Release Notes for Cisco 4000 Series ISRs, Cisco IOS XE Everest 16.4

First Published: 2016-11-30

Last Modified: 2017-05-01

Cisco 4000 Series Integrated Services Routers Overview

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)

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 Everest 16.4.1 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 IOX XE Everest 16.4.1.

Table 1: Recommended Firmware Versions

Cisco 4000 Series ISRs	Existing RoMmon	Cisco Field-Programmable Devices
Cisco 4451 ISR	15.3(3r)S1	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	15.4(2r)S	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	15.4(3r)S3	14101324
Cisco 4331 ISR	15.4(3r)S5	14101324
Cisco 4321 ISR	15.4(3r)S5	14101324
Cisco 4221 ISR	15.4(3r)S5	14101324

Upgrading the ROMMON Version on the Cisco 4000 Series ISR

For information about ROMMON and upgrading procedure, see the "ROM Monitor Overview and Basic Procedures" section in the Hardware Installation Guide for the Cisco 4000 Series Integrated Services Routers .

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
- Dial on Demand, on page 4
- 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 of8GB 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 225 concurrent IPsec tunnels is exceeded, no more tunnels are allowed and the following error message appears:

```
%CERM-4-TUNNEL_LIMIT: Maximum tunnel limit of 225 reached for Crypto functionality with
securityk9 technology package license.
```

- When the throughput value for the inbound (decrypted) traffic exceeds 85Mbps, subsequent IPsec traffic in that direction will be dropped and the following message will be displayed:

```
%IOSXE-4-PLATFORM:cpp_cp: QFP:0.0 Thread:001 TS:00000001786413378010
%CERM_DP-4-DP_RX_BW_LIMIT: Maximum Rx Bandwidth limit of 85000 Kbps reached for Crypto
functionality with securityk9 technology package license.
```

- To avoid this restriction and enable full IPsec functionality on the router, install an HSECK9 feature license.
- 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.

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 .

New Features and Important Notes About Cisco 4000 Series ISRs Release Everest 16.4.1

This section describes new features in Cisco IOS XE Everest 16.4.1 that are supported on the Cisco 4000 Series ISRs.

New Software Features in Cisco 4000 Series ISR Release Cisco IOS XE Everest 16.4.1

The following features are supported by the Cisco 4000 Series Integrated Services Routers for Cisco IOS XE Everest 16.4.1:

- For information on migrating from existing Cisco IOS XE 3S releases to the Cisco IOS XE Everest 16.4.1 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.
- 802.1X Support on Cisco 4000 Series ISRs and Switch Modules— For detailed information, see the following Cisco document: Cisco 4-Port and 8-Port Layer 2 Gigabit EtherSwitch Network Interface Module Configuration Guide for Cisco 4000 Series ISR.
- Cisco 4221 ISR—For detailed information, see the following Cisco documents: Hardware Installation Guide for the Cisco 4000 Series Integrated Services Router and Cisco 4000 Series ISRs Software Configuration Guide.
- Cisco V.150.1 Minimum Essential Requirements—The Cisco V.150.1 Minimum Essential Requirements feature complies with the requirements of the National Security Agency (NSA) SCIP-216 Minimum Essential Requirements (MER) for V.150.1 recommendation. The SCIP-216 recommendation has simplified the existing V.150.1 requirements. Beginning with Cisco IOS XE Everest 16.4.1, Cisco V.150.1 MER feature is enhanced to support interoperability with third-party devices.
- Cisco SSL 6.0 FOM—Cisco SSL 6.0 is used to upgrade openssl to 1.0.2 g. The security updates will be available for the next three years. From Cisco IOS XE Everest 16.4.1, RC4 and DES ciphers have been blocked and will no longer be supported as they are considered vulnerable.
- CLI for Showing Applications Assigned to a Specific Traffic-class and Business-relevancy—This feature provides support for matching two attribute/attribute-value combinations using the show ip nbar attribute command. More information about this command is available at this link: Cisco IOS Quality of Service Solutions Command Reference.
- CME SIP:Night Service (Mixed Mode)—For detailed information, see the following Cisco doucment: Cisco Unified Communications Manager Express System Administrator Guide.
- CME SIP:Secondary CME for SIP Phones—For detailed information, see the following Cisco doucment: Cisco Unified Communications Manager Express System Administrator Guide.
- CME SIP:VHG Enhancements—For detailed information, see the following Cisco doucment: Cisco Unified Communications Manager Express System Administrator Guide.
- DMVPN Multiple Tunnel Termination—For detailed information, see the following Cisco document: Dynamic Multipoint VPN Configuration Guide.
- DNA SA Border Support—For detailed information, see the following Cisco document: IP Routing: LISP Configuration Guide.
- Extension Assigner—For detailed information, see the following Cisco doucment: Cisco Unified Communications Manager Express System Administrator Guide.
- IOX Support on Cisco 4000 Series ISRs—For detailed information, see the following Cisco doucment: Cisco IOx Local Manager Reference Guide.
- Native Dual-Stack Support Over IPv6 Transport on Cisco 4000 Series ISRs—For detailed information, see the following Cisco doucment: Configuring Security for VPNs with IPsec.

