



Cisco IWAN Application on APIC-EM Release Notes, Release 1.6.2

First Published: 2018-12-20

Cisco IWAN Application on APIC-EM Release Notes, Release 1.6.2

These release notes provide a summary of the components in Cisco Intelligent Wide Area Network Application (Cisco IWAN App), Release 1.6.2.

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 1.6.2

The following features are available in Cisco IWAN App Release 1.6.2.

Feature Name	Description
PKI Certificate Renewal Alarm	Displays an alarm to indicate that a PKI certificate renewal has occurred for a specific device on a hub or branch site. Alerts you to perform a write memory on the device if the startup-config does not match the running-config.

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 1.6.x](#) 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 1.6.2

Cisco IWAN App Release 1.6.2 supports the following Cisco router platforms and software releases.



Note All devices operating at a single site (hub or branch) must use the same operating system version.

Example: Cisco IOS XE Everest 16.6.1

Platform	Models	Software Release
Cisco 4000 Series Integrated Services Routers	ISR 4221	Cisco IOS XE Everest 16.6.2 ¹
	ISR 4321	Cisco IOS XE Everest 16.6.1
	ISR 4331	Cisco IOS XE Denali 16.3.5
	ISR 4351	
	ISR 4431	
	ISR 4451-X	

Platform	Models	Software Release
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 Everest 16.6.1 Cisco IOS XE Everest 16.6.2 Cisco IOS XE Denali 16.3.5

Platform	Models	Software Release
Cisco 1100 Series Integrated Services Routers		Cisco IOS XE Everest 16.6.2

Platform	Models	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	
	C1111-8PLTEEAWC	
	C1111-8PLTEEAWD	
	C1111-8PLTEEAWE	
	C1111-8PLTEEAWF	
	C1111-8PLTEEAWG	
	C1111-8PLTEEAWH	
	C1111-8PLTEEAWI	
	C1111-8PLTEEAWJ	
	C1111-8PLTEEAWK	
	C1111-8PLTEEAWL	
	C1111-8PLTEEAWM	
	C1111-8PLTEEAWN	
	C1111-8PLTEEAWO	
	C1111-8PLTEEAWP	
	C1111-8PLTEEAWQ	
	C1111-8PLTEEAWR	
	C1111-8PLTEEAWS	
	C1111-8PLTEEAWT	
	C1111-8PLTEEAWU	
	C1111-8PLTEEAWV	
	C1111-8PLTEEAWW	
	C1111-8PLTEEAWX	
	C1111-8PLTEEAWY	
	C1111-8PLTEEAWZ	
	C1111-8PWA	
	C1111-8PWB	
	C1111-8PWE	
	C1111-8PWF	
	C1111-8PWH	
	C1111-8PWN	
	C1111-8PWQ	

Platform	Models	Software Release
	C1111-8PWR C1111-8PWZ C1116-4P C1116-4PLTEEA C1116-4PLTEEAWA C1116-4PLTEEAWZ C1116-4PWE C1117-4P C1117-4PLTEEA C1117-4PLTEEAWA C1117-4PLTEEAWZ C1117-4PLTELA C1117-4PLTELAZ C1117-4PLTELAZ C1117-4PM C1117-4PMLTEEA C1117-4PMLTEEAWA C1117-4PMLTEEAWZ C1117-4PMWE C1117-4PWA C1117-4PWE C1117-4PWZ	
Virtual Routers	Cloud Services Router 1000V ENCS 5400 (ISRv)	Cisco IOS XE Everest 16.6.1 Cisco IOS XE Everest 16.6.2 Cisco IOS XE Denali 16.3.5

Platform	Models	Software Release
Cisco Integrated Services Routers Generation 2 (ISR-G2) Series Routers—800 Series	C891-24X-K9 C891F-K9 C891FW-A-K9 C891FW-E-K9 C892-FSP-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 15.7(3)M
Cisco Integrated Services Routers Generation 2 (ISR-G2) Series Routers—1900 Series	ISR 1921 ISR 1941	Cisco IOS 15.7(3)M
Cisco Integrated Services Routers Generation 2 (ISR-G2) Series Routers—2900 Series	ISR 2901 ISR 2911 ISR 2921 ISR 2951	Cisco IOS 15.7(3)M

Platform	Models	Software Release
Cisco Integrated Services Routers Generation 2 (ISR-G2) Series Routers—3900 Series	ISR 3925 ISR 3925E ISR 3945 ISR 3945-E	Cisco IOS 15.7(3)M

