Cisco 4000 Series Integrated Services Routers Release Notes, Cisco IOS XE Denali 16.2

Published: March 31, 2016
Last Updated: July 6, 2016

This document provides information about the Cisco IOS XE Denali 16.2 software release for the Cisco 4000 Series Integrated Services Routers (ISRs) and consists of the following sections:

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 ISR 4400 Series	Cisco ISR 4300 Series
Cisco ISR 4431	Cisco ISR 4321
Cisco ISR 4451	Cisco ISR 4331
	Cisco ISR 4351

Migrating to Cisco IOS XE Denali 16.2

The *Cisco IOS XE Denali 16.2 Migration Guide for Access and Edge Routers* contains important information for migrating successfully from Cisco IOS XE 3S to Cisco IOS XE 16.2. Before you begin the migration, read this information to ensure that you have completed all the prerequisites and understand the migration process.

For a list of caveats in this release, see the Open Caveats - Cisco IOS XE Denali 16.2.1, page 10 section.

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 Denali 16.2 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 provides information about the recommended Rommon and CPLD versions for releases prior to Cisco IOX XE Denali 16.2.1.

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

Upgrading the ROMMON Version on the Cisco 4000 Series ISR

For information about ROMMON version that is needed to load the Cisco IOS Denaili 16.2.1 image on a Cisco ISR 4000 Series, see the *Cisco IOS XE Denali 16.2 Migration Guide for Access and Edge Routers*.

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
- Cisco ISR-WAAS and AppNav-XE Service
- IPsec Traffic
- Dial on Demand
- USB Etoken

Cisco Unified Threat Defense

The Cisco Unified Threat Defense (UTD) service requires a minimum of 8GB of DRAM and 200GB SSD.

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 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.

New Features and Important Notes About Cisco 4000 Series ISRs Release Denali 16.2.1

This section describes new features in Cisco IOS XE Denali 16.2.1 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 Denali 16.2.1

The following features are supported by the Cisco 4000 Series Integrated Services Routers for Cisco IOS XE Denali 16.2.1:

- For information on migrating from existing Cisco IOS XE 3S releases to the Cisco IOS XE Denali 16.2.1 release, see *Cisco IOS XE Denali 16.2 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.
- 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. For information on how access the Web User Interface, see Configure the Router for

Web User Interface, page 6.

- Cisco Unified Border Element (CUBE) is supported on ISR 4K platforms running Cisco IOS XE Denali 16.2.1 release. For more information on CUBE support in Cisco IOS XE Denali 16.2.1, see *http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/configuration/cube-book/read-me-first.html.*
- Cisco Unified Communications Manager Express (Unified CME) and Cisco Unified Survivability Remote Site Telephony (Unified SRST) is supported on ISR 4K platforms running Cisco IOS XE Denali 16.2.1.

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.

Entering the Configuration Commands Manually

If you don't 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.

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

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 config 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.

```
Router(config)# username name privilege 15 secret 0 password
```

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
```

If you are going to connect the PC directly to the router, the PC must be on the same subnet as this interface.

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 server
```

To configure the router as an https server, enter the **ip http secure-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 routers, Cisco IOS XE Denali 16.2.1 Caveats 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.

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 Denali 16.2.2

There are no open caveats in this release.

Resolved Caveats - Cisco IOS XE Denali 16.2.2

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

Identifier	Description
CSCuu97639	PQ latency is higher than two minutes in recent MCP_DEV.
CSCuw48857	Cisco 4300 Series ISR platform crashes while executing the **show platform hardware crypto-device utilization** command.
CSCuy21483	Cisco 4451 ISR may experience a reload when you configure the MGCP and SIP gateway.
CSCuy34939	Add 64-bit support for ngiolite driver on CGE7.
CSCuy38895	Traceback is seen when you boot the router.
CSCuy85653	One way audio via Cisco 4000 Series ISR is resumed from IP phone after SNR.
CSCuy86464	Unable to upgrade firmware for xDSL modules on Cisco 4000 Series ISR platforms.
CSCuy97725	Physical interface issue is seen with primary and backup with PPPoE.
CSCuz09783	Zone-based firewall asynchronous memory API change for Cisco 4300 Series platform.

Open Caveats - Cisco IOS XE Denali 16.2.1

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

Identifier	Description
CSCuu55586	Cisco 4431 ISR does not scale at the level of Cisco 4451 ISR for multiple features.
CSCux65367	UP37: Performance degradation with IPSEC + QoS combination of >-30%.
CSCux71187	Cisco 4451 ISR displays Kernel messages with overnight traffic.
CSCux79441	Cisco 4451 ISR crashes during boot up.
CSCux94113	IPv4 uncap CEF: Cisco 4331 ISR and Cisco 4351 ISR has performance drop for CEF of >-5%.
CSCux98318	CGE7: PPC kernel core dump is not generated, which triggers the kernel crash.
CSCux79326	Web User Interface does not list any L3 interface if VRF is set to None for Call Home profile.
CSCuy59673	ISR-WAAS instance is lost after upgrading router image from mcp_dev to Cisco IOS XE Denali 16.2.
CSCuy68883	You need to enter “webui” in the URL to access Web User Interface for Cisco 4421 router.
CSCuy70650	Cisco 4451 ISR and Cisco 4421 ISR disk performance is not good with 3.10 kernel.
CSCuy74063	HTTP services are broken for Denali images.
CSCuy78780	Issues in snap shot values in alerts tab of the Smart call page.
CSCuy84498	Cisco 4000 series snort activation fails after Cisco IOS XE Denali 16.2 upgrade
CSCuy86464	Cisco IOS XE Denali 16.2: xDSL firmware upgrade is failing.
CSCuz74838	The SNMP crashes.

Resolved Caveats - Cisco IOS XE Denali 16.2.1

There are no resolved caveats in this release.

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 Denali 16.x.

Cisco IOS Software Documentation

The Cisco IOS XE Denali 16.x software documentation set consists of Cisco IOS XE Denali 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 Denali 16.x release train. These Cisco IOS command references support all Cisco platforms that are running any Cisco IOS XE Denali 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, submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.