



Release Notes for Cisco IWAN Release 2.2

First Published: 04/03/2017

Last Updated: 09/07/2017

This release notes document provide information about Cisco Intelligent WAN (IWAN) Solution, Release 2.2.

Contents

- [Introduction, page 1](#)
- [What's New in Cisco IWAN Release 2.2, page 2](#)
- [System Requirements, page 3](#)
- [Limitations and Restrictions, page 6](#)
- [Caveats, page 6](#)
- [Software Download Information, page 11](#)
- [Related Documentation, page 11](#)
- [Obtain Documentation and Submit a Service Request, page 12](#)

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.

What's New in Cisco IWAN Release 2.2

The new features and enhancements in Cisco IWAN Release 2.2, introduced via Cisco IOS XE Denali 16.3.3 are as follows:

- [PfRv3 Probe Reduction, page 2](#)
- [PfRv3 Site Prefix Splitting, page 2](#)
- [DMVPN Multiple Tunnel Termination, page 2](#)
- [Cisco IWAN App Release 1.4.0, page 2](#)

PfRv3 Probe Reduction

The PfRv3 probe reduction feature allows reducing the probing of traffic on channels that do not carry any traffic.

For more information, see the following Cisco document:

<http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/pfrv3/configuration/xr-16/pfrv3-xr-16-book/pfr-probe-reduction.html>

PfRv3 Site Prefix Splitting

The PfRv3 Site Prefix 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:

<http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/pfrv3/configuration/xr-16/pfrv3-xr-16-book/pfrv3-site-prefix.html>

DMVPN Multiple Tunnel Termination

The DMVPN Multiple Tunnel Termination feature provides support for multiple tunnel terminations (interfaces) on the same VRF in a hub device.

For more information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/xr-16/sec-conn-dmvpn-xr-16-book/sec-conn-dmvpn-multiple.html

Cisco IWAN App Release 1.4.0

The new features and functions available in Cisco IWAN App Release 1.4.0 are as follows:

- 4G Support on Cisco 4000 Series Integrated Services Routers
- APIC-EM behind NAT
- Custom configuration (beta)
- Custom application deletion
- Day 0 and Day N QoS Bandwidth Modifications
- Day N WAN bandwidth update for hub or spoke site
- Day N WAN IP updated for spoke site
- Spoke behind NAT
- Support for ASR1000 Series routers for spoke sites

- Support for Cisco IOS XE Denali 16.x
- Support for NBAR2 Protocol Pack
- Support multiple DHCP servers on a hub site

For more information, see the following Cisco document:

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Intelligent_WAN/release/notes/1-4-0/iwan-release-notes-1-4-0.html#con_161183

System Requirements

The following sections describe the system requirements for Cisco IWAN 2.1.1, which are as follows:

- [Supported Cisco Platforms and Software Releases, page 3](#)
- [Software Requirements, page 5](#)
- [Platforms and their Roles, page 6](#)

Supported Cisco Platforms and Software Releases

Cisco IWAN 2.2 supports the following Cisco devices and software releases.

Platform	Model	Cisco IOS Software Release
Cisco ISR 4000 Series Routers	ISR 4451x ISR 4431 ISR 4351 ISR 4331 ISR 4321	Cisco IOS XE Denali 16.3.3 or higher maintenance releases of Cisco IOS XE Denali 16.3.x.
Cisco ASR 1000 Series Routers	ASR 1001-X ASR 1001-HX ASR 1002-X ASR 1002-HX ASR 1004 ASR 1006 ASR 1006-X	Cisco IOS XE Denali 16.3.3 or higher maintenance releases of Cisco IOS XE Denali 16.3.x.

Platform	Model	Cisco IOS Software Release
Cisco CSR 1000v Series Routers	Cloud Services Router 1000v	Cisco IOS XE Denali 16.3.3 or higher maintenance releases of Cisco IOS XE Denali 16.3.x.
Cisco ISR-G2 Series Routers	C891-24X-K9 C891F-K9 C891FW-A-K9 C891FW-E-K9 C892FSP-K9 C896VAG-LTE-GA-K9 C896VA-K9 C897VAB-K9 C897VAG-LTE-GA-K9 C897VAG-LTE-LA-K9 C897VAGW-LTE-GAEK9 C897VA-K9 C897VAMG-LTE-GA-K9 C897VA-M-K9 C897VAM-W-E-K9 C897VAW-A-K9 C897VAW-E-K9 C898EAG-LTE-GA-K9 C898EAG-LTE-LA-K9 C898EA-K9 C899G-LTE-GA-K9 C899G-LTE-JP-K9 C899G-LTE-LA-K9 C899G-LTE-NA-K9 C899G-LTE-ST-K9 C899G-LTE-VZ-K9 C891F-K9 C891FW-A-K9 C891FW-E-K9 C892FSP-K9 C896VAG-LTE-GA-K9 C896VA-K9 C897VAB-K9 C897VAG-LTE-GA-K9 C897VAG-LTE-LA-K9 C897VAGW-LTE-GAEK9 C897VA-K9 C897VAMG-LTE-GA-K9 C897VA-M-K9 C897VAM-W-E-K9 C897VAW-A-K9 C897VAW-E-K9 C898EAG-LTE-GA-K9 C898EAG-LTE-LA-K9 C898EA-K9 C899G-LTE-GA-K9 C899G-LTE-JP-K9 C899G-LTE-LA-K9 C899G-LTE-NA-K9 C899G-LTE-ST-K9 C899G-LTE-VZ-K9	Cisco IOS 15.6(3)M2 or higher maintenance releases of Cisco IOS 15.6(3)M.

