

# Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.10.171.0

---

**First Published:** 2022-03-04

**Last Modified:** 2022-08-30

## About the Release Notes

This release notes document describes what is new or changed in this release, instructions to upgrade to this release, and provides information about the open and resolved caveats for this release. Unless otherwise noted, in this document, Cisco Wireless Controllers are referred to as *controllers*, and Cisco lightweight access points are referred to as *access points* or *APs*.

## Supported Cisco Wireless Controller Platforms

The following controller platforms are supported in this release:

- Cisco 3504 Wireless Controller
- Cisco 5520 Wireless Controller
- Cisco 8540 Wireless Controller
- Cisco Virtual Wireless Controller (vWLC) on the following platforms:
  - VMware vSphere Hypervisor (ESXi) Version 5.x and 6.x
  - Hyper-V on Microsoft Server 2012 and later versions (support introduced in Release 8.4)
  - Kernel-based virtual machine (KVM) (support introduced in Release 8.1). After KVM is deployed, we recommend that you do not downgrade to a Cisco Wireless release that is earlier than Release 8.1).
- Cisco Wireless Controllers for High Availability for Cisco 3504 Wireless Controller, Cisco 5520 Wireless Controller, and Cisco 8540 Wireless Controller
- Cisco Mobility Express



---

**Note** In a network that includes Cisco Catalyst Center (formerly Cisco DNA Center) and Cisco AireOS controller, and the controller fails provisioning with **Error NA serv CA certificate file transfer failed** error, as a workaround, we recommend you reboot the affected AireOS controller.

---

## Supported Cisco Access Point Platforms

The following Cisco AP platforms are supported in this release:

- Cisco Catalyst 9105 Access Points
  - C9105AXI: VID 03 and earlier
  - C9105AXW: VID 01
- Cisco Catalyst 9130 Access Points
  - C9130AXE: VID 02 and earlier
  - C9130AXI: VID 02 and earlier
- Cisco Catalyst 9120 Access Points
  - C9120AXI: VID 06 and earlier
  - C9120AXE: VID 06 and earlier
  - C9120AXP: All VIDs
- Cisco Catalyst 9117 Access Points
- Cisco Catalyst 9115 Access Points
- Cisco Aironet 700 Series Access Points
- Cisco Aironet 700W Series Access Points
- Cisco AP803 Integrated Access Point
- Integrated Access Point on Cisco 1100, 1101, and 1109 Integrated Services Routers
- Cisco Aironet 1700 Series Access Points
- Cisco Aironet 1800 Series Access Points
- Cisco Aironet 1810 Series OfficeExtend Access Points
- Cisco Aironet 1810W Series Access Points
- Cisco Aironet 1815 Series Access Points
- Cisco Aironet 1830 Series Access Points
- Cisco Aironet 1840 Series Access Points
- Cisco Aironet 1850 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 ASA 5506W-AP702
- Cisco Aironet 1530 Series Access Points
- Cisco Aironet 1540 Series Access Points
- Cisco Aironet 1560 Series Access Points
- Cisco Aironet 1570 Series Access Points
- Cisco Industrial Wireless 3700 Series Access Points
- Cisco Catalyst IW6300 Heavy Duty Series Access Points
- Cisco 6300 Series Embedded Services Access Points

Cisco AP803 is an integrated access point module on the Cisco 800 Series Integrated Services Routers (ISRs). For more information about the stock-keeping units (SKUs) for the AP803 Cisco ISRs, see:

<http://www.cisco.com/c/en/us/products/routers/800-series-routers/brochure-listing.html>.

For more information about the integrated access point on Cisco 1100 ISR, see the product data sheet:

<https://www.cisco.com/c/en/us/products/collateral/routers/1000-series-integrated-services-routers-isr/datasheet-c78-739512.html>.

For information about the Cisco Wireless software releases that support specific Cisco access point modules, see the "[Software Release Support for Specific Access Point Modules](#)" section in the *Cisco Wireless Solutions Software Compatibility Matrix* document.

## What's New in Release 8.10.171.0

This section provides a brief introduction to the new features and enhancements that are introduced in this release.



