Recommended Cisco IOS XE Releases for Catalyst 9800 Wireless LAN Controllers

Contents

Introduction

Background

TAC Recommended Builds

- Cisco IOS XE 26.2
  - 26.2.1
- Cisco IOS XE 26.1
  - 26.1.2
  - 26.1.1
- Cisco IOS XE 17.18
  - 17.18.5
  - 17.18.4a
  - 17.18.3
  - 17.18.2
  - 17.18.1
- Cisco IOS XE 17.17.1
- Cisco IOS XE 17.16.1
- Cisco IOS XE 17.15
  - 17.15.6
  - 17.15.5
  - 17.15.4d
  - 17.15.4b
  - 17.15.4
  - 17.15.3
  - 17.15.2b
  - 17.15.2
  - 17.15.1
- Cisco IOS XE 17.14.1
- Dublin 17.12
  - 17.12.8
  - 17.12.7a
  - 17.12.6a
  - 17.12.6
  - 17.12.5
  - 17.12.4
  - 17.12.3
  - 17.12.2
- Cupertino 17.9
  - 17.9.10
  - 17.9.9
- Bengaluru 17.6
  - 17.6.8
- Amsterdam 17.3

17.3.8a

Gibraltar 16.x

Field Programmable (FPGA) Firmware on Hardware 9800 WLC

High Availability Software Maintenance on 9800 WLC

ISSU

Software Maintenance Upgrade (SMU) Patch

Access Point Service Pack

Access Point Device Pack

Guidelines and Requirements

Cisco.com Location of SMUs, APSP and APDP images for different 9800s

Note for Software Defined Access (SDA)

Inter Release Controller Mobility (IRCM)

Features supported On Catalyst 9800 Series Wireless LAN Controllers

Introduction

This document describes how to find the most reliable Cisco IOS® XE software for Catalyst 9800 Wireless LAN Controllers (C9800 WLCs).

Background

The information in this document is applicable to different form factors of C9800 WLC, including:

- Appliances (9800-40, 9800-80,9800-L, CW9800M, CW9800H1, CW9800H2)
- Virtual Controllers (9800-CL in private and public cloud environments)
- Embedded Wireless Controllers on Catalyst 9000 Series switches
- Embedded Wireless Controllers on Catalyst Access Points (EWC-AP)

Access Point models supported by the C9800 include:

- Cisco IOS based 11ac Wave 1 Access Points (1700/2700/3700/1572) (not in all releases)
- COS based 11ac Wave 2 Access points (1800/2800/3800/4800/1540/1560)
- COS based Catalyst 11ax 91xx Series Access Points (9105/9115/9117/9120/9130/9136/9164/9166)
- Cisco Wireless 917x Series Access Points (CW9171/CW9172/CW9174/CW9176/CW9178/CW9179)

Co-existence of AireOS WLCs with C9800 WLC is taken into account for these recommendations. The recommendations cover all the releases of Cisco IOS® XE software applicable to all form factors of 9800 WLCs. Typically, a newly released version (either maintenance release or new code train) is given a minimum of 6-8 weeks soak time in the field, and only if no catastrophic issues are reported, it becomes a candidate for Cisco general recommendation. These recommendations are updated as we receive feedback through internal testing, TAC cases, and so on.

TAC Recommended Builds

Note:
1) SMUs and APSPs require a Network Advantage License. For deployments with Network Essentials license, Escalation Image that can be requested from Cisco TAC. Upgrading to an Escalation Image requires downtime.
2) APSPs are incremental, that is each APSP version includes fixes from all previous versions of APSPs.
3) Latest APSP is always recommended. Evaluate the bugs under APSP and apply those APSPs that includes fixes for AP models in your deployment.
4) Most of the short-lived releases like Cisco IOS XE releases 17.10.1, 17.11.1 and older maintenance releases like 17.9.1, 17.9.2 are not mentioned in this document as they have reached End of Vulnerability / Security Support. End of Life (EOL) notices of all the Cisco IOS XE releases for C9800 WLC can be reviewed at EoL Bulletin.
5) The document only lists bug fixes for the releases that we see in a large set of deployments. For bugs affecting specific releases, use the Bug Search Tool.

