Release Notes for Cisco 4000 Series ISRs, Cisco IOS XE Gibraltar 16.10.x

First Published: 2018-07-19

Last Modified: 2018-07-19

Cisco 4000 Series Integrated Services Routers Overview

Note Explore the Content Hub, the all new portal that offers an enhanced product documentation experience.

- Use faceted search to locate content that is most relevant to you.
- Create customized PDFs for ready reference.
- Benefit from context-based recommendations.

Get started with the Content Hub at content.cisco.com to craft a personalized documentation experience.

Do provide feedback about your experience with the Content Hub.

The Cisco 4000 Series ISRs are modular routers with LAN and WAN connections that can be configured by means of interface modules, including Cisco Enhanced Service Modules (SM-Xs), and Network Interface Modules (NIMs).

Note The Cisco IOS XE Bengaluru 17.4.1a is the first release for Cisco 4000 Series Integrated Services Routers in the Cisco IOS XE Bengaluru 17.4.1 release series.

The following table lists the router models that belong to the Cisco 4000 Series ISRs.

Cisco 4400 Series ISR	Cisco 4300 Series ISR	Cisco 4200 Series ISR
Cisco 4431 ISR	Cisco 4321 ISR	Cisco 4221 ISR
Cisco 4451 ISR	Cisco 4331 ISR	
Cisco 4461 ISR	Cisco 4351 ISR	

System Requirements

The following are the minimum system requirements:

Note There is no change in the system requirements from the earlier releases.

- Memory: 4GB DDR3 up to 16GB
- Hard Drive: 200GB or higher (Optional). (The hard drive is only required for running services such as Cisco ISR-WAAS.)
- Flash Storage: 4GB to 32GB

  Note There is no change in the flash storage size from the earlier releases. The flash storage size must be equal to the system memory size.

- NIMs and SM-Xs: Modules (Optional)
- NIM SSD (Optional)

For more information, see the Cisco 4000 Series ISRs Data Sheet.

Determining the Software Version

You can use the following commands to verify your software version:

- For a consolidated package, use the **show version** command
- For individual sub-packages, use the **show version installed** command

Upgrading to a New Software Release

To install or upgrade, obtain a Cisco IOS XE Gibraltar 16.12.1a consolidated package (image) from Cisco.com. You can find software images at http://software.cisco.com/download/navigator.html. To run the router using individual sub-packages, you also must first download the consolidated package and extract the individual sub-packages from a consolidated package.

Note When you upgrade from one Cisco IOS XE release to another, you may see *%Invalid IPV6 address* error in the console log file. To rectify this error, enter global configuration mode, and re-enter the missing IPv6 alias commands and save the configuration. The commands will be persistent on subsequent reloads.

For more information on upgrading the software, see the How to Install and Upgrade the Software section of the Software Configuration Guide for the Cisco 4000 Series ISRs.

Recommended Firmware Versions

Table 1: Recommended Firmware Versions, on page 3 provides information about the recommended Rommon and CPLD versions for releases prior to Cisco IOS XE Everest 16.4.1.

Table 1: Recommended Firmware Versions

Cisco 4000 Series ISRs	Existing RoMmon	Cisco Field-Programmable Devices
Cisco 4451 ISR	16.7(4r)	15010638 **Note** Upgrade CLI output has a typo and it would show the version incorrectly as 15010738 instead of 15010638. This does not impact the upgrade.
Cisco 4431 ISR	16.7(4r)	15010638 **Note** Upgrade CLI output has a typo and it would show the version incorrectly as 15010738 instead of 15010638. This does not impact the upgrade.
Cisco 4351 ISR	16.7(5r)	14101324
Cisco 4331 ISR	16.7(5r)	14101324
Cisco 4321 ISR	16.7(5r)	14101324
Cisco 4221 ISR	16.7(5r)	14101324

Upgrading the ROMMON Version on the Cisco 4000 Series ISR

For information about ROMMON compatability matrix, and ROMMON upgrading procedure, see the ROMMON Compatability Matrix and "ROMMON Overview and Basic Procedures" sections in the Upgrading Field-Programmable Hardware Devices for Cisco 4000 Series ISRs.

Upgrading Field-Programmable Hardware Devices

The hardware-programmable firmware is upgraded when Cisco 4000 Series ISR contains an incompatible version of the hardware-programmable firmware. To do this upgrade, a hardware-programmable firmware package is released to customers.

