# Release Notes for Cisco 4000 Series ISRs, Cisco IOS XE Fuji 16.8.x

**First Published:** 2018-03-31

**Last Modified:** 2018-04-24

## 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).

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 4351 ISR | |

### System Requirements

The following are the minimum system requirements:

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

- NIM SSD (Optional)

For more information, see the .

# 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 Fuji 16.9.1 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 need to first download the consolidated package and extract the individual sub-packages from a consolidated package.

For information about upgrading software, see the "How to Install and Upgrade Software" section in the Software Configuration Guide for the Cisco 4000 Series ISRs.

## Recommended Firmware Versions

Table 1: Recommended Firmware Versions, on page 2 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<br>**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<br>**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(3r) | 14101324 |
| Cisco 4331 ISR | 16.7(3r) | 14101324 |
| Cisco 4321 ISR | 16.7(3r) | 14101324 |
| Cisco 4221 ISR | 16.7(3r) | 14101324 |

## Upgrading the ROMMON Version on the Cisco 4000 Series ISR

For information about ROMMON and upgrading procedure, see the "ROMMON Overview and Basic Procedures" section 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 3
- Cisco ISR-WAAS and AppNav-XE Service, on page 3
- IPsec Traffic, on page 3
- USB Etoken, 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.

### CUBE–SRTP Calls

Cisco IOS XE Everest release 16.5.1 is not recommended for Cisco Unified Border Element deployment involving SRTP calls.

### Encrypted Traffic Analytics Record

When the router is reloaded with large configuration, the router generates a high number of messages for initializing the features in data plane and the Encrypted Traffic Analytics (ETA) record may not be exported. This happens only when the ETA **inactive timeout** command is configured on the router. To avoid this issue, you can configure the **inactive timeout** commad after the router reloads.

### 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.

## New Features and Important Notes About Cisco 4000 Series ISRs Release Fuji 16.8.1

This section describes new features in Cisco IOS XE Fuji 16.8 that are supported on the Cisco 4000 Series ISRs.

# New and Changed Information

## New Hardware Features in Cisco IOS XE Fuji 16.8.1

The following features are supported by the Cisco 4000 Series Integrated Services Routers for Cisco IOS XE Fuji 16.8.1:

- NIM-4SHDSL-EA—For detailed information, see the following Cisco documents: https://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/software/feature/guide/GSHDSL_EFM_ATM_NIM.html and https://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/NIM/hardware/installation/guide/G-SHDSL-NIM-HIG.html.

## New Software Features in Cisco 4000 Series ISR Release Cisco IOS XE Fuji 16.8.1

The following features are supported by the Cisco 4000 Series Integrated Services Routers for Cisco IOS XE Fuji 16.8.1:

- For information on migrating from existing Cisco IOS XE 3S releases to the Cisco IOS XE Fuji 16.8.1 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.
- Ability to Use Suite B Algorithms with GIKEv2 with Registration Interface—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_getvpn/configuration/xe-16-7/sec-get-vpn-xe-16-8-book/sec-get-vpn-suiteb.html.
- Addition of TR-111 Support—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/bbdsl/configuration/xe-16-8/bba-xe-16-8-book/bba-tr-069-agent.html.
- Advertise IPv6 Link Endpoint Information—For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_isis/configuration/xe-16-8/irs-xe-16-8-book/irs-is-is-advertise-ipv6-link-endpoint-info.html.
- Aggregate Mode Support for RAR over PPPoE—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/routers/access/4400/software/configuration/xe-16-8/isr4400swcfg-xe-16-8-book/isr4400swcfg-xe-16-8-book-1_chapter_011000.html#reference_lfm_l2r_s1b.
- Cisco 4000 Series ISR Baseline Programmability 4GbE Platform Support—For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/168/b_168_programmability_cg/cli_python_module.html.
- Direct Cloud Access IWAN2.3—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/pfrv3/configuration/xe-16-8/pfrv3-xe-16-8-book.html.
- Guest Shell (On-Box Python)- Python programmability provides a Python module that allows users to interact with the IOS using CLIs. The feature is now available on Cisco 4000 Series Integrated Services Router models with a minimum of 4 GB RAM. Pls reword, GuestShell not runs on all ISR4K variants. Prior to 16.8 it only worked on 8G platforms.
- HSECK9 License Enhancement—Limits for number of tunnels and crypto throughput are enhanced in this release. New throughput limit is 250 Mbps each direction and number of tunnels is 1000.

