Cisco IWAN Application on APIC-EM Release Notes, Release 1.4.0

First Published: 2017-02-21

Last Modified: 2017-02-21

Introduction

These release notes provide a summary of the components in Cisco Intelligent Wide Area Network Application (Cisco IWAN App), Release 1.4.0.

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 1.4.0

The following new features are available in Cisco IWAN App Release 1.4.0.

Feature Name	Description
4G Support on Cisco 4000 Series Integrated Services Routers	Support for configuring 4G cellular technology connections on Cisco 4000 Series Integrated Services Routers at branch sites.
APIC-EM behind NAT	Support for APIC-EM controller behind NAT. Previously supported for greenfield sites; this version adds support for brownfield sites.
Custom configuration (beta)	Mechanism to execute configuration commands on devices in the IWAN network.

Feature Name	Description
Custom application deletion	Ability to delete Cisco IWAN App custom applications.
Day 0 and Day N QoS Bandwidth Modifications	• Ability to allocate user-defined bandwidth percentages to a priority QoS class model and other class models during provisioning (Day 0). • Ability to modify user-defined bandwidth percentages to a priority QoS class model and other class models after provisioning (Day N).
Day N WAN bandwidth update for hub or spoke site	Ability to change the upload or download WAN bandwidth after a hub or spoke site is provisioned (“day N”).
Day N WAN IP updated for spoke site	Ability to change WAN IP address, mask, or next-hop configured on a spoke after the site has been provisioned (“day N”).
Spoke behind NAT	Support for spoke sites behind NAT.
Support for ASR1000 Series routers for spoke sites	Support for the following Cisco ASR 1000 Aggregation Services Routers at spoke sites: ASR1001-X, ASR 1001, ASR 1002, ASR 1002-X, ASR 1001-HX, ASR 1002-HX.
Support for Cisco IOS XE Denali 16.x	Support for routers running Cisco IOS XE Denali 16.3.3.
Support for NBAR2 Protocol Pack	Support for NBAR2 Protocol Pack 27.0.0, which provides new application protocols and improves existing protocols. **Note** If a router has NBAR custom application defined in a previous version of Cisco IWAN App and the custom applications name conflicts with the name of a new protocol in NBAR2 Protocol Pack 27.0.0, the custom application will be renamed as c_<original-custom-app-name>.
Support multiple DHCP servers on a hub site	Ability to add up to 5 DHCP servers on a hub site.

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 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

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

Platform	Models	Software Release
Cisco 4000 Series Integrated Services Routers	4321 4331 4351 4431-X 4451-X	Cisco IOS XE 3.16.5aS Cisco IOS XE Denali 16.3.3
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 3.16.5aS Cisco IOS XE Denali 16.3.3
Cisco CSR 1000v Series Routers	Cloud Services Router 1000V	Cisco IOS XE 3.16.5aS Cisco IOS XE Denali 16.3.3

Platform	Models	Software Release
Cisco Integrated Services Routers Generation 2 (ISR-G2) Series Routers	ISR 3945 ISR 3945-ISM ISR 3945-E ISR 3945E-ISM ISR 3925 ISR 3925-ISM ISR 3925E ISR 3925E-ISM ISR 2951 ISR 2951-ISM ISR 2921 ISR 2921-ISM ISR 2911 ISR 2911-ISM ISR 2901 ISR 2901-ISM ISR 1941 ISR 1941-ISM ISR 1921 ISR 1921-ISM ISR 892-FSP	Cisco IOS 15.6(3)M2

Note IWAN is not supported on Cisco Catalyst 8000 Edge Platforms.