Generally, an upgrade is necessary only when a system message indicates one of the field-programmable devices on the Cisco 4000 Series ISR needs an upgrade, or a Cisco technical support representative suggests an upgrade.

From Cisco IOS XE Release 3.10S onwards, you must upgrade the CPLD firmware to support the incompatible versions of the firmware on the Cisco 4000 Series ISR. For upgrade procedures, see the Upgrading Field-Programmable Hardware Devices for Cisco 4000 Series ISRs.

Feature Navigator

You can use Cisco Feature Navigator to find information about feature, platform, and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on cisco.com is not required.

Limitations and Restrictions

The following limitations and restrictions apply to all releases:

• Cisco Unified Threat Defense , on page 4

Cisco Unified Threat Defense

The Cisco Unified Threat Defense (UTD) service requires a minimum of 1 to 4 GB of DRAM.

Cisco ISR-WAAS and AppNav-XE Service

The Cisco ISR-WAAS/AppNav service requires a system to be configured with a minimum of 8GB of DRAM and 16GB flash storage. For large service profiles, 16GB of DRAM and 32GB flash storage is required. Also, Cisco ISR-WAAS requires a minimum of 200GB SSD.

IPsec Traffic

IPsec traffic is restricted on the Cisco ISR 4451-X. The router has the same IPsec functionality as a Cisco ISR G2. The default behavior of the router will be as follows (unless an HSECK9 license is installed):

- If the limit of 1000 concurrent IPsec tunnels is exceeded, no more tunnels are allowed and the following error message appears:

```
%CERM-4-TUNNEL_LIMIT: Maximum tunnel limit of 1000 reached for Crypto functionality with
securityk9 technology package license.
```

- The throughput encrypted traffic supports 250 Mbps.
- The Cisco 4000 Series ISR does not currently support nested SA transformation such as:

```
crypto ipsec transform-set transform-1 ah-sha-hmac esp-3des esp-md5-hmac
crypto ipsec transform-set transform-1 ah-md5-hmac esp-3des esp-md5-hmac
```

- The Cisco 4000 Series ISR does not currently support COMP-LZS configuration.

USB Etoken

USB Etoken is not supported on Cisco IOS XE Denali 16.2.1.

Unified Communication on Cisco 4000 Series ISR

- For T1/E1 clocking design and configuration changes, For detailed information, see the following Cisco document: T1/E1 Voice and WAN Configuration Guide.
- For Cisco ISR 4000 Series UC features interpretation with CUCM versions, For detailed information, see the following Cisco document: Compatibility Matrix .
- For High density DSPfarm PVDM (SM-X-PVDM) and PVDM4 DSP planning, For detailed information, see the following Cisco document: DSP Calculator for DSP planning .

Yang Data Models

Effective with Cisco IOS XE Everest 16.5.1b, the Cisco IOS XE YANG models are available in the form of individual feature modules with new module names, namespaces and prefixes. Revision statements embedded in the YANG files indicate if there has been a model revision.

Navigate to *https://github.com/YangModels/yang* > *vendor* > *cisco* > *xe* >*1651*, to see the new, main cisco-IOS-XE-native module and individual feature modules attached to this node.

There are also XPATH changes for the access-list in the *Cisco-IOS-XE-acl.yang* schema.

The *README.md* file in the above Github location highlights these and other changes with examples.

CTI Configuration

CME does not support CTI configurations on Cisco 4000 Series ISRs.

New and Changed Information

New Hardware Features in Cisco IOS XE Gibraltar 16.10.1a

The following hardware is introduced in Cisco IOS XE Gibraltar 16.10.1a:

- Cisco 450 Voice Gateways - For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/routers/access/vg450/hardware/installation/guide/b_Vg450_hig.html.

New Software Features in Cisco 4000 Series ISRs Release Cisco IOS XE Gibraltar 16.10.1a

Important Starting from Cisco IOS XE Gibraltar 16.10.1a, PAK licenses are no longer valid for your device. You must migrate to Cisco Smart Licensing before you upgrade to the 16.10.1a version. To learn more about Cisco Smart Licensing, see the Smart Licensing Conifguration Guide.

For a more detailed overview on Cisco Licensing, go to https://cisco.com/go/licensingguide.