Cisco Wireless Platform	Recommended Release
Cisco Catalyst Wireless CW9800L	Cisco IOS XE 17.18.4a with SMU and APSP3
Cisco Catalyst Wireless CW9800M, CW9800H1, CW9800H2	Cisco IOS XE 17.18.4a with APSP3
Cisco Catalyst C9800-CL, C9800-40, C9800-80, C9800-L	Cisco IOS XE 17.18.4a with SMU and APSP3
Embedded Wireless Controller (EWC) on APs	Cisco IOS XE 17.15.5 with APSP5
Embedded Wireless Controller (EWC) on Catalyst switches	Cisco IOS XE 17.18.4 with APSP3
Any WLC controller platform supporting Cisco Wireless APs CW917x (9171, 9172, 9174, 9176, 9178, 9179)	Cisco IOS XE 17.18.4a with APSP3

Table 1. Summary View of Recommended Cisco IOS XE Release for different WLC platforms

Cisco IOS XE 26.2

26.2 is an extended-release train and 26.2.1 is marked as General Availability, which marks the start of a 48-month period of maintenance releases for this train.

26.2 drops support for 11ac wave2 access points such as the 1800, 2800,3800 and 4800 series.

26.2.1

Cisco IOS XE 26.2.1 is the first release of its train (GA) and therefore is not marked as generally recommended. Further 26.2 maintenance releases are considered for recommendation later on.

Cisco IOS XE 26.1

Cisco IOS XE 26.1 is the first train that uses Cisco new numbering scheme of two extended release per year (see this document for more information).

26.1 is an extended-release train and 26.1.1 is marked as General Availability, which marks the start of a 48-month period of maintenance releases for this train.

26.1 drops support for C9117 access points and marks the start of Cisco Resilient Infrastructure security initiative (learn more at Cisco 9800 Wireless Resilient Infrastructure).

26.1.2

Due to Cisco IOS XE Software Security Hardening Release: August 2026, Cisco recommends that all customers who were running on the 26 train to migrate to 26.1.2, but to check this remediation for doing so. Note that the APSP is available even to Essentials level license customers.

Cisco advises that you use 26.1.2 along with APSP1, if you need specific features described in the 26.1 release notes.

If you use a 9800-CL or CW9800L or 9800L, Cisco advises you install the SMU for CSCwv98483

26.1.1

Cisco IOS XE 26.1.1 is the first release of its train (GA) and therefore is not marked as generally recommended. Further 26.1 maintenance releases are considered for recommendation later on.

Cisco IOS XE 17.18

Cisco IOS XE 17.18 is a long-lived release train. The new features supported in this release are listed in the release notes.

17.18.5

17.18.5 contains the hardening brought by 17.18.4 in response to the August 2026 notice and also includes the fixes added by APSPs.

It is evaluated currently for becoming the next recommended release in the 17.18 train.

17.18.4a

Due to Cisco IOS XE Software Security Hardening Release: August 2026, Cisco published 17.18.4a with the security hardening required. However, Cisco advises you to check this remediation if you are considering this release. Note that the APSP is available even to Essentials level license customers.

APSP2 is now out (and includes the fix from APSP1) and brings stability improvements to Wifi 7 APs (among other fixes) issues that were present already in 17.18.3. See the release notes: https://www.cisco.com/web/software/286325254/176135/Public_Release_Notes_9800_APSP_17_18_4a.pdf

Cisco recommends to run 17.18.4a with APSP2.

If you use a 9800-CL or CW9800L or 9800L, Cisco advises you install the SMU for CSCwv98483

Note: If you use SDA wireless on an embedded controller on a switch, the release is called 17.18.4 for both the switch and wireless package. It is called 17.18.4a only on standalone controllers.