- IOS-XE: VRRPv3 MIB-based on RFC 6527—For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/routers/access/4400/technical_references/4400_mib_guide/isr4400_MIB.html.
- IPv6 Enablement: SGACL Enforcement—For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cts/configuration/xe-16-8/sec-usr-cts-xe-16-8-book/sec-cts-sgacl.html.
- IPv6 Enablement: Inline Tagging and Caching—For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cts/configuration/xe-16-8/sec-usr-cts-xe-16-8-book/sec-cts-sgacl.html.
- Line Command Access Class VRF Awarenesss—For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/bbdsl/configuration/xe-16-8/bba-xe-16-8-book/bba-vrf-aware-access-class-line.html.
- Model-Based AAA—Implements the NETCONF Access Control Model (NACM). NACM is a form of role-based access control (RBAC) specified in RFC 6536.
- NETCONF Global Session Lock and Kill Session—Provides a global lock and the ability to kill non-responsive sessions in NETCONF. During a session conflict or client misuse of the global lock, NETCONF sessions can be monitored via the show netconf-yang sessions command, and non-responsive sessions can be cleared using the clear configuration lock command.
- NETCONF and RESTCONF Debug commands—Commands for debugging were added.
- PKI: OCSP Enhancement—The Online Certificate Status Protocol (OCSP) for the Public Key Infrastructure (PKI) component supports receiving multiple OCSP single-responses in Cisco IOS. You can use PKI debugs such as “CRYPTO_PKI: Number of singleResponses in OCSP response: 10” to see the number of single responses received in an OCSP response. For more details, see RFC 6960.
- PKI Serviceability—Serviceability helps to understand certificate enrolment, reenrolment, and rollover failures, triggering of events related to the mentioned events, as well as CRL failures. As part of this feature, the following serviceability improvements are supported for Public Key Infrastructure (PKI), which helps track the sequence of events that happened before a certificate expiry or a certificate validation failure. Use the **show tech-support PKI** command to see information about PKI. Refer to the Security Command Reference for details about this show command.
- Serviceability of UTD—For detailed information, see the following Cisco document: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xe-16-8/sec-data-utd-xe-16-8-book.html.
- Support SPAN on Drop for Packets Dropped via the Forwarding Pipeline—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/lanswitch/configuration/xe-16-8/lanswitch-xe-16-8-book/lnsw-conf-erspan.html.
- Support for Voice Hunt Group Features on Cisco Unified Survivable Remote Site Telephony—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cusrst/admin/sccp_sip_srst/configuration/guide/SCCP_and_SIP_SRST_Admin_Guide/enhanced_srst.html.
- Support for Music on Hold from a Live Feed on Unified CME—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/cmemoh.html.

- Support for Voice Hunt Group with Shared Lines on Unified CME—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/cmecover.html.
- Visibility Enhancements—For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xe-16-8/sec-data-utd-xe-16-8-book/snort-ips.html .
- VRF Support for Export of Encrypted Traffic Analytics—For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_eta/configuration/xe-16-8/sec-data-encrypted-traffic-analytics-xe-16-8-book.html
- VXLAN Fragment UDP Source Port—For detailed information, see the following Cisco document: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/configuration/xe-16-8/ce-xe-16-8-book/vxlan-gpe-tunnel.html
- 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 16.8.1:
  - Day Zero Configuration
  - Python Developer Sandbox
  - Debug Bundle
  - Troubleshooting Audit Support
  - 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 to https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1681.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.Starting with Cisco IOS XE 16.8.1, the Operational Data Parser Polling feature is deprecated. All operational data models product provide direct operational data model access, hence this feature is no longer required.

## 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.
- You can use the Cisco IOS CLI to enter the necessary configuration commands. To use this method, see Entering the Configuration Commands Manually, on page 7.

### 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 Fast Ethernet 0 configured.

```
Router(config)# int FastEthernet0
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
```

## Caveats

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.