The following features are supported by the Cisco 4000 Series Integrated Services Routers for Cisco IOS XE Gibraltar 16.10.1a:

- Cisco Smart Licensing - The Smart Licensing Client feature is a standardized licensing platform that simplifies the Cisco software experience and helps you understand how Cisco software is used across your network. Smart Licensing is the next generation licensing platform for all Cisco software products. To learn what is Smart Licensing and how to use this licensing model, see the Smart Licensing Conifguration Guide.

  For a more detailed overview on Cisco Licensing, go to https://cisco.com/go/licensingguide.

- For information on migrating from existing Cisco IOS XE 3S releases to the Cisco IOS XE Gibraltar 16.10.1 release, see Cisco IOS XE Everest 16.4.1 Migration Guide for Access and Edge Routers.

- Supported Technology Configuration Guides—When a technology is supported on Cisco 4000 series ISR, the corresponding technology configuration guide is displayed on the product landing page.

- BNG: Enhancement to Show Tech Subscriber—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/isg/command/isg-cr-book/isg_m1.html#wp3145726977.

- Boot Statement Check: When upgrading their IOS software image, customers might sometimes delete their old image without updating the boot statement. This could result in entering the ROMMON (ROM Monitor) mode. To recover from the ROMMON mode, the following enhancements are supported for different use cases: 1. Reload the router with config-reg configuration -- Before reloading, the router checks if the first boot statement points to an image that exists and verifies it. If the image is missing or invalid, the users are prompted for confirmation to proceed with reload of the router. 2. Reload the router

with config-register 0x2102 - auto boot – The router checks if the boot variable is set properly, and accordingly prompts the users to proceed with caution. 3. Reload the router with config-register 0x2102 - auto boot and the boot variable (bootvar) is set, but there is no image in bootvar set path – The router checks if the bootvar is properly set and if there is any image set in the bootvar path. If there is no image in the bootvar path (hard disk/bootflash/flash, and so on), then the reload is cancelled with a warning message, and the users are prompted to correct the boot statement or copy the image to hard disk. 4. Auto boot and boot variable is set – If the image is present in the bootvar path, then the router reload is allowed.

- Cisco X.25 & XOT Support on Cisco 4000 Series ISRs—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/wan_smxl/configuration/xe-16-10/wan_smxl_xe16_10_book/wan-smxl-overview.html.
- Direct Cloud Access—For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/pfrv3/configuration/xe-16-10/pfrv3-xe-16-10-book/pfrv3.html.
- gRPC Dial-in and Dial-out—For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/1610/b_1610_programmability_cg/model_driven_telemetry.html
- IPv6: DNS Proxy Support for IPv6—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dns/configuration/xe-16-10/dns-xe-16-10-book/configuring_dns.html.
- IPv6: Proxy in VRF, DNS Request Gets—For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dns/configuration/xe-16-10/dns-xe-16-10-book/configuring_dns.html
- PMIPv6 Unequal Load Balance—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mob_pmipv6/configuration/xe-16-10/mob-pmipv6-xe-16-10-book/imo-pmipv6-multipath-support.html.
- RIB/CEF Routing: Enhancement to Show Tech Routing—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/isg/command/isg-cr-book/isg_m1.html#wp3145726977.
- Medium Density Fixed Port Analog Voice Gatewaysg—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/routers/access/vg450/hardware/installation/guide/b_Vg450_hig.html.

  .
- Time-Division Multiplexing Media Recording—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/NIM/software/configuration/guide/4gen-t1-e1-nim-guide.html#id_87022

  .
- MPLS over DMVPN—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/xe-16-10/sec-conn-dmvpn-xe-16-10-book/sec-conn-dmvpn-xe-16-10-book_chapter_010000.html#id_87580.
- Model Driven Telemetry-gRPC Dial-Out: Expands existing Model Driven Telemetry capabilities with the addition of gRPC protocol support and Dial-Out (configured) telemetry subscriptions.
- CUBE Media Proxy—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/configuration/cube-book/voi-cube-media-proxy.html.

- NAT CLI Simplification—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr/command/ipaddr-cr-book.html.
- OSPF: Statistics per OSPF Neighbor—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/command/ipv6-cr-book/ipv6-s5.html.
- PPPoE Control Traffic—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_plcshp/configuration/xe-16-8/qos-plcshp-xe-16-8-book/qos-plcshp-ctrl-pln-plc.html.
- SIP TLS Support on CUBE—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/configuration/cube-book/voi-cube-sip-tls.html.
- Smart Licensing—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/smart-licensing/qsg/b_Smart_Licensing_QuickStart.html.

