Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Amsterdam 17.1.x

First Published: 2020-02-22

Last Modified: 2020-06-19

Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Amsterdam 17.1.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 Catalyst 9800 Series Wireless Controllers are Cisco IOS XE based 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 Catalyst 9800 controllers are enterprise ready to power your business-critical operations and transform end-customer experiences:

- The controllers come with high availability (HA) 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 or a Cisco Catalyst access point (AP).
- The controllers can be managed using Cisco Digital Network Architecture (DNA) 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 Catalyst 9800 Series 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 of the Cisco IOS-XE programmability-related topics on the Cisco Catalyst 9800 controllers are supported by DevNet, either through community-based support or through DevNet developer support. For more information, go to https://developer.cisco.com.

What's New in Cisco IOS XE Amsterdam 17.1.1t

There are no new features or enhancements in this release.

What's New in Cisco IOS XE Amsterdam 17.1.1s

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

Accounting of AP Events: The RADIUS server to monitor the network with respect to access points. If an access point goes down and then comes up, the RADIUS server keeps a record of all the APs that were down and have come up. For more information, see the Accounting of AP Events chapter.

Adaptive WIPS: The Cisco Adaptive Wireless Intrusion Prevention System (aWIPS) feature is a wireless intrusion threat detection and mitigation mechanism. aWIPS uses an advanced approach to wireless threat detection and performance management. The AP detects the threats and generates alarms. It combines network traffic analysis, network device and topology information, signature-based techniques, and anomaly detection to deliver highly accurate and complete wireless threat prevention. For more information, see the Adaptive WIPS chapter.

Advance mDNS Policy Support: Using this feature, you can configure the local or native profile for an mDNS policy from service-template or an mDNS service policy for a specific VLAN. For more information, see the Multicast Domain Name System (mDNS) chapter.

Basic Service Set Coloring: BSS Coloring is a new provision that allows devices operating in the same frequency space to quickly distinguish between packets from their own BSS and packets from an Overlapping BSS (OBSS). For more information, see the BSS Coloring chapter.

Clean Air - Persistent Device Avoidance: Persistent device avoidance feature is a part of spectrum management. Some interference devices such as outdoor bridges and microwave ovens transmit signals only when required. These devices can cause significant interference to the local WLAN. CleanAir detects and stores persistent device information in the controller. This information is used to mitigate interfering channels. For more information, see the Persistent Device Avoidance chapter.

Device Ecosystem Analytics: The Device Ecosystem Analytics feature enhances the enterprise Wi-Fi experience for client devices by providing a set of data analytics tools for analysing wireless client device behaviour. With device profiling enabled on the controller, information is exchanged between the client device and the controller and AP. This data is encrypted using AES-256-CBC to ensure device security. This is applicable for Cisco device ecosystem partners only. For more information, see the Device Ecosystem chapter.

DHCP Server Response Time: The DHCP Server Response Time feature measures the round trip time (RTT) for every DHCP server transaction, in order to realize the server response time and the DHCP-server connectivity latency.

Express Wi-Fi by Facebook: Express Wi-Fi by Facebook is a cloud-based, low-cost solution for local entrepreneurs and SMBs in emerging countries to provide Wi-Fi access. Using Express Wi-Fi by Facebook, users can buy data packs and find nearby hotspots. The Express Wi-Fi by Facebook feature is enabled through

a FlexConnect deployment based on the cloud-hosted controller where the Cisco AP performs client-related functions such as web authentication, captive portal redirect, matching and accounting of traffic classes and connection to the RADIUS server. For more information, see the Express Wi-Fi by Facebook chapter.

FastLocate for Cisco Catalyst Series Access Points: The FastLocate feature enables higher location refresh rates by collecting RSSI or location information through data packets received by the APs. Using these data packets, location-based services (LBS) updates are initiated by the network and are available more frequently. For more information, see the FastLocate for Cisco Catalyst Series Access Points chapter.

iPSK Peer-2-Peer Blocking: The iPSK P2P feature provides the functionality of blocking the peer to peer traffic, if any two peers (clients) do not share the same iPSK keys on a WLAN. For more information, see the **Configuring Advanced WLAN Properties** section in WLANs chapter.

