of RCT, HSR introduces the HSR header with HSR ETHERTYPE after the L2 MACSA address or VLAN tag fields.</p> <p>Only HSR-SAN mode is supported in 17.3.1 on IE 3400 Advanced ONLY (including ie3400H+). It is <i>not</i> supported on ESS 3300 or ie3200 / 3300.</p>
Source Specific Multicast – IPv4	Network Advantage	<p>Source Specific Multicast (SSM). SSM is an extension of IP multicast where datagram traffic is forwarded to receivers from only those multicast sources that the receivers have explicitly joined. For multicast groups configured for SSM, only source-specific multicast distribution trees (not shared trees) are created.</p>

Feature Name	License Level	Description, and Documentation Link Information
IPv6 Multicast Routing	Network Advantage	<p>Cisco software supports the following protocols to implement IPv6 multicast routing:</p> <ul style="list-style-type: none"> <li>• PIM SSM</li> <li>• MLD</li> </ul> <p>PIM SSM functionality is similar to that of IPv4 as mentioned in section 2.10 MLD. It is used by IPv6 devices to discover multicast listeners (nodes that want to receive multicast packets destined for specific multicast addresses) on directly attached links. There are two versions:</p> <ul style="list-style-type: none"> <li>• MLD version 1 is based on version 2 of the Internet Group Management Protocol (IGMP) for IPv4.</li> <li>• MLD version 2 is based on version 3 of the IGMP for IPv4.</li> </ul>
HSRP Aware PIM	Network Advantage	<p>Protocol Independent Multicast (PIM) has no inherent redundancy capabilities and its operation is completely independent of Hot Standby Router Protocol (HSRP) group states. As a result, IP multicast traffic is forwarded not necessarily by the same device as is elected by HSRP. HSRP Aware PIM enables multicast traffic to be forwarded through the HSRP active router (AR), allowing PIM to leverage HSRP redundancy, avoid potential duplicate traffic, and enable failover, depending on the HSRP states in the device. The PIM designated router (DR) runs on the same gateway as the HSRP AR and maintains mroute states.</p>
Full POST	Network Essentials	<p>POST feature tests the hardware to verify that all components of the device are present and operational.</p>

Feature Name	License Level	Description, and Documentation Link Information
<p>Smart Software Manager On-Prem (SSM On-Prem) Support for Smart Licensing Using Policy</p> <p><b>Note</b> This feature applies to Cisco Catalyst IE3x00 Rugged Series Switches, Cisco IE 3400 Heavy Duty Series Switches, and Cisco Embedded Services 3300 Series Switches in IOS-XE 17.3.3.</p>	<p>—</p>	<p>SSM On-Prem is an asset manager, which works with CSSM. It enables you to administer products and licenses on your premises instead of having to directly connect to CSSM.</p> <p>Here, a product instance is connected to SSM On-Prem, and SSM On-Prem becomes the single point of interface with CSSM. The product instance can be configured to <i>push</i> the required information to SSM On-Prem. Alternatively, SSM On-Prem can be set-up to <i>pull</i> the required information from a product instance at a configurable frequency. After usage information is available in SSM On-Prem, you must synchronize the same with CSSM, to ensure that the product instance count, license count and license usage information is the same on both, CSSM and SSM On-Prem. Offline and online options are available for synchronization between CSSM and SSM On-Prem.</p> <p>Minimum Required SSM On-Prem Version: Version 8, Release 202102.</p> <p>Minimum Required Cisco IOS XE Version: Cisco IOS XE 17.3.3.</p> <p>A license level does not apply.</p>

## Important Notes

### 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.

However, you may need to upgrade the software, depending on which base switch and expansion 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 [FN72400 - New Hardware Versions of Cisco Catalyst IE3400 Rugged/IE3400H Heavy Duty Series Will Be Supported with Minimum Software Release - Software Upgrade Recommended](#) on Cisco.com.

If you have...	Then...
Older versions of the base switch and expansion module	No action is required; however, we recommend that you upgrade to IOS-XE 17.31 or later.
Newer versions of the base switch and expansion module	Deploy one of the supported releases of IOS-XE. Otherwise, you see an error message telling you that the release that you are using is not supported.
Newer version of the base switch with an older version of the expansion module	The supported releases are 17.3.1 through 17.3.8. Do not downgrade to earlier releases.
Older version of the base switch with a newer version of the expansion module	Deploy one of the supported releases of IOS-XE. Otherwise, you see an error message telling you that the release that you are using is not supported. The supported releases are 17.3.6 through 17.3.8. Do not downgrade to earlier releases.