17.18.3

17.18.3 is the third release of the 17.18 train.

APSP3 is now available for 17.18.3. APSP release notes.

17.18.2

17.18.2 is the second release of the 17.18 train which introduces support for the Cisco Catalyst Wireless CW9800L platform.

Note: ISSU on CW9800L in 17.18.2, 17.18.3, 26.1.1 is affected by Cisco bug ID CSCwt98619 and requires use of *install activate issu force* command in CLI or *Override* option in GUI.
Native ISSU support (via CatC and without CLI force command or GUI Override option) is restored in 17.18.4a and 26.1.2.

17.18.1

17.18.1 is the first release of the 17.18 train and is now not recommended to run anymore, consider upgrading to 17.18.3.

Cisco IOS XE 17.17.1

Cisco IOS XE 17.17 is a short-lived release with no MRs planned. The new features supported in this release are listed in 17.17.1 Release Notes.

Cisco IOS XE 17.16.1

Cisco IOS XE 17.16 is a short-lived release with no MRs planned. It is important to note that Cisco IOS XE 17.16 does not support Wi-Fi 7 APs and does not allow Cisco IOS-based APs to join anymore. The new features supported in this release are listed in 17.16.1 Release Notes.

Cisco IOS XE 17.15

Cisco IOS XE 17.15 is a long-live train with several maintenance releases (MR) planned. The new features supported in this release are listed in 17.15.1 Release Notes.

Cisco recommends 17.15.6 for all deployments when Wi-Fi 7 features are not actively used or if you were already on the 17.15 train. If you want to enable Wi-Fi 7 features on some of your SSIDs, TAC recommends you consider the 17.18.4a train.

17.15.6

Due to Cisco IOS XE Software Security Hardening Release: August 2026, Cisco published 17.15.6 with the security hardening required. Cisco recommends you read this remediation if you are considering this release. Note that the APSP is available even to Essentials level license customers.

APSP3 (which includes the fix from APSP1) brings stability improvements to Wifi 7 APs issues (among other fixes) that were present already in 17.15.5. See the release notes.

If you use a 9800-CL or CW9800L or 9800L, Cisco advises you install the SMU for CSCwv98483

This is the new recommended release in the 17.15 train.

17.15.5

17.15.5 contains all the fixes from all the 17.15.4 releases, including the fix for ISSU upgrades and the fix for CAPWAP denial of service security advisory CVE-2026-20086 and Cisco bug ID CSCwp13209 affecting the CW9800 hardware models.

APSP5 is now available for 17.15.5. See the release notes.

17.15.4d

17.15.4d has been posted with all the fixes previously in 17.15.4b+ the latest APSP.

17.15.4b

17.15.4b has been posted with all the fixes previously in 17.15.4 on top of the fix for the mDNS issue (Cisco bug ID CSCwr09565). It continues to be considered a stable release when all the APSPs are added, however 17.15.4d regroups all of them in a single software along with the ISSU upgrade issue fix.

17.15.4

17.15.4 has been removed for download from cisco.com due to an mDNS gateway regression (Cisco bug ID CSCwr09565).

17.15.3

Cisco IOS XE 17.15.3 is the second maintenance release in the 17.15 release train.

17.15.2b

Cisco IOS XE 17.15.2b is introduced only to support CW9172I access point deployments and you are expected to upgrade to Cisco IOS XE 17.15.4b.

17.15.2

Cisco IOS XE 17.15.2 is the first maintenance release in the 17.15 release train and introduces support for:

- WiFi7
  - Access Points (CW9176I, CW9176D1, CW9178I)
  - Multi-Link Operation (MLO) for WiFi7 APs
  - WPA3 Security Considerations
- Global Use AP (Decoupling of AP PID/SKU from boot mode and regulatory domain)
- Cisco Network Subscription
- AP AnyLocate / UltraWide Band Ranging Technology

⚠ **Caution**: For Flexconnect deployments with Local Switching, client roam on a webauth SSID could randomly cause client to lose reachability to its gateway. See details in Cisco bug ID CSCwn17412.

