Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Amsterdam Release 17.2.x

First Published: 2020-03-31

Last Modified: 2020-06-19

Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Amsterdam 17.2.x

Introduction to Cisco Catalyst 9800 Series Wireless Controllers

The Cisco Catalyst 9800 Series Wireless Controllers comprise next-generation wireless controllers (referred to as *controller* in this document) built for intent-based networking. The controllers use Cisco IOS XE software and integrate the radio frequency (RF) capabilities from Cisco Aironet with the intent-based networking capabilities of Cisco IOS XE to create a best-in-class wireless experience for your organization.

The controllers are enterprise ready to power your business-critical operations and transform end-customer experiences:

- The controllers come with high availability and seamless software updates that are enabled by hot and cold patching. This keeps your clients and services up and running always, both during planned and unplanned events.
- The controllers come with built-in security, including secure boot, run-time defenses, image signing, integrity verification, and hardware authenticity.
- The controllers can be deployed anywhere to enable wireless connectivity, for example, on an on-premise device, on cloud (public or private), or embedded on a Cisco Catalyst switch (for SDA deployments) or a Cisco Catalyst access point (AP).
- The controllers can be managed using Cisco Catalyst Center, programmability interfaces, for example, NETCONF and YANG,or web-based GUI or CLI.
- The controllers are built on a modular operating system. Open and programmable APIs enable the automation of your day zero to day *n* network operations. Model-driven streaming telemetry provides deep insights into your network and client health.

The controllers are available in multiple form factors to cater to your deployment options:

- Catalyst 9800 Series Wireless Controller Appliance
- Catalyst 9800 Series Wireless Controller for Cloud
- Catalyst 9800 Embedded Wireless Controller for a Cisco Switch

Note All the Cisco IOS XE programmability-related topics on the controllers are supported by DevNet, either through community-based support or through DevNet developer support. For more information, go to https://developer.cisco.com.

Note For information about the recommended Cisco IOS XE releases for Cisco Catalyst 9800 Series Wireless Controllers, see the documentation at:

https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/214749-tac-recommended-ios-xe-builds-for-wirele.html

What's New in Cisco IOS XE Amsterdam 17.2.1a

There are no new features or enhancements in this release.

What's New in Cisco IOS XE Amsterdam 17.2.1

This section provides information about the new features and enhancements in this release.

Aironet Extensions IE (CCX IE) Advertise AP Name: Aironet Extensions Information Elements (IE) is an attribute used by Cisco devices for better connectivity. IE has been enhanced to include the AP Name as an additional information that compatible clients can use. The Cisco Client Extensions (CCX) uses this information to associate with the best AP. For more information, see the Aironet Extensions IE (CCX IE) - Advertise AP Name chapter.

BSSID Counters: The BSSID Counters feature helps to retrieve the BSSID statistics when a client is associated with a WLAN for every configured interval. A new configuration is introduced in the controller per AP profile to enable or disable BSSID statistics on the access points. For more information, see the BSSID Counters chapter.

The following commands are introduced:

- **bssid-stats bssid-stats-frequency** *bssid-timer-seconds*
- **bssid-neighbor-stats interval** *bssid-interval*

Default Gateway Check: Starting from this release, the method to configure the gateway IP has been modified. The **ip default-gateway** *gateway-ip* command is not used. Instead, the gateway IP is selected based on the static routes configured. From among the static routes configured, the gateway IP that falls in the same subnet as the RMI subnet is chosen. If no matching static route is found, gateway failover will not work (even if management gateway-failover is enabled). For more information, see the *Redundancy Management Interface* section in High Availability chapter.

DHCP-required for Flex Local Switching: When this feature is enabled, the client will be able to pass traffic only if it has obtained an IP address through DHCP. In earlier releases DHCP required was only available for central switching. From this release, local switching is supported. For more information, see the Configuring DHCP-Required for FlexConnect section.

Dot11i Roaming: In this release, you can create a Mobility Domain ID (MDID) for each of the APs. All the APs configured with the same MDID share the PMK cache keys even if they are in different site tags. MDID supports PMK cache distribution in both, central authentication and local authentication. For more information, see the Mobility Domain ID - Dot11i Roaming chapter.

Dot11r Support for FlexConnect Local Authentication: From this release, fast transition is supported for FlexConnect local authentication, with local switching deployments. From this release onwards, PMK sharing is also supported via Mobility Domain ID (MDID). MDID is used by 802.11r to define a network in which an 802.11r fast roam is supported. For more information, see the Dot11r Support for FlexConnect Local Authentication chapter.

Static Tri-Radio Support: The Cisco Catalyst 9130 Access Points are designed for high density deployments. The 5 GHz radio can be statically configured as a single 8x8 radio or dual 4x4 radios operating and two channels in the 5GHz band. The modes can be manually configured using CLI. For more information, see the Cisco Access Points with Tri-Radio chapter.

The following commands are introduced:

- **ap name** *ap-name* **dot11 5ghz slot 1 dual-radio mode {disable | enable }**
- **ap triradio {disable | enable}**
- **show ap triradio summary**

Fabric in a Box With External Fabric Edge: Starting with this release, the fabric in a box (FiaB) topology supports external fabric edge nodes. In a fabric enabled wireless environment using FiaB (border node, control plane, fabric edge, and wireless controller in the same box), you can expand the network by adding external fabric edge nodes. For more information, see the Fabric in a Box with External Fabric Edge chapter.

IPv6 Non-AVC QoS Support: This features brings IPV6 QoS (excluding AVC) to flex local switching and Fabric deployments. In these modes, the client traffic doesn't go through the controller, so the QoS Marking, Policing and Dropping is done at the AP. For more information, see the IPv6 Non-AVC QoS Support chapter.

