



Cisco IWAN Application on APIC-EM Release Notes, Release 1.5.2

First Published: 2017-09-08

Last Modified: 2017-09-08

Cisco IWAN Application on APIC-EM Release Notes, Release 1.5.2

These release notes provide a summary of the components in Cisco Intelligent Wide Area Network Application (Cisco IWAN App), Release 1.5.2.

Cisco IWAN App (or the Cisco IWAN on APIC-EM) extends Software Defined Networking to the branch with an application-centric approach based on business policy and application rules. This provides IT centralized management with distributed enforcement across the network.

Cisco IWAN App automates and orchestrates Cisco IWAN deployments with an intuitive browser-based GUI. A new router can be provisioned in a matter of minutes without any knowledge of the Command Line Interface (CLI). Business priorities are translated into network policies based on Cisco best practices and validated designs. Cisco IWAN App dramatically reduces the time required for configuring advanced network services through the use of automation and simple, predefined workflows.

Cisco IWAN App offers a turnkey solution that allows IT to get out of the weeds of managing low-level semantics like VPN, QoS, optimization, ACL policies. Instead, IT can focus on the bigger picture, such as, aligning network resources with business priorities and delivering outstanding user experience that result in better business outcomes.

Cisco IWAN App includes the following features:

- Zero touch provisioning—Plug and play for remote devices without user intervention
- Simple workflows—Use case driven with step-by-step and site-to-site provisioning
- Business level policies—Rules drive network actions, abstraction of underlying policy configuration
- Network monitoring—Status, alerting of network issues

What's New in Cisco IWAN App Release 1.5.2

The following features are available in Cisco IWAN App Release 1.5.2.

Feature Name	Description
Multi-tunnel termination (MTT)	Support for multiple WAN links for a hub device. Multiple links may be added to a device at the time of site provisioning (Day 0) or after provisioning (Day N). This feature is available both for primary and transit hub sites.
Global Day N modification of QoS bandwidth at service profile level	Ability to allocate user-defined bandwidth percentages to a QoS class model after provisioning (Day N). Any WAN connection using the class model is updated, whether the connection is at a hub or branch site.
4G Support for MPLS Cloud	Support for 4G WAN links on a private MPLS cloud. Before this release, 4G WAN links were supported only on a public INET cloud. <ul style="list-style-type: none"> • All topologies are supported. • Any topology may include one 4G-cellular interface. • The 4G-cellular interface may be used for WAN clouds, not within a LAN.
Enhanced IP Pool provisioning options	Ability to configure IP address pools for Service Provider (overlay) and management loopback. Ability to modify Service Provider label, type, and address pool until hub provisioning is complete.
Improved support for replacing a provisioned hub device (RMA)	Ability to replace a provisioned device (Day N) on a hub site, ensuring that the new router operates exactly like the router that has been replaced.
Additional Cisco ISR 89x routers support	Support added for several Cisco ISR 89x routers for branch sites. See the release notes for details.

Separation of Cisco IWAN Application from APIC-EM Releases

Cisco IWAN app release 1.3.2 introduced a new approach to IWAN app releases. Beginning with this release:

- The IWAN app has been decoupled from the APIC-EM release schedule, and from the APIC-EM installation and upgrade processes.
- IWAN app release numbering is now independent of APIC-EM release numbering.
- Download the IWAN app separately from APIC-EM, then install or upgrade the app using the APIC-EM “App Management” page. See [Cisco IWAN Application on Cisco APIC-EM User Guide, Release 1.5.0](#) for details about deployment.

Integral Part of APIC-EM

While the release schedule and installation are now handled separately from APIC-EM, Cisco IWAN App continues to be an integral part of APIC-EM and continues to appear in the APIC-EM GUI as before.

System requirements for the APIC-EM continue to apply to Cisco IWAN App.

See [Cisco IWAN App Software Compatibility in Cisco IWAN App Release](#) for information about the software compatible with Cisco IWAN App releases, including APIC-EM and Cisco Prime Infrastructure versions.

Supported Cisco Platforms and Software Releases in Cisco IWAN App Release 1.5.2

Cisco IWAN App Release 1.5.2 supports the following Cisco router platforms and software releases.