17.15.1

Cisco IOS XE 17.15.1 is the first version of the 17.15 train. For all hardware and features supported starting 17.13.1, 17.14.1, and 17.15.1, Cisco recommends you to migrate your deployment to 17.15.4b.

17.15.1 contains the fix for the "regreSSHion" vulnerability on access points depicted in Cisco bug IDs CVE-2024-6387 and CSCwk62269.

Cisco IOS XE 17.14.1

Cisco IOS XE 17.14.1 is a short-lived release with no MRs planned. The new features supported in this release are listed in 17.14.1 Release Notes. This is the first release to support newer Catalyst 9800 Series WLCs.

- Cisco Catalyst CW9800M Wireless Controller
- Cisco Catalyst CW9800H1 and CW9800H2 Wireless Controller

For all new hardware and features supported starting 17.13.1 or 17.14.1, Cisco recommends upgrading to 17.15.2d.

Dublin 17.12

The new features supported in this release are listed in 17.12.1 Release Notes. Cisco recommends 17.12.7a if you need to stay on 17.12 train (for example, if you have 11ac wave 1 APs). Start planning your migration to 17.15.5, if Wi-Fi7 features are not in use or to 17.18.3 for Wi-Fi7 deployments. This is a direct upgrade. Refer to Upgrade Path to 17.15.x or Upgrade Path to 17.18.x.

17.12.8

Due to Cisco IOS XE Software Security Hardening Release: August 2026, Cisco published 17.12.8 with the security hardening required. Cisco recommends this remediation if you are considering this release.

17.12.7a

17.12.7a contains all the fixes from the 17.12.6 APSPs including Cisco bug ID CSCwf25731 where the cnssdamon.log file can grow too large and impact future upgrades.

17.12.6a

17.12.6a contains all the fixes from 17.12.6 on top of the mDNS issue fix (Cisco bug ID CSCwr09565).

APSP1 contains the fix for Cisco bug ID CSCwf25731 where cnssdeamon log file on the AP grows too large and impacts future upgrade by filling the flash partition. Cisco recommends installing APSP4 which contains all the necessary fixes if you want to stay on 17.12.6a or to move to 17.12.7a.

17.12.6

17.12.6 has been removed for download from cisco.com due to an mDNS gateway regression (Cisco bug ID CSCwr09565).

17.12.5

Cisco IOS XE 17.12.5 is the fourth bug-fix release in the 17.12 train. It incorporates the fixes in SMUs and APSPs for 17.12.4 and many more bug fixes.

Cisco bug ID SMU CSCwo62157. Reload SMU, Memory leak observed in tdl_mac_addr object.

17.12.5 APSP6 includes fixes listed in release notes.

17.12.4

Cisco IOS XE 17.12.4 is the third bug-fix release in the 17.12 train.

17.12.4 APSP8 or 17.12.4.208 includes fixes listed in 17.12.4 APSP8 release notes.

17.12.3

Cisco IOS XE 17.12.3 is the second bug-fix release in the 17.12 train.

⚠ **Caution**:
1) In case you have an SD-Access deployment, be aware of Cisco bug ID CSCwj04031: WLC forces SGT to 0 when the client releases IPv6 link-local address. Contact TAC to get a SMU patch if you are affected.
2) For HA deployments, Ha failover could lead to config loss on C9800 WLC leading to wireless outage. This is tracked under Cisco bug ID CSCwj73634 where config can be lost upon HA failover.

17.12.2

Cisco IOS XE 17.12.2 is the first bug-fix release in the 17.12 train and includes the fix for Cisco bug IDs CVE-2023-20198, CVE-2023-20273, and CSCwh87343.