IPv6 Support for Encrypted Traffic Analytics: Starting with this release, Encrypted Traffic Analytics (ETA) inspection for IPv6 traffic is supported. This release also supports other options like using allowed list of traffic, exporting ETA records, exporting records over IPFIX (netflow v10), and so on. For more information, see the Encrypted Traffic Analytics chapter.

IPv6 Local Authentication: Starting with this release, IPv6 is supported on the Flex APs in local authentication mode.

IPv6 Router Advertisement Forwarding for a Wired Guest: Using this feature, wired guest clients get IPv6 connectivity from the IPv6 Router Advertisement(RA) message sent by the IPv6 router. See the Wired Guest Access chapter.

IPv6: Flexible NetFlow: Starting with this release, IPv6 flow monitor is supported on Wave 2 APs. You can attach two flow monitors in a policy profile per direction (input and output) and per IP version (IPv4 and IPv6) in local (central switching) mode, when NBAR runs in the controller. However, only one flow monitor is supported per direction (input and output) and per IP version (IPv4 and IPv6) in flexconnect and fabric modes on Wave 2 APs, when NBAR runs on the corresponding AP. For more information, see Application Visibility and Control chapter.

In-Service Software Upgrade: In-Service Software Upgrade (ISSU) is a process that upgrades an image to another image on a device while the network continues to forward packets. ISSU helps network administrators avoid a network outage when performing a software upgrade. For more information, see the In-Service Software Upgrade chapter.

Attention ISSU feature is in beta test program. It 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). For feedback and support, contact c9800-issu-support@external.cisco.com.

Link Aggregation Control Protocol: Link Aggregation Control Protocol (LACP) is part of an IEEE specification (802.3ad) that allows you to bundle several physical ports together to form a single logical channel. For more information, see LACP chapter.

Mesh and Flex + Mesh support on 80.211ac Wave 2 Indoor APs: Starting from this release, the Mesh feature is supported on the following APs: 4800, 3800, 2800, 1850, 1830, 1815I, 1815W and 1800I.

Microsoft Hyper-V Support for Catalyst 9800-CL Wireless Controller: Starting with this release, you can install Catalyst 9800 Cloud Wireless Controller in a Microsoft Hyper-V environment. For more information, see Installing the Controller in Microsoft Hyper-V Hypervisor chapter.

mDNS Gateway with Guest Anchor Support and mDNS Bridging: When mDNS gateway is enabled, client requests on the guest LAN or WLAN are responded at the guest anchor or guest foreign. See the mDNS Gateway with Guest Anchor Support and mDNS Bridging section.

Multi-auth Support for Guest Clients: This feature is an enhancement to the existing feature where the guest clients can authenticate to the guest network using the additional authentication protocols. See the Wireless Guest Access chapter.

Network Address Translation for Mobility Groups: The Network Address Translation for Mobility Groups feature supports the establishment of mobility tunnels between peer controllers when one or both peers are behind a NAT. For more information, see NAT Support on Mobility Groups chapter.

OpenDNS Integration: Starting with this release, Cisco Umbrella in Flex-mode supports multiple profiles. For more information, see the Cisco Umbrella chapter.

Port Aggregation Protocol: Port aggregation protocol (PAgP) is a Cisco-proprietary protocol that you can run on the controllers to support PAgP. PAgP facilitates the automatic creation of EtherChannels by exchanging PAgP packets between Ethernet ports. For more information, see PAgP chapter.

Policy Enforcement and Usage Monitoring: The Policy Enforcement and Usage Monitoring feature enforces dynamic QoS policies and upstream and downstream TCP or UDP data rates on 802.11 clients seamlessly. This feature ensures that clients do not have to get dissociated from the network. Various authentication methods like 802.1X, PSK, and web authentication are supported. For more information, see the Policy Enforcement and Usage Monitoring chapter.

Redundant Management Interface: The Redundancy Management Interface (RMI) is used as a secondary link between the active and standby controllers. This interface is the same as the Wireless Management Interface and the IP address on this interface is configured in the same subnet as the Wireless Management Interface. For more information, see the Redundancy Management Interface (RMI) chapter.

