



Release Notes for Cisco IWAN Release 2.3

First Published: 2018-08-28

Release Notes for Cisco IWAN Release 2.3

This release notes document provide information about Cisco Intelligent WAN (IWAN) Solution, Release 2.3.

Contents

Introduction

This release notes provide a summary of the components in the latest release of the Cisco Intelligent Wide Area Network (Cisco IWAN) Solution.

Cisco IWAN is a prescriptive solution for leveraging multiple transport providers, including low cost business grade broadband services as part of your WAN transport strategy. IWAN is a suite of components that brings all the WAN optimization, performance routing, and security levels of leased lines and expensive MPLS VPN services to the public Internet. IWAN makes it possible to get the performance, reliability and security benefits of private and virtual private network services while allowing the option of using more attractively priced service offerings and require simpler peering relationships with the transport provider. The same prescriptive design may be used with any transport provider; an important flexibility to have when multiple regional providers are needed.

Cisco IWAN can be implemented using Command Line Interface (CLI) commands on the routers of the hub and branch sites.

Recommended Release for Cisco IWAN Release 2.3

It is recommended that you use [Cisco IOS XE Fuji 16.9.1](#) for Cisco IWAN.

What's New in Cisco IWAN Release 2.3

The new features and enhancements in Cisco IWAN Release 2.3, introduced via Cisco IOS XE Fuji 16.8.1 is as follows:

Direct Cloud Access IWAN 2.3

The Direct Cloud Access (DCA) feature helps customers to optimize their Software as a service (SaaS) applications (Office 365, Google, etc.) with better performance and reduced cost. It continuously measures and monitors the performance of each SaaS application along with local break out path as well as backhaul path, and chooses the suitable in policy path to provide the most optimal user experience.

For more 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/pfrv3-dca.html>



Note IWAN App does not support DCA.

PfRv3 Site TC Splitting

The PfRv3 Site TC Splitting feature allows controlling the prefix length for the learned site prefixes. This allows controlling the granularity of the traffic class, thereby enabling better load sharing of the traffic classes. This feature is enabled by default.

For more information, see the following Cisco document: <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/pfrv3/configuration/xe-16/pfrv3-xe-16-book/pfrv3-site-prefix.html>.

System Requirements

The following sections describe the system requirements for Cisco IWAN 2.3, which are as follows:

Supported Cisco Platforms and Software Releases

Cisco IWAN 2.3

Platform	Model	Cisco IOS Software Release
Cisco ISR 4000 Series Routers	ISR 4221 ISR 4321 ISR 4331 ISR 4351 ISR 4431 ISR 4451-X	Cisco IOS XE Fuji 16.8.1 or higher maintenance releases of Cisco IOS XE Fuji 16.8.x.
Cisco ASR 1000 Series Routers	ASR 1001 ASR 1001-X ASR 1001-HX ASR 1002 ASR 1002-X ASR 1002-HX ASR 1004 ASR 1006 ASR 1006-X ASR 1009-X ASR 1013	Cisco IOS XE Fuji 16.8.1 or higher maintenance releases of Cisco IOS XE Fuji 16.8.x.

Platform	Model	Cisco IOS Software Release
Virtual Routers	ENCS 5400 (ISRv) Cloud Services Router 1000v	Cisco IOS XE Fuji 16.8.1 or higher maintenance releases of Cisco IOS XE Fuji 16.8.x.

Platform	Model	Cisco IOS Software Release
Cisco ISR 1000 Series Routers		Cisco IOS XE Fuji 16.8.1 or higher maintenance releases of Cisco IOS XE Fuji 16.8.x.