  For a more detailed overview on Cisco Licensing, go to https://cisco.com/go/licensingguide.
- Support for Cisco Jabber, ATA 191, and KEM Modules—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/admin/configuration/manual/cmeadm/cmebasic.html.
- Enhancement to Show Tech PFR—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/pfrv3/configuration/xe-16-10/pfrv3-xe-16-10-book/pfrv3.html
- VXLAN GPE P2MP Tunnels Support—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/configuration/xe-16-10/ce-xe-16-10-book.htm
- Web User Interface—Supports an embedded GUI-based device-management tool that provides the ability to provision the router, simplifies device deployment and manageability, and enhances user experience. The following features are supported on Web User Interface from Cisco IOS XE Fuji 16.9.1:
  - Smart Licensing and Specific License Reservation
  - Quality of Service/Cisco Application Visibility and Control (AVC)
  - VLAN/VTP

  Note The VLANs feature is supported only on routers with switch port module or routers with built-in switch port

  - For information on how to access the Web User Interface, see Configure the Router for Web User Interface section.
- YANG Data Models—For the list of Cisco IOS XE YANG models available with this release, navigate tottps://github.com/YangModels/yang/tree/master/vendor/cisco/xe/16101. Revision statements embedded in the YANG files indicate if there has been a model revision. The README.md file in the same github location highlights changes that have been made in the release.

Configure the Cellular Back-off Operation

For a router with 3G/4G interface, sometimes service provider network might be busy, congested, in maintenance or in fault state. In such circumstances, service provider network rejects session activation request from the router by returning reject cause code 33 as a response of the activation request. After the router receives the reject cause, the router uses the back-off operation with the pre-defined timer value which could be carrier-specific. While back-off operation is in progress, no new session activation request is sent out from the router. After the back-off period is up, new session activation request is sent out from the router.

Note: There is no command to disable the cellular back-off feature on the router.

The following example shows how to configure the cellular back-off feature to stop continuous session activation requests back to the router:

```
Router#show cell 0/2/0 all
Profile 1, Packet Session Status = INACTIVE
Profile 2, Packet Session Status = INACTIVE
Profile 3, Packet Session Status = INACTIVE
.
.
.
Success rate is 0 percent (0/5)
Router#show cell 0/2/0 c
Profile 1, Packet Session Status = INACTIVE
Profile 2, Packet Session Status = INACTIVE
Profile 3, Packet Session Status = INACTIVE
RouterCall end mode = 3GPP
RouterSession disconnect reason type = 3GPP specification defined(6)
RouterSession disconnect reason = Option unsubscribed(33)
RouterEnforcing cellular interface back-off
 Period of back-off = 1 minute(s)
Profile 4, Packet Session Status = INACTIVE
...
Profile 16, Packet Session Status = INACTIVE

.
.
.
Profile 16, Packet Session Status = INACTIVE
```

Configure the Router for Web User Interface

This section explains how to configure the router to access Web User Interface. Web User Interface require the following basic configuration to connect to the router and manage it.

- An HTTP or HTTPs server must be enabled with local authentication.
- A local user account with privilege level 15 and accompanying password must be configured.
- Vty line with protocol ssh/telnet must be enabled with local authentication. This is needed for interactive commands.
- For more information on how to configure the router for Web User Interface, see Cisco 4000 Series ISRs Software Configuration Guide, Cisco IOS XE 17.

Entering the Configuration Commands Manually

To enter the Cisco IOS commands manually, complete the following steps:

Before you begin

If you do not want to use the factory default configuration because the router already has a configuration, or for any other reason, you can use the procedure in this section to add each required command to the configuration.

Procedure

Step 1 Log on to the router through the Console port or through an Ethernet port.

Step 2 If you use the Console port, and no running configuration is present in the router, the Setup command Facility starts automatically, and displays the following text:

```
--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]:
```

Enter no so that you can enter Cisco IOS CLI commands directly.

If the Setup Command Facility does not start automatically, a running configuration is present, and you should go to the next step.

Step 3 When the router displays the user EXEC mode prompt, enter the **enable** command, and the enable password, if one is configured, as shown in the following example:

```
Router> enable
password password
```

Step 4 Enter config mode by entering the **configure terminal** command, as shown in the following example.

```
Router> config terminal
Router(config)#
```

Step 5 Using the command syntax shown, create a user account with privilege level 15.