Platform	Models	Software Release
Cisco 4000 Series Integrated Services Routers	ISR 4321 ISR 4331 ISR 4351 ISR 4431-X ISR 4451-X	Cisco IOS XE Denali 16.3.3 ¹
Cisco ASR 1000 Series Aggregation Services Routers	ASR1001 ASR 1001-X ASR 1001-HX ASR 1002 ASR 1002-X ASR 1002-HX ASR 1004 ASR 1006 ASR 1006-X	Cisco IOS XE Denali 16.3.3
Cisco CSR 1000v Series Routers	Cloud Services Router 1000V	Cisco IOS XE Denali 16.3.3

Platform	Models	Software Release
Cisco Integrated Services Routers Generation 2 (ISR-G2) Series Routers	ENCS 5400 (ISRv—supported on Cisco IOS XE Denali 16.3.3) 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 3925E-ISM ISR 3925-ISM ISR 3945 ISR 3945-E ISR 3945E-ISM ISR 3945-ISM	Cisco IOS 15.6(3)M2

Platform	Models	Software Release
Cisco Integrated Services Routers Generation 2 (ISR-G2) Series Routers (continued)		Cisco IOS 15.6(3)M2

Platform	Models	Software Release
	C892-FSP	
	C897VA	
	C897VAB	
	C897VAG-LTE-GA	
	C897VAG-LTE-GA-K9	
	C897VAG-LTE-LA	
	C897VAGW-LTE-GAE	
	C897VA-M	
	C897VAMG-LTE-GA	
	C897VA-M-K9	
	C897VAM-W-E	
	C897VAW-A	
	ISR 897VAW-E	
	C898EA	
	C898EAG-LTE-GA	
	C898EAG-LTE-LA	
	C899G-LTE-GA	
	C899G-LTE-JP	
	C899G-LTE-LA	
	C899G-LTE-NA	
	C899G-LTE-ST	
	C899G-LTE-VZ	
	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	

Platform	Models	Software Release
	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	

¹ This release is required on hub devices to support Multi-tunnel Termination [MTT] (multiple WAN links) feature. Hence, Cisco IOS XE Everest 16.4.1 is not supported.

Limitations and Restrictions



Note

It is recommended that you upgrade to NBAR2 Advanced Protocol Pack 27.0.0 on your devices with the recommended latest Cisco IOS and Cisco IOS XE software releases.

When using EasyQoS and Cisco IWAN App on APIC-EM, you must adhere to the following:

- The network segments for each solution are disjoint. A device controlled by the IWAN solution cannot simultaneously be controlled by the EasyQoS solution. Application are of global scope across APIC-EM and as such, custom applications created in EasyQoS application may show up in the IWAN solution if applicable to the WAN solution.
- You must complete the following tasks on devices claimed by EasyQoS, to bring them in the IWAN workflow:
 - QoS policy tags should be removed prior to being claimed
 - The device must be cleaned of remaining EasyQoS policy or configuration and the device must be brought to greenfield state.

Hub Router EIGRP Process Downtime During Upgrade

When upgrading to Cisco IWAN App 1.5.1, after clicking the **Upgrade Network** button (a required step in the upgrade process), Cisco IWAN App pushes a series of commands to the hub BR routers, which triggers routing table updates from hub routers to branch site routers. During this update and resynchronization process,

the hub router's EIGRP process is inactive. The length of this EIGRP downtime depends on the number of branch site routers undergoing update, and may be several minutes.

This occurs only when operating a network with addressing within one of the following subnets: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16.

Caveats

Open Caveats in Cisco IWAN App Release 1.5.2

Caveat ID Number	Description
CSCvc46613	Spoke provision failure due to multiple users are defined and the not all of them are tried
CSCvb95745	Unable to add a device that was deleted with the site that failed at business policy config phase
CSCve03315	Custom Config: Repeated appearance of custom-template in form view
CSCvf29226	Spoke site with OSPF as LAN provisioning failed due to EIGRP flap
CSCvf89415	Missing summary-address under af-interface in MTT scenario
CSCvf89331	IWAN APP 1.5.2.387: Transit HUB Failed deployment
CSCvf33086	Device Sync failure for c898 brown field provision with pppoe
CSCvf38414	Transit Hub (MTT) failed with "Internal Error" on App Policy Update
CSCvf25809	Day-N QoS profile update for 4G interface failed with fetching bandwidth detail error
CSCvf23932	JDBC exception caused DB query failure when click newly discovered device list

Resolved Caveats in Cisco IWAN App Release 1.5.2

Caveat ID Number	Description
CSCvf86596	Provision a new site causing EIGRP flap in all sites
CSCvd04725	Hub AR ACLs not removed when branch sites are deleted
CSCvc16668	SA: Alarm tab seen on the site with no alarms shown on UI
CSCve21086	[SA] Generic Alarm thrown for requirements not met due to incorrect MTU size
CSCve17599	[SA] WAN interface discovery failure alarm recommended actions need more details

