Release Notes for Cisco Catalyst IE3x00 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches, Cisco IOS XE Gibraltar 16.12.x

First Published: 2019-07-31

Last Modified: 2021-09-24

Release Notes for Cisco Catalyst IE3x00 Rugged and ESS3300 Series Switches, Cisco IOS XE Gibraltar 16.12.x

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.

Software Features for Cisco Catalyst IE and ESS Switches in Cisco IOS XE Gibraltar 16.12.1

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

Feature Name	Description, Documentation Link and License Level Information
VRF-lite support	VRF-lite is a feature that enables a service provider to support two or more VPNs, where IP addresses can be overlapped among the VPNs. VRF-lite uses input interfaces to distinguish routes for different VPNs and forms virtual packet-forwarding tables by associating one or more Layer 3 interfaces with each VRF. Interfaces in a VRF can be either physical, such as Ethernet ports, or logical, such as VLAN SVIs, but a Layer 3 interface cannot belong to more than one VRF at any time.
MRP Support	MRP, defined in International Electrotechnical Commission (IEC) standard 62439-2, provides fast convergence in a ring network topology for Industrial Automation networks. MRP Media Redundancy Manager (MRM) defines its maximum recovery times for a ring in the following range: 10 ms, 30 ms, 200 ms and 500 ms. **Note** The default maximum recovery time on the Cisco IE switch is 200 ms for a ring composed of up to 50 nodes. You can configure the switch to use the 500 ms recovery time profile as described in Configuring MRP Manage **Restriction** Release 16.12.1 supports MRP CLI Mode only. Profinet mode is not supported in this release.
PRP Support	Parallel Redundancy Protocol (PRP) is defined in the International Standard IEC 62439-3. PRP is designed to provide hitless redundancy (zero recovery time after failures) in Ethernet networks.
Layer 2 NAT Support	One-to-one (1:1) Layer 2 NAT is a service that allows the assignment of a unique public IP address to an existing private IP address (end device), so that the end device can communicate on both the private and public subnets. This service is configured in a L2NAT enabled device and is the public “alias” of the IP address physically programmed on the end device. This is typically represented by a table in the L2NAT device. Layer 2 NAT has two translation tables where private-to-public and public-to-private subnet translations can be defined. Layer 2 NAT is a hardware based implementation which provides the same high level of (bump-on-the-wire) performance throughout switch loading. This implementation also supports multiple VLAN’s through the L2NAT boundary for enhanced network segmentation. Ring architecture support is built into Layer 2 NAT which allows for redundancy through the L2NAT boundary.
MACsec Support	MACsec, defined in 802.1AE, is a wire-rate hop-to-hop Layer 2 encryption technology that uses out-of-band methods for encryption keying. The MACsec Key Agreement (MKA) Protocol, defined in 802.1X-2010, provides the required session keys and manages the required encryption keys used by the underlying MACsec protocol.

Feature Name	Description, Documentation Link and License Level Information
Routed Port Support	A routed port is a physical port that acts like a port on a router; it does not have to be connected to a router. A routed port is not associated with a particular VLAN, as is an access port. A routed port behaves like a regular router interface, except that it does not support VLAN subinterfaces. Routed ports can be configured with a Layer 3 routing protocol. A routed port is a Layer 3 interface only and does not support Layer 2 protocols, such as STP. Configure routed ports by putting the interface into Layer 3 mode with the **no switchport** interface configuration command. Then assign an IP address to the port, enable routing, and assign routing protocol characteristics by using the ip routing and router *protocol global configuration* commands. **Note** Entering a **no switchport** interface configuration command shuts down the interface and then re-enables it, which might generate messages on the device to which the interface is connected. When you put an interface that is in Layer 2 mode into Layer 3 mode, the previous configuration information related to the affected interface might be lost. The number of routed ports that you can configure is not limited by software. However, the interrelationship between this number and the number of other features being configured might impact CPU performance because of hardware limitations. See Configuring Layer 3 Interfaces for information about what happens when hardware resource limitations are reached. **Note** For full Layer 3 routing, you must have the IP services image installed on the switch
USB Support (IE 3x00)	All IE 3x00 systems will have two USB ports with Type-A connector on the front panel. Both ports are USB 2.0 only. These ports can be used for USB sticks and the Bluetooth dongle. They are not to be used in hazardous location. Each USB port can provide a maximum current of 500mA at 5V, with 600mA total available for both ports. USB flash drives will only support the VFAT file system. There is no maximum limit for the USB flash to work in any of the 3 platforms. USB flash supports the data storage in IMSP. User can copy the data to/from the USB on the device. Booting a device with the image in the USB is not supported in 16.12. It is considered for the future release along with WebUI.
REP Preferred Support	One edge port in the REP segment acts as the primary edge port; the other as the secondary edge port. It is the primary edge port that always participates in VLAN load balancing in the segment. REP VLAN balancing is achieved by blocking some VLANs at a configured alternate port and all other VLANs at the primary edge port. When you configure VLAN load balancing, you can specify the alternate port. By entering the **preferred** keyword to select the port that you previously configured as the preferred alternate port with the **rep segment** *segment-id* **preferred** interface configuration command.