Cupertino 17.9

17.9.10

Due to Cisco IOS XE Software Security Hardening Release: August 2026, Cisco published 17.9.10 with the security hardening required. Cisco recommends this remediation if you are considering this release.

17.9.9

Cisco IOS XE 17.9.x is a long-lived train with several maintenance releases (MRs). 17.9 has reached End of Software Maintenance as documented in 17.9 End of Life bulletin. Only one more psirt-only release is expected in 17.9 train. Cisco recommends migrating to 17.15.5 or 17.18.3 (if using Wi-Fi7 features). Depending on AP models in use, this can be a direct upgrade or a staggered upgrade. Refer to Upgrade Path to 17.15.x or Upgrade Path to 17.18.x for more details.

Bengaluru 17.6

Cisco IOS XE 17.6.x is a long-lived train with several maintenance releases (MRs). 17.6 has reached End of Software Maintenance as documented in 17.6 End of Life bulletin. Cisco recommends you to migrate to 17.15.5 or 17.18.3 (if using Wi-Fi7 features). Depending on AP models in use, this can be a direct upgrade or a staggered upgrade. Refer to Upgrade Path to 17.15.x or Upgrade Path to 17.18.x for more details.

17.6.8

Cisco IOS XE 17.6.8 is the last maintenance release that provides fixes for recent vulnerability advisories.

Amsterdam 17.3

Cisco IOS XE 17.3.x is a long-lived train with several maintenance releases (MRs). 17.3 has reached End of Software Maintenance as documented in 17.3 End of Life Bulletin. Cisco recommends you to migrate to 17.15.5 or 17.18.3 (if using Wi-Fi7 features). Depending on AP models in use, this can be a direct upgrade or a staggered upgrade. Refer to Upgrade Path to 17.15.x or Upgrade Path to 17.18.x for more details.

17.3.8a

Cisco IOS XE 17.3.8a is the last bug-fix MR in the 17.3 release train. If you cannot migrate to recommended release and need to stay on 17.3 train, Cisco recommends 17.3.8a.

Gibraltar 16.x

Cisco IOS XE 16.10.1 is the first release of Cisco IOS XE software that officially supports Catalyst 9800 SKUs (Appliances: 9800-40, 9800-80; 9800 on private/public cloud; 9800-CL, as well as 9800 software on Catalyst 9300 Switches) and is currently end-of-life (EoL). Two releases were published for 16.x release train: 16.11.1 (EoL) and 16.12.1 (EoL). Cisco IOS XE 16.12.1 was the first long-lived traing for C9800 WLCs which added support for 9800-L, 9800-CL on Google Cloud and Embedded Wireless Controller on Catalyst Access Point (EWC-AP), among other features.

16.12.8

This is the last maintenance release (MR) in the 16.x train. Cisco recommends you to migrate your deployment to 17.15.5 or 17.18.3 (if using Wi-Fi7 features). This migration requires staggered upgrade. Refer to Upgrade Path to 17.15.x or Upgrade Path to 17.18.x for more details.

Field Programmable (FPGA) Firmware on Hardware 9800 WLC

On physical Catalyst 9800 WLCs (9800L, 9800-40, 9800-80), besides Cisco IOS XE, there are two other pieces of code that can and can require an upgrade:

- ROM Monitor (ROMMON) – The bootstrap program that initializes hardware and boots the Cisco IOS XE software on the C9800 appliance. You can check the ROMMON version running on your appliance by executing this command.

```
#show rom-monitor chassis {active | standby} R0
```

- PHY – The physical layer, specifically, the Shared Port Adapter (SPA) module that supports the front end distribution and uplink ports on C9800 appliances. It can also be called Ethernet/Hardware Programmables. You can view the PHY version running on your appliance by executing this command.

```
#show platform hardware chassis active qfp datapath pmd ifdev | include FW
```

New firmware is typically released to protect the health of the system (temperature sensors, fan, power supply and so on) and to address problems with data forwarding in and out of the physical ports. Cisco recommends upgrading to latest FPGA firmware available.