### Use of CTS Before Upgrade

If CTS is used before upgrading to 17.3.3, and the device is booted from sdflash, after upgrading to 17.3.3, use the following command to ensure CTS works after upgrade.

```
Switch# cts credentials id swith1 password xxxxx
```

### 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 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.

## Cisco Catalyst IE3x00 Rugged, IE3400 Heavy Duty and ESS3300 Series Switches—Model Numbers (17.3.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 <sup>1</sup>	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

	<b>Default License Level<sup>1</sup></b>	<b>Description</b>
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
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

	<b>Default License Level<sup>1</sup></b>	<b>Description</b>
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-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
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 .

	<b>Default License Level<sup>1</sup></b>	<b>Description</b>
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 .

<sup>1</sup> 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.

<b>Expansion Module</b>	<b>Description</b>
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.

Expansion Module	Description
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](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 <sup>2</sup>	512 MB <sup>3</sup>	256	1280 x 800 or higher	Small

<sup>2</sup> We recommend 1 GHz

<sup>3</sup> 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 17.3.x

Release	Image Type	File Name
Cisco IOS XE.17.3.8	Universal	ie3x00-universalk9.17.03.08.SPA.bin
		ess3x00-universalk9.17.03.08.SPA.bin
	NPE	ie3x00-universalk9_npe.17.03.08.SPA.bin
Cisco IOS XE.17.3.7	Universal	ie3x00-universalk9.17.03.07.SPA.bin
		ess3x00-universalk9.17.03.07.SPA.bin
	NPE	ie3x00-universalk9_npe.17.03.07.SPA.bin
Cisco IOS XE.17.3.6	Universal	ie3x00-universalk9.17.03.06.SPA.bin
		ess3x00-universalk9.17.03.06.SPA.bin
	NPE	ie3x00-universalk9_npe.17.03.06.SPA.bin
Cisco IOS XE.17.3.5	Universal	ie3x00-universalk9.17.03.05.SPA.bin
		ess3x00-universalk9.17.03.05.SPA.bin
	NPE	ie3x00-universalk9_npe.17.03.05.SPA.bin

Release	Image Type	File Name
Cisco IOS XE.17.3.4	Universal	ie3x00-universalk9.17.03.04.SPA.bin
		ess3x00-universalk9.17.03.04.SPA.bin
	NPE	ie3x00-universalk9_npe.17.03.04.SPA.bin
Cisco IOS XE.17.3.3	Universal	ie3x00-universalk9.17.03.03.SPA.bin
		ess3x00-universalk9.17.03.03.SPA.bin
	NPE	ie3x00-universalk9_npe.17.03.03.SPA.bin
Cisco IOS XE.17.3.2	Universal	ie3x00-universalk9.17.03.02a.SPA.bin
		ess3x00-universalk9.17.03.02a.SPA.bin
	NPE	ie3x00-universalk9_npe.17.03.02a.SPA.bin
Cisco IOS XE.17.3.1	Universal	ie3x00-universalk9.17.03.01.SPA.bin
		ess3x00-universalk9.17.03.01.SPA.bin
	NPE	ie3x00-universalk9_npe.17.03.01.SPA.bin

### Automatic Boot Loader Upgrade 17.3.x

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	<pre> Boot loader may be upgraded to version "7.1.5" for IE3x00 and ESS-3300.  Checking Bootloader upgrade... ... Bootloader upgrade successful </pre>

### 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/isol-petra/ie3x00-universalk9.17.03.01.SPA.bin

Destination filename [ie3x00-universalk9.17.03.01.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-universalk9.17.03.01.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-universalk9.17.03.01.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-universalk9.17.03.01.SPA.bin;

Boot Variables on next reload:
BOOT variable = sdflash:ie3x00-universalk9.17.03.01.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— <b>install add file</b> <i>filename</i> [ <b>activate commit</b> ]	
<b>add file tftp:</b> <i>filename</i>	Copies the install file package from a remote location to the device and performs a compatibility check for the platform and image versions.
<b>activate</b> [ <b>auto-abort-timer</b> ]	Activates the file, and reloads the device. The <b>auto-abort-timer</b> keyword automatically rolls back image activation.
<b>commit</b>	Makes changes persistent over reloads.
<b>remove</b>	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 Levels

The software features available on Cisco Catalyst IE3x00 Rugged and ESS3300 switches fall under these base or add-on license levels.

For a summarized list of features in each license level, see the product datasheets.

#### Base Licenses

- Network Essentials
- Network Advantage—Includes features available with the Network Essentials license and more.

#### Add-On Licenses

Add-On licenses require Network Essentials or Network Advantage as a pre-requisite. The features available with add-on license levels provide Cisco innovations on the switch, as well as on the Cisco Digital Network Architecture Center (Cisco DNA Center).