¹ Applies to Cisco ISR 4221 Router

Notes and Limitations

EasyQoS

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 1.6.2, 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 1.6.2

Caveat ID Number	Description
CSCvg24770	Transit Hub provisioning failed- Internal Error
CSCvg16446	Cannot recover from customer configuration failure
CSCvc46613	Spoke provision failure due to multiple users are defined and the not all of them are tried

Caveat ID Number	Description
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
CSCvg42688	IWAN App 1.6 and Prime 3.2.1: Issues loading Queue Drop charts when apps are in Critical health
CSCvg46690	PnP 1.6.0: Image upgrade fails for Dual Router deployment via IWAN App
CSCvn43334	UI should throw validation error when QOS aggregate mode is not configured in a port-channel scenario
CSCvn75095	Deleting THUB/BR from a POP results in improper route-map configs on the router

Resolved Caveats in Cisco IWAN App Release 1.6.2

Caveat ID Number	Description
CSCvj61564	IWAN App configures tunnels with 1.1.1.1 destination address
CSCvk65203	Uploading a Certified IOS Release in IWAN App removes SNMP V3 credentials or SNMP V2 Write Community
CSCvm22417	APIC-EM 1.6.1, IWAN-APP 1.6.1: Hub failure because of CLI 'channel-unreachable-timer 4'
CSCvk33558	Adding CLI to change EIGRP external AD
CSCvm36353	Cellular deployment fails when trying to deploy from the cellular interface
CSCvm96796	Unable to use port-channel interface for hub lan for ISR 4K on 16.6.4

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 minimum 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
1.6.2	1.6.3	3.2.1 with Device Pack-1	6.1.2	Cisco IOS XE Denali 16.3.5 Cisco IOS XE Everest 16.6.1 ² Cisco IOS XE Everest 16.6.2 (Cisco ISR 4221 Router & Cisco ISR 1100 Series Routers) Cisco IOS XE Fuji 16.9.1	15.7(3)M 15.6(3)M3	32.0.0	1.6.0
1.6.1	1.6.1	3.2.1 with Device Pack-1	6.1.2	Cisco IOS XE Everest 16.6.1 Cisco IOS XE Everest 16.6.2 (Cisco ISR 4221 Router & Cisco ISR 1100 Series Routers) Cisco IOS XE Denali 16.3.5	15.7(3)M 15.6(3)M3	32.0.0	1.6.0

IWAN App	APIC-EM	Prime Infrastructure	Network Collector - Linux	OS on ASR1000 Series, ISR4000 Series, and CSR1000V Series Routers	OS on ISR-G2 Series Routers	Protocol Pack	Plug and Play
1.6.0	1.6.0	3.2.1 with Device Pack-1	6.1.2	Cisco IOS XE Everest 16.6.1 Cisco IOS XE Everest 16.6.2 (Cisco ISR 4221 Router & Cisco ISR 1100 Series Routers) Cisco IOS XE Denali 16.3.5	15.7(3)M 15.6(3)M3	32.0.0	1.6.0
1.5.2	1.5.0	3.2	Linux 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
1.5.1	1.5.0	3.2	Linux 6.1.2	Cisco IOS XE Denali 16.3.3 ⁴	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	Linux 6.1	Cisco IOS XE 3.16.5aS ⁵ 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 In this table, Cisco IOS XE release numbers refer to the specified release and later maintenance releases (“point releases”) in the series. For example, 16.6.1 refers to 16.6.1 and later releases of 16.6.x.

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 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.

⁵ Link: <https://software.cisco.com/download/special/release.html?config=684110644675436ad1349ee490ed79ff>



Note If you require a fix for CSCve99738 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
- 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 4451-X—Hub, branch, or dedicated master controller
- ISR 4221—Branch
- ISR 4321—Branch
- ISR 4331—Branch
- ISR 4351—Branch
- ISR 4431—Branch
- ISRV 5406—Branch
- ISRV 5408—Branch
- ISRV 5412—Branch