---

**Note** For a complete list of all the documentation published for Cisco Wireless Release 8.10, see the Documentation Roadmap at: <https://www.cisco.com/c/en/us/td/docs/wireless/doc-roadmap/doc-roadmap-release-810.html>

---

## HTTP Strict-Transport-Security Policy

From this release onwards, by enabling the HTTP Strict Transport Security (HSTS) policy on the controller, you may access the controller GUI only with a client browser that uses HTTPS protocol.



---

**Note** For more information about configuring HTTP Strict-Transport-Security Policy, see [https://www.cisco.com/content/en/us/td/docs/wireless/controller/8-10/config-guide/b\\_cg810/administration\\_of\\_cisco\\_wlc.html#hsts\\_policy](https://www.cisco.com/content/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/administration_of_cisco_wlc.html#hsts_policy)

---

## Software Release Types and Recommendations

*Table 1: Release Types*

Release Type	Description	Benefit
Maintenance Deployment (MD)	Software releases that provide bug-fix support and ongoing software maintenance. These releases are categorized as Maintenance Deployment (MD).  These releases are long-living releases with ongoing software maintenance.	Provides you with a software release that offers stability and long support duration with periodic maintenance releases (MRs).
Early Deployment (ED)	Software releases that provide new features and new hardware platform support in addition to bug fixes. These releases are categorized as Early Deployment (ED).  These releases are short-lived releases.	Allows you to deploy the latest features and new hardware platforms or modules.

For detailed release recommendations, see the *Guidelines for Cisco Wireless Software Release Migration Bulletin* at:

<http://www.cisco.com/c/en/us/products/collateral/wireless/8500-series-wireless-controllers/bulletin-c25-730741.html>.

*Table 2: Upgrade Path to Cisco Wireless Release 8.10.171.0*

Current Software Release	Upgrade Path to Release 8.10.171.0
8.5.x	You can upgrade directly to Release 8.10.171.0.
8.6.x	You can upgrade directly to Release 8.10.171.0.
8.7.x	You can upgrade directly to Release 8.10.171.0.
8.8.x	You can upgrade directly to Release 8.10.171.0.
8.9.x	You can upgrade directly to Release 8.10.171.0.
8.10.x	You can upgrade directly to Release 8.10.171.0.

## Upgrading a Cisco Wireless Release

This section describes the guidelines and limitations that you must be aware of when you are upgrading the Cisco Wireless release and the procedure to upgrade.

## Guidelines and Limitations

- An existing WLAN with ? in its name continues to be supported with this upgrade. However, you cannot include ? in the name when creating a new WLAN.
- If an AP locks out the console due to default management user credentials, you must configure the controller AP global credential with non-default username and password to get access to the AP console.
- WPA3 upgrade and downgrade guidelines:
  - If you want to upgrade from Release 8.5 to 8.10 and have WPA1 configured with none of the WPA1 AKM valid for Release 8.10, the WPA1 configuration is disabled after the upgrade.
  - If you downgrade from Release 8.10 to Release 8.5, if any AKM for SAE is configured, the AKM validation fails after the downgrade. The security is set to WPA2 and AKM to 802.1X. However, PMF configuration is retained, which results in an error.
  - FT set to enabled state and PMF set to Required state is allowed in Release 8.10 because PMF and FT configurations are decoupled. However, in Release 8.5, this configuration is invalid. Therefore, upon downgrading to Release 8.5, the WLAN might be disabled.
- Software downgrade guidelines for Release 8.10:
  - If you plan to downgrade the Cisco controller from Release 8.10 software, we recommend you to downgrade to Release 8.5.151.0 or later release to prevent the controller configuration files from being corrupted.
  - If you have configured new country codes in Release 8.10 and if you plan to downgrade to an earlier release, then we recommend that you remove the new country code configurations prior to the downgrade. For more information, see [CSCvq91895](#).
- Before downgrading or upgrading the Cisco Controller to another release check for APs or AP modes support. Ensure that only supported APs are connected and also the APs are moved to supported modes on the release that the controller is upgraded or downgraded to.
- Legacy clients that require RC4 or 3DES encryption type are not supported in Local EAP authentication.
- If you downgrade to Release 8.0.140.0 or 8.0.15x.0, and later upgrade to a later release and also have the multiple country code feature configured, then the configuration file could get corrupted. When you try to upgrade to a later release, special characters are added in the country list causing issues when loading the configuration. For more information, see [CSCve41740](#).