Lobby Admin Access and Client Whitelisting: The global administrator creates and enables lobby admin users access to the WLAN. Lobby administrators adds or deletes a client from the allowed list to manage the association with a WLAN or an SSID through the GUI interface only. Changes in GUI include enabling lobby admin access by global administrator, creating new client allowed list by the lobby admin, managing client allowed list by the lobby admin. For more information, see the Lobby Admin Accounts chapter.

Note In the existing implementation of the Client Whitelisting feature, WLAN specific allowed list client is added as a wildcard client. This behaviour will be modified in the upcoming major (extended maintenance) release.

Multi-LAG: Multi Link Aggregation Group (multi-LAG) provides flexibility in connecting controller to multiple switching infrastructures. Using multi-LAG, you can connect the multiple uplinks from the controller to separated uplink switches. For more information, see the Link Aggregation Group chapter.

Multicast Filtering: In this release, the Multicast Filtering feature is supported on Layer 3 for IPv4. When you enable this feature, the APs will stop forwarding multicast packets to the clients. For more information, see the Multicast Filtering chapter.

The following command is introduced:

- **multicast filter**

Open Roaming: This feature enables mobile users to automatically and seamlessly roam across Wi-Fi and cellular networks. The new configuration template of the open roaming ANQP server simplifies the setup of a Hotspot 2.0 ANQP server. For more information, see the Hotspot 2.0 chapter.

The following command is introduced:

- **open-roaming oi**

The following command was modified and **type** and **open-roaming** keywords were added.

- **wireless hotspot anqp-server**

Opportunistic Key Caching (OKC) Enabling: A new configuration per WLAN in the controller is introduced from this release, to disable or enable Fast-Secure roaming with OKC at the access point. For more information, see the Opportunistic Key Caching chapter.

The following command is introduced:

- **no okc**

QBSS-Load Information Element (IE): In this release, the QoS Basic Set Service (QBSS) load is automatically enabled with Wi-Fi Multimedia (WMM). A separate configuration knob is introduced to include or exclude QBSS load information element (IE), which is sent in beacon frames and probe responses. For more information, see the QoS Basic Set Service chapter.

The following command is introduced:

- **qbss-load**

Remote LAN Local Switching: Starting with this release, after a CAPWAP DOWN/UP state, existing RLAN local switched client details are not available in the controller.

SGT and VN Attributes Display: Starting with this release, in the web UI, the Policy tab in the Clients page displays the Output VN and Output SGT attributes for Server Policies and Resultant Policies.

Spectrum Analysis: Network administrators receive RF violation issues from end-users or RF issue from DNAC. To analyze the violation, network administrators selects the required access point and analyzes the spectrogram stream. For more information, see the Spectrum Analysis chapter.

Support for Cisco Catalyst Industrial Wireless 6300 Heavy Duty Series Access Point: Starting with this release, bridge mode is supported on the IW6300 AP.

IW 6300 APs deliver secure, scalable, and flexible wireless connectivity to the most hazardous of industrial environments. Using this AP, you can deploy wireless connectivity anywhere, and stay online during the most extreme weather, in consistently hazardous areas, or during dangerous industrial events. It also provides upgraded 802.11ac Wave 2 capability and provides up to 867-Mbps data rate with 2 x 2 MIMO and 2 spatial streams. For more information about Cisco Catalyst Industrial Wireless 6300 AP, see https://www.cisco.com/c/en/us/products/wireless/industrial-wireless-6300-series/index.html

Cisco Catalyst Industrial Wireless 6300 AP supports the following modes:

- Local Mode
- Flex Connect Mode
- Monitor Mode
- WGB Mode

- Bridge Mode
- Flex + Bridge Mode

Target Wake Time: Target wake time (TWT) allows an AP to manage activity in the Wi-Fi network, in order to minimize medium contention between Stations (STAs), and to reduce the required amount of time that an STA in the power-save mode needs to be awake. This is achieved by allocating STAs to operate at non-overlapping times, and/or frequencies, and concentrate the frame exchanges in predefined service periods. For more information, see the Target Wake Time chapter.

Web UI Features

The following list shows the newly introduced web UI features and their path.

- **BSS Coloring Support**: Configuration > Wireless > Access Points
- **Device Ecosystem Intelligent Client Scan Reports with MBO**: Configuration > Tags & Profiles > WLANs
- **Lobby Admin Access and Client Whitelisting**: Administration > User Administration
- **Tri-radio Support**: Configuration > Wireless > Access Points

Behavior Changes

- Sensor mode is not supported on the APs.
- From this release onwards, Guestshell can access files only from the *guest-share* directory.

MIBs

The following MIBs were modified by adding new OIDs:

- CISCO-LWAPP-AP-MIB.my
  - cLApDot11IfDualRadioMode
  - cLApDot11IfDualRadioCapable
  - cLApDot11IfRadioFRACapable
  - cLApDot11IfDualRadioOperation
  - cLApDot11IfRadioRole
  - cLApDot11IfRadioRoleOperation
  - cLApProfileWindowSize
  - cLApProfileCredentialGlobalSecretType
  - cLApProfileCredentialGlobalPasswordType
  - cLApProfile802dot1xSupplicantPasswordType
  - cLApProfileBssidEnableStats
  - cLApProfileBssidStatsFrequency

- CISCO-LWAPP-RRM-MIB.my
  - clRrmBcoMode
  - clrRrmTriRadioMode
- CISCO-LWAPP-WLAN-SECURITY-MIB.my
  - cLWSecDot11OsenEnable
- CISCO-LWAPP-WLAN-MIB.my
  - cLWlanOpportunisticKeyCaching
  - cLWlan11axTwtBroadcastSupport
- CISCO-LWAPP-WLAN-MIB.my
  - clGuestLanMobileStationProfileName

Supported Hardware

The following table lists the supported virtual and hardware platforms. (See Table 3: Supported PIDs and Ports, on page 7 for the list of supported modules.)