Platform	Model	Cisco IOS Software Release
	C1111-4P	
	C1111-4PLTEEA	
	C1111-4PLTELA	
	C1111-4PWA	
	C1111-4PWB	
	C1111-4PWD	
	C1111-4PWE	
	C1111-4PWF	
	C1111-4PWH	
	C1111-4PWN	
	C1111-4PWQ	
	C1111-4PWR	
	C1111-4PWZ	
	C1111-8P	
	C1111-8PLTEEA	
	C1111-8PLTEEAWA	
	C1111-8PLTEEAWB	
	C1111-8PLTEEAWE	
	C1111-8PLTEEAWR	
	C1111-8PLTELA	
	C1111-8PLTELAWD	
	C1111-8PLTELAWF	
	C1111-8PLTELAWH	
	C1111-8PLTELAWN	
	C1111-8PLTELAWQ	
	C1111-8PLTELAWZ	
	C1111-8PWA	
	C1111-8PWB	
	C1111-8PWE	
	C1111-8PWF	
	C1111-8PWH	
	C1111-8PWN	
	C1111-8PWQ	

Platform	Model	Cisco IOS Software Release
	C1111-8PWR	
	C1111-8PWZ	
	C1116-4P	
	C1116-4PLTEEA	
	C1116-4PLTEEAWA	
	C1116-4PWE	
	C1117-4P	
	C1117-4PLTEEA	
	C1117-4PLTEEAWA	
	C1117-4PLTEEAWA	
	C1117-4PLTELA	
	C1117-4PLTELAWZ	
	C1117-4PM	
	C1117-4PMLTEEA	
	C1117-4PMLTEEAWA	
	C1117-4PMWE	
	C1117-4PWA	
	C1117-4PWE	
	C1117-4PWZ	



Note DCA feature is not supported on ISR-G2's.

Software Requirements

Cisco Wide Area Application Services

Cisco Wide Area Application Services (WAAS) release 6.4.1a or higher.

Cisco Prime Infrastructure

Cisco Prime Infrastructure release 3.1.5 or higher is supported in Cisco IWAN Release 2.3 for single VRF PfR and AVC Monitoring. Multi VRF PfR Monitoring is not supported.

IWAN Controller

IWAN Controller Release 1.5 is supported.



Note DCA feature is not supported through IWAN App. The IWAN App can be used to configured generic IWAN configurations.

LiveAction

LiveAction version 6.2 or higher is suggested.

Platforms and their Roles

Platform	Role
Cisco ISR 1000 Series Routers	Branch site
Cisco ISR 4000 Series Routers	Hub site (ISR 4451, ISR4431) with limited scale and performance; but not recommended. Branch site (ISR 4221, ISR 4321, ISR 4451, ISR 4431 models) Master controller, standby master controller or transit master controller (ISR 4451, ISR 4431 models)
Cisco ASR 1000 Series Routers	Hub site Branch site Master controller, standby master controller or transit master controller.
Cisco CSR 1000v Series Routers	Hub site Branch site Master controller, standby master controller or transit master controller.
Cisco ENCS Routers	Hub site Branch site Master controller, standby master controller or transit master controller.

Limitations and Restrictions

This section lists limitations and restrictions in Cisco IWAN 2.3:

- All devices on a site—master and border routers—must have the same software version.
- In IWAN POP, a PfRv3 master controller and a PfR border router must be configured in different devices.
- The recommended upgrade procedure must be completed. Upgrades can be incremental. The upgrade procedure is available here:

http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Intelligent_WAN/upgrade/iwan-upgrade.html

- The following are the default commands in Cisco IWAN Release 2.3:

- **ip nhrp shortcut**
- **if state nhrp**
- **ip nhrp multicast dynamic**
- **nhrp holdtime 600 seconds**

Note: The above are default commands on devices with Cisco IOS XE Release Fuji 16.9.1.

- The default unreachable timer in PfRv3 is 4 seconds.
- If the branch devices are upgraded before the hub devices, the PfRv3 unreachable timer must be set to four seconds on the hub routers.
- A message appears when a branch device, enabled with MD5 password, establishes a TCP connection with a master controller on port 17749. However, the branch device is not able to establish a connection because the server socket might not be open or the master controller may be down. This message might be misleading and has no functional impact on the system.
- When the primary service provider link goes down, communication between spokes will be down. To avoid this, configure the max-secondary-path ibgp command when configuring EIGRP or BGP on a branch device. The value of the command must be n-1 where n is the number of service provider multiplied by number of data centers. If a network has two data centers and two service providers, the value of the command must be three.