---

**Note** Upgrade and downgrade between other releases does not result in this issue.

---

- After downloading the new software to the Cisco APs, it is possible that a Cisco AP may get stuck in an upgrading image state. In such a scenario, it might be necessary to forcefully reboot the controller to download a new controller software image or to reboot the controller after the download of the new controller software image. You can forcefully reboot the controller by entering the **reset system forced** command.
- It is not possible to download some of the older configurations from the controller because of the Multicast and IP address validations. See the "Restrictions on Configuring Multicast Mode" section in the *Cisco*

*Wireless Controller Configuration Guide* for detailed information about platform support for global multicast and multicast mode.

- When a client sends an HTTP request, the controller intercepts it for redirection to the login page. If the HTTP GET request that is intercepted by the controller is longer than 2000 bytes, the controller drops the packet. Track the Caveat ID [CSCuy81133](#) for a possible enhancement to address this restriction.
- When downgrading from one release to an earlier release, you might lose the configuration from your current release. The workaround is to reload the previous controller configuration files that are saved in the backup server, or to reconfigure the controller.
- When you upgrade a controller to an intermediate release, wait until all the APs that are associated with the controller are upgraded to the intermediate release before you install the latest controller software. In large networks, it can take some time to download the software on each AP.
- You can upgrade to a new release of the controller software or downgrade to an earlier release even if FIPS is enabled.
- When you upgrade to the latest software release, the software on the APs associated with the controller is also automatically upgraded. When an AP is loading software, each of its LEDs blinks in succession.
- Controllers support standard SNMP MIB files. MIBs can be downloaded from the software download page on Cisco.com.
- The controller software that is factory-installed on your controller and is automatically downloaded to the APs after a release upgrade and whenever an AP joins a controller. We recommend that you install the latest software version available for maximum operational benefit.
- Ensure that you have a TFTP, HTTP, FTP, or SFTP server available for the software upgrade. Follow these guidelines when setting up a server:
  - Ensure that your TFTP server supports files that are larger than the size of controller software image. Some TFTP servers that support files of this size are tftpd32 and the TFTP server within Cisco Prime Infrastructure. If you attempt to download the controller software image and your TFTP server does not support files of this size, the following error message appears:

```
TFTP failure while storing in flash
```

- If you are upgrading through the distribution system network port, the TFTP or FTP server can be on the same subnet or a different subnet because the distribution system port is routable.
- The controller Bootloader stores a copy of the active primary image and the backup image. If the primary image becomes corrupted, you can use the Bootloader to boot with the backup image.

With the backup image stored before rebooting, from the **Boot Options** menu, choose **Option 2: Run Backup Image** to boot from the backup image. Then, upgrade with a known working image and reboot controller.

- You can control the addresses that are sent in the Control and Provisioning of Wireless Access Points (CAPWAP) discovery responses when NAT is enabled on the Management Interface, using the following command:

```
config network ap-discovery nat-ip-only {enable | disable}
```

The following are the details of the command:

**enable**—Enables use of NAT IP only in a discovery response. This is the default. Use this command if all the APs are outside the NAT gateway.

**disable**—Enables use of both NAT IP and non-NAT IP in a discovery response. Use this command if APs are on the inside and outside the NAT gateway, for example, Local Mode and OfficeExtend APs are on the same controller.



---

**Note** To avoid stranding of APs, you must disable the AP link latency (if enabled) before you use the disable option in the **config network ap-discovery nat-ip-only** command. To disable AP link latency, use the **config ap link-latency disable all** command.

---

- Do not power down the controller or any AP during the upgrade process. If you do this, the software image might get corrupted. Upgrading the controller with a large number of APs can take as long as 30 minutes, depending on the size of your network. However, with the increased number of concurrent AP upgrades supported, the upgrade time should be significantly reduced. The APs must remain powered, and controller must not be reset during this time.
- After you perform the following functions on the controller, reboot it for the changes to take effect:
  - Enable or disable LAG.
  - Enable a feature that is dependent on certificates (such as HTTPS and web authentication).
  - Add a new license or modify an existing license.



---

**Note** Reboot is not required if you are using Right-to-Use licenses.

---

- Increase the priority of a license.
- Enable HA.
- Install the SSL certificate.
- Configure the database size.
- Install the vendor-device certificate.
- Download the CA certificate.
- Upload the configuration file.
- Install the Web Authentication certificate.
- Make changes to the management interface or the virtual interface.