Table 1: Supported Virtual and Hardware Platforms

Platform	Description
Cisco Catalyst 9800-80 Wireless Controller	A modular wireless controller with up to 100-GE modular uplinks and seamless software updates. The controller occupies 2-rack unit space and supports multiple module uplinks.
Cisco Catalyst 9800-40 Wireless Controller	A fixed wireless controller with seamless software updates for mid-size to large enterprises. The controller occupies 1-rack unit space and provides four 1-GE or 10-GE uplink ports.
Cisco Catalyst 9800 Wireless Controller for Cloud	A virtual form factor of the Catalyst 9800 Wireless Controller that can be deployed in a private cloud (supports ESXi, KVM, Microsoft Hyper-V, and NFVIS on ENCS hypervisors), or in the public cloud as Infrastructure as a Service (IaaS) in Amazon Web Services (AWS) and Google Cloud Platform (GCP) marketplace.
Cisco Catalyst 9800 Embedded Wireless Controller for Switch	The Catalyst 9800 Wireless Controller software for the Cisco Catalyst 9000 switches bring the wired and wireless infrastructure together with consistent policy and management. This deployment model supports only SD Access, which is a highly secure solution for small campuses and distributed branches.

Platform	Description
Cisco Catalyst 9800-L Wireless Controller	The Cisco Catalyst 9800-L Wireless Controller is the first low-end controller that provides a significant boost in performance and features.

The following table lists the host environments supported for private and public cloud.

Table 2: Supported Host Environments for Public and Private Cloud

Host Environment	Software Version
VMware ESXi	• VMware ESXi vSphere 6.0, 6.7, and 7.0 • VMware ESXi vCenter 6.0, 6.5, 6.7 and 7.0
KVM	• Ubuntu 14.04.5 LTS, Ubuntu 16.04.5 LTS
AWS	AWS EC2 platform
NFVIS	ENCS 3.8.1 and 3.9.1
GCP	GCP marketplace
Microsoft Hyper-V	Windows 2019 Server and Windows Server 2016 (Version 1607) with Hyper-V Manager (Version 10.0.14393)

The following table lists the supported Cisco Catalyst 9800 Series Wireless Controller hardware models.

The Base PIDs are the model numbers of the controller.

The Bundled PIDs indicate the orderable part numbers for the Base PIDs that are bundled with a particular network module. Running the **show version**, **show module** or **show inventory** command on such a controller (bundled PID) displays its Base PID.

Note that unsupported SFPs will bring down a port. Only Cisco-supported SFPs (GLC-LH-SMD and GLC-SX-MMD) should be used on the RP port of C9800-80-K9 and C9800-40-K9.

Table 3: Supported PIDs and Ports

Controller Model	Description
C9800-CL-K9	Cisco Catalyst Wireless Controller as an infrastructure for Cloud.

Controller Model	Description
C9800-80-K9	Eight 1/10-Gigabit Ethernet SFP or SFP+ ports and two power supply slots. The following SFPs are supported: • GLC-BX-D • GLC-BX-U • GLC-EX-SMD • GLC-LH-SMD • GLC-SX-MMD • GLC-ZX-SMD • GLC-TE
	The following enhanced SFPs are supported: • SFP-10G-AOC1M • SFP-10G-AOC2M • SFP-10G-AOC3M • SFP-10G-AOC5M • SFP-10G-AOC7M • SFP-10G-AOC10M • SFP-10G-SR • SFP-10G-SR-S • SFP-10G-SR-X • SFP-10G-ER • SFP-10G-ZR • SFP-H10GB-ACU7M • SFP-H10GB-ACU10M • DWDM-SFP10G-30.33 • DWDM-SFP10G-61.41

Controller Model	Description
	The following QSFP+s are supported: • QSFP-40G-SR4 • QSFP-40G-LR4 • QSFP-40GE-LR4 • QSFP-40G-ER4 • QSFP-40G-SR4-S • QSFP-40G-LR4-S • QSFP-40G-SR-BD • QSFP-40G-BD-RX • QSFP-100G-SR4-S • QSFP-100G-LR4-S
C9800-40-K9	Four 1/10-Gigabit Ethernet SFP or SFP+ ports and two power supply slots The following SFPs are supported: • GLC-BX-D • GLC-BX-U • GLC-LH-SMD • GLC-SX-MMD • GLC-EX-SMD • GLC-ZX-SMD • GLC-TE

Controller Model	Description
	The following enhanced SFPs are supported: • SFP-10G-AOC1M • SFP-10G-AOC2M • SFP-10G-AOC3M • SFP-10G-AOC5M • SFP-10G-AOC7M • SFP-10G-AOC10M • SFP-10G-SR • SFP-10G-SR-S • SFP-10G-SR-X • SFP-10G-ER • SFP-10G-ZR • SFP-H10GB-ACU7M • SFP-H10GB-ACU10M • DWDM-SFP10G-30.33 - DWDM-SFP10G-61.41
C9800-L-C-K9	• 4x2.5/2-Gigabit ports • 2x10/5/2.5/1-Gigabit ports The following SFPs are supported: • GLC-BX-D • GLC-BX-U • GLC-LH-SMD • GLC-SX-MMD • GLC-ZX-SMD • GLC-TE

Controller Model	Description
C9800-L-F-K9	• 4x2.5/2-Gigabit ports • 2x10/1-Gigabit ports The following SFPs are supported: • GLC-BX-D • GLC-BX-U • GLC-SX-MMD • GLC-ZX-SMD • GLC-TE • SFP-10G-SR • SFP-10G-SR-S • SFP-10G-SR-X • SFP-H10GB-ACU7M • SFP-H10GB-ACU10M

Optics Modules

Cisco Catalyst 9800 Series Wireless Controller supports a wide range of optics. The list of supported optics is updated on a regular basis. See the tables at the following location for the latest transceiver module compatibility information:

https://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

Supported APs

The following Cisco APs are supported in this release.