Platform	Model	Cisco IOS Software Release
Cisco ISR-G2 Series Routers (continued)	ISR 1921 ISR 1921-ISM ISR 1941 ISR 1941-ISM ISR 2901 ISR 2901-ISM ISR 2911 ISR 2911-ISM ISR 2921 ISR 2921-ISM ISR 2951 ISR 2951-ISM ISR 3925 ISR 3925E ISR 3925-ISM ISR 3945 ISR 3945-E ISR 3945-ISM ISR 841-M ISR 890F ISR 890FW ISR 890W ISR 892FSP	Cisco IOS 15.6(3)M2 or higher maintenance releases of Cisco IOS 15.6(3)M.

Software Requirements

Cisco Wide Area Application Services

Cisco Wide Area Application Services (WAAS) release 6.2.3b or higher.

Cisco Prime Infrastructure

Cisco Prime Infrastructure release 3.1.5 or higher is supported in Cisco IWAN Release 2.2 for single VRF PfR and AVC Monitoring. Multi VRF PfR Monitoring is not supported.

IWAN Controller

IWAN Controller Release 1.4 is supported.

LiveAction

LiveAction version 5.2 or higher is suggested.

Platforms and their Roles

Platform	Role
Cisco ISR 4000 Series Routers	Hub site (ISR 4451, ISR 4431 models) Branch site 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	Branch site Master controller, standby master controller or transit master controller
Cisco ISR-G2 Series Routers	Branch site (ISR 890 series, ISR 1900 series, ISR 2900 series, ISR 3900 series)

Limitations and Restrictions

This section lists limitations and restrictions in Cisco IWAN 2.2:

- Because a fix for CSCve98696 is not available in Cisco IOS XE Denali 16.3.4, it is recommended that you do not use Cisco IOS XE Denali 16.3.4. You can use Cisco IOS XE Denali 16.3.3, instead.
- In IWAN POP, a PfR 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 2.2:
 - **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 Denali 16.3.3, not for devices with Cisco IOS Release 15.6(3)M2.
- 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.

Caveats

- [Cisco Bug Search Tool, page 6](#)
- [Caveats in Cisco IWAN 2.2, page 7](#)

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.

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.

Caveats in Cisco IWAN 2.2

This section provides information about the caveats in Cisco IWAN 2.2.

- [Caveats in Cisco IWAN 2.2, page 8](#)
- [Caveats in Cisco IOS XE Denali 16.3.3, page 8](#)
- [Caveats in Cisco IOS Release 15.6\(3\)M2, page 9](#)

- [Caveats in Prime Infrastructure 3.1.5, page 11](#)

Caveats in Cisco IWAN 2.2

Identifier	Description
CSCvc46230	PfRv3: Unexpected Reload While Evaluating/Moving TC's Between Channels
CSCvc90428	PLR interface disappears for multiple DC when the router is reloaded
CSCvd18900	Border Routers sending incorrect NetFlow causing issues in site topology for HUB MC on Prime
CSCvd29705	PfR Monitoring do not display VRF101 data and reports FVRF incorrectly
CSCvd29676	IWAN2.2 Multi VRF High values reported for TCA jitter in site to site details