SFTP and SCP Support on Cisco Aironet Wave 2 and Catalyst Series Access Points: Secure Copy Protocol (SCP) and SSH File Transfer Protocol (SFTP) provide a secure and authenticated method for uploading core files from the AP to an external server. The SFTP procedures can be invoked using the **copy** command, which is similar to that of SCP and TFTP. For more information, see the Configuring Secure Shell chapter.

Support for IPv6 in Cisco Hyperlocation or BLE Configuration: IPv6 is supported in Cisco Hyperlocation or BLE configuration from this release. For more information, see Cisco Hyperlocation chapter.

TLS 1.2 support for EAP-FAST: Starting from this release, TLS 1.2 is supported in EAP-FAST authentication protocol when the controller performs local eap authentication. For more information, see 802.1x Support chapter.

UDP Lite support: The UDP Lite support feature is an enhancement to the existing IPv6 functionality to support the UDP Lite protocol. For more information, see the IPv6 CAPWAP UDP Lite Support chapter.

VLAN Override Post IP Learn (Guest & non-Guest): You can enable the VLAN Override feature using the AAA override configuration in Policy Profile. For more information, see WLAN Security chapter.

WebUI Enhancements: Using the web UI and CLIs, you can now sort WLAN summary in ascending or descending order based on the client count and data usage. Similarly, you can also sort AP summary in ascending or descending order based on the client count, data usage, and throughput. The following commands are introduced:

- **show wlan summary sort** { **ascending** | **descending** } { **client-count** | **data-usage** }
- **show ap summary sort** { **ascending** | **descending** } { **client-count** | **data-usage** | **throughput** }
- **clear wlan sort statistics**
- **clear ap sort statistics**

For more information on these commands, see the Cisco Catalyst 9800 Series Wireless Controller Command Reference, Cisco IOS XE Amsterdam 17.1.1s.

Webauth Sleeping Client Support: The web authentication sleeping clients feature supports multiple combinations of authentications for a given client, which are configured on the WLAN profile. For more information, see the Cisco Umbrella chapter.

Support for Cisco Industrial Wireless 3702 Access Point: Starting with this release, IW3702 AP is supported.

For more information about Cisco Industrial Wireless 3702 AP, see https://www.cisco.com/c/en/us/products/wireless/industrial-wireless-3700-series/index.html

Support for Cisco Catalyst Industrial Wireless 6300 Heavy Duty Series Access Point: Starting with this release, IW6300 AP is supported in local mode. This AP is not supported in bridge mode.

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 9130 Access Points :

Extending Cisco's intent-based network and perfect for networks of all sizes, the Cisco Catalyst 9130 Series scales to meet the growing demands of IoT while fully supporting the latest innovations and new technologies. The Cisco Catalyst 9130 Series is also a leader in performance, security, and analytics.

For more information about Cisco Catalyst 9130 APs, see: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/nb-06-cat-9130-ser-ap-ds-cte-en.html

Unsupported SFPs:

From this release, only supported SFPs will work. If you use a nonsupported SFP, the port will not function.

Behavior Change

- **FQDN URL Filtering Support:** Until Cisco IOS XE Gibraltar 16.12.x, the URL filter could be added by referencing the default ACL in the flex profile. From Cisco IOS XE Gibraltar 17.1.1 onwards, you can no longer reference the default ACL as it is prevented using a validation rule.
- From this release, a new gateway reachability check is introduced. The APs send periodic ICMP echo requests (ping) to the default gateway to check for connectivity. You need to ensure traffic filtering between the APs and the default gateway (like ACLs) allow ICMP pings between the AP and the default gateway. If these pings are blocked, even if the connectivity between the controller and the AP is active, the APs will reload at 4 hours interval.
- **Client Debug Bundle:** If embedded packet capture (EPC) is already enabled and is active from a different source, debug bundle with EPC cannot be started. To use EPC with debug bundle, stop EPC (enabled from a different source) and restart it with debug bundle.

