Release Notes for Cisco 4000 Series ISRs, Cisco IOS XE Everest 16.5

First Published: 2017-04-17

Last Modified: 2017-04-17

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.

Dial on Demand

Dial on demand feature is not supported on Cisco 4000 series platform.

CUBE–SRTP Calls

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

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 Everest 16.5.1b

This section describes new features in Cisco IOS XE Everest 16.5.1b that are supported on the Cisco 4000 Series ISRs.

New and Changed Information

New Software Features in Cisco 4000 Series ISR Release Cisco IOS XE Everest 16.5.1b

The following features are supported by the Cisco 4000 Series Integrated Services Routers for Cisco IOS XE Everest 16.5.1b:

- For information on migrating from existing Cisco IOS XE 3S releases to the Cisco IOS XE Everest 16.5.1b 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.
- Application Hosting—For detailed information, see the following Cisco document: Data Models Configuration Guide
- Cisco Cloud Redirection over an IPv4 and IPv6 Network— For detailed information, see the following Cisco document: Cisco Network Plug-n-Play Agent Configuration Guide, Cisco IOS XE Everest 16.5.1b.
- Cisco Network PnP Discovery Over 4G Interface—For detailed information, see the following Cisco document: Cisco Network Plug-n-Play Agent Configuration Guide, Cisco IOS XE Everest 16.5.1b.
- Configuring a Switch using Cisco Network Plug and Play—For detailed information, see the following Cisco document: Cisco Network Plug-n-Play Agent Configuration Guide, Cisco IOS XE Everest 16.5.1b
- DHCP Option based Discovery over an IPv6 Network —For detailed information, see the following Cisco document: Cisco Network Plug-n-Play Agent Configuration Guide, Cisco IOS XE Everest 16.5.1b.
- DNS-based Discovery over an IPv6 Network—For detailed information, see the following Cisco document: Cisco Network Plug-n-Play Agent Configuration Guide, Cisco IOS XE Everest 16.5.1b.
- CUBE Support for SRTP-SRTP and SRTP-RTP Interworking with NGE Cipher Suites—For detailed information, see the following Cisco doucment:http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/configuration/cube-book/srtp-srtp-interworking.html.
- ICMP Inspection Improvement—With the Internet Control Message Protocol (ICMP) Inspection enhancement, after configuring the icmp unreachable allow command, the ICMP packets are passed through the zone-based firewall (ZBFW) even if the ICMP packets do not have Access Control List (ACL) to match ICMP of type 3. For detailed information, see the following Cisco document: http:/ /

www.cisco.com/ c/ en/ us/ td/ docs/ ios-xml/ ios/ sec_data_zbf/ configuration/ xe-16/ sec-data-zbf-xe-16-book/ fw-stateful-icmp.html.

- In Service Model Updates—For detailed information, see the following Cisco document: Data Models Configuration Guide.
- Multi-Party Hardware conference support for CME—For detailed information, see the following Cisco document:http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/admin/configuration/manual/cmeadm/cmeconf.html
- New endpoints support-8821, 8845 and 8865-with CME—For detailed information, see the following Cisco document:http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/feature/phone_feature/phone_feature_support_guide.html
- Preboot Execution Environment (PXE) Client.For detailed information, see the following Cisco document: Data Models Configuration Guide
- Scripting: Python 2.7/3.0—For detailed information, see the following Cisco document: Data Models Configuration Guide.
- Smart licensing for CME—For detailed information, see the following Cisco document:http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/admin/configuration/manual/cmeadm/cmeover.html
- Smart Licensing—For detailed information, see the following Cisco doucment: http://www.cisco.com/c/en/us/td/docs/routers/access/4400/software/configuration/guide/isr4400swcfg/isr4400swcfg_chapter_010011.html.

  For a more detailed overview on Cisco Licensing, go to https://cisco.com/go/licensingguide.
- TR-069 Agent Support on Cisco 4000 Series ISRs—For detailed information, see the following Cisco doucment: http://www.cisco.com/c/en/us/td/docs/ios/bbdsl/configuration/guide/bba_tr069_agent.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 Everest 16.5.1:
  - Configuring Application Visibility—Enhanced to provide reports in a graphical representation format.
  - Troubleshooting—Allows you to troubleshoot some of the basic features.
- Zero Touch Provisioning—For detailed information, see the following Cisco document: Data Models Configuration Guide.

For information on how to access the Web User Interface, see Configure the Router for Web User Interface section.

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.

Filter	Description
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 Everest 16.5.1b

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

Identifier	Description
CSCvc79509	Cisco 4331 ISR memory becomes insufficient and crashes after overnight stress PUNT flow2path request
CSCvd42370	Call failures during bulk call processing of SRTP-RTP flows.

Resolved Caveats - Cisco IOS XE Everest 16.5.1b

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

Identifier	Description
CSCvd01349	Cisco 4221 ISR router reports an unknown health state for the load average when you view the show platform software status control-processor.
CSCvc27565	Cisco 4321 ISR crashes when a large packet is sent.
CSCvc34308	In Cisco 4331 ISR boot up issue seen with most of the CCO images with 16.4(2)r rommon.
CSCvc45316	Cisco 4000 Serires ISR: IGMP joins under VRF from SM-X Switch module that is shown in global IGMP table.
CSCvc65935	NAT66 feature crashes when you ping from inside to outside.
CSCvc48376	Cisco 43xx ISR: Environmental monitoring is not enabled and messages are causing confusions.

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 Everest 16.x software documentation set consists of Cisco IOS XE Everest 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 Everest 16.x release train. These Cisco IOS command references support all Cisco platforms that are running any Cisco IOS XE Everest 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.