Indoor Access Points

- Cisco Aironet 1700 Series Access Points
- Cisco Aironet 1800 Series Access Points
- Cisco Aironet 2700 Series Access Points
- Cisco Aironet 2800 Series Access Points
- Cisco Aironet 3700 Series Access Points
- Cisco Aironet 3800 Series Access Points
- Cisco Aironet 4800 Series Access Points
- Cisco Catalyst 9115AXI Access Points

- Cisco Catalyst 9117AXI Access Points
- Cisco Catalyst 9120AXI Access Points (VID 06 or earlier) - supported from 17.3.1 to 17.3.5
- Cisco Catalyst 9120AXI Access Points (VID 07 or earlier) - supported in 17.3.6
- Cisco Catalyst 9120AXE Access Points (VID 06 or earlier) - supported from 17.3.1 to 17.3.5
- Cisco Catalyst 9120AXE Access Points (VID 07 or earlier) - supported in 17.3.6
- Cisco Catalyst 9120AXP Access Points
- Cisco Catalyst 9130AXI Access Points (VID 03 or earlier) - supported in 17.3.6

  For information about Cisco Catalyst 9105, 9120, or 9130 Access Points support, see the Field Notice 72424.
- Cisco Catalyst 9130AXE Access Points

Outdoor Access Points

- Cisco Aironet 1542 Access Points
- Cisco Aironet 1560 Series Access Points
- Cisco Aironet 1570 Series Access Points
- Cisco Industrial Wireless 3700 Series Access Points
- Cisco Catalyst Industrial Wireless 6300 Heavy Duty Series Access Point
- Cisco 6300 Series Embedded Services Access Point
- Cisco Catalyst 9124AXI Access Points - supported from 17.3.4
- Cisco Catalyst 9124AXD Access Points - supported from 17.3.4
- Cisco Catalyst 9124AXE Access Points - supported from 17.3.5a

Integrated Access Points

- Integrated Access Point on Cisco 1100 ISR

Network Sensor

- Cisco Aironet 1800s Active Sensor

For information about Cisco Wireless software releases that support specific Cisco AP modules, see the "Software Release Support for Specific Access Point Modules" section in the *Cisco Wireless Solutions Software Compatibility Matrix* document.

Compatibility Matrix

The following table provides software compatibility information. For more information, see Cisco Wireless Solutions Software Compatibility Matrix

Table 4: Compatibility Informaton

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability	Cisco Catalyst Center	Cisco CMX
IOS XE 26.1.2	3.4 3.3 3.2 3.1 3.0 2.7 * all with latest patches	Not Available	8.10.196.0 8.10.190.0 8.10.185.0 8.10.183.0 8.10.182.0 8.10.181.0 8.10.171.0 8.10.162.0 8.10.151.0 8.10.142.0 8.10.130.0 8.5.176.2 8.5.182.104	See Cisco Catalyst Center Compatibility Information	11.1.1 11.1.0 11.0.1 11.0.0 10.6.3
IOS XE 26.1.1	3.4 3.3 3.2 3.1 3.0 2.7 * all with latest patches	Not Available	8.10.196.0 8.10.190.0 8.10.185.0 8.10.183.0 8.10.182.0 8.10.181.0 8.10.171.0 8.10.162.0 8.10.151.0 8.10.142.0 8.10.130.0 8.5.176.2 8.5.182.104	See Cisco Catalyst Center Compatibility Information	11.1.1 11.1.0 11.0.1 11.0.0 10.6.3

Table 5: Compatibility Information

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability	Cisco Catalyst Center	Cisco CMX
Amsterdam 17.2.1	2.7 2.6 2.4	3.8	8.10.171.0 8.10.162.0 8.10.122.0 8.10.121.0 8.10.113.0 8.10.112.0 8.10.105.0 8.9.111.0 8.9.100.0 8.8.125.0 8.8.120.0 8.8.111.0 8.5.164.0	See Cisco Catalyst Center Compatibility Information	10.6.2 10.6.0 10.5.1

GUI System Requirements

The following subsections list the hardware and software required to access the Cisco Catalyst 9800 Controller GUI.

Table 6: Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[1]	512 MB[2]	256	1280 x 800 or higher	Small

[1] We recommend 1 GHz.
[2] We recommend 1-GB DRAM.

Software Requirements

Operating Systems:

- Windows 7 or later

- Mac OS X 10.11 or later

Browsers:

- Google Chrome: Version 59 or later (on Windows and Mac)
- Microsoft Edge: Version 40 or later (on Windows)
- Safari: Version 10 or later (on Mac)
- Mozilla Firefox: Version 60 or later (on Windows and Mac)

Note Firefox Version 63.x is not supported.

Before You Upgrade

To ensure a smooth upgrade and prevent potential boot loop issues with APs, review these **Field Notice** and **technical documentation**. It is critical to complete these actions prior to initiating your upgrade.

1. FN74383: Field Notice
2. Validate and Recover Catalyst APs on 17.12

Other guidelines before you upgrade

Ensure that you familiarize yourself with the following points before proceeding with the upgrade:

- ERSPAN is not supported on the Cisco Catalyst 9800 Series Wireless Controller platform. Although the CLI allows you to enter **monitor session** commands for ERSPAN configuration, do not configure monitor session for ERSPAN on the controller. If an ERSPAN monitor session is configured, the configuration cannot be deleted from the controller.
- When you upgrade from Cisco IOS XE 17.9.5 or 17.12.2 to Cisco IOS XE 17.15.x, the controller WebUI does not support images greater than 1.5 GB.

  Workaround:

  - Upgrade using the CLI commands, or,
  - Upgrade to a fixed release first, and then upgrade to 17.15.x.