## Upgrading Cisco Wireless Software (GUI)

### Procedure

- 
- Step 1** Upload your controller configuration files to a server to back up the configuration files.
- Note** We highly recommend that you back up your controller configuration files prior to upgrading the controller software.
- Step 2** Follow these steps to obtain controller software:
- Browse to the Software Download portal at: <https://software.cisco.com/download/home>.
  - Search for the controller model.
  - Click **Wireless LAN Controller Software**.
  - The software releases are labeled as described here to help you determine which release to download. Click a controller software release number:
    - Early Deployment (ED)—These software releases provide new features and new hardware platform support as well as bug fixes.
    - Maintenance Deployment (MD)—These software releases provide bug fixes and ongoing software maintenance.
    - Deferred (DF)—These software releases have been deferred. We recommend that you migrate to an upgraded release.
  - Click the filename *<filename.aes>*.
  - Click **Download**.
  - Read the Cisco End User Software License Agreement and click **Agree**.
  - Save the file to your hard drive.
  - Repeat steps *a* through *h* to download the remaining file.
- Step 3** Copy the controller software file *<filename.aes>* to the default directory on your TFTP, FTP, SFTP, or USB server.
- Step 4** (Optional) Disable the controller 802.11 networks.
- Note** For busy networks, controllers on high utilization, and small controller platforms, we recommend that you disable the 802.11 networks as a precautionary measure.
- Step 5** Choose **Commands > Download File** to open the **Download File to Controller** page.
- Step 6** From the **File Type** drop-down list, choose **Code**.
- Step 7** From the **Transfer Mode** drop-down list, choose **TFTP**, **FTP**, **SFTP**, **HTTP**, or **USB**.
- Step 8** Enter the corresponding server details as prompted.
- Note** Server details are not required if you choose HTTP as the transfer mode.
- Step 9** Click **Download** to download the software to the controller.
- A message indicating the status of the download is displayed.
- Note** Ensure that you choose the **File Type** as **Code** for both the images.

- Step 10** After the download is complete, click **Reboot**.
- Step 11** If you are prompted to save your changes, click **Save and Reboot**.
- Step 12** Click **OK** to confirm your decision to reboot the controller.
- Step 13** If you have disabled the 802.11 networks, reenale them.
- Step 14** (Optional) To verify that the controller software is installed on your controller, on the controller GUI, click **Monitor** and view the **Software Version** field under **Controller Summary**.

## CIMC Utility Upgrade for 5520 and 8540 Controllers

The AIR-CT5520-K9 and AIR-CT8540-K9 controller models are based on Cisco UCS server C series, C220 and C240 M4 respectively. These controller models have CIMC utility that can edit or monitor low-level physical parts such as power, memory, disks, fan, temperature, and provide remote console access to the controllers.

We recommend that you upgrade the CIMC utility to a version that has been certified to be used with these controllers. Controllers that have older versions of CIMC installed are susceptible to rebooting without being able to access FlexFlash, with the result that the manufacturing certificates are unavailable, and thus SSH and HTTPS connections will fail, and access points will be unable to join. See: [CSCvo33873](#). The recommended versions addresses the vulnerability tracked in [CSCvo01180](#) caveat.

The certified CIMC images are available at the following locations:

**Table 3: CIMC Utility Software Image Information**

Controller	Current CIMC Version	Recommended CIMC Version	Link to Download the CIMC Utility Software Image
Cisco 5520 Wireless Controller Cisco 8540 Wireless Controller	2.x	3.0(4r)	<a href="https://software.cisco.com/download/home/286281345/type/283850974/release/3.0(4r)">https://software.cisco.com/download/home/286281345/type/283850974/release/3.0(4r)</a>  <b>Note</b> We recommend you to upgrade the firmware from 2.0(13i) to 3.0(4r) using TFTP, SCP protocols only.
Cisco 5520 Wireless Controller Cisco 8540 Wireless Controller	3.0(4d)	3.0(4r)	<a href="https://software.cisco.com/download/home/286281345/type/283850974/release/3.0(4r)">https://software.cisco.com/download/home/286281345/type/283850974/release/3.0(4r)</a>
Cisco 5520 Wireless Controller Cisco 8540 Wireless Controller	4.0(1a)	4.0(2n)	<a href="https://software.cisco.com/download/home/286281345/type/283850974/release/4.0(2n)">https://software.cisco.com/download/home/286281345/type/283850974/release/4.0(2n)</a>

**Table 4: Firmware Upgrade Path to 4.x version**

Current Firmware Version	Upgrade Path to 4.x version
2.x	You must upgrade to a 3.x version and then upgrade to the recommended 4.x version.
3.x	You can upgrade directly to the recommended 4.x version.