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 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 1.4.0

Caveat ID Number	Headline
CSCvd22094	Custom apps were not pushed into Hub routers after upgrade from 1.3.2 to 1.4 + IWAN app bundle 413
CSCvd21483	Prime 3.1.5: Devices in Collection Failure state on Prime Inventory
CSCvb95745	Unable to add a device that was deleted with the site that failed at business policy config phase
CSCvc46613	Spoke provision failure due to multiple users are defined and the not all of them are tried
CSCvd01622	Device inventory shows device in "Unknown" state after upgrade from 1.3.2 to 1.4
CSCvd01892	IWAN App 1.4.0 + Prime 3.1.5: Intermittent QoS Class Map Stats issue
CSCvd12920	IWAN App 1.4.0 + Prime 3.1.5: No historical data under pfr dashboard after 24 hrs
CSCvd12966	Inventory collection failing on Prime when SNMPv3 mode is changed on IWAN App post APIC-EM site sync
CSCvd02096	IWAN App 1.4.0 + Prime 3.1.5: False Compliance warning on spokes after Day-N BR addition
CSCvb24793	Spoke provision failed at Device addition to inventory FAILURE if WAN IP is changed during provision

Caveat ID Number	Headline
CSCvd04725	Hub AR ACLs not removed when branch sites are deleted
CSCvd06887	Cannot discover device with global discovery, but device can be added through inventory app
CSCvc86828	Sync device failed while provisioning BF L3 SR3L site

Resolved Caveats in Cisco IWAN App Release 1.4.0

Caveat ID Number	Headline
CSCvc11092	UI not able to populate the drop down menu for bandwidth, interfaces, etc with latest Chrome browser
CSCvc14842	QoS failure at \"platform qos port-channel-aggregate < port-channel # >\" config at port-channel interface
CSCvc14850	VLAN type should not be required to be unique or mandatory
CSCvc48625	IP Pool page throwing max VLAN number validation for BF SS Pool
CSCvc36435	SVI (VLAN) interface needs to be filtered out for WAN use

Open Caveats, Service Assurance Feature, Beta Release

Caveat ID Number	Headline
CSCvc16668	Service Assurance: Alarm tab seen on the site with no alarms shown on UI
CSCvc07291	Service Assurance: Uncontrolled TC alarm not shown for sites with no policy for backup link
CSCvc36842	Service Assurance: No route is found at device is Misleading under child Alarm

Resolved Caveats, Service Assurance Feature, Beta Release

Caveat ID Number	Headline
CSCvc32302	Service Assurance: Site doesn't have valid loopback configured in vrf 'default'
CSCvc46191	Service Assurance stuck at loading screen after enabling post upgrade
CSCvc01995	Incorrect Alarm field value on Site Details Page under Alarms Tab
CSCvc28965	Service Assurance: Monitoring Page Critical button dropdown shows Error: Unable to load data
CSCvc42733	Service Assurance flagging channel state check failed alarm for deleted sites

Caveat ID Number	Headline
CSCvc55635	IWAN App Upgrade: reset_grapevine needed for Service Assurance in upgrade scenarios

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

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[1] 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

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
1.6.1	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
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	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		

[1] 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.

[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
- 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, on page 7.

Supported Hub Devices — Required License

- 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

- 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 4321—Branch
- ISR 4331—Branch
- ISR 4351—Branch
- ISR 4431—Hub, branch, or dedicated master controller
- ISR 4451—Hub, branch, or dedicated master controller

- ISR 1921—Branch
- ISR 1921-ISM—Branch
- ISR G2 1941—Branch
- ISR 1941-ISM—Branch
- ISR 2901—Branch
- ISR 2901-ISM—Branch
- ISR 2911—Branch
- ISR 2911-ISM—Branch
- ISR G2 2921—Branch
- ISR 2921-ISM—Branch
- ISR G2 2951—Branch
- ISR G2 2951-ISM—Branch
- ISR G2 3925—Branch
- ISR G2 3925-E—Branch
- ISR G2 3925-ISM—Branch
- ISR 3925E-ISM—Branch
- ISR G2 3945—Branch
- ISR G2 3945-E—Branch
- ISR G2 3945-ISM—Branch
- ISR 3945E-ISM—Branch
- ISR G2 892-FSP—Branch
- ISR 897VA-M-K9—Branch
- ISR 897VAB-K9—Branch
- ISR 896VAG-LET-GA-K9—Branch
- ISRv—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.