- Nginx/HTTP - Web Security Features for 16.4—For detailed information, see the following Cisco document: HTTP Services Configuration Guide.
- OpenDNS Connector Enhancements for Cisco IOS XE Everest 16.4.1—Supports the following: TXT record support, Packet tracing on LAN interface, and OpenDNS debugabilty and serviceability. For detailed information, see the following Cisco document: Security Configuration Guide: Cisco Umbrella Branch.
- PAT NAT Overload Over an Elastic IP on Cisco 4000 Series ISRs—The PAT NAT overload over an Elastic IP on Cisco 4000 Series ISRs feature prevents creating extra duplicated mapping entries when you configure NAT with interface overload on the cellular interface, pppoe dialer interface, and other interfaces with elastic IP by doing shut and no shut. The PAT NAT overload over an Elastic IP on Cisco 4000 Series ISRs feature also prevents stopping DUAL ISP NAT PAT overload on IOS-XE when the interface is down. NAT process breaks after the dialer interface connectivity drops to the upstream service provider is resolved.
- QoS: Tunnel Pre-classify Uses Internal Address for Fair-queue Distribution—For detailed information, see the following Cisco doucment: QoS Modular QoS Command-Line Interface Configuration Guide.
- Secondary Dial Tone—For detailed information, see the following Cisco doucment: Cisco Unified Communications Manager Express System Administrator Guide.
- Support for BACD with Loopback Flows—For detailed information, see the following Cisco doucment: Cisco Unified CME B-ACD and Tcl Call-Handling Applications.
- Transfer Recall—For detailed information, see the following Cisco doucment: Cisco Unified Communications Manager Express System Administrator Guide.
- Transcoding Support on CME—For detailed information, see the following Cisco doucment: Cisco Unified Communications Manager Express System Administrator Guide.
- TrustSec SGACL Monitor Mode on Routers—For detailed information, see the following Cisco doucment: Cisco TrustSec Configuration Guide.
- UTD Snort IPS Enhancements for Cisco IOS XE Everest 16.4.1—Adds a feature for displaying the list of active signatures. For detailed information, see the following Cisco document: Security Configuration Guide: Unified Threat Defense.
- 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 16.4.1:
    - Cellular Interface—Cellular Interface feature supports the Fourth Generation (4G) Long-Term Evolution (LTE) and its primary application is Cellular WAN connectivity, which functions as a primary or backup data link for critical data applications.
    - Configuring Application Visibility—Enhanced to include Application Signatures identifier based on NBAR engine version 28. NBAR engine version changes if you update the protocol package.
    - Site-to-Site VPN—A Virtual Private Network (VPN) allows you to protect traffic that travels over lines that your organization may not own or control.VPNs can encrypt traffic sent over these lines and authenticate peers before any traffic is sent. Site-to-Site VPN feature allows you to create a VPN network connecting two routers.

- XMPP Protocol Support on Ciso Plug and Play Agent— The Ciso Plug and Play Agent does not support XMPP protocol from 16.4 onwards. For detailed information, see the following Cisco document: Cisco Open Plug-n-Play Agent Configuration Guide.
- Zone Based Firewall:Per-filter Stats Enhancement—For detailed information, see the following Cisco document: Security Configuration Guide: Zone-Based Policy Firewall.
- Zone Based Firewall and NAT Internop on WCCP Interface—For detailed information, see the following Cisco document: Security Configuration Guide: Zone-Based Policy Firewall .

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.
- 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.

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.

SUMMARY STEPS

1. In your browser, navigate to the Cisco Bug Search Tool .
2. If you are redirected to a Log In page, enter your registered Cisco.com username and password and then, click Log In.
3. To search for a specific bug, enter the bug ID in the Search For field and press Enter.
4. To search for bugs related to a specific software release, do the following:
5. To see more content about a specific bug, you can do the following:
6. To restrict the results of a search, choose from one or more of the following filters:

DETAILED STEPS

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 Everest 16.4.1, on page 11
- Resolved Caveats - Cisco IOS XE Everest 16.4.1, on page 11
- Open Caveats - Cisco IOS XE Everest 16.4.2, on page 12