Step 6 If no router interface is configured with an IP address, configure one so that you can access the router over the network. The following example shows the interface GigabitEthernet 0/0/0 configured.

```
Router(config)# interface gigabitethernet 0/0/0
Router(config-if)# ip address 10.10.10.1 255.255.255.248
Router(config-if)# no shutdown
Router(config-if)# exit
```

Step 7 Configure the router as an http server for nonsecure communication, or as an https server for secure communication. To configure the router as an http server, enter the **ip http server** command shown in the example:

```
Router(config)# ip http secure-server
```

Step 8 Configure the router for local authentication, by entering the ip http authentication local command, as shown in the example:

```
Router(config)# ip http authentication local
```

Step 9 Configure the vty lines for privilege level 15. For nonsecure access, enter the transport input telnet command. For secure access, enter the transport input telnet ssh command. An example of these commands follows:

```
Router(config)# line vty 0 4
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
```

```
Router(config-line)# transport output telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# transport output telnet ssh
Router(config-line)# exit
Router(config)# line vty 5 15
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport output telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# transport output telnet ssh
Router(config-line)# end
```

Resolved and Open Bugs

This section provides information about the caveats in Cisco 4000 Series Integrated Services Routers and describe unexpected behavior. Severity 1 caveats are the most serious caveats. Severity 2 caveats are less serious. Severity 3 caveats are moderate caveats. This section includes severity 1, severity 2, and selected severity 3 caveats.

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool . This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products. Within the Cisco Bug Search Tool, each bug is given a unique identifier (ID) with a pattern of CSCxxNNNNN, where x is any letter (a-z) and N is any number (0-9). The bug IDs are frequently referenced in Cisco documentation, such as Security Advisories, Field Notices and other Cisco support documents. Technical Assistance Center (TAC) engineers or other Cisco staff can also provide you with the ID for a specific bug. The Cisco Bug Search Tool enables you to filter the bugs so that you only see those in which you are interested.

In addition to being able to search for a specific bug ID, or for all bugs in a product and release, you can filter the open and/or resolved bugs by one or more of the following criteria:

- Last modified date
- Status, such as fixed (resolved) or open
- Severity
- Support cases

You can save searches that you perform frequently. You can also bookmark the URL for a search and email the URL for those search results.

Note If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.

We recommend that you view the field notices for the current release to determine whether your software or hardware platforms are affected. You can access the field notices from the following location:

http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html

Using the Cisco Bug Search Tool

For more information about how to use the Cisco Bug Search Tool , including how to set email alerts for bugs and to save bugs and searches, see Bug Search Tool Help & FAQ .

Before You Begin

Note You must have a Cisco.com account to log in and access the Cisco Bug Search Tool . If you do not have one, you can register for an account.

Procedure

Step 1 In your browser, navigate to the Cisco Bug Search Tool .

Step 2 If you are redirected to a Log In page, enter your registered Cisco.com username and password and then, click Log In.

Step 3 To search for a specific bug, enter the bug ID in the Search For field and press Enter.

Step 4 To search for bugs related to a specific software release, do the following:

a) In the Product field, choose Series/Model from the drop-down list and then enter the product name in the text field. If you begin to type the product name, the Cisco Bug Search Tool provides you with a drop-down list of the top ten matches. If you do not see this product listed, continue typing to narrow the search results.

b) In the Releases field, enter the release for which you want to see bugs.

The Cisco Bug Search Tool displays a preview of the results of your search below your search criteria.

Step 5 To see more content about a specific bug, you can do the following:

- Mouse over a bug in the preview to display a pop-up with more information about that bug.
- Click on the hyperlinked bug headline to open a page with the detailed bug information.

Step 6 To restrict the results of a search, choose from one or more of the following filters:

Filter	Description
Modified Date	A predefined date range, such as last week or last six months.
Status	A specific type of bug, such as open or fixed.
Severity	The bug severity level as defined by Cisco. For definitions of the bug severity levels, see Bug Search Tool Help & FAQ .
Rating	The rating assigned to the bug by users of the Cisco Bug Search Tool .
Support Cases	Whether a support case has been opened or not.

Your search results update when you choose a filter.

Resolved and Open Bugs in Cisco 4000 Series Integrated Services Routers

This section contains the following topics:

Open Caveats - Cisco IOS XE Gibraltar 16.10.2

There are no open caveats in Cisco IOS XE Gibraltar 16.10.2 release.