- DNA Essentials
- DNA Advantage— Includes features available with the DNA Essentials license and more.

### Feature Licenses

Feature licenses are bound to a specific feature or set of features. Feature licenses can be enabled regardless of Base License (Network Advantage or Network Essential). Feature licenses are smart licenses as well and require a smart account to be activated.

MRP requires a feature license. There are two MRP licenses available for Cisco IE3x00.

- LIC-MRP-MGR-XE= MRP Ring Manager license.
- LIC-MRP-CLIENT-XE= MRP Ring Client License.

To enable enforced feature licenses, such as MRP:

1. Obtain the authorization code for feature licensing, using the following command:

```
license smart authorization request add [mrp_client|mrp_manager] local
```

2. Enable the licensing by using the following command:

```
platform license feature [mrp-client | mrp-manager]
```

## 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.

## 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 Amsterdam 17.3.x

There are no open caveats in Cisco IOS XE Amsterdam 17.3.7.

### Resolved Caveats in Cisco IOS XE Amsterdam 17.3.8

Identifier	Description
<a href="#">CSCwh87343</a>	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability

**Resolved Caveats in Cisco IOS XE Amsterdam 17.3.7**

Identifier	Description
<a href="#">CSCwc58174</a>	Loop Triggered when use wrong Portchannel member
<a href="#">CSCwd73631</a>	IE3300 could not handle fragmented PIM bootstrap received in Trunk port
<a href="#">CSCwd97578</a>	Log is generate after link flapping: Error: LPM IPv4 100% capacity is reached

**Resolved Caveats in Cisco IOS XE Amsterdam 17.3.6**

Identifier	Description
<a href="#">CSCwa91196</a>	IE-3300 - QoS Policy stops applying QoS markings after switch reboot or power-cycle
<a href="#">CSCwb02945</a>	IE3400H-FE - Unable to configure MTU other than 1500 in 3400 FE switch with network essentials
<a href="#">CSCwb32319</a>	EPC on IE3300 switches dropping packets of flows not allowed in the ACL filter
<a href="#">CSCwb41302</a>	Interface Gi2/1 in expansion module IEM-3400-8S not working in 17.X releases
<a href="#">CSCwb46595</a>	IE3300 16P expansion module granting POE to ports where power inline never was configured
<a href="#">CSCwb66011</a>	interface vlan with unassigned ip address generating ICMPv6 Router Solicitation (IE-3300)
<a href="#">CSCwc07172</a>	When we are having IOX/Cybervision enabled on the switch and attempt to soft reload it hangs

**Resolved Caveats in Cisco IOS XE Amsterdam 17.3.5**

Identifier	Description
<a href="#">CSCvz63447</a>	EIGRP Hello counter increased by 2 for each received Hello packet
<a href="#">CSCvv58266</a>	IE3x00 switch unable to communicate with the radius server if not using server-private
<a href="#">CSCvy42555</a>	DHCP: Enabling dhcp snooping causes dhcp offer on voice-vlan port to be untagged
<a href="#">CSCwa30349</a>	VACL affecting traffic on nonspecified vlans on IE3x00
<a href="#">CSCvy51154</a>	CRC errors observed in IE3x00 with auto speed and duplex settings

**Resolved Caveats in Cisco IOS XE Amsterdam 17.3.4**

Identifier	Description
<a href="#">CSCvx48788</a>	IE3x00: When a trunk port changed to access, in the hardware STP table is the same interface found in FORWARDING state on all the vlans.
<a href="#">CSCvx57000</a>	IE3x00: Uni-directional routed traffic won't take an alternate path when the primary link failed.
<a href="#">CSCvx66354</a>	IE-3300/IE-3400: L4 ACLs not summarized properly causing some entries to not take effect.

Identifier	Description
<a href="#">CSCvx82015</a>	IE3x00: Reload makes AUTH session not created for few endpoints.
<a href="#">CSCvw67744</a>	IE3x00: PTP devices from a specific vendor fail to synchronize clocks.
<a href="#">CSCvw93228</a>	IE3400H: Ipv6 SSM multicast packets choke TM queue, resulting in loss of SM mode traffic.
<a href="#">CSCvx52870</a>	IE3400H - Dying gasp signal is not generated.
<a href="#">CSCvx57271</a>	IE3x00: Dying-gasp is not working in trunk mode.
<a href="#">CSCvy00929</a>	IE3200: No ARP information for dying-gasp trap after 15 minutes although ARP table shows normal.
<a href="#">CSCvy34521</a>	Memory leak in IOSd.