- When you upgrade from Cisco IOS XE Dublin 17.12.3 to 17.12.4 or Cisco IOS XE 17.15.1, the Cisco Catalyst Wi-Fi 6 and 6E APs fail to upgrade the AP image.

  Workaround:

  - Reboot the impacted APs through the power cycle.

  For more information, see CSCwm08044

Caution During controller upgrade or reboot, if route processor ports are connected to any Cisco switch, ensure that the route processor ports are not flapped (shut/no shut process). Otherwise, it may lead to a kernel crash.

- ISSU feature is supported only within and between major releases, for example, 17.3.x (within a release) and 17.3.x to 17.6.x (among major releases).
- Controller upgrade from Cisco IOS XE Bengaluru 17.3.x to Cisco IOS XE Bengaluru 17.6.x or Cisco IOS XE Cupertino 17.9.x or later using ISSU may fail if the **domain** command is configured. Ensure that you run the **no domain** command before starting an ISSU upgrade because the **domain** command has been removed from Cisco IOS XE Bengaluru 17.6.x.
- Controller upgrade from Cisco IOS XE Bengaluru 17.3.x to any release using ISSU may fail if the **snmp-server enable traps hsrp** command is configured. Ensure that you remove the **snmp-server enable traps hsrp** command from the configuration before starting an ISSU upgrade because the **snmp-server enable traps hsrp** command has been removed from Cisco IOS XE Bengaluru 17.4.x.
- Controller upgrade to Cisco IOS XE Dublin 17.12.x from any prior release using ISSU may fail if the **snmp-server enable traps license** command is configured. Ensure that you remove the **snmp-server enable traps license** command from the configuration before starting an ISSU upgrade because the **snmp-server enable traps license** command has been removed from Cisco IOS XE Dublin 17.12.x.
- Rolling AP upgrade, which is a part of the ISSU feature, is not supported for mesh APs.*ISSU feature is in Beta for this release.*
- Ensure that you add Authentication and Key Management (AKM) setting when you configure WPA3. In older releases, this scenario was not mandatory which resulted in an invalid configuration. However, from 17.9 and higher releases, this invalid scenario is detected and prevented.

Cisco Catalyst APs may enter a boot loop if you upgrade software versions earlier than 17.9.4 over a WAN link. For more information, see: https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/220443-how-to-avoid-boot-loop-due-to-corrupted.html.

The following Wave 1 APs are not supported from 17.4 to 17.9.2, 17.10.x, 17.11.x, 17.13.x, 17.14.x, and 17.15.x:

- **Cisco Aironet 1570 Series Access Point**
- **Cisco Aironet 1700 Series Access Point**
- **Cisco Aironet 2700 Series Access Point**
- **Cisco Aironet 3700 Series Access Point**

Note

- Support for the above APs was reintroduced from Cisco IOS XE Cupertino 17.9.3.
- Support for these APs does not extend beyond the normal product lifecycle support. Refer to the individual End-of-Support bulletins on Cisco.com.
- Feature support is on parity with the 17.3.x release. Features introduced in 17.4.1 or later are not supported on these APs in the 17.9.3 release.
- You can migrate directly to 17.9.3 from 17.3.x, where x=4c or later.

- From Cisco IOS XE Dublin 17.10.x, Key Exchange and MAC algorithms like diffie-hellman-group14-sha1, hmac-sha1, hmac-sha2-256, and hmac-sha2-512 are not supported by default and it may impact some SSH clients that only support these algorithms. If required, you can add them manually. For information on manually adding these algorithms, see the **SSH Algorithms for Common Criteria Certification** document available at: https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m_sec-secure-shell-algorithm-ccc.html
- If APs fail to detect the backup image after running the **archive download-sw** command, perform the following steps:

  1. Upload the image using the **no-reload** option of the **archive download-sw** command:

     ```
     Device# archive download-sw /no-reload tftp://<tftp_server_ip>/<image_name>
     ```

  2. Restart the CAPWAP process using **capwap ap restart** command. This allows the AP to use the correct backup image after the restart (reload is not required.)

     ```
     Device# capwap ap restart
     ```

Caution The AP will lose connection to the controller during the join process. When the AP joins the new controller, it will see a new image in the backup partition. So, the AP will not download a new image from the controller.

- Fragmentation lower than 1500 is not supported for the RADIUS packets generated by wireless clients in the Gi0 (OOB) interface.
- Cisco IOS XE allows you to encrypt all the passwords used on the device. This includes user passwords and SSID passwords (PSK). For more information, see the "Password Encryption" section of the Cisco Catalyst 9800 Series Configuration Best Practices document.
- While upgrading to Cisco IOS XE 17.3.x and later releases, if the **ip http active-session-modules none** command is enabled, you will not be able to access the controller GUI using HTTPS. To access the GUI using HTTPS, run the following commands in the order specified below:

  1. **ip http session-module-list pkilist OPENRESTY_PKI**
  2. **ip http active-session-modules pkilist**

- Cisco Aironet 1815T OfficeExtend Access Point will be in local mode when connected to the controller. However, when it functions as a standalone AP, it gets converted to FlexConnect mode.