## Caveats in Cisco 4000 Series Integrated Services Routers

This section contains the following topics:

## Open Caveats - Cisco IOS XE Fuji 16.8.1

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

| Caveat ID Number | Description |
|---|---|
| CSCvf34608 | Excessive "Reflector" Tracelogs |
| CSCvg93505 | Cisco 4400 Series ISRs as primary KS crashed while removing gikev2(suite-b) group from KS |
| CSCvg95213 | Cisco 4400 Series ISRs: speed/duplex disappear from **show run** after **shut down** and **reload**. |
| CSCvh02575 | PLATFORM_INFRA-5-IOS_INTR_OVER_LIMIT error with traceback. |
| CSCvh24986 | Failed to get LSC certificate from Microsoft CA. |
| CSCvh47124 | Next-hop is wrong in route-import table on branch when you delete the WAN interface and reconfigure it<br>. |
| CSCvh57108 | CPUHOG on QoS statistics collection for DMVPN. QoS crash with DMVPN/NHRP. |
| CSCvh60766 | Cisco4431 ISR crashed while verifying performance at IPv6 MPLS scale. |
| CSCvh62615 | There is junk entry in route-import table on branch when shutdown/no shutdown WAN interface<br>. |
| CSCvh66033 | IKEv2 - Crash with segmentation fault when debugs crypto ikev2 are enabled. |
| CSCvh66642 | uIDB leaks at the DMVPN hub if the route to remote NBMA is not learned. |
| CSCvh78116 | IOS-XE: HTTP WebUI works even when disabled. |
| CSCvh79640 | Cisco 4000 Series ISRs: BDI unreachable when interface has HSRP-enabled subinterfaces. |
| CSCvh89773 | Bootloop due to file system errors. |
| CSCvh91443 | Cisco 4000 Series ISRs: Crashed due to CPUHOG Net background. |
| CSCvh97818 | The show voice call command missing print out dsp statistics in Cisco 4000 Series ISRs. |
| CSCvi01745 | cpp_cp_svr crashes, causing reload. |
| CSCvi02816 | ZBF not able to identify the WAAS optimized flow and drops ACK. |
| CSCvf82853 | RPID not updated in Transfer Scenario involving TDM trunk. |

| Caveat ID Number | Description |
|---|---|
| CSCvg06563 | BE4K Memory leak during bulk register request from portal. |
| CSCvg30991 | IOS-XE routers: Memory leak observed on process ivr: peer_item_t in AFW_application_process. |
| CSCvg40933 | MoH not heard when conf initiator drops from conference [specifically when Holdee xfers the call] |
| CSCvg42218 | BE4K VRF failed to associate if binding is used in tenant. |
| CSCvh41761 | Media failure when RTP port 6784 is allocated by CUBE. |
| CSCvh61030 | Present Call Idle State does not work with Seq Vhg with Shared lines. |
| CSCvh63857 | Memory leak in some SBC functions. |
| CSCvh82112 | Memory leak under process RECMSPAPP in IOSd. |
| CSCvh89821 | Router crash due to oce_process_ipv4_adj_perf<br>. |
| CSCvh95689 | CME SIP: MWI stops updating when using Solicited Notify option with CUE<br>. |
| CSCvh97268 | Vcube doesnot stream audio from a .wav file on bootflash. |
| CSCvh97818 | The **show voice call** command is missing print out dsp statistics in Cisco 4000 Series ISRs. |
| CSCvi00751 | Network information title is not localized to Japanese. |
| CSCvi00768 | Directory "records" string is displaying with invalid characters. |
| CSCvi00998 | Session transport tcp in voice register template is not working with autoreg phone configs. |
| CSCvi01650 | SIP Out-of-Dialog option Ping Group Shows Dial-Peers Marked as none. |
| CSCvi03536 | Local Directory search returns "No Records Found" when a Day 2 entry is used in "Last Name" field<br>. |
| CSCvi06417 | SIP stack matching the dial-peer when processing NOTIFY message causing call routing issues<br>. |
| CSCvi06897 | Dialpeer matching for inbound SIP profile fails with VRFs<br>. |