Feature Name	Description, Documentation Link and License Level Information
Layer 3 ACL Support	You configure access lists on a Layer 3 switch to provide basic security for your network. If you do not configure ACLs, all packets passing through the switch could be allowed onto all parts of the network. You can use ACLs to control which hosts can access different parts of a network or to decide which types of traffic are forwarded or blocked at router interfaces. For example, you can allow e-mail traffic to be forwarded but not Telnet traffic. ACLs can be configured to block inbound traffic, outbound traffic, or both. Support: • VACL not supported on SVI interface. • When VACL and PACL both are applicable for a packet then PACL takes precedence over VACL and VACL is not applied in such a case. • Max 255 aces per VACL • No explicit limit on total vlan’s defined, because tcam is not carved into components, whenever enough space in tcam isn’t available to accept the new configuration, error shall be thrown with a syslog. • Logging not supported on egress ACL. • On L3-ACL, non-ip ACL is not supported. • L4OP in ACLs is limited by the hardware to a maximum of 8 L4OP for UDP and 8 L4OP for TCP, for a total of 16 global L4OP. Keep in mind that the "range" operator consumes 2 L4OP.

Feature Name	Description, Documentation Link and License Level Information
PTP over PRP Support	Precision Time Protocol (PTP) can operate over Parallel Redundancy Protocol (PRP). PRP provides high availability through redundancy for PTP. The PRP method of achieving redundancy by parallel transmission over two independent paths (see Information About PRP) does not work for PTP as it does for other traffic. The delay experienced by a frame is not the same in the two LANs, and some frames are modified in the transparent clocks (TCs) while transiting through the LAN. A Dually Attached Node (DAN) does not receive the same PTP message from both ports even when the source is the same. Specifically: • Sync/Follow_Up messages are modified by TCs to adjust the correction field. • Boundary Clocks (BCs) present in the LAN are not PRP-aware and would generate their own Announce and Sync frames with no Redundancy Control Trailer (RCT) appended. • Follow_Up frames are generated by every 2-step clock and carry no RCT. • TCs are not PRP-aware and not obliged to forward the RCT, which is a message part that comes after the payload. Previously, PTP traffic was allowed only on LAN-A to avoid the issues with PTP and parallel transmission described above. However, if LAN-A went down, PTP synchronization was lost. To enable PTP to leverage the benefit of redundancy offered by the underlying PRP infrastructure, PTP packets over PRP networks are handled differently than other types of traffic. The implementation of the PTP over PRP feature is based on the PTP over PRP operation detailed in IEC 62439-3:2016, *Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)*. This approach overcomes the problems mentioned above by not appending an RCT to PTP packets and bypassing the PRP duplicate/discard logic for PTP packets.
Trustsec	Cisco TrustSec® technology helps protect critical assets from malware and bad intent by controlling access to your applications, equipment, and users. Cisco TrustSec software-defined segmentation simplifies the security controls in your network and provides consistent, automated policy across campuses, branches, and data centers whether users connect through wired, wireless, or VPN. Automation is enabled through the distribution of rich contextual information to network decision points. **Restriction** In 16.12.1, SGT, SGACL, are supported on IE3400 models only. An IEM3400 expansion model is required for SGT and SGACL, to expand ports beyond the base. SXP is supported on all models.
OSPF	OSPF is an Interior Gateway Protocol (IGP) developed by the OSPF working group of the Internet Engineering Task Force (IETF). OSPF was designed expressly for IP networks and it supports IP subnetting and tagging of externally derived routing information. OSPF also allows packet authentication and uses IP multicast when sending and receiving packets.