Important Notes

- The Cisco Catalyst 9800-L Wireless Controller may fail to respond to BREAK signals received on its console port during boot time preventing the user from getting to the ROMMON. This problem is observed on the controllers manufactured till November 2019, with the default config-register setting of 0x2102. This problem can be avoided if you set the config-register to 0x2002. This problem is fixed in the 16.12(3r) ROMMON for Cisco Catalyst 9800-L Wireless Controller. For steps on how to upgrade the ROMMON,

see the *Upgrading ROMMON for Cisco Catalyst 9800-L Wireless Controllers* section of Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers.

- 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. However, you can manually change the block size value to 8192 K using the **ip tftp blocksize** command in global configuration mode to speed up the transfer process.
- We recommend that you configure the **password encryption aes** and the **key config-key password-encrypt** *key* commands to encrypt your password.
- The features and functions that work on IPv4 networks with IPv4 addresses also works on IPv6 networks with IPv6 addresses. For a list of unsupported features, see the Unsupported Features section of the *Native IPv6* feature.
- If you encounter ERR_SSL_VERSION_OR_CIPHER_MISMATCH error from the GUI after a reboot or system crash, we recommend that you regenerate the trustpoint certificate.

  The procedure to generate a new self signed trustpoint is as follows:

```
configure terminal
no crypto pki trustpoint <trustpoint_name>
no ip http server
no ip http secure-server
ip http server
ip http secure-server
ip http authentication <local/aaa>
! use local or aaa as applicable.
```

- You cannot mix open configuration models with CLI-based, GUI-based, or DNA Center-based configurations. However, if you decide to use multiple model types, they must remain independent of each other. For example, in open configuration models, you can only manage configurations that have been created using an open configuration model, not a CLI-based or GUI-based model. Configurations that are created using open configuration models cannot be modified using a GUI-based model, or CLI-based model, or any other model.
- SNMPv3 user configuration is not reflected in the running configuration. Only SNMPv3 group configuration is visible.
- The Cisco Catalyst 9800 Series Wireless Controller has a service port, which is referred to as *GigabitEthernet 0* port. You cannot use this port for RADIUS, SNMP, DNAC Telemetry, and other communications.

  The service port only supports the following IP protocols:

  - HTTP
  - HTTPS
  - SSH
  - Licensing for Smart Licensing feature to communicate with CSSM

- Cisco Prime Infrastructure release version 3.8 does not support Cisco Catalyst Wireless Controller versions 16.12 and 17.1
- To migrate public IP address from 16.12.x to 17.x. ensure that you configure the **service internal** command. Failing to do so will not carry forward the IP address.

Supported Hardware

The following table lists the supported virtual and hardware platforms. (See Table 3: Supported PIDs and Ports, on page 8 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.
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

Host Environment	Software Version
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.
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

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
	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

Controller Model	Description
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
	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
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
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 - supports only local mode
- 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

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.

Table 4: Compatibility Information

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco CMX	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability	Cisco DNA Center
Amsterdam 17.1.1s	2.7 2.6 2.4	10.6.2 10.6 10.5.1	3.7.1	8.10.171.0 8.10.162.0 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 DNA Center Compatibility Information

GUI System Requirements

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

Table 5: 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.

The controller GUI uses Virtual Terminal (VTY) lines for processing HTTP requests. At times, when multiple connections are open, the default number of VTY lines of 15 set by the device might get exhausted. Therefore, we recommendthat you increase the number of VTY lines to 50.

To increase the VTY lines in a device, run the following commands in the following order:

1. **device#** configure terminal
2. **device(config)#** line vty 50

   A best practice is to configure the service tcp-keepalives to monitor the TCP connection to the device.
3. **device(config)#** service tcp-keepalives-in
4. **device(config)#** service tcp-keepalives-out

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 17.1.x
- **Image**: Universal
- **File Name**: C9800-universalk9_wlc.17.1.x.SPA.bin

Software Installation Commands

Cisco IOS XE Amsterdam 17.1.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.