Resolved Caveats - Cisco IOS XE Gibraltar 16.10.2

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCvn02171	HOLE is not created when 'acl default passthrough' configured
CSCvn28017	ISR4331 Routers May Crash When "eigrp default-route-tag" Configured on IPv4 AF
CSCvn30138	Crash with show service-insertion service-context command in AppNav Cluster
CSCvn38590	CTS policies download fails with Missing/Incomplete ACEs error
CSCvn51553	QFP crashes with a HW interrupt
CSCvn72973	Device is getting crashed on the "cts role-based enforcement"
CSCvo00968	Radius attr 32 NAS-IDENTIFIIER not sending the FQDN.
CSCvo03458	PKI "revocation check crl none" does not fallback if CRL not reachable
CSCvo08337	Crash when inserting second NIM-2MFT-T1/E1 in 4331
CSCvo24170	Crash due to chunk corruption in ISIS code
CSCvo25785	Crash on an LNS router in process ACCT Periodic Proc
CSCvo27553	PKI incorrect fingerprint calulation during CA authentication
CSCvo38985	Crash at the VRF configuration

Open Caveats - Cisco IOS XE Gibraltar 16.10.1a

All open bugs for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCvj17326	Cisco 4000 Series ISR crashes in o2_cavm_pci_unlock when forwarding large packets for VPLS.
CSCvm25851	Qfp-bqs-internal ucode still crashes with fix in CSCvc35307.
CSCvm39485	Small clock changes or time drifts can cause GETVPN TBAR drops (GDOI/IPSEC-PI)
CSCvm51112	"clear crypto sa vrf MyVrf" triggers crash after updating pre-shared-keys
CSCvm55018	A control plane delete command to flush the queue is not being drained out of the command queue.

Caveat ID Number	Description
CSCvm57021	Crash in CENT-MC-0 process after Doubly-linked list corruption.
CSCvm75066	MPLSoVPN: Change behavior of default route in NHRP. Must insert 0.0.0.0/0 instead of /32.
CSCvm76452	IPSec background crash while sending SNMP trap.
CSCvm76464	The device crashes due to QoS in case of 4k subscribers per subinterface
CSCvm78937	The device crashes when running show ip nhrp brief.
CSCvm80502	Traceroute not working when sourced from NAT Inside interface.
CSCvm81807	The "fman" crashes after calling bipc_buffer_alloc after CPP_FNF_EVENT_MONITOR_CREATE.
CSCvm91323	The device crashes with reload reason: LocalSoftADR and core file generated cpp-mcplo-ucode.
CSCvm93159	Cisco 4000 Series ISRs IPSec VPN with extendable NAT can not be established.
CSCvm93589	Performance monitor not working when "collect transport round-trip-time" is configured.
CSCvm93725	Cisco 4331 ISR static MAC add/remove breaks physical link connectivity.
CSCvm93794	FlexVPN MPLS - label in CEF not added when shortcut to hub is created (by glitch)
CSCvm99745	It does not allow to configure multiple CFM IP SLA with the same source MEP on Cisco 4000 Series ISRs.
CSCvm99778	IOS-PKI: grant auto trustpoint <tp_name> does not work with IOS Sub CA
CSCvn01894	The device IF down/up happen when config "plim ethernet vlan filter disable" with copper SFP.
CSCvn07478	Ethernet FRR switchover takes more than 200ms on EPA10 and EPA100 if remote Rx fiber is pulled.
CSCvn07614	Out of Band DTMF events not Passing to CUCM via SCCP When Using IOS MTP.
CSCvn08656	Cisco 4000 Sereis ISRs netflow miss MMA after DMVPN flapping.
CSCvn09472	The cpp_cp_svr memory leak in module: IPHC Svr Info_st.
CSCvn12253	The software crashes due to watchdog after entered switchport command.
CSCvn14454	iWAN router PDP crashes.
CSCvn17655	Removing ip flow monitor from an interface caused ESP crash.
CSCvn18757	The device crashes after removing a service-policy while the BQS is stuck.
CSCvn19382	A crash is seen after comparing tunnel FIB entries.