- The Cisco Catalyst 9800-L Wireless Controller may fail to respond to the BREAK signals received on its console port during boot time, preventing users from getting to the ROMMON. This problem is observed on the controllers manufactured until November 2019, with the default config-register setting of 0x2102. This problem can be avoided if you set config-register to 0x2002. This problem is fixed in the 16.12(3r) ROMMON for Cisco Catalyst 9800-L Wireless Controller. For information about how to upgrade the ROMMON, see the Upgrading ROMMON for Cisco Catalyst 9800-L Wireless Controllers section of the Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers document.
- By default, the controller uses a TFTP block size value of 512, which is the lowest possible value. This default setting is used to ensure interoperability with legacy TFTP servers. If required, you can change the block size value to 8192 to speed up the transfer process, using the **ip tftp blocksize** command in global configuration mode.
- We recommend that you configure the **password encryption aes** and the **key config-key password-encrypt** *key* commands to encrypt your password.
- If the following error message is displayed after a reboot or system crash, we recommend that you regenerate the trustpoint certificate:

  ```
  ERR_SSL_VERSION_OR_CIPHER_MISMATCH
  ```

  Use the following commands in the order specified below to generate a new self-signed trustpoint certificate:

  1. device# **configure terminal**
  2. device(config)# **no crypto pki trustpoint** *trustpoint_name*
  3. device(config)# **no ip http server**
  4. device(config)# **no ip http secure-server**
  5. device(config)# **ip http server**
  6. device(config)# **ip http secure-server**
  7. device(config)# **ip http authentication** *local/aaa*

- Do not deploy OVA files directly to VMware ESXi 6.5. We recommend that you use an OVF tool to deploy the OVA files.
- Ensure that you remove the controller from Cisco Prime Infrastructure before disabling or enabling Netconf-YANG. Otherwise, the system may reload unexpectedly.
- Unidirectional Link Detection (UDLD) protocol is not supported.
- SIP media session snooping is not supported on FlexConnect local switching deployments.
- The Cisco Catalyst 9800 Series Wireless Controllers (C9800-CL, C9800-L, C9800-40, and C9800-80) support a maximum of 14,000 leases with internal DHCP scope.
- Configuring the mobility MAC address using the **wireless mobility mac-address** command is mandatory for both HA and 802.11r.
- If you have Cisco Catalyst 9120 (E/I/P) and Cisco Catalyst 9130 (E) APs in your network and you want to downgrade, use only Cisco IOS XE Gibraltar 16.12.1t. Do not downgrade to Cisco IOS XE Gibraltar 16.12.1s.

- The following SNMP variables are not supported:
  - CISCO-LWAPP-WLAN-MIB: cLWlanMdnsMode
  - CISCO-LWAPP-AP-MIB.my: cLApDot11IfRptncPresent, cLApDot11IfDartPresent
- If you are upgrading from Cisco IOS XE Gibraltar 16.11.x or an earlier release, ensure that you unconfigure the *advipservices* boot-level licenses on both the active and standby controllers using the **no license boot level advipservices** command before the upgrade. Note that the **license boot level advipservices** command is not available in Cisco IOS XE Gibraltar 16.12.1s and 16.12.2s.
- The Cisco Catalyst 9800 Series Wireless Controller has a service port that is referred to as *GigabitEthernet 0* port.

  The following protocols and features are supported through this port:
  - Cisco Catalyst Center
  - Cisco Smart Software Manager
  - Cisco Prime Infrastructure
  - Telnet
  - Controller GUI
  - HTTP
  - HTTPS
  - Licensing for Smart Licensing feature to communicate with CSSM
  - SSH
- During device upgrade using GUI, if a switchover occurs, the session expires and the upgrade process gets terminated. As a result, the GUI cannot display the upgrade state or status.
- From Cisco IOS XE Bengaluru 17.4.1 onwards, the telemetry solution provides a name for the receiver address instead of the IP address for telemetry data. This is an additional option. During the controller downgrade and subsequent upgrade, there is likely to be an issue—the upgrade version uses the newly named receivers, and these are not recognized in the downgrade. The new configuration gets rejected and fails in the subsequent upgrade. Configuration loss can be avoided when the upgrade or downgrade is performed from Cisco Catalyst Center.
- Communication between Cisco Catalyst 9800 Series Wireless Controller and Cisco Prime Infrastructure uses different ports:
  - All the configurations and templates available in Cisco Prime Infrastructure are pushed through SNMP and CLI, using UDP port 161.
  - Operational data for controller is obtained over SNMP, using UDP port 162.
  - AP and client operational data leverage streaming telemetry:
    - Cisco Prime Infrastructure to controller: TCP port 830 is used by Cisco Prime Infrastructure to push the telemetry configuration to the controller (using NETCONF).
    - Controller to Cisco Prime Infrastructure: TCP port 20828 is used for Cisco IOS XE 16.10.x and 16.11.x, and TCP port 20830 is used for Cisco IOS XE 16.12.x, 17.1.x and later releases.

- To migrate public IP address from 16.12.x to 17.x. ensure that you configure the **service internal** command. If you do not configure the **service internal** command, the IP address does not get carried forward.
- RLAN support with Virtual Routing and Forwarding (VRF) is not available.
- When you encounter the SNMP error *SNMP_ERRORSTATUS_NOACCESS 6*, it means that the specified SNMP variable is not accessible.
- We recommend that you perform a controller reload whenever there is a change in the controller's clock time to reflect an earlier time.

Note The DTLS version (DTLSv1.0) is deprecated for Cisco Aironet 1800 based on latest security policies. Therefore, any new out-of-box deployments of Cisco Aironet 1800 APs will fail to join the controller and you will get the following error message:

```
%APMGR_TRACE_MESSAGE-3-WLC_GEN_ERR: Chassis 1 R0/2: wncd: Error in AP Join, AP <AP-name>,
mac:<MAC-address>Model AIR-AP1815W-D-K9, AP negotiated unexpected DTLS version v1.0
```

To onboard new Cisco Aironet 1800 APs and to establish a CAPWAP connection, explicitly set the DTLS version to 1.0 in the controller using the following configuration:

```
config terminal
ap dtls-version dtls_1_0
end
```

Note that setting the DTLS version to 1.0 affects all the existing AP CAPWAP connections. We recommend that you apply the configuration only during a maintenance window. After the APs download the new image and join the controller, ensure that you remove the configuration.

To upgrade the field programmable hardware devices for Cisco Catalyst 9800 Series Wireless Controllers, see *Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers*.