Guidelines and Restrictions

Software

- Do not use more than 31 characters for AP names. If the AP name is 32 characters or more, it may lead to a controller crash.
- Do not deploy OVA files directly to VMware ESXi 6.5. We recommend that you use an OVF tool to deploy the OVA files.
- Firefox Version 63.x is not supported.
- Ensure that you remove the controller from Cisco Prime 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.
- Rolling AP upgrade that is part of ISSU feature is not supported for Mesh APs.*ISSU feature is in Beta for this release.*
- 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 mobility MAC address (**wireless mobility mac-address**) is mandatory for both High-Availability and 802.11r.
- When you configure the Cisco Catalyst 9800 Series Wireless controllers with Cisco Aironet 3700 Series Access Points, through IPv6, and then connect IPv6 capable clients, the IP addresses of all the IPv6 clients are not updated on the controller.
- **Behavior Change in WLAN Mapping to default-policy-profile**: From Cisco IOS XE Gibraltar 16.12.2s onwards, automatic WLAN mapping to the default policy profile under the default policy tag has been removed. If you are upgrading from a release earlier than Cisco IOS XE Gibraltar 16.12.2s, and if your wireless network uses default policy tag, it will go down due to the default mapping change. To restore the network operation, add the required WLAN to policy mappings under the default policy tag.
- If you have Cisco Catalyst 9120E/I/P and Cisco Catalyst 9130E APs in your network and you want downgrade to an earlier version, we recommend that you use only Cisco IOS XE Gibraltar 16.12.1t. Do not downgrade to Cisco IOS XE Gibraltar 16.12.1s.
- If you are upgrading from Cisco IOS XE Gibraltar 16.12.2 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 this command is not available on the Cisco Catalyst 9800 Wireless Controller for Cloud (9800-CL).

Interoperability with Clients

This section describes the interoperability of the controller software with client devices.

The following table lists the configurations used for testing client devices.

Table 6: Test Configuration for Interoperability

Hardware or Software Parameter	Hardware or Software Type
Release	Cisco IOS XE Amsterdam 17.1.x
Cisco Wireless Controller	See Supported Hardware, on page 7.
Access Points	See Supported APs, on page 11.
Radio	• 802.11ax • 802.11ac • 802.11a • 802.11g • 802.11n
Security	Open, PSK (WPA2-AES), 802.1X (WPA2-AES) (EAP-FAST, EAP-TLS) 802.11ax
RADIUS	See Compatibility Matrix, on page 13
Types of tests	Connectivity, traffic (ICMP), and roaming between two APs

The following table lists the client types on which the tests were conducted. Client types included laptops, hand-held devices, phones, and printers.

Table 7: Client Types

Client Type and Name	Driver or Software Version
Wi-Fi 6 Devices (Mobile Phone and Laptop)	
Apple iPhone 11	iOS 14.1
Apple iPhone SE 2020	iOS 14.1
Dell Intel AX1650w	Windows 10 (21.90.2.1)
Dell Latitude 5491 (Intel AX200)	Windows 10 Pro (21.40.2)
Samsung S20	Android 10
Samsung S10 (SM-G973U1)	Android 9.0 (One UI 1.1)
Samsung S10e (SM-G970U1)	Android 9.0 (One UI 1.1)
Samsung Galaxy S10+	Android 9.0
Samsung Galaxy Fold 2	Android 10
Samsung Galaxy Flip Z	Android 10
Samsung Note 20	Android 10
Laptops	
Acer Aspire E 15 E5-573-3870 (Qualcomm Atheros QCA9377)	Windows 10 Pro (12.0.0.832)
Apple Macbook Air 11 inch	OS Sierra 10.12.6
Apple Macbook Air 13 inch	OS Catalina 10.15.4
Apple Macbook Air 13 inch	OS High Sierra 10.13.4
Macbook Pro Retina	OS Mojave 10.14.3
Macbook Pro Retina 13 inch early 2015	OS Mojave 10.14.3
Dell Inspiron 2020 Chromebook	Chrome OS 75.0.3770.129
Google Pixelbook Go	Chrome OS 84.0.4147.136
HP chromebook 11a	Chrome OS 76.0.3809.136
Samsung Chromebook 4+	Chrome OS 77.0.3865.105
Dell Latitude 3480 (Qualcomm DELL wireless 1820)	Win 10 Pro (12.0.0.242)
Dell Inspiron 15-7569 (Intel Dual Band Wireless-AC 3165)	Windows 10 Home (18.32.0.5)
Dell Latitude E5540 (Intel Dual Band Wireless AC7260)	Windows 7 Professional (21.10.1)