Caveat ID Number	Description
CSCvd66978	Cisco 4300 ISR is considered as SKU and processing DLC conversion with red alert/warning.
CSCvm58916	Hseck9 and macsec licenses are present in SL-Only when the configs are not present.
CSCvm65937	Cisco 4351 ISR: Licenses go to OOC and then later gets authorized even when tags are available in VA.
CSCvn01251	Cicco Smart Licensing: Router hangs when downgrading from Cisco IOS XE 16.10 to Cisco IOS XE 16.6.4 CCO image (SL Registered).
CSCvm75711	Wrong licenses listed in show version output when router boots with Cisco IOS XE 16.10.1 image.
CSCvm81231	DLC status seen as complete in **show platform software lic dlc** inspite of DLC conversion failure on the device.
CSCvm79483	Router gets double registered and consumes two licenses on the same device.
CSCvm88430	HSECk9 which was AUTH before after deregiter is still available.
CSCvn14895	DLC conversion is converting more than what is listed in **show platform dlc** on production server.
CSCvn06149	Error in Quantity tab to reserve licenses on SLR.
CSCvn14928	Hseck9 license count seen 0 inspite of the license being DLC converted.
CSCvn15214	Device registered to CSSM loosing the registration on upgrade from Cisco IOS XE 16.06.04 CCO SL-mode to Cisco IOS XE 16.10.01.
CSCvm63242	IOS_LICENSE_IMAGE_APPLICATION-3-FAILED: license request failed logs on upgrading to Cisco IOS XE 16.10 image.
CSCvn16433	SKU, Quantity and Smart License values seen incorrect/empty on Satellite Server 5.0.1 in Stage environment.
CSCvn16537	Authorized HSeck9 license not recorded in VA for the registered product instance.
CSCvm62646	Clean up unwanted interfaces under call-home like appnav.
CSCvn20629	Hseck9 license not displayed as consumed on CSSM portal after DLC conversion.
CSCvn22505	Device registration to Satellite 5.0.1 production failing with reason failure to send HTTP messages.
CSCvn22535	Inconsistency between license naming conventions between CSSM and Satellite under conversion history.
CSCvn23045	Conversion History Tab missing on Satellite server 6.0.1 production.

Resolved Caveats - Cisco IOS XE Gibraltar 16.10.1a

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCve14080	Error message "LID: Handle 0x0 is invalid" filling console log.s
CSCvg32796	External Interface on the PfR MC stuck in the shutdown state.
CSCvg54267	Cisco IOS and IOS XE Software Cisco Discovery Protocol Denial of Service vulnerability.
CSCvg56110	Error and pending objects when mma policy flap with egress monitor for multi-VRF case.
CSCvh49364	PFRv3 Incorrect time-stamp in traffic-class router change history.
CSCvh57657	NAT MIB not populated when using traditional NAT
CSCvh97101	NAT-HA on Cisco 2900s breaks if it is asymmetric routing.
CSCvi13686	Cisco 4000 Series ISR - Outbound faxes originating from certain fax servers may fail to send.
CSCvi32156	Router crashes when DMVPN tunnel moves accoss ports.
CSCvi50061	Evaluate NTP vulnerabilities.
CSCvi63425	Cisco 4400 ISR router cpp crashed when configured HSRP with PMIPv6.
CSCvi63840	VIF interface counters do not increment with multicast service reflection on IOS-XE.
CSCvi81216	Cisco 4000 Series ISR LISP-Ping src Looback(lo is EID) has been dropped after reloading.
CSCvi90729	IKEv2 CoA does not work with ISE (coa-push=TRUE instead of true).
CSCvi94425	TBAR issues on KS after running "clear crypto gdoi ks coop role".
CSCvj01098	Evaluation of IOS-XE and IOS for OpenSSL CVE-2018-0739 and CVE-2018-0733.
CSCvj02081	CPP crash on L2TP router.
CSCvj03263	H225 gatekeeper request dropping under "ALG PARSER" with ZBF.
CSCvj06909	Reverse-route configuration is unsupported under gdoi crypto map.
CSCvj08248	Packet throughput drops down when enable tunnel visibility with single tcp flow(>1MPPS).
CSCvj11876	Provide Passthrough Reason in IOS-XE for AppNav.
CSCvj13382	IOS-XE FIPS mode is enabled by default in QFP even if it is not enabled in CLI.
CSCvj16489	Enabling IPSec Anti-Replay with SNS in an IPSec profile enables it globally.