### Resolved Caveats in Cisco IOS XE Amsterdam 17.3.3

Identifier	Description
<a href="#">CSCvt57821</a>	PTP forward mode needs a reload to get activated on switch, works fine after reload.
<a href="#">CSCvv15504</a>	IE-3300/IE-3400: Tracebacks seen on reload with link established with Cu SFPs forced speed/duplex.
<a href="#">CSCvv41455</a>	Host switch is not provisioned with DHCP option 150 during day-0 boot up from the DHCP server C9300.
<a href="#">CSCvv91077</a>	FNF: Restricting the minimum timeout value in configurations.
<a href="#">CSCvw21016</a>	Traffic drop observed in HSRP topology when ping reply is taking HSRP standby path.
<a href="#">CSCvw38886</a>	PRP: Unable to reach access devices over PRP channel interface with any vlan configured.
<a href="#">CSCvw65202</a>	Flooding on physical ports for traffic destined to CV center.
<a href="#">CSCvw66345</a>	IE3400 - Software-forwarding observed with Dot1X on 17.3.2a.
<a href="#">CSCvw67128</a>	SL Policy: Purchase info should be protected and shouldn't be able to erase.
<a href="#">CSCvw79787</a>	IE3400H port is up but no ingress traffic is registered.
<a href="#">CSCvw87310</a>	IE3300: Critical software exception reload during collect show tech output.
<a href="#">CSCvw97442</a>	IE3400H auto medium is not disabled for copper ports for 1/1 and 1/2.
<a href="#">CSCvx12483</a>	WebUI: Unable to access the GUI on some IE3x00s using HTTPS.
<a href="#">CSCvx25216</a>	IE3400/H: CTS credentials are not synced with swap drive commands.
<a href="#">CSCvx32737</a>	IE3400H: Packet duplication observed for DHCP unicast packets with IPDT enabled.
<a href="#">CSCvx37011</a>	Port blip/flap seen in peer & IXIA ports during the DUT bootup.

**Resolved Caveats in Cisco IOS XE Amsterdam 17.3.2**

Identifier	Description
<a href="#">CSCvu81558</a>	CRC errors observed with IE3400H/IE3400 with 10Mbps speed in Half-Duplex Mode.
<a href="#">CSCvu85569</a>	When IE3300 has Auto-QoS configured, it prevents the AP from registering.
<a href="#">CSCvv24989</a>	Spanning tree blocked port moves to forwarding state in the ASIC, causing a loop.
<a href="#">CSCvv36403</a>	Access-session closed mode not learning new mac address.
<a href="#">CSCvv29516</a>	With SLR license on - unable to move from NA to NE license.
<a href="#">CSCvv39283</a>	Software-forwarding still observed with "no ip redirects" configured.
<a href="#">CSCvv43693</a>	Router entry reprogramming upon mac add/deletion/move.
<a href="#">CSCvv43931</a>	QoS policy causing VDANs to not communicate across PRP channel redbox.
<a href="#">CSCvv50025</a>	Mac-move not allowing to learn a mac address on a valid port.
<a href="#">CSCvv61938</a>	Mac learnt via CTS Port SGT enabled interface leaves MATM entry while ages out.
<a href="#">CSCvv71131</a>	After updating the firmware on the IE3400 and a reload happens, the auth sessions fail to establish.
<a href="#">CSCvv89846</a>	Interface / SVI MAC of one device overlaps with other device interfaces / SVI MAC address.
<a href="#">CSCvy34521</a>	When checking memory usage and committed memory, the IOSd process is incrementing.

**Resolved Caveats in Cisco IOS XE Amsterdam 17.3.1**

Identifier	Description
<a href="#">CSCvs30801</a>	dACL download is failing when number of ACEs are 30 with both webauth and dot1x session.
<a href="#">CSCvs40032</a>	TCAM entries create/update/modify is not happening properly with both IPv4 and IPv6 dACL.
<a href="#">CSCvt02699</a>	IE3300/3400 - DHCPV6 clients unable to receive an IP address with IE3x00 as V6DHCP server.
<a href="#">CSCvt03350</a>	QinQ: mac-learning disabled on dot1q-tunnel port after port-sec and storm-control.
<a href="#">CSCvt16054</a>	WEBAUTH: on reaching 255aces/port, new incoming http connections are allowed without auth.
<a href="#">CSCvt20731</a>	[RSPAN]: Remote-Span issues with Port-Channel.
<a href="#">CSCvt30079</a>	IE-3400H external alarm relay does not truly clear a fault from the system.
<a href="#">CSCwb87126</a>	IE3300: Policy map and ACLs not working on more than four 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>

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](#).