Client Type and Name	Driver or Software Version
Dell XPS 12 v9250 (Intel Dual Band Wireless AC 8260)	Windows 10 (19.50.1.6)
Dell Latitude 5491 (Intel AX200)	Windows 10 Pro (21.40.2)
Dell XPS Latitude12 9250 (Intel Dual Band Wireless AC 8260)	Windows 10 Home (21.40.0)
Lenovo Yoga C630 Snapdragon 850 (Qualcomm AC 2x2 Svc)	Windows 10 (1.0.10440.0)
Lenovo Thinkpad Yoga 460 (Intel Dual Band Wireless-AC 9260)	Windows 10 Pro (21.40.0)
Note For clients using Intel wireless cards, we recommend that you to update to the latest Intel wireless drivers if the advertised SSIDs are not visible.	
Tablets	
Apple iPad Pro	iOS 13.5
Apple iPad Air2 MGLW2LL/A	iOS 12.4.1
Apple iPad Mini 4 9.0.1 MK872LL/A	iOS 11.4.1
Apple iPad Mini 2 ME279LL/A	iOS 12.0
Microsoft Surface Pro 3 – 11ac	Qualcomm Atheros QCA61x4A
Microsoft Surface Pro 3 – 11ax	Intel AX201 chipset. Driver v21.40.1.3
Microsoft Surface Pro 7 – 11ax	Intel Wi-Fi chip (HarrisonPeak AX201) (11ax, WPA3)
Microsoft Surface Pro X – 11ac & WPA3	WCN3998 Wi-Fi Chip (11ac, WPA3)
Mobile Phones	
Apple iPhone 5	iOS 12.4.1
Apple iPhone 6s	iOS 13.5
Apple iPhone 8	iOS 13.5
Apple iPhone X MQA52LL/A	iOS 13.5
Apple iPhone 11	iOS 14.1
Apple iPhone SE MLY12LL/A	iOS 11.3
ASCOM SH1 Myco2	Build 2.1
ASCOM SH1 Myco2	Build 4.5
ASCOM Myco 3 v1.2.3	Android 8.1
Drager Delta	VG9.0.2
Drager M300.3	VG2.4
Drager M300.4	VG2.4

Client Type and Name	Driver or Software Version
Drager M540	DG6.0.2 (1.2.6)
Google Pixel 2	Android 10
Google Pixel 3	Android 11
Google Pixel 3a	Android 11
Google Pixel 4	Android 11
Huawei Mate 20 pro	Android 9.0
Huawei P20 Pro	Android 9.0
Huawei P40	Android 10
LG v40 ThinQ	Android 9.0
One Plus 8	Android 10
Oppo Find X2	Android 10
Redmi K20 Pro	Android 10
Samsung Galaxy S7	Andriod 6.0.1
Samsung Galaxy S7 SM - G930F	Android 8.0
Samsung Galaxy S8	Android 8.0
Samsung Galaxy S9+ - G965U1	Android 9.0
Samsung Galaxy SM - G950U	Android 7.0
Sony Experia 1 ii	Android 10
Sony Experia xz3	Android 9.0
Xiaomi Mi10	Android 10
Spectralink 8744	Android 5.1.1
Spectralink Versity Phones 9540	Android 8.1
Vocera Badges B3000n	4.3.2.5
Vocera Smart Badges V5000	5.0.4.30
Zebra MC40	Android 5.0
Zebra MC40N0	Android 4.1.1
Zebra MC92N0	Android 4.4.4
Zebra TC51	Android 7.1.2
Zebra TC52	Android 8.1.0
Zebra TC55	Android 8.1.0
Zebra TC57	Android 8.1.0