Catalyst IE3x00 Rugged and ESS3300 Supported Hardware

Cisco Catalyst IE3x00 Rugged, IE 3400 Heavy Duty and ESS3300 Series Switches—Model Numbers (16.12.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
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

	Default License Level[1]	Description
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
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-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-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-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.

Web UI System Requirements

The Web UI is http/https browser based Switch management tool running on the switch. The following subsections list the hardware and software required to access the Web UI.

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.

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 directory names of other software images that you might have stored in flash memory.

Software Images

Release	Image Type	File Name
Cisco IOS XE.16.12.6	Universal	ie3x00-universalk9.16.12.06.SPA.bin
		ess3x00-universalk9.16.12.06.SPA.bin
	NPE	ie3x00-universalk9_npe.16.12.06.SPA.bin
Cisco IOS XE.16.12.5	Universal	ie3x00-universalk9.16.12.05.SPA.bin
		ess3x00-universalk9.16.12.05.SPA.bin
	NPE	ie3x00-universalk9_npe.16.12.05.SPA.bin

Release	Image Type	File Name
Cisco IOS XE.16.12.4	Universal	ie3x00-universalk9.16.12.04.SPA.bin
		ess3x00-universalk9.16.12.04.SPA.bin
	NPE	ie3x00-universalk9_npe.16.12.04.SPA.bin
Cisco IOS XE.16.12.3	Universal	ie3x00-universalk9.16.12.03.SPA.bin
		ess3x00-universalk9.16.12.03.SPA.bin
	NPE	ie3x00-universalk9_npe.16.12.03.SPA.bin
Cisco IOS XE.16.12.2	Universal	ie3x00-universalk9.16.12.02.SPA.bin
		ess3x00-universalk9.16.12.02.SPA.bin
	NPE	ie3x00-universalk9_npe.16.12.02.SPA.bin
Cisco IOS XE.16.12.1	Universal	ie3x00-universalk9.16.12.01.SPA.bin
		ess3x00-universalk9.16.12.01.SPA.bin
	NPE	ie3x00-universalk9_npe.16.12.01.SPA.bin

Automatic Boot Loader Upgrade

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

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

Caution Do not power cycle your switch during the upgrade.

Scenario	Automatic Boot Loader Response

If you boot Cisco IOS XE the first time	Boot loader may be upgraded to version "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

Summary of Software Installation Commands	
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.

Summary of Software Installation Commands	
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 Levels

The software features available on Cisco Catalyst ie3x00 Rugged and ESS3300 switches, fall under these base or add-on license levels.

Base Licenses

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

Add-On Licenses

Add-On Licenses require a 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.

To find information about platform support and to know which license levels a feature is available with, use Cisco Feature Navigator. To access Cisco Feature Navigator, go to https://www.cisco.com/go/cfn. An account on cisco.com is not required.

Feature Licenses

Feature Licenses are bound to aspecific 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 2 MRP licenses available for IE3x00.

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

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

Use "platform license feature [mrp-client | mrp-manager]" to add the license, then follow the SL or SLR process to activate the feature license.

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.

License Levels - Usage Guidelines

- Base licenses (Network-Advantage) are ordered and fulfilled only with a permanent license type.
- Add-on licenses (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 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, registering, de-registering, moving, and transferring licenses. 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.

Known Issues

This section contains information about the known issues in this release.

IGMP Snooping and Unregistered Multicast Packet Forwarding

- *Symptoms*: Although the mrouter port is configured and multicast receivers have sent igmp-joins to listen to registered multicast streams, unknown multicast streams that ingress the switch are forwarded to all the ports. The flooding may lead to reduction in bandwidth for registered multicast traffic.
- *Conditions*: The issue occurs when the switch receives unregistered multicast packets with a pure L2 configuration and an external IGMP snooping querier is configured on the VLAN. There should not be a membership join received on any VLAN ports.
- *Workaround*: To stop the VLAN, execute the command **`switchport block multicast`** on that interface, as shown in the following example:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface gigabitEthernet 1/10
Switch(config-if)#switchport block ?
  multicast  Block unknown multicast addresses
  unicast    Block unknown unicast addresses