## Resolved Caveats - Cisco IOS XE Fuji 16.8.1

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

| Caveat ID Number | Description |
|---|---|
| CSCvf68261 | Crashes when printing IPSEC anti-replay error. |
| CSCvf87437 | High memory utilization in the QFP of QM RM process. |
| CSCvf92182 | The show platform software rg f0 services rg-id 1 verbose shows network address backwards. |
| CSCvf95141 | Zone-based Firewall crashes on standby. |
| CSCvg01760 | Traceback-CPUHog seen on the device. |
| CSCvg28614 | Cisco 4000 Series ISR dialer interface traceroute is abnormal although communication is OK. |
| CSCvg36246 | SM-X-ES3s port connected to Ethernet-Internal x/0/0 always become block port. |
| CSCvg38872 | Crash observed while sending 40K 4Kb pkt size html session with ETA configured on ESP 100. |
| CSCvh69641 | Cisco 4000 Series ISR core file is seen @cvmx_pow_work_response_async. |
| CSCvg34986 | Media recording on IOS-XE does not work if a refer is received immediately after the call is answered<br>. |
| CSCvh04245 | TDM-IP, QoS marking is varying to 0 and EF for the same RTP stream. |

## Open Caveats - Cisco IOS XE Fuji 16.8.2

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

| Caveat ID Number | Description |
|---|---|
| CSCvj17326 | Cisco 4400 ISR crashes in o2_cavm_pci_unlock when forwarding large packets for VPLS |
| CSCvj71660 | IKEv2 IPSec Tunnel stops passing traffic after two days, Tunnel remains up. |
| CSCvj78876 | CUBE: FPI Hung Sessions and Provisioning Failures observed in Standby CUBE. |
| CSCvk02072 | Hoot-n-holler multicast traffic marked with DSCP 0. |
| CSCvk02773 | Standby crashed when defaulting vlan config reconfig vlan config with fnf/et-analytics. |
| CSCvk60184 | Random crash of data plane with SRTP-SRTP / SRTP-RTP load tests. |
| CSCvk69075 | No calls shown in output "show call active voice brief" on CUBE & stale entries are present. |
| CSCvk71907 | Adaptive QOS : Target shape rate is set to floor rate when lower floor and ceiling rates are used |
| CSCvm01420 | CUBE crashes at sipSPI_ipip_vcc_CheckCodecSetTyp.e |

| Caveat ID Number | Description |
|---|---|
| CSCvm02627 | Incorrect Contact port 5060 used instead of 5061 by CUBE in "302 Moved Temporarily" message. |
| CSCvm16619 | CPP-mcplo-ucode crash while encrypting SIP packets with ALG NAT for SIP. |
| CSCvm20374 | Polaris Router - CPUHog - SNMP ENGINE crashed with Watchdog timeout. |
| CSCvm41298 | qfp-ucode-utah crashed with memory corruption. |
| CSCvm45589 | The initial IVR is not played when using custom BACD script in Cisco 4000 Series ISRs. |
| CSCvm51112 | "clear crypto sa vrf MyVrf" triggers crash after updating pre-shared-keys |
| CSCvm55465 | BGP updates missing ISIS advertising-bits led to LDP label purge on peer. |

## Resolved Caveats - Cisco IOS XE Fuji 16.8.2

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

| Caveat ID Number | Description |
|---|---|
| CSCuz14861 | IOS-XE Fails to correctly populate RTCP SSRC Field |
| CSCvf07576 | router reloaded when doing show BGP RT filter routes |
| CSCvf29213 | PFRV3: Site Prefix shows unreachable after removing and adding the specific route for the prefix |
| CSCvg29037 | Traceback is observed during mid-call media IP and port change |
| CSCvg62161 | Prefix SID delete after SSO. |
| CSCvh57108 | CPUHOG on QoS statistics collection for DMVPN. QoS crash with DMVPN/NHRP. |
| CSCvh57657 | NAT MIB not populated when using traditional NAT |
| CSCvh82112 | Polaris Routers - Memory leak under process RECMSPAPP in IOSd |
| CSCvh83319 | Interop vrrp doesnt work between cedge and vedge |
| CSCvh85788 | Local LAN-only prefix present in master route-import table but not present in site prefix DB |
| CSCvh91443 | ISR4k Crashed due to CPUHOG Net background. |
| CSCvh92275 | QoS Overrides loadbalancing to per prefix even with only session level policing applied |
| CSCvi01558 | iBGP dynamic peer using TTL 1 |
| CSCvi02816 | ZBF not able to identify the WAAS optimized flow and drops ACK |
| CSCvi06312 | Subsystem stopped: ios-emul-oper-db due to bgp table issue |