Client Type and Name	Driver or Software Version
Zebra TC70	Android 6.1
Zebra TC75	Android 6.1.1
Printers	
Zebra QLn320 Printer	LINK OS 6.3
Zebra ZT230 Printer	LINK OS 6.3
Zebra ZQ310 Printer	LINK OS 6.3
Zebra ZD410 Printer	LINK OS 6.3
Zebra ZT410 Printer	LINK OS 6.3
Zebra ZQ610 Printer	LINK OS 6.3
Zebra ZQ620 Printer	LINK OS 6.3
Wireless Module	
Intel 11ax 200	Driver v22.20.0
Intel AC 9260	Driver v21.40.0
Intel Dual Band Wireless AC 8260	Driver v19.50.1.6

Caveats

Caveats describe unexpected behavior in Cisco IOS releases in a product. Caveats 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 a caveat, click the corresponding identifier.

Open Caveats for Cisco IOS XE Amsterdam 17.1.1t

There are no new open caveats for this release.

Open Caveats for Cisco IOS XE Amsterdam 17.1.1s

Caveat ID	Description
CSCvk79897	The **show ap dot11 {24ghz | 5ghz} cleanair air-quality summary** command is displaying empty AP names.
CSCvq31779	AP accounting ON/OFF messages are sent to all the RADIUS servers, when multiple servers are configured in the server group.
CSCvq53489	The web UI page is hanging while updating interface or policy on the ETA global configuration.
CSCvq56486	Flexconnect URLs and ACLs are not retained when AP reboots in standalone mode.
CSCvq61643	The controller fails to install on the Hyper-V with generation 2 default configuration. However, it starts to work after disabling secure boot.
CSCvq66539	Mobilityd CPU hog traceback is observed after a switchover.
CSCvq77275	Catalyst 9800 Series Wireless Controller for Cloud that is hosted on the Hyper-V drops upstream packets.
CSCvr09334	The **show ap auto-rf dot11 24ghz** command is not displaying the Cisco Aironet 4800 series AP entries after a day.
CSCvr46316	The controller is not populating the AP load information in discovery response.
CSCvr70395	The controller is not sending delete event for AP impersonation.
CSCvs11453	DNS resolution for RADIUS and TACACS is getting delayed, after the controller power cycle.
CSCvs15446	Traceback is observed after reloading the Cisco Catalyst 9800-L Series Wireless Controller that is in HA mode.
CSCvs20264	The controller is not reporting off-channel interference.
CSCvs45249	Unable to enter a valid URL in the urlfilter.
CSCvs60927	Frequent AP channel changes are observed on the 5-GHz band radio.
CSCvs61180	Traceback is observed intermittently during the memory allocation.
CSCvs70513	The **show wireless stats** command is showing negative value while shutting down the AP from admin state.

Resolved Caveats for Cisco IOS XE Amsterdam 17.1.1t

Caveat ID	Description
CSCvs87888	Evaluation of Cisco Catalyst 9100 Series APs for Kr00k attack.
CSCvt17801	AP 2800/3800/4800/1560/IW 6300 gets into a loop after attempting to join controller with FIPS enabled.
CSCvt47413	IW-6300H/1562/2800/3800/4800 series APs are failing DFS compliance
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 17.1.1s

Caveat ID	Description
CSCvf53989	Smart licensing summary shows "ASR_1000_AdvIpservices".
CSCvp65565	Add clear install state command.
CSCvr08701	APs are unable to form a tunnel due to Interprocessor Communication (IPC) channel back pressure.
CSCvr66201	System reloads unexpectedly and loses partial configuration due to wncd and cpp-mcplo failure.
CSCvq36007	Cisco Aironet 2800 and 3800 series APs are unable to send proper sequence number and burst rate in the upstream direction.
CSCvq65396	Cisco Catalyst 9800 Series Wireless Controller for Cloud is unable to save the configuration.
CSCvq78875	Controller reboots after changing the tags on the APs simultaneously.
CSCvq86040	Switch with an embedded wireless controller reloads unexpectedly.
CSCvq91503	Web UI is not configuring authentication type change correctly (from PSK to Open Authentication and back).
CSCvq95330	Cisco Wave 2 APs: workgroup bridge (WGB) is not sending Internet Access Point Protocol (IAPP) message in static IP configuration.
CSCvq95642	Multicast IPv6 packets that are received from the clients are causing a loop, which results in a major uplink bandwidth utilization issue.
CSCvq99561	Controller is sending 5 GHz band as 2.4 GHz band for an associated client to Cisco CMX.
CSCvr02462	Cisco Catalyst 9120 AXE AP is continuously rebooting when connected to Cisco IOS XE Gibraltar 16.12.1 release.