Caveats in Cisco IOS XE Denali 16.3.3

Identifier	Description
CSCvc81017	ISR4k:EssNoEncapInfo drop seen for pkts transit via PPPoA
CSCvc16495	Power supplies showing "ps fail" when they function fine
CSCvc07319	Random Netclock error messages appearing on console
CSCvc06453	As1k @ CFM traffic frames being sent with 2 dot1q tags
CSCvb30256	ASR1000-2T+20X1GE: More than 1Gbps traffic is reported on 1GE port
CSCvb49832	ASR1k-ELC- XCVR disabled after router reload and interface is down
CSCvc06521	EPA-18X1GE and EPA-10x10GE reloads unexpectedly with traffic and EPA OIR
CSCvc89102	ASR1000 doesn't send PPP ECHO Reply
CSCvb01450	IP/ARP connection failed between two direct-connected interfaces
CSCvc23830	Vlan Oversubscription packets are not working.
CSCvd10362	Deletion of channel-group failed on QFP when FR encaps set on associated Serial Int.
CSCvc15571	applying MPLS-TE command on an interface stops the complete traffic
CSCvb31243	IOSd crash in QoS stats
CSCvb36753	Ingress Unicast traffic not received on the BDI.
CSCvc91743	Platform does not trigger license release when the port moves into error disable state
CSCvb21886	POS interface doesn't come up on clearing alarms
CSCvc89965	After reload route policy processing not re-evaluate with route-map using match RPKI
CSCvd16828	Route Reflector re-sends duplicate information to PE's using RTFilter AF
CSCvd15140	Router crashes using show BGP commands
CSCvd06688	Traceback: loop in Crypto ACL creates CPUHOG then crash at large scale
CSCvc78492	Unable to pass traffic if spoke to spoke fails to build in phase 2
CSCvc46230	PfRv3: Unexpected Reload While Evaluating/Moving TC's Between Channels
CSCvc48813	BQS unable to resume processing leading to pending objects constantly increasing
CSCvb82048	Dual QFP Crash triggered by removing service policy from interface with mixed shaper feature enabled
CSCvb76638	POLARIS 16.4: fman_fp and cpp_cp core files seen with L3VPN profile
CSCvb09881	IWAN NBAR may cause a reload with pa_offset_to_addr

Identifier	Description
CSCVa47695	Entry leak in the SID_CAM leading to SID_CAM_OVERFLOW
CSCVb87341	Ping to ASR1k with a MTU of 10000 Bytes and record option set fails
CSCVd04871	Crash after IWAN does a recalculation in the RIB

Caveats in Cisco IOS Release 15.6(3)M2

Identifier	Description
CSCVb63245	Show aaa servers command results in crash due to SSH process stacklow
CSCVa24325	NSF/SSO feature not honouring TCP MSS
CSCuz61536	CGR1240 : GPS LED not work
CSCVb10757	CGR1240: Gig2/1 and Gig2/2 LEDs got mixed up while using SFP
CSCuz33789	Wifi LED does't turn on in CGR1000 router with IOS
CSCuz52529	Evaluation of cgr1000 for OpenSSL May 2016
CSCVa12766	Memory corruption, crash from Cavium GE driver on CGR 2010
CSCVb00288	CME No ringback after blind transfer
CSCuz87695	SCCP Phones on CME not forwarding video packets on outbound calls
CSCVa14170	+ Dialing not work in SRST with overlap signal for sccp phones
CSCVb14350	7861 - Adding speed-dial on button 16 causes loss of blf-speed-dial keys
CSCVa08774	Call unpark doesnot work when translation profile is applied.
CSCVa65425	IOS does not consider rule set containing translation and reject rule
CSCuy84435	shared line SIP-SCCP not working on ESRST gateway
CSCVa46047	SIP phones shows 1 hour time delay when summer time is configured
CSCuz96364	IPV4 address negotiated by the aggregator not installed
CSCVa14742	VRF Routes sent via DHCP do not appear in RIB after reload
CSCVb72052	Crash: STACKLOW crash while configuring mDNS
CSCVa39516	EIGRP /30 Serial Point-to-Point Subnet Not deleted after link down
CSCux41072	EIGRP sending hello messages with interface in passive mode.
CSCVb35836	2921: "ethernet lmi ce" is configured by default
CSCVa72881	crash due to Auth-proxy HTTP daemon process failing
CSCVa50683	"CWS Telemetry Process" Crash on Whitelist Upgrade With CSCup94022 Fix
CSCVa75774	CWS/ISR 1900 15.5(3)M1 whitelist download enable stops updating
CSCVb50917	ingress ping results in packet loss if not using a large size packet
CSCuz32027	RIP is accepting the packets even if its not from RIP port
CSCVb64704	C3900 in CUBE B2B HA setup, standby crash under voip traffic
CSCuz46782	CUBE - No audio for DO-EO FA when PRACK enabled on incoming call leg
CSCVa55916	CUBE crash in resolve_sig_ip_address_to_bind NULL ccb
CSCVa70943	CUBE DTMF p-type does not adhere to the signaling
CSCuz74014	CUBE responds 500 Internal Server Error to received= instead of via
CSCuz71250	Router crashes when parsing ack for mid call