Upgrade Procedure along with the specific defects that for which new firmware was released if documented at Upgrade C9800 FPGA.

These are the versions for each platform:

ROMMON	Ethernet PHY	Fiber PHY	
9800-L-F	16.12(3r)	N/A	17.11.1

9800-L-C	16.12(3r)	17.11.1	N/A
9800-40	17.12(1r)	N/A	16.0.0
9800-80	17.12(2r)	N/A	16.0.0
CW9800M	17.15(2r)	N/A	N/A
CW9800H1	17.15(1r)	N/A	N/A
CW9800H2	17.15(1r)	N/A	N/A
CW9800L	17.18(1r)	N/A	N/A

High Availability Software Maintenance on 9800 WLC

C9800 provides multiple features that ensure availability during software maintenance phase of the deployment lifecycle. These include In-Service Software Upgrade (ISSU), Rolling AP upgrade, Hot and Cold Patch to address WLC defects or psirts, AP patches to address AP specific fixes as well as to support newer AP models on existing controller code.

ISSU

ISSU support was introduced in 17.3.1 and is limited to long-lived releases (17.3.x, 17.6.x, and 17.9.x). That is, ISSU works:

1. Within long-lived major releases, for example, 17.3.x to 17.3.y, 17.6.x to 17.6.y, 17.9.x to 17.9.y
2. Between long-lived major releases, for example, 17.3.x to 17.6.x, 17.3.x to 17.9.x

Note: This is limited to two long-lived releases after the current supported long-lived release.

ISSU is NOT supported:

1. Within minor releases of short-lived release trains, for example 17.4.x to 17.4.y or 17.5.x to 17.5.y
2. Between minor and major releases of short-lived release trains, for example 17.4.x to 17.5.x
3. Between long-lived and short-lived releases 17.3.x to 17.4.x or 17.5.x to 17.6.x

Software Maintenance Upgrade (SMU) Patch

C9800 supports both Cold and Hot Patching which enables bug fixes to be provided as a Software Maintenance Upgrade (SMU) file.

- Hot Patch - System reload is not required meaning WLC and APs continue to operate. In case of 9800 Stateful Switchover (SSO) pair, SMU install process applies the patch to both chassis.
- Cold Patch - System reload is needed for Cold Patch. In case of 9800 SSO pair, cold patch can be applied without downtime.

Access Point Service Pack

Fixes for software defects on Access Points (APs) can be delivered via Access Point Service Packs. This requires reload of the APs but not of the 9800 WLC.

Access Point Device Pack

Support for newer AP models is made available on existing WLC code, without needing WLC code upgrade. This AP only supports the features available in existing WLC code.