Caveat ID	Description
CSCvr03652	Fast Transition dot1x fails in standalone mode.
CSCvr07053	AP crashes and reboots.
CSCvr09722	Cisco Aironet 1832 APs: Association is denied because AP is unable to handle additional associated STAs.
CSCvr11358	Wncd process is crashing on the newly active controller immediately after the switchover.
CSCvr22918	Cisco Catalyst 9115AX nd 9120AX APs: Beacons are corrupted when non-broadcasted SSID is configured.
CSCvr27555	5 GHz radios are going down when the country code is changed to MK.
CSCvr33062	Samsung S10 clients are not able to connect to the WPA2+WPA3-SAE+PSK+FT PSK+PSK-SHA2 mixed mode.
CSCvr35679	Cisco Centralized Key Management (CCKM) and roaming failure due to RN mismatch.
CSCvr38675	Client connectivity failure is observed after LAN link flap.
CSCvr59882	Web UI QoS page is not loading and is showing the following message: HTTP-4-SERVER_CONN_RATE_EXCEED.
CSCvr98394	Clients are not able to associate to CCKM SSID for flexconnect.
CSCvs02781	Controller web UI is not sending redirect URL for webauth clients.
CSCvs63593	AP3802-P-k9 Transmit Power Violation with AIR-ANT2513P4M-N (13dBi) W52 Japan Outdoor.
CSCvs77251	Controller is unable to send proper sequence and burst rate upstream.
CSCvs40004	Cisco Catalyst 9800-L Copper Series Wireless Controller fails to install authorization code due to NO_AUTH_CODE_FOUND.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, visit the Cisco TAC website at:

https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213949-wireless-debugging-and-log-collection-on.html

Go to **Product Support** and select your product from the list or enter the name of your product. Look under **Troubleshoot and Alerts** to find information about the problem that you are experiencing.

Related Documentation

Information about Cisco IOS XE is available at:

https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-xe/index.html

Cisco Validated Designs documents are available at:

https://www.cisco.com/go/designzone

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use the Cisco MIB Locator found at:

http://www.cisco.com/go/mibs

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

The installation guide for your controller is available at:

- Hardware Installation Guides

For all Cisco Wireless Controller software-related documentation, see:

https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/tsd-products-support-series-home.html

Cisco Catalyst 9800 Wireless Controller Data Sheets

- Cisco Catalyst 9800-CL Wireless Controller: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-cl-wireless-controller-cloud/nb-06-cat9800-cl-cloud-wirel-data-sheet-ctp-en.html
- Cisco Catalyst 9800-80 Wireless Controller: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/nb-06-cat9800-80-wirel-mod-data-sheet-ctp-en.html
- Cisco Catalyst 9800-40 Wireless Controller: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/nb-06-cat9800-wirel-cont-data-sheet-ctp-en.html
- Cisco Catalyst 9800-L Wireless Controller: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/datasheet-c78-742434.html

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 Products Comparison

- Use this tool to compare the specifications of Cisco wireless APs and controllers:

  https://www.cisco.com/c/en/us/products/wireless/wireless-lan-controller/product-comparison.html

- Wireless LAN Compliance Lookup:

  https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html

- Cisco AireOS to Cisco Catalyst 9800 Wireless Controller Feature Comparison Matrix:

  https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/AireOS_Cat_9800_Feature_Comparison_Matrix.html

Cisco Prime Infrastructure

Cisco Prime Infrastructure Documentation

Cisco Connected Mobile Experiences

Cisco Connected Mobile Experiences Documentation

Cisco DNA Center

Cisco DNA Center Documentation

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.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.