- For information about upgrading the CIMC utility version 2.x , see the *Introduction to Cisco IMC Secure Boot* section in the *Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 3.0*:

[https://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/c/sw/cli/config/guide/3\\_0/b\\_Cisco\\_UCS\\_C-Series\\_CLI\\_Configuration\\_Guide\\_301/b\\_Cisco\\_UCS\\_C-Series\\_CLI\\_Configuration\\_Guide\\_201\\_chapter\\_01101.html#d92865e458a1635](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/cli/config/guide/3_0/b_Cisco_UCS_C-Series_CLI_Configuration_Guide_301/b_Cisco_UCS_C-Series_CLI_Configuration_Guide_201_chapter_01101.html#d92865e458a1635)

For information about upgrading the CIMC utility version 2.x using webUI , see the *Updating the Firmware* section [https://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/c/sw/gui/config/guide/3\\_0/b\\_Cisco\\_UCS\\_C-Series\\_GUI\\_Configuration\\_Guide\\_for\\_HTML5\\_Based\\_Servers\\_301/b\\_Cisco\\_UCS\\_C-Series\\_GUI\\_Configuration\\_Guide\\_207\\_chapter\\_01101.html#task\\_C137961E9E8A4927A1F08740184594CA](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/gui/config/guide/3_0/b_Cisco_UCS_C-Series_GUI_Configuration_Guide_for_HTML5_Based_Servers_301/b_Cisco_UCS_C-Series_GUI_Configuration_Guide_207_chapter_01101.html#task_C137961E9E8A4927A1F08740184594CA).



**Note** When upgrading the firmware using the webUI method, you must select **Install Firmware through Remote Server** option when prompted in the webUI.

- For information about upgrading the CIMC utility, see the *Updating the Firmware on Cisco UCS C-Series Servers* chapter in the *Cisco Host Upgrade Utility 3.0 User Guide*:

[https://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/c/sw/lomug/2-0-x/3\\_0/b\\_huu\\_3\\_0\\_1/b\\_huu\\_2\\_0\\_13\\_chapter\\_011.html](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/lomug/2-0-x/3_0/b_huu_3_0_1/b_huu_2_0_13_chapter_011.html)

**• Updating Firmware Using the Update All Option**

This section mentions specific details when using CIMC utility with Cisco 5520 or 8540 controllers. For general information about the software and UCS chassis, see *Release Notes for Cisco UCS C-Series Software, Release 3.0(4)* at:

[https://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/release/notes/b\\_UCS\\_C-Series\\_Release\\_Notes\\_3\\_0\\_4.html](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/release/notes/b_UCS_C-Series_Release_Notes_3_0_4.html)

*Release Notes for Cisco UCS C-Series Software, Release 4.0(2)* at:

[https://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/release/notes/b\\_UCS\\_C-Series\\_RN\\_4\\_0\\_2.html](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/release/notes/b_UCS_C-Series_RN_4_0_2.html)

**Table 5: Resolved Caveats for Release 4.0(2f)**

Caveat ID	Description
CSCvn80088	NI-HUU fails to handle the special characters in the password of CIFS remote share

**Table 6: Resolved Caveats for Release 3.0(4I)**

Caveat ID	Description
<a href="#">CSCvp41543</a>	SSH weak KeyExchange algorithm [diffie-hellman-group14-sha1] has to be removed

## Interoperability with Other Clients

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

The following table describes the configuration that is used for testing the client devices.