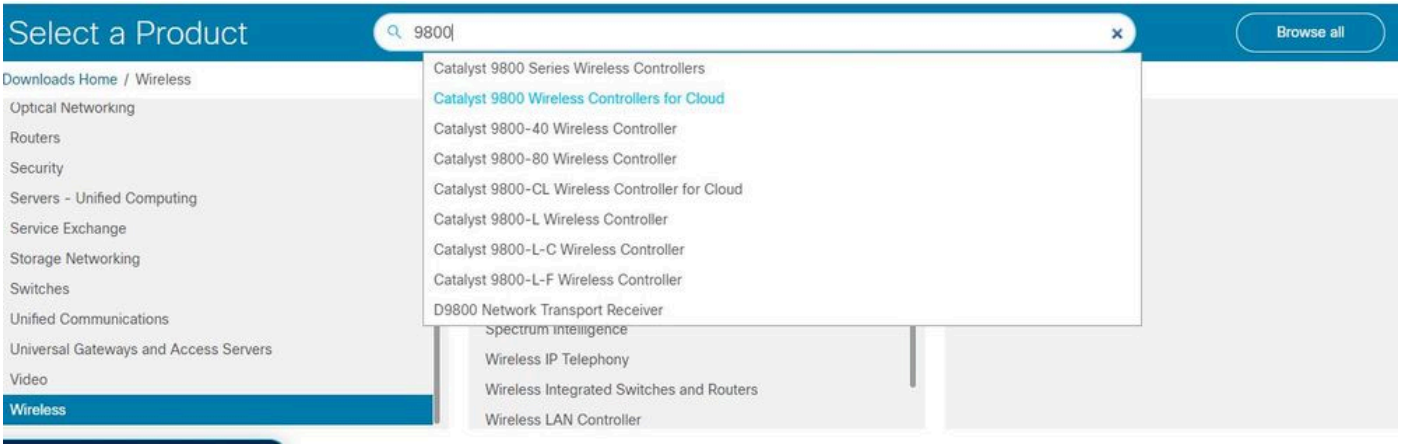
Guidelines and Requirements

1. SMU patches are only generated for long-lived releases like 16.12, 17.3, 17.6, 17.9 and so on *after* their MD release.
2. SMUs can only be applied on 9800 WLC running Network Advantage License at the minimum. Learn more at Wireless Features Matrix for different Licenses.
3. SMUs that are applicable to most deployments, are posted to cisco.com.
4. SMU or a patch is not possible for all bug fixes. Code changes involved in the bug fix typically determine the patchability.
5. Applicability of SMU is evaluated on a per-defect basis. If your C9800 qualifies for an SMU patch, based on its licensing and you need an SMU for a specific defect, please engage Cisco Technical Assistance Center (TAC) to get the bug evaluated.

Refer to the C9800 WLC Patching Guide for more details on these capabilities.

Cisco.com Location of SMUs, APSP and APDP images for different 9800s

Step 1. At Software Download, enter 9800 in the search bar and choose the 9800 form factor applicable to you.



Step 2. From the **Software Type** menu, choose **SMU**, **APSP**, or **APDP** as needed.



Note for Software Defined Access (SDA)

Always refer to the SDA Compatibility Matrix for code combination recommendations that work best for SDA. It lists specific combinations of code on Cisco DNA Center, the Identity Service Engine (ISE), switches, routers and Wireless LAN Controller codes that have been tested by the SDA Solution Test team at Cisco.

Inter Release Controller Mobility (IRCM)

- IRCM is not supported with 2504/7510/vWLC Controllers and only supported with 5508/8510/5520/8540/3504 platforms
- For Inter-Release Controller Mobility (IRCM) compatibility with AireOS WLCs, in general:
  - Cisco recommends AireOS 8.10.196.0 for all deployments.
  - For deployments with older WLCs or Access Points in their environment that cannot be upgraded past AireOS 8.5, TAC recommends 8.5.182.109 (8.5.182.111 for 3504s) IRCM code.

Note: Not all 8.5 code versions support IRCM. 8.5 IRCM versions available on cisco.com include 8.5.164.0, 8.5.164.216, 8.5.176.0, 8.5.176.1. 8.5.176.2, and 8.5.182.104.

⚠ **Caution**:
Deployments with 1800 series APs (1815/1830/1850) running 8.10.185.0 through 8.10.196.0 can report spuriously high channel utilization in 5Ghz, resulting in performance problems, owing to a regression caused by the commit of Cisco bug ID CSCwb51757.
For 1815 series APs, the fix is in 8.10.190.9 / 8.10.196.7, available from TAC.
For 1830/1850 series APs, as this fix is unavailable in the 8.10 code train, to avoid this problem, AireOS deployments encountering this issue need to downgrade to code prior to the Cisco bug ID CSCwb51757 commit, 8.10.183.0.

For AireOS recommended code, see Recommended AireOS Wireless LAN Controller Releases.

Features supported On Catalyst 9800 Series Wireless LAN Controllers

Release Notes

Cisco IOS XE Wireless Feature List per Release

AireOS to Cisco IOS XE feature Comparison Matrix

Access Point and WLC Selector