Open Caveats - Cisco IOS XE Everest 16.4.1

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

Identifier	Description
CSCvb35300	Reload boot time is longer than expected on Cisco 4221 ISR and Cisco 4321 ISR.
CSCvb59583	cpp_sp traceback is seen when you remove the CTS enforcement on Cisco 4000 Series ISR.
CSCvb83122	Possible intermittent interface failure to rx traffic.
CSCvb94424	FTP hang with Cisco 4451 ISR IOS XE utd ova Snort IPS + ISR waas feature
CSCvc03290	Cisco 4000 Series ISRs are not scaling to known targets for NAT44 PAT on Cisco IOS XE 16.4.1.
CSCvc08339	On Cisco 4331 ISR, frame-relay circuits does not come up.
CSCvc11012	When you use Cisco 4221 ISR for IWAN 2.2 running IOS V164, PFR Domain TCA UNREACHABLE continuously. Path changed continuously.

Resolved Caveats - Cisco IOS XE Everest 16.4.1

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

Identifier	Description
CSCvb10321	Cisco 4300 Sereis ISR crashes at cent_show_master_exits command.

Identifier	Description
CSCvb10340	Cisco 4400 ISR single branch crashed at _be_cent_get_prot_pfx.
CSCvb89706	Cisco 4221 ISR is crashing for some images and stuck in ROMMON mode.

Open Caveats - Cisco IOS XE Everest 16.4.2

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

Identifier	Description
CSCvd97881	IOSd crashes due to chasfs process.
CSCvd98709	Kernel crashes due to critical process fault on fp_0_0.
CSCve12409	WAAS cpp_mcplo_ucode crashes.
CSCvd47657	Router crashes due to voice call in Cisco IOS XE Everest 16.4.1 release.
CSCvc08361	A crash is observed in TCP-TLS B2B call scenario in Cisco IOS XE 3.17 release.
CSCve07263	The **shut** and **no-shut** command of the VTI tunnel leaves the tunnel in Up/Down state.

Resolved Caveats-Cisco IOS XE Everest 16.4.2

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

Identifier	Description
CSCuz51603	Multicast crashes with invalid leaf pointer.
CSCva05558	IKEv2 IPv6 GRE IPSec fails to stabilize.
CSCva70115	Multiple crashes are seen after migrating from Cisco 3841 to Cisco 4331 ISR.
CSCva97469	V-access interface is spawned for a specific remote spoke and is in protocol down state.
CSCvb95663	NIM-2GE-CU-SFP: Cannot ping GLBP Gateway IP address.

Identifier	Description
CSCvc08339	Cisco 4331 ISR with NIM-1MFT-T1/E1 and Frame-relay circuit does not come up.
CSCvc19234	Stale MPLS forwarding entry is seen in **show mpls forwarding** output.
CSCvc19844	Symptom: Even after an area is removed from topology, SID database does not remove the area.
CSCvc23238	SRTE: when the interface address is removed, traceback is seen and adj-sids not destroyed.
CSCvc26824	ACP is not getting created after you save and reload.
CSCvc27565	Cisco 4321 ISR crashes when sending a large packet.
CSCvc34308	Cisco 4331 ISR: Intermittent Boot up issue is seen with most of the CCO images with 16.4(2)r rommon.
CSCvc45316	IGMP groups under VRF are shown under global table.
CSCvc54049	Ignore home address broken in MAG/LMA.
CSCvc54211	SRTE tunnel keeps on flapping and protected ADJ is created with repair path having invalid out label when OSPF Segment routing is disabled on the NBR.
CSCvc59750	When you take longer than ~15 seconds to enter username/password credentials, IKEv2/IPSEC Anyconnect session will establish briefly, then disconnect within a few seconds.
CSCvc63958	Outgoing SIP calls to Cisco Unity Express (CUE) and certain ITSP providers fail, as provider rejects the call due to the initial INVITE containing an Authorization header.
CSCvc90685	Accounting stop message not going to pmipv6 tunnel in LMA when tunnel is brought down.
CSCvc99738	KEv2 tunnel negotiation between two Cisco routers fails in IKE AUTH exchange post upgrading one of the routers to Cisco IOS 15.5(3)S5 or 15.5(3)M5. release.

Identifier	Description
CSCvd09584	BGP EVPN RR incorrectly reflects EVPN IMED (type 3) route PMSI attribute with VNI as MPLS label.
CSCvd29093	Cisco 4000 Series ISR ucode crash when decrypting a ipsec packet with length between 3820 and 3840.
CSCvd40880	After modifying a crypto acl and waiting for a rekey the crypto map config is removed.
CSCvd69373	KEv2: Unable to initiate IKE session to a specific peer due to 'in-neg' SA Leak

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.

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.