**Table 7: Test Bed Configuration for Interoperability**

Hardware or Software Parameter	Hardware or Software Configuration Type
Release	8.10.x
Cisco Wireless Controller	Cisco 3504 Wireless Controller
Access Points	Cisco 9130, 9120 and 3800 APs
Radio	802.11ax (2.4 GHz or 5 GHz), 802.11ac, 802.11a, 802.11g, 802.11n (2.4 GHz or 5 GHz)
Security	Open, WPA3-SAE/OWE ( WPA3 Supported Clients), WPA2+WPA3 ( Mixed Mode) PSK (WPA2-AES), 802.1X (WPA2-AES)(EAP-PEAP)
RADIUS	Cisco ISE 2.5
Types of tests	Association, Traffic ( TCP/UDP/ICMP) and Roaming between APs

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

**Table 8: Client Types**

Client Type and Name	Driver / Software Version
<b>Wi-Fi 6 Devices (Mobile Phone and Laptop)</b>	
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)

<b>Client Type and Name</b>	<b>Driver / Software Version</b>
Samsung Galaxy S10+	Android 9.0
Samsung Galaxy Fold 2	Android 10
Samsung Galaxy Flip Z	Android 10
Samsung Note 20	Android 10
<b>Laptops</b>	
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)
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)
<b>Note</b>	For clients using Intel wireless cards, we recommend you to update to the latest Intel wireless drivers if advertised SSIDs are not visible.
<b>Tablets</b>	

<b>Client Type and Name</b>	<b>Driver / Software Version</b>
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)
<b>Mobile Phones</b>	
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
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

<b>Client Type and Name</b>	<b>Driver / Software Version</b>
Oppo Find X2	Android 10
Redmi K20 Pro	Android 10
Samsung Galaxy S7	Android 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 Xperia 1 ii	Android 10
Sony Xperia 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 Ver: 4.1.1
Zebra MC92N0	Android Ver: 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
Zebra TC70	Android 6.1
Zebra TC75	Android 6.1.1
<b>Printers</b>	
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
<b>Wireless Module</b>	

Client Type and Name	Driver / Software Version
Intel I1ax 200	Driver v21.40.1.3, v21.20.1.1
Intel AC 9260	Driver v21.40.0
Intel Dual Band Wireless AC 8260	Driver v19.50.1.6

## Key Features Not Supported in Controller Platforms

This section lists the features that are not supported on various controller platforms:




---

**Note** In a converged access environment that has controllers running AireOS code, High Availability Client SSO and native IPv6 are not supported.

---

### Key Features Not Supported in Cisco 3504 Wireless Controller

- Cisco WLAN Express Setup Over-the-Air Provisioning
- Mobility controller functionality in converged access mode
- VPN Termination (such as IPsec and L2TP)

### Key Features Not Supported in Cisco 5520 and 8540 Wireless Controllers

- Internal DHCP Server
- Mobility controller functionality in converged access mode
- VPN termination (such as IPsec and L2TP)
- Fragmented pings on any interface

### Key Features Not Supported in Cisco Virtual Wireless Controller

- Cisco Umbrella
- Software-defined access
- Domain-based ACLs
- Internal DHCP server
- Cisco TrustSec
- Access points in local mode
- Mobility or Guest Anchor role
- Wired Guest
- Multicast




---

**Note** FlexConnect locally switched multicast traffic is bridged transparently for both wired and wireless on the same VLAN. FlexConnect APs do not limit traffic based on IGMP or MLD snooping.

---

- FlexConnect central switching in large-scale deployments




---

**Note**

- FlexConnect central switching is supported in only small-scale deployments, wherein the total traffic on controller ports is not more than 500 Mbps.
- FlexConnect local switching is supported.

---

- Central switching on Microsoft Hyper-V deployments
- AP and Client SSO in High Availability
- PMIPv6
- Datagram Transport Layer Security (DTLS)
- EoGRE (Supported only in local switching mode)
- Workgroup bridges
- Client downstream rate limiting for central switching
- SHA2 certificates
- Controller integration with Lync SDN API
- Cisco OfficeExtend Access Points

## Key Features Not Supported in Access Point Platforms

This section lists the key features that are not supported on various Cisco Aironet AP platforms. For detailed information about feature support on Cisco Aironet Wave 2 and 802.11ax APs, see:

[https://www.cisco.com/c/en/us/td/docs/wireless/access\\_point/feature-matrix/ap-feature-matrix.html](https://www.cisco.com/c/en/us/td/docs/wireless/access_point/feature-matrix/ap-feature-matrix.html)