Caveat ID Number	Description
CSCvj16818	Cisco 4331 ISR crashes immediately following auto-CA certificate renewal.
CSCvj17682	The Cisco 4300 ISR MAC filtering incorrectly set on builtin ports.
CSCvj20302	Cisco 4000 Series ISR MTP not performing RFC2833 payload type conversion.
CSCvj25678	The device crashes after failing to modify xcode.
CSCvj29593	The debug platform condition start causes keepalive failures with Vasi interface.
CSCvj41550	The default channel operation state changing from I/O to D/O failed when zero-sla enabled.
CSCvj47957	Packet trace does not work with re-injected UTD packets.
CSCvj50005	Cisco 4000 Series PPE ucode crash when processing ipsec traffic on CWS tunnel.
CSCvj50410	Cisco 4331 ISR no collisions count up on duplex mismatch condition.
CSCvj51510	The device crashes after service-policy APPNAV change on WAAS instance.
CSCvj53634	The OID - adslAtucCurrOutputPwr returns incorrect output.
CSCvj57502	The memory leak@CENT-BR-0 when change the path label frequently.
CSCvj61603	The **dtmf-interworking rtp-nte** command breaking software MTP.
CSCvj71853	The **sdavc_ppdk.pack force** command not accepted during boot up.
CSCvj72273	GETVPN Key Servers after split may generate TEK with same SPI but different key material.
CSCvj76662	GetVPN TBAR failure does not generate syslogs.
CSCvj84158	PfRv3: BR may crash due to Channel Creation/Modification and Next-Hop State (Copied from CSCva72274).
CSCvj86316	Different ISP name smartprobes are received in branch WAN interface, the channel cannot detect.
CSCvj90426	Dash i2c Kernel message outputted during boot up.
CSCvj90814	Cisco 4000 Series ISR crashes due to memory corruption.
CSCvj91448	PKI:-IP address parsing issue while printing the subject name if classless IP is used in Trustpoint.
CSCvk00074	cBR-8 crash after issuing show platform hardware qfp active infrastructure bqs
CSCvk02072	Hoot-n-holler multicast traffic marked with DSCP 0.
CSCvk12152	Unable to remove command ip nat inside destination.
CSCvk27007	MGCP status remains Down after IOS upgrade caused by CSCvh70570.

Caveat ID Number	Description
CSCvk29692	DSP detected FXO "supervisory disconnect dualtone mid-call" is treated as CNG tone.
CSCvk30939	Memory corruption at PKI session end.
CSCvk34152	Invalid throughput level in the "show version" output.
CSCvk53938	IOS-XE : IPv6 ACL for Tunnel QoS not matched.
CSCvk62278	DSCP value for MGCP signaling traffic cannot be configured.
CSCvk62742	The on demand PCM captures fail on some IOS-XE versions.
CSCvk63602	WAAS Policy Configuration push may caused AppNav Class-maps programming issue in TCAM.
CSCvk65072	The device crashes due ZBF + NAT.
CSCvk70428	Router crashed when enrollment type changed from http to pem in between certificate request process.
CSCvm03696	ISDN PRI calls getting dropped with cause 47 because of bad interaction between CDAPI and TSP layers.
CSCvm14346	The devices memory corruption of mdl_tbl due to fia-history CLI.
CSCvm66103	The device crashes due to communication failure - IPC (Inter-Procedure Call) messages between DSP and RP.
CSCvm67419	Cisco 4400 ISR MACsec drops small frames.
CSCvm98429	Cisco IOS XE Gibraltar 16.10 startup-config got wiped out when load image with config-register set to 2142.

Related Documentation

Platform-Specific Documentation

For information about the Cisco 4000 Series ISRs and associated services and modules, see:

Documentation Roadmap for the Cisco 4000 Series ISRs,Cisco IOS XE 16.x .

Cisco IOS Software Documentation

The Cisco IOS XE Fuji 16.x software documentation set consists of Cisco IOS XE Fuji 16.x configuration guides and Cisco IOS command references. The configuration guides are consolidated platform-independent configuration guides organized and presented by technology. There is one set of configuration guides and command references for the Cisco IOS XE Fuji 16.x release train. These Cisco IOS command references support all Cisco platforms that are running any Cisco IOS XE Fuji 16.x software image.

See http://www.cisco.com/en/US/products/ps11174/tsd_products_support_series_home.html

Information in the configuration guides often includes related content that is shared across software releases and platforms.

Additionally, you can use Cisco Feature Navigator to find information about feature, platform, and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on cisco.com is not required.

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.

© 2019 Cisco Systems, Inc. All rights reserved.