Switch(config-if)#switchport block mu
Switch(config-if)#switchport block multicast
```

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

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 Gibraltar 16.12.x

Identifier	Description
CSCvo31697	The basic traffic is not forwarded across routed port until reboot with max user vlan configured.
CSCvo47740	Device does not adhere to its policy-map when oversubscribed.
CSCvq51010 (IE 3x00 only)	Traffic is getting flooded when configuring MACSEC on MRP BLOCKED.

Identifier	Description
CSCvr49453	Amber LED doesn't emit through light pipe for ports g2/5-6 (IEM-3300-6T2S).
CSCvr62487	Alarm Out is inverted.
CSCvs06943	Format usbflash0/1 options are only formatting to FAT32/vfat.
CSCvu86619	show tech-support port interface CLI may cause a crash when an invalid interface type is specified

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.6

Identifier	Description
CSCvw66345	IE3400 - Software-forwarding observed with Dot1X on 17.3.2a
CSCvw67744	IE3x00: PTP devices from a specific vendor fail to synchronize clocks when device is in forward mode
CSCvx12483	Web UI: Unable to access the GUI on some IE3x00 using HTTPS
CSCvx57271	Dying-gasp is not working in trunk mode
CSCvx66354	IE-3300/IE-3400: L4 ACLs not summarised properly causing some entries to not take effect
CSCvy42555	DHCP: Enabling dhcp snooping causes dhcp offer on voice-vlan port to be untagged

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.5

Identifier	Description
CSCvu50267	IE3400H drops packets with specific TCP sequence number.
CSCvu71779	Total output drops counter in show int x/y displays 0 when packets drop.
CSCvu74821	Delayed learning resulting unicast flood for long time and causing application impact.
CSCvu85569	When IE3300 has Auto-QoS configured, it prevents the AP from registering.
CSCvv24989	Spanning tree Blocked port moves to Forwarding state in the asic causing a loop.
CSCvv28310	IE3x00 crashes when served as HTTP server and image copy is initiated.
CSCvv29516	With SLR license on - unable to move from NA to NE license.
CSCvv39283	Software-forwarding observed with "no ip redirects" configured.
CSCvv43693	Router entry reprogramming upon mac add/deletion/move.
CSCvv50025	Mac-move not allowing to learn a mac address on a valid port.
CSCvv61938	Mac learnt via CTS Port SGT enabled interface leaves MATM entry while ages out.

Identifier	Description
CSCvv71131	After updating the firmware on the IE3400 and reload happens, the auth sessions fail to establish.
CSCvv89846	Interface / SVI Mac of one device overlaps with other device interfaces / SVI mac address.
CSCvw14308	Crash observed while removing - vlan in "IMSP DOT1X Process."
CSCvw18043	Unexpected routing observed for broadcast IP packet on subnet that does not match SVI.
CSCvw24101	Memory Leak on middle buffers, when DHCP snooping is enabled on IE3x00/ESS3300.
CSCvw29468	ARP packet duplication seen when IPDT enabled on the box.

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.4

Identifier	Description
CSCvt75704	Unicast ARP requests are reflected back on received ports when Dynamic APR Inspection is enabled.
CSCvt05022	IE3x00 STP BLK port pass through HSRP GARP packet.
CSCvt13209	Mac learnt not updating in \"sh mac address-table notification change\".
CSCvt98814	The physical member of the port-channel is logged as an input interface when DAI failures happen.

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.3

Identifier	Description
CSCvs55595	The custom SISF policy is not working with Dynamic ARP inspection (DAI) enabled.
CSCvs16099	ESS-3300 SYS LED is Off.

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.2

Identifier	Description
CSCvr18473	The custom SISF policy is not working on IE3x00.
CSCvr47365	Cisco IOS and IOS XE Software Common Industrial Protocol Denial of Service Vulnerabilities.

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.1

Identifier	Description
CSCvo08000	Jumbo frame bytes support not working on IE3400.

Identifier	Description
CSCvo36953 (IE 3x00 only)	Show inventory details needs to be unique for Adv Non-poe.
CSCvo56242	Traceback seen after express setup in IE3400-8T2S.

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 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 Services.

- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- 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.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) 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.

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)

© 2019–2021 Cisco Systems, Inc. All rights reserved.