## Key Features Not Supported in Cisco Aironet 1800i, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800, 3800, and 4800 Series APs

*Table 9: Key Features Not Supported in Cisco Aironet 1800i, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800, 3800, and 4800 Series APs*

Operational Modes	<ul style="list-style-type: none"> <li>• Autonomous Bridge and Workgroup Bridge (WGB) mode           <ul style="list-style-type: none"> <li><b>Note</b> WGB is supported in Cisco Aironet 2800, 3800 Series APs.</li> </ul> </li> <li>• Mesh mode           <ul style="list-style-type: none"> <li><b>Note</b> Mesh mode is supported in Cisco Aironet 1815i, 1815m, 1830, 1850, 2800, 3800, and 4800 Series APs in Release 8.10.x.</li> </ul> </li> <li>• LAG behind NAT or PAT environment</li> </ul>
Protocols	<ul style="list-style-type: none"> <li>• Full Cisco Compatible Extensions (CCX) support</li> <li>• Rogue Location Discovery Protocol (RLDP)</li> <li>• Telnet</li> </ul>
Security	<ul style="list-style-type: none"> <li>• CKIP, CMIC, and LEAP with Dynamic WEP</li> <li>• Static WEP for CKIP</li> <li>• WPA2 + TKIP           <ul style="list-style-type: none"> <li><b>Note</b> WPA +TKIP and TKIP + AES protocols are supported.</li> </ul> </li> </ul>
Quality of Service	<p>Cisco Air Time Fairness (ATF)</p> <ul style="list-style-type: none"> <li><b>Note</b> ATF is supported in Cisco Aironet 2800, 3800, and 4800 Series APs in Release 8.10.</li> </ul>
FlexConnect Features	<ul style="list-style-type: none"> <li>• PPPoE</li> <li>• Multicast to Unicast (MC2UC)           <ul style="list-style-type: none"> <li><b>Note</b> VideoStream is supported</li> </ul> </li> <li>• Traffic Specification (TSpec)           <ul style="list-style-type: none"> <li>• Cisco Compatible eXtensions (CCX)</li> <li>• Call Admission Control (CAC)</li> </ul> </li> <li>• VSA/Realm Match Authentication</li> <li>• SIP snooping with FlexConnect in local switching mode</li> </ul>



**Note** For Cisco Aironet 1850 Series AP technical specifications with details on currently supported features, see the [Cisco Aironet 1850 Series Access Points Data Sheet](#).

## Key Features Not Supported in Cisco Aironet 1800i, 1810 OEAP, and 1810W Series APs

*Table 10: Key Features Not Supported in Cisco Aironet 1800i, 1810 OEAP, and 1810W Series APs*

Operational Modes	Mobility Express
FlexConnect Features	Local AP authentication
Location Services	Data RSSI (Fast Locate)

## Key Features Not Supported in Cisco Aironet 1830, 1850, and 1815 Series APs

*Table 11: Key Features Not Supported in Cisco Aironet 1830, 1850, and 1815 Series APs*

Operational Modes	Mobility Express is not supported in Cisco 1815t APs.
FlexConnect Features	Local AP Authentication
Location Services	Data RSSI (Fast Locate)

## Key Features Not Supported in Mesh Networks

- Load-based call admission control (CAC). Mesh networks support only bandwidth-based CAC or static CAC
- High availability (Fast heartbeat and primary discovery join timer)
- AP acting as supplicant with EAP-FASTv1 and 802.1X authentication
- AP join priority (Mesh APs have a fixed priority)
- Location-based services

## Key Features Not Supported in Cisco Aironet 1540 Mesh APs

- Dynamic Mesh backhaul data rate.



**Note** We recommend that you keep the Bridge data rate of the AP as auto.

- Background scanning
- Noise-tolerant fast convergence

## Key Features Not Supported on Cisco Aironet 1560 APs

- MAC Authentication FlexConnect Local Authentication
- Noise-tolerant fast convergence
- Static WEP

## Key Features Not Supported on Cisco Catalyst IW6300 Heavy Duty Series AP and 6300 Series Embedded Services AP

- MAC Authentication FlexConnect Local Authentication
- Noise-tolerant fast convergence
- Static WEP