Caveat ID Number	Description
CSCvd83658	[SA] Wrong entry in hub alarm for eigrp saf entry -- showing non-existing SAF entry
CSCve19568	[SA]DMVPN alarm shows NBMA/peers are ping unreachable when they are reachable via ping
CSCve21952	“Set Geo” field for transit pop disappears if click on deleting transit pop then cancelled
CSCve21281	UI should limit custom app URL length to 29 characters - Add a tool tip about the 30 characters
CSCvc07291	SA: Uncontrolled TC alarm not shown for sites with no policy for backup link
CSCvc36842	[SA] No route is found at device is Misleading under child Alarm

System Requirements

The following sections describe the system requirements for Cisco IWAN App:

Hardware Requirements

Cisco IWAN App requires a server with the following capabilities/software:

- Server—64-bit x86
- CPU—6 (2.4GHz)
- RAM—32GB

Note: For a multi-host hardware deployment (two or three hosts), 32GB RAM is sufficient for each host.

- Storage—500 Gigabytes or preferably 1 Terabyte HDD
- Network Adapter—1x
- 200 MBps Disk I/O speed

Software Requirements

For Cisco IWAN on APIC-EM, the following software is required on the server:

- Browser
 - Chrome (version 50.0 or higher)
 - Mozilla Firefox (version 46.0 or higher)

Cisco IWAN App Software Compatibility in Cisco IWAN App Release

The following table describes compatible and recommended software versions for operation with the Cisco IWAN application, running on Cisco APIC-EM.

IWAN App	APIC-EM	Prime Infrastructure	Network Collector - LiveNX	OS on ASR1000 Series, ISR4000 Series, and CSR1000V Series Routers	OS on ISR-G2 Series Routers	Protocol Pack	Plug and Play
1.5.2	1.5.0	3.2	LiveNX 6.1.2	Cisco IOS XE Denali 16.3.3 ²	Cisco IOS Release 15.6(3)M2	27.0.0 31.0.0	1.5.0 1.5.1
1.5.1	1.5.0	3.2	LiveNX 6.1.2	Cisco IOS XE Denali 16.3.3 ³	Cisco IOS Release 15.6(3)M2	27.0.0 31.0.0	1.5.0 1.5.1
1.4.2	1.4.2 1.5.0	3.1.6	LiveNX 6.1	Cisco IOS XE 3.16.5aS ⁴ Cisco IOS XE Denali 16.3.3	Cisco IOS Release 15.6(3)M2	27.0.0	
1.3.2	1.3.2	3.1.4 Update 1	N/A	IOS XE 3.16.4bS (15.5(3)S4)	Cisco IOS Release 15.5(3)M4a		

² This release is required on hub devices to support Multi-tunnel Termination [MTT] (multiple WAN links) feature. Hence, Cisco IOS XE Everest 16.4.1 is not supported.

³ This release is required on hub devices to support Multi-tunnel Termination [MTT] (multiple WAN links) feature. Hence, Cisco IOS XE Everest 16.4.1 is not supported.

⁴ Link: <https://software.cisco.com/download/special/release.html?config=684110644675436ad1349ee490ed79ff>



Note

If you require a fix for CSCvc99738 and CSCvb66590, choose Cisco IOS XE 3.16.5aS and Cisco IOS release 15.5(3)M5a.

Firewall Requirements

If there is a firewall between the branch and the APIC-EM controller, please ensure that the following ports are open:

- Branch to the APIC-EM controller:
 - PKI—TCP 80
 - PNP—TCP 80, 443
 - NTP—UDP 123
- APIC-EM controller to branch:
 - SNMP—TCP and UDP ports: 161, 162
 - SSH—TCP 22
 - ECHO—TCP 7
- Internet branch to hub routers:
 - GRE and IPsec—UDP 500, 4500, IP—50

If there is a firewall between APIC-EM and Prime Infrastructure, ensure that port 443 is open for APIC-EM to access Prime Infrastructure API.

NetFlow Collectors

NetFlow collector provides Application Visibility. The supported NetFlow collectors for Cisco IWAN App are LiveNX and Cisco Prime. For information about compatible versions of Cisco Prime Infrastructure and other software, see [Cisco IWAN App Software Compatibility in Cisco IWAN App Release](#), on page 10.

Supported Hub Devices — Required License

See [Platforms and their Roles](#) for details per model.

- ASR 1000 Series
 - License—Image with licenses for Advanced IP Services or Advanced Enterprise Services
- ISR 4451 and 4431
 - License—Appx and Security

The following is a sample configuration that shows how to enable IPsec license and accept the End User License Agreement (EULA) on Cisco ASR 1000 Series Aggregation Services Routers.

```
Router(config)# crypto ipsec profile TEST
Router(ipsec-profile)# exit
Router(config)# interface tunnel 123
Router(config-if)# tunnel protection ipsec profile TEST
```



Note

The configuration must be removed after the EULA is accepted.