Caveats

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, you can also see the Help & FAQ within the Bug Search Tool.

About the 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

Before You Begin

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.

Using the Bug Search Tool

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:

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.

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.

1. 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.

Caveats in Cisco IWAN 2.3

This section provides information about the caveats in Cisco IWAN 2.3.

Identifier	Description
CSCvh62562	IWAN2.3: Umbrella policy does not give an option to get the DNS server info through dhcp
CSCvi31854	ASR1k (HUB BR) does not delete the cli configs from database
CSCvg87767	NBAR Standard application names not present in domain map config
CSCvh02442	IWAN2.3 DCA Ingress ping or other mechanism needed

Software Download Information

The following table provides the path on [Download Software](#) page for downloading the software for Cisco IWAN Release 2.3.

Software	Path
Cisco IOS XE Software	Downloads Home > IOS and NX-OS Software > IOS XE > IOS XE S > IOS XE 3S > Routers > product series > platform series > platform > IOS XE Software > Fuji-16.9.1(ED) For more information, see, Software Download: ASR 1002-HX Router page .

Software	Path
Prime Infrastructure 3.1 Software	Downloads Home > Products > Cloud and Systems Management > Routing and Switching Management > Network Management Solutions > Prime Infrastructure > Prime Infrastructure 3.1 > Prime Infrastructure Patches-3.1.5 For more information, see Software Download: Prime Infrastructure 3.1 page.
Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) 1.4 Software	Products > Cloud and Systems Management > Policy and Automation Controllers > Application Policy Infrastructure Controller Enterprise Module (APIC-EM) > APIC-1.4 (IWAN) For more information, see Software Download: Application Policy Infrastructure Controller Enterprise Module (APIC-EM) .
Cisco Wide Area Application Services Software	Products > Application Networking Services > Wide Area Application Services > Wide Area Application Services (WAAS) Software > Wide Area Application Services (WAAS) Software-6.4.1a For more information, see Software Download: Products .

Related Documentation

Documentation	Description
Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide	Information about the underlying Cisco APIC-EM product including deployment steps, verification, and troubleshooting.
Cisco IWAN Technology Design Guides	Cisco IWAN designs are explained in the Cisco IWAN technology design guides. Look for the guides in the Cisco Validated Designs (CVDs)
Cisco Open Plug-n-Play Agent Configuration Guide	PnP Agent documentation for Cisco IOS XE.
Cisco Prime Infrastructure 3.1.5	Refer to this guide for information about Cisco Prime Infrastructure, which can be used to configure Cisco IWAN.
Cisco Prime Infrastructure 3.1 Release Notes	Description of the features and caveats for Cisco Prime Infrastructure.
Configuration Guide for Network Plug and Play on APIC-EM	Documents the PnP server application in the APIC-EM.
Live Action	Documentation on LiveAction software.
Cisco IWAN Application on APIC-EM Release Notes	Description of the features, system requirements, prerequisites, and caveats for the Cisco Intelligent Wide Area Network Application (Cisco IWAN App).

Documentation	Description
Release Notes for Cisco Network Plug and Play	Description of the features and caveats for Cisco Network Plug and Play.
Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module	Description of the features and caveats for the Cisco Application Policy Infrastructure Controller Enterprise Module (Cisco APIC-EM).
Solution Guide for Cisco Network Plug and Play	Overview of the Plug and Play solution, component descriptions, summary of major use cases, and basic deployment requirements, guidelines, limitations, prerequisites, and troubleshooting tips.
Cisco IWAN Application on APIC-EM User Guide	Information about the installation, deployment, configuration of Cisco IWAN on APIC-EM. Explains the Cisco IWAN GUI and how to manage connected devices and hosts within your network.

Obtain Documentation and Submit 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](#) . The RSS feeds are a free service.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks . Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2018 Cisco Systems, Inc. All rights reserved.