- C891-24X-K9—Branch
- C891F-K9—Branch
- C891FW-A-K9—Branch
- C891FW-E-K9—Branch
- C892FSP-K9—Branch
- C896VAG-LTE-GA-K9—Branch
- C896VA-K9—Branch
- C897VAB-K9—Branch
- C897VA-K9—Branch
- C897VAG-LTE-GA-K9—Branch
- C897VAG-LTE-LA-K9—Branch
- C897VAGW-LTE-GAEK9—Branch
- C897VAMG-LTE-GA-K9—Branch
- C897VA-M-K9—Branch
- C897VAM-W-E-K9—Branch
- C897VAW-A-K9—Branch
- C897VAW-E-K9—Branch
- C898-EA-K9—Branch
- C898EAG-LTE-GA-K9—Branch
- C898EAG-LTE-LA-K9—Branch
- C899G-LTE-GA-K9—Branch
- C899G-LTE-JP-K9—Branch
- C899G-LTE-LA-K9—Branch
- C899G-LTE-NA-K9—Branch
- C899G-LTE-ST-K9—Branch
- C899G-LTE-VZ-K9—Branch
- ISR 1921—Branch
- ISR 1941—Branch
- ISR 2901—Branch
- ISR 2911—Branch
- ISR 2921—Branch
- ISR 2951—Branch

- ISR 3925—Branch
- ISR 3925E—Branch
- ISR 3945—Branch
- ISR 3945-E—Branch
- C1111-4P—Branch
- C1111-4PLTEEA—Branch
- C1111-4PLTELA—Branch
- C1111-4PWA—Branch
- C1111-4PWB—Branch
- C1111-4PWD—Branch
- C1111-4PWE—Branch
- C1111-4PWF—Branch
- C1111-4PWH—Branch
- C1111-4PWN—Branch
- C1111-4PWQ—Branch
- C1111-4PWR—Branch
- C1111-4PWZ—Branch
- C1111-8P—Branch
- C1111-8PLTEEA—Branch
- C1111-8PLTEEAWA—Branch
- C1111-8PLTEEAWB—Branch
- C1111-8PLTEEAWC—Branch
- C1111-8PLTEEAWD—Branch
- C1111-8PLTEEAWE—Branch
- C1111-8PLTEEAWF—Branch
- C1111-8PLTEEAWG—Branch
- C1111-8PLTEEAWH—Branch
- C1111-8PLTEEAWI—Branch
- C1111-8PLTEEAWJ—Branch
- C1111-8PLTEEAWK—Branch
- C1111-8PLTEEAWL—Branch
- C1111-8PLTEEAWM—Branch
- C1111-8PLTEEAWN—Branch
- C1111-8PLTEEAWO—Branch
- C1111-8PLTEEAWP—Branch
- C1111-8PLTEEAWQ—Branch
- C1111-8PLTEEAWR—Branch
- C1111-8PLTEEAWS—Branch
- C1111-8PLTEEAWT—Branch
- C1111-8PLTEEAWU—Branch
- C1111-8PLTEEAWV—Branch
- C1111-8PLTEEAWW—Branch
- C1111-8PLTEEAWX—Branch
- C1111-8PLTEEAWY—Branch
- C1111-8PLTEEAWZ—Branch
- C1111-8PLTELA—Branch
- C1111-8PLTELAWD—Branch
- C1111-8PLTELAWF—Branch
- C1111-8PLTELAWH—Branch
- C1111-8PLTELAWN—Branch
- C1111-8PLTELAWQ—Branch
- C1111-8PLTELAWZ—Branch
- C1111-8PWA—Branch
- C1111-8PWB—Branch

- C1111-8PWE—Branch
- C1111-8PWF—Branch
- C1111-8PWH—Branch
- C1111-8PWN—Branch
- C1111-8PWQ—Branch
- C1111-8PWR—Branch
- C1111-8PWZ—Branch
- C1116-4P—Branch
- C1116-4PLTEEA—Branch
- C1116-4PLTEEAWE—Branch
- C1116-4PWE—Branch
- C1117-4P—Branch
- C1117-4PLTEEA—Branch
- C1117-4PLTEEAWA—Branch
- C1117-4PLTEEAWE—Branch
- C1117-4PLTELA—Branch
- C1117-4PLTELAWZ—Branch
- C1117-4PM—Branch
- C1117-4PMLTEEA—Branch
- C1117-4PMLTEEAWE—Branch
- C1117-4PMWE—Branch
- C1117-4PWA—Branch
- C1117-4PWE—Branch
- C1117-4PWZ—Branch

Related Documentation

Documentation	Description
Cisco IWAN Application on Cisco APIC-EM User Guide, Release 1.6.x	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.

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.
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).

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact you’re looking for with the technologies that matter, visit [Cisco Services](#).
- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

Cisco Bug Search Tool

[Cisco Bug Search Tool](#) (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