Identifier	Description
CSCvb29204	BenignCertain on IOS and IOS-XE
CSCuz59190	GOS contains an outdated, vulnerable version of the OpenSSH server
CSCuz62775	ir892 Bundle install fails with SSH source interface configured
CSCva21638	issue in show isis nei detail
CSCvb53347	C841M PPP LED turns off even if one PPP up session exists
CSCvb39648	Fa0 port shows at C899G platform
CSCva79876	"Show controller VDSL 0" output is hanged with VDSL2-LINE-MIB
CSCva63462	only ipbasek9 not shaping on 15.5(3)M3
CSCva97725	rj45-auto-detect-polarity enable/disable behavior and shut/noshut timing
CSCva30241	[Firebee-to-WAN IGMP Snoop] Ports fwd traffic though there are no revers
CSCva46723	Small buffers leak with PPP
CSCvb08828	"no ip routing" + "ip default-gateway" config issue on C888-K9 device
CSCva60405	ALIGN-3-SPURIOUS Errors due to ATM OAM
CSCva96491	ATM config lost due to nbar
CSCvb71086	CWS + NVI NAT not working for web traffic
CSCvb36740	NIGHTLY Build FAILED for 15.6T (t_base_6)
CSCuz98690	IWAN auto-tunnel - incomplete adjacencies on ISR G2
CSCvb60498	Need to support SSMO Label format as per 3GPP TS 23.003/RFC 5149bis
CSCva32123	ALIGN-3-TRACE during boot on ISR-G2
CSCva36329	PAT entry using the same port which is configured for static NAT
CSCva19043	incorrect statistics regarding bandwidth utilization at each BR
CSCvb48912	SNMP crashes getting ntpAssociationEntry with low/fragmented memory condition
CSCuz77746	16.3 throttle: serial interface goes down after enabling ppp
CSCuy70502	show memory summary includes garbled characters
CSCva83993	Cisco SIP Gateway adds port 5060 to contact header in response
CSCuz10760	SIP SRST phone registration issues.
CSCvb60417	Router actin as HPR/SNA node crash every 2 hours
CSCva77149	Router crash when polling NOTIFICATION-LOG-MIB
CSCvb03342	IOS SSL VPN stuck reverse route blackholing IKEv2 connections
CSCva34598	Down change delay expired of track, without counting delay down time
CSCuz53590	Router crashes when trying to assign an bridge-goup
CSCva64393	CUBE e164-pattern-map doesn't parse the last line of the config file
CSCva22889	SWMTP route T.38 UDPTL Seq=65,72-79=RTP_Payload to (RTP UDP+1)=RTCP port
CSCvb58179	add new cas-custom CLI clear-bwd-in-seize for E1-R2
CSCva34382	Caller continue to hear ringback tone even after agent answers call.
CSCva00551	Cisco Router may crash on SIP MA Process Due to sstrncpy()
CSCvb16274	PPTP Start-Control-Connection-Reply packet leaks router memory contents
CSCva08727	WebUI: Tacacs not sending username with command authz/acct
CSCvb54653	Incoming SMS not showing syslog messages IOS 15.6(2)T
CSCvb61277	Add recovery mechanism in Linux_app to auto recover

Caveats in Prime Infrastructure 3.1.5

Identifier	Description
CSCvd29676	IWAN2.2 Multi VRF High values reported for TCA jitter in site to site details
CSCvd29606	IWAN2.2 Multi VRF. RC events do not display VRF information

Software Download Information

The following table provides the path on [Download Software](#) page for downloading the software for Cisco IWAN Release 2.2.

Software	Path
Cisco IOS XE Software	Downloads Home > Products > IOS and NX-OS Software > IOS XE > IOS XE S > IOS XE Release 2 > Routers > platform > IOS XE Software-Denali-16.3.3(ED) (https://software.cisco.com/download/release.html?mdfid=284932298&flowid=48622&softwareid=282046477&release=Denali-16.3.3&rellifecycle=ED&relind=AVAILABLE&reltype=latest)
Cisco IOS Software	Downloads Home > Products > IOS and NX-OS Software > IOS > IOS Software Release 15M&T > IOS Software Release 15.6M&T > Routers > platform > IOS Software-15.6(3)M2 (https://software.cisco.com/download/release.html?mdfid=282530906&flowid=78147&softwareid=280805680&release=15.4.3M7&relind=AVAILABLE&rellifecycle=MD&reltype=latest)
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 (https://software.cisco.com/download/release.html?mdfid=286304360&flowid=79748&softwareid=284272933&release=3.1.5&relind=AVAILABLE&rellifecycle=&reltype=latest)
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) (https://software.cisco.com/download/release.html?mdfid=286208072&flowid=77162&softwareid=286291196&release=1.4%20(IWAN)&relind=AVAILABLE&rellifecycle=&reltype=latest)
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-6.2.3b (https://software.cisco.com/download/release.html?mdfid=280484571&flowid=122&softwareid=280836712&release=6.2.3b&relind=AVAILABLE&rellifecycle=&reltype=latest)

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) on APIC-EM.
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)

© 2017 Cisco Systems, Inc. All rights reserved.