Supported Spoke Devices — Required License

See [Platforms and their Roles](#) for details per model.

- ASR 1000 Series
 - License—Advanced IP Services or Advanced Enterprise Services
- CSR1000v Series
 - License—AX throughput
- ISR 4000 Series
 - License—Appx and Security
- ISR G2 Series
 - License—Advanced IP Services (for ISR G2 892-FSP), Data, and Security

Platforms and their Roles

- ASR 1001—Hub, branch, or dedicated master controller
- ASR 1001-X—Hub, branch, or dedicated master controller
- ASR 1001-HX Router—Branch
- ASR 1002—Branch or dedicated master controller
- ASR 1002-X—Hub, branch, or dedicated master controller
- ASR 1002-HX Router—Hub and branch
- ASR1004—Hub or dedicated master controller
- ASR1006—Hub or dedicated master controller
- ASR1006-X—Hub or dedicated master controller
- CSR 1000v—Branch or dedicated master controller
- ISR 4431—Hub, branch, or dedicated master controller
- ISR 4451—Hub, branch, or dedicated master controller
- C891-24X-K9—Branch
- C891F-K9—Branch
- C891FW-A-K9—Branch
- C891FW-E-K9—Branch
- C892-FSP—Branch
- C892FSP-K9—Branch

- C896VAG-LTE-GA-K9—Branch
- C897VAB—Branch
- C897VAB-K9—Branch
- C897VA—Branch
- C897VAG-LTE-GA—Branch
- C897VAG-LTE-GA-K9—Branch
- C897VAG-LTE-GA-K9—Branch
- C897VAG-LTE-LA—Branch
- C897VAG-LTE-LA-K9—Branch
- C897VAGW-LTE-GAE—Branch
- C897VAGW-LTE-GAEK9—Branch
- C897VA-K9—Branch
- C897VA-M—Branch
- C897VAMG-LTE-GA—Branch
- C897VAMG-LTE-GA-K9—Branch
- C897VA-M-K9—Branch
- C897VA-M-K9—Branch
- C897VAM-W-E—Branch
- C897VAM-W-E-K9—Branch
- C897VAW-A—Branch
- C897VAW-A-K9—Branch
- C897VAW-E—Branch
- C897VAW-E-K9—Branch
- C898EA—Branch
- C898EAG-LTE-GA—Branch
- C898EAG-LTE-GA-K9—Branch
- C898EAG-LTE-LA—Branch
- C898EAG-LTE-LA-K9—Branch
- C898EA-K9—Branch
- C899G-LTE-GA—Branch
- C899G-LTE-GA-K9—Branch
- C899G-LTE-JP—Branch
- C899G-LTE-JP-K9—Branch

- C899G-LTE-LA—Branch
- C899G-LTE-LA-K9—Branch
- C899G-LTE-NA—Branch
- C899G-LTE-NA-K9—Branch
- C899G-LTE-ST—Branch
- C899G-LTE-ST-K9—Branch
- C899G-LTE-VZ—Branch
- C899G-LTE-VZ-K9—Branch
- ISR 1921—Branch
- ISR 1921-ISM—Branch
- ISR 1941—Branch
- ISR 1941-ISM—Branch
- ISR 2901—Branch
- ISR 2901-ISM—Branch
- ISR 2911—Branch
- ISR 2911-ISM—Branch
- ISR 2921—Branch
- ISR 2921-ISM—Branch
- ISR 2951—Branch
- ISR 2951-ISM—Branch
- ISR 3925—Branch
- ISR 3925E—Branch
- ISR 3925E-ISM—Branch
- ISR 3925-ISM—Branch
- ISR 3945—Branch
- ISR 3945-E—Branch
- ISR 3945E-ISM—Branch
- ISR 3945-ISM—Branch
- ISR 4321—Branch
- ISR 4331—Branch
- ISR 4351—Branch
- ISRv 5406—Branch
- ISRv 5408—Branch

- ISRV 5412—Branch

Related Documentation

Documentation	Description
Cisco IWAN Application on Cisco APIC-EM User Guide, Release 1.5.0	Information about 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.
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.
Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM	Information about Cisco Network Plug and Play solution.
Cisco Prime Infrastructure Documentation	Information about configuration guides, deployment guides, release notes, and other Cisco Prime Infrastructure documentation.
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.
Release Notes for Cisco Network Plug and Play, Release 1.5x	Description of the features and caveats for Cisco Network Plug and Play.
Release Notes for Cisco Application Policy Infrastructure Controller Enterprise Module, Release 1.5.0.x	Description of the features and caveats for the Cisco Application Policy Infrastructure Controller Enterprise Module (Cisco APIC-EM).

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.

© 2017 Cisco Systems, Inc. All rights reserved.