Important Before you begin a downgrade process, you must manually remove the configurations which are applicable in the current version but not in older version. Otherwise, you might encounter an unexpected behavior.

Upgrading the Controller Software

This section describes the various aspects of upgrading the controller software.

Finding the Software Version

The package files for the Cisco IOS XE software are stored in the system board flash device (flash:).

Use the **show version** privileged EXEC command to see the software version that is running on your controller.

Note Although the **show version** output always shows the software image running on the controller, the model name shown at the end of the output is the factory configuration, and does not change if you upgrade the software license.

Use the **show install summary** privileged EXEC command to see the information about the active package.

Use the **dir** *filesystem:* privileged EXEC command to see the directory names of other software images that you have stored in flash memory.

Software Images

- **Release**: Cisco IOS XE Amsterdam 17.2.x
- **Image**: Universal
- **File Name**: C9800-universalk9_wlc.17.2.x.SPA.bin

Software Installation Commands

Cisco IOS XE Amsterdam 17.2.x	
To install and activate a specified file, and to commit changes to be persistent across reloads, run the following command: **device# install add file** *filename* **[activate |commit]** To separately install, activate, commit, end, or remove the installation file, run the following command: **device# install ?** **Note** We recommend that you use the GUI for installation.	
add file tftp: *filename*	Copies the install file package from a remote location to a device, and performs a compatibility check for the platform and image versions.
activateauto-abort-timer]	Activates the file and reloads the device. The **auto-abort-timer** keyword automatically rolls back image activation.
commit	Makes changes that are persistent over reloads.
rollback to committed	Rolls back the update to the last committed version.
abort	Cancels file activation, and rolls back to the version that was running before the current installation procedure started.
remove	Deletes all unused and inactive software installation files.

Licensing

This section provides information about the licensing packages for the features that are available in the Cisco Catalyst 9800 Series Wireless Controller.

The software features that are available on the controller fall under these license categories:

- AIR DNA Essentials (AIR-DNA-E)
- AIR DNA Advantage (AIR-DNA-A) (Includes the features that are available with the Cisco DNA Essentials license and more.)

Note The controller starts with *AIR-DNA-A* as the default. Any change in the license level requires a reboot.

Note After adding new license in the Cisco Smart Software Manager (CSSM) for customer virtual account, run the **license smart renew auth** command on the controller to get the license status changed from Out OF Compliance to Authorized.

Base Licenses

Base licenses are perpetual licenses and can be used even after the expiry of *Air-DNA-A* and *AIR-DNA-E*. Base licenses include:

- AIR Network Essentials (AIR-NE)
- AIR Network Advantage (AIR-NA) (Includes the features that are available in the Network Essentials license.)

License Term

The licenses are available for a three, five, or seven-year periods.

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide.

Issues

Issues describe unexpected behavior in Cisco IOS releases in a product. Issues that are listed as Open in a prior release are carried forward to the next release as either Open or Resolved.

Note All incremental releases contain fixes from the current release.

Cisco Bug Search Tool

The Cisco Bug Search Tool (BST) allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The BST is designed to improve the effectiveness in network risk management and device troubleshooting. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of an issue, click the corresponding identifier.

Open Caveats for Cisco IOS XE Amsterdam 17.2.1a

Caveat ID	Description
CSCvu00121	Cisco Aironet AP 185x/184x reboots by deadlock triggered kernel panic in radio driver code.

Open Caveats for Cisco IOS XE Amsterdam 17.2.1

Caveat ID	Description
CSCvm75074	Correct the severity level of logs generated by smart-agent from notice to debug.
CSCvt01659	Client traffic is stuck, after controller receives the Change of Authorization (CoA) as part of Local Web Authentication (LWA) and Central Web Authentication (CWA).
CSCvt11877	Random switchovers are observed on the Cisco Catalyst 9800 Wireless Controller for Cloud in HA mode.
CSCvt19736	11ax feature is automatically enabled after upgrading from Cisco IOS XE 16.12.2s to Cisco IOS XE 17.1.1s.
CSCvt29596	Current Tx rate for 802.11ax clients are displayed incorrectly on the controller.
CSCvt35141	Deny webauth WLANs from being tagged to authentication servers that has load balancing enabled.
CSCvt35766	Controller is allowing WPA-TKIP + WPA2, without any encryption.
CSCvt37835	Client is unable to associate when extended supported rates are used.
CSCvt41035	AP 360 view is not showing client count, ch/tx/rx utilization for 2.4 GHz, but shows for 5 GHz.
CSCvt41053	AP shows incorrect WLAN to VLAN assignment.
CSCvt41519	Controller reloads unexpectedly when an AP with same name of an existing AP joins.
CSCvt42261	Cisco DNA Centre Swim upgrade failed.

Caveat ID	Description
CSCvt46733	Cisco Catalyst 9800 Series Wireless Controller Address Resolution Protocol (ARP) handling design change.
CSCvt47787	Roaming is not successful when NAC is enabled in the policy profile.
CSCvt48319	Remove all client lists from the **show tech wireless** command output.
CSCvt49983	The **show ap auto RF** command output is displaying invalid values for some APs.
CSCvt52436	Controller is unable to downgrade license.
CSCvt55482	Controller displays incorrect number of interferers.
CSCvt57421	Cisco Aironet 4800 AP is underpowered when USB is disabled.

Resolved Caveats for Cisco IOS XE Amsterdam 17.2.1a

Caveat ID	Description
CSCvt47413	IW-6300H/1562/2800/3800/4800 series APs are failing DFS compliance
CSCvt98797	Channel Availability Check (CAC) is skipped after channel change on 2800/3800/4800/1560/IW6300
CSCvu02495	Wave 2 AP boot failure with message saying bad lzma header and AP unable to boot and join controller.