| Caveat ID Number | Description |
|---|---|
| CSCvi08303 | Standby RP Reloads due to Config Sync Failure When Applied Service-insertion WAAS on Physical Int |
| CSCvi08470 | OSPF: process crashed when the interface priority is configured for 0. |
| CSCvi16454 | Router crash due to PuntInject Keepalive Process - kmalloc failures |
| CSCvi22835 | Vz: Non-Polaris to Polaris ISSU compatibility issue |
| CSCvi25380 | Cisco IOS XE Software Authent., Author., and Accounting Login Authent. Remote Code Execution Vuln. |
| CSCvi26061 | RP crash @policymap_associated_to_multiple_instances |
| CSCvi34314 | ISR/C1100: interface down/up does not renew dhcp assigned ip address |
| CSCvi35232 | CME/BE4K crashes when trying to check help command for new device type BEKEM |
| CSCvi36875 | Restored DB is session-lock locked out with insane timeout after boot |
| CSCvi44988 | C1111-8P: random commands may trigger TACACS+ to crash |
| CSCvi54878 | Memory leaks seen at PKI_name_list_add(0xa139cc0)+0x3e |
| CSCvi55920 | ISR 4K Crashes issuing "show call active voice" |
| CSCvi62764 | OSPF SSPF/SRTE: absolute value configured for the SRTE tunnel not configured by OSPF. |
| CSCvi65958 | Standby RP crashes due to Memory usage in ospf_insert_multicast_workQ |
| CSCvi72996 | NMR TTL is wrongly considering eid-record of 0.0.0.0/0 for its calculation |
| CSCvi74088 | link local multicast packets are received when the SVI is in down state |
| CSCvi83419 | Router crash when removing route-target and with hard clear |
| CSCvi91714 | IPv6 address not assigned or delayed when RA Guard is enabled |
| CSCvi95775 | Reverse-tunnel routes under PMIPv6 MAG config not using configured distance metric |
| CSCvi96450 | Router crashed when lsp-mtu is changed |
| CSCvi98373 | msmr+xtr carsh during scale wireless roaming |
| CSCvj17682 | MAC filtering incorrectly set on builtin ports of ISR4300 |
| CSCvj20302 | ISR4k MTP not performing RFC2833 payload type conversion |
| CSCvj29593 | debug platform condition start causes keepalive failures with Vasi interface |
| CSCvj41224 | Crash when doing SNMP walk and applying QOS over a GRE tunnel |
| CSCvj49476 | Telnet Sessions Hang/Become unavailable at execution of "show run" |

| Caveat ID Number | Description |
|---|---|
| CSCvj52681 | dynamic vlan assignment causes all sisf entires under the port to be deleted |
| CSCvj71845 | Backup path incorrect for ring topology where high ISIS cost is configured on 1 link. |
| CSCvj73544 | ospf routing loop for external route with multiple VLINKs/ABRs |
| CSCvj78083 | Path of Last Resort Sending Probes in Standby State |
| CSCvj90089 | Crash while doing a conference call |
| CSCvj95351 | OSPF SR uloop : After issuing "clear ip ospf process". ospf process crashed. |
| CSCvk00824 | ISR1100 drops incoming ISIS Hello packets with "point-to-point" enabled, session is down |
| CSCvk37875 | High Availability system with two Voice Gateways - Crash |
| CSCvk50734 | Device Tracking - Memory leak observed with IPv6 NS/NA Packets . |
| CSCvk52495 | IP SLA multicast appear as "Unknown" |
| CSCvk66880 | CUBE incorrectly fomats SIP SDP |
| CSCvk69093 | CUBE is not responding to SIP INFO |
| CSCvm32630 | Crash due to out-of-memory condition Memory leak@CENT-BR-0 |

# 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.

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.