Resolved Caveats for Cisco IOS XE Amsterdam 17.2.1

Caveat ID	Description
CSCvk79909	Remove all standby R0 commands from the **show tech wireless** command output.
CSCvq66798	External web authentication log out page is not working.
CSCvq68047	OpenDNS resolver IPs are not coming with NETCONF/RESTCONF with defaults.
CSCvq70386	The **show hw-module subslot 0/1 transceiver 0 idprom brief** command failed to show any output.
CSCvq80854	Simplify WLAN configuration for Layer 2 and Layer 3 security options.
CSCvr09334	The **show ap auto-rf dot11 24ghz** command output is not displaying entries of Cisco Aironet 4800 AP, after a day.

Caveat ID	Description
CSCvr13531	Core files under standby bootflash is shown twice on the web UI.
CSCvr24930	Controller is displaying *wncd crash@ewlc_dgram_msg_and_msgbuf_free* message with In-Service Software Upgrade (ISSU) flow in scale.
CSCvr26579	Controller deauthenticates client when receiving DHCP release from the client.
CSCvr44175	System displays memory warning during controller image download.
CSCvr45109	Traceback is observed on the standby controller while unconfiguring port-channel.
CSCvr52588	QoS police configuration is deleted after adding or removing it to policy profile using web UI.
CSCvr70395	Controller is sending delete event for AP impersonation.
CSCvr71770	Wired multicast Domain Name System (mDNS) packet is getting punted to WNCD.
CSCvr84336	Client is stuck in IP learn state with flex mode AP.
CSCvr91736	Web UI is not displaying slot-2 details in 360 degree view.
CSCvr96040	NETCONF/RESTCONF server is not reachable after a switchover.
CSCvs01799	Stack_mgr process logs only the internal btrace logs.
CSCvs03191	Controller is unable to scale above 3000 new allowed list users with multiple WLANs using bulk import.
CSCvs15446	Cisco Catalyst 9800-L Wireless Controller HA: Traceback is observed after reload.
CSCvs17412	Backhaul configuration for PSK is showing error as resource not found.
CSCvs20264	Off-channel interference is not being reported.
CSCvs21105	Update & Apply to Device button is not working after configuring FT-PSK with WPA2+WPA3 in web UI.
CSCvs31054	Btman core has been observed.
CSCvs34222	Print a warning message during packet (SWPortMacConflict) drop.
CSCvs45249	Unable to enter a valid URL for urlfilter.
CSCvs60927	Frequent AP channel changes are observed on the 5GHz band radio.
CSCvs63467	IPv6 dual stack is not working.

Caveat ID	Description
CSCvs72078	Client retries and Rx packets on Cisco DNA Centre is different from the value seen on the AP.
CSCvs72524	Though dynamic channel allocation (DCA) is set to be OFF, it is still assigning channels to AP radios.
CSCvt13127	Controller is not able to display medium power when AP sends 25W message.
CSCvt16139	Controller is not sending redirect URL if client is already trying to authenticate.
CSCvt31798	Controller running Cisco IOS XE Gibraltar 16.12.3 software is not sending RSSI messages over NMSP.
CSCvt55181	Unable to configure SNMP settings using GUI in Japanese mode.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see Troubleshooting TechNotes.

Related Documentation

- Information about Cisco IOS XE
- Cisco Validated Design documents
- MIB Locator to locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets

Cisco Wireless Controller

For more information about the Cisco wireless controller, lightweight APs, and mesh APs, see these documents:

- Cisco Wireless Solutions Software Compatibility Matrix
- Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide
- Cisco Catalyst 9800 Series Wireless Controller Command Reference
- Cisco Catalyst 9800 Series Configuration Best Practices
- In-Service Software Upgrade Matrix
- Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers

The installation guide for your controller is available at:

- Hardware Installation Guides

All Cisco Wireless Controller software-related documentation

Cisco Wireless Access Points Detailed Channels and Maximum Power Settings

For detailed channels and maximum power settings for Cisco Wireless indoor and outdoor APs, and country support per release, see:

Detailed Channels and Maximum Power Settings Document for Supported Access Points

Feature Matrix for Cisco Wireless Access Points

Feature Matrix for Cisco Wireless Access Points

Cisco Catalyst 9800 Series Wireless Controller Data Sheets

- *Cisco Catalyst 9800-CL Wireless Controller for Cloud Data Sheet*
- *Cisco Catalyst 9800-80 Wireless Controller Data Sheet*
- *Cisco Catalyst 9800-40 Wireless Controller Data Sheet*
- *Cisco Catalyst 9800-L Wireless Controller Data Sheet*

Cisco Embedded Wireless Controller on Catalyst Access Points

For more information about the Cisco Embedded Wireless Controller on Catalyst Access Points, see:

https://www.cisco.com/c/en/us/support/wireless/embedded-wireless-controller-catalyst-access-points/tsd-products-support-series-home.html

Wireless Product Comparison

- Compare specifications of Cisco wireless APs and controllers
- Wireless LAN Compliance Lookup
- Cisco AireOS to Cisco Catalyst 9800 Wireless Controller Feature Comparison Matrix

Cisco Access Points–Statement of Volatility

The STATEMENT OF VOLATILITY is an engineering document that provides information about the device, the location of its memory components, and the methods for clearing device memory. Refer to the data security policies and practices of your organization and take the necessary steps required to protect your devices or network environment.

The Cisco Aironet and Catalyst AP Statement of Volatility (SoV) documents are available on the Cisco Trust Portal.

You can search by the AP model to view the SoV document.

Cisco Prime Infrastructure

Cisco Prime Infrastructure Documentation

Cisco Connected Mobile Experiences

Cisco Connected Mobile Experiences Documentation

Cisco Catalyst Center

Cisco Catalyst Center Documentation

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results 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 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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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)

© 2020 Cisco Systems, Inc. All rights reserved.