## Unfixed and Fixed Issues in Release 8.10.190.0

### Open Caveats

**Table 12: Open Caveats**

Identifier	Headline
<a href="#">CSCvv30453</a>	Cisco 1800APs: add FW checksum and auto refresh to avoid FW assert radio crash by bitflip
<a href="#">CSCvv83264</a>	Cisco 9120AX AP Correctable ECC Error detected when booting up
<a href="#">CSCvw70260</a>	Cisco Aironet 1572EAC Access Point does not respond to the Canadian EIRP regulation
<a href="#">CSCvy59547</a>	GUI displays incorrect tagged VLAN data
<a href="#">CSCvz35716</a>	Cisco 3802 AP: ME Controller reloads unexpectedly with OOM due to: process naconnector
<a href="#">CSCvz59191</a>	APs do not send NDP packets on slot 1
<a href="#">CSCvz86461</a>	Cisco 9120AX AP Not Forwarding the EAP Identity Request Downstream over the air
<a href="#">CSCvz95502</a>	WGB Wired Clients MAC Flapping Between The Actual Port And the WGB Switch Port
<a href="#">CSCvz96924</a>	Cisco 9130 Access Point does not send M1 over the Air
<a href="#">CSCwa06456</a>	Cisco 9130AX AP on 17.6.2 EFT software: radio FW/ucode crash
<a href="#">CSCwa14744</a>	Cisco 9130AX AP reloads unexpectedly due to PC is at __qdf_bug+0x0/0x8 osif_delete_vap_wait_and_free

Identifier	Headline
<a href="#">CSCwa19345</a>	Cisco 9115AX AP: assert:"SCB_DEL_IN_PROGRESS(scbb)" failed: "wlc_assoc.c:11911" wl: Bad Address
<a href="#">CSCwa31596</a>	Cisco 9130AX AP: high channel utilization and client lags with 9 or more clients using MS TEAMS
<a href="#">CSCwa33537</a>	Cisco 9117AX AP radio reloads unexpectedly
<a href="#">CSCwa49112</a>	Cisco 3802 FQI/NMI reset: loop_delay & wlRecv
<a href="#">CSCwa52440</a>	Cisco 9117AX AP reloads unexpectedly due radio failure(radio recovery failed)Beacons stuck on Radio1
<a href="#">CSCwa53592</a>	Cisco 9120AX APs show as Flexible Radio Assignment (FRA) not capable on 17.3.4c release
<a href="#">CSCwa53727</a>	Cisco 9117AX AP reloads unexpectedly at cmnos_thread.c:3493
<a href="#">CSCwa53745</a>	Cisco 9117AX AP reloads unexpectedly at whal_recv.c:629
<a href="#">CSCwa53763</a>	Cisco 9117AX AP reloads unexpectedly at whal_xmit.c:3663
<a href="#">CSCwa54943</a>	Cisco 1810 AP restarts abnormally on the controller due to Out of Memory
<a href="#">CSCwa73818</a>	Cisco 9130AX AP radio firmware crash: ar_wal_peer.c:8149 Assertion !WAL_IS_TID_QOS_DATA
<a href="#">CSCwa75050</a>	Factory reset via physical button is not always working
<a href="#">CSCwa76008</a>	The value of "Channel Center Segment 0" in " VHT Operation Info"
<a href="#">CSCwa76206</a>	Kernel panic : PC is at mv_pp3_dev_open+0xbfc/0x1014 on 17.3.5EFT
<a href="#">CSCwa76218</a>	Kernel panic : PC is at pci_common_init_dev+0xa4/0x2c0 on 17.3.5EFT
<a href="#">CSCwa78281</a>	Getting RRM errors when U3 stats feature disabled on Cisco Wave 2 APs
<a href="#">CSCwa79564</a>	Cisco 2800,3800 APs on 8.10.162: Power Type displayed is incorrect when static power is set to 15.4W
<a href="#">CSCwa81190</a>	Null pointer de-reference in wlc_wnm_is_wnmsleeping
<a href="#">CSCwa95705</a>	Cisco 2802 AP reloads unexpectedly due to FIQ/NMI reset

## Resolved Caveats

**Table 13: Resolved Caveats**

Identifier	Headline
<a href="#">CSCvi48253</a>	Self-signed certificates expire on 00:00 1 Jan 2020 UTC, cannot be created after the time expires

Identifier	Headline
<a href="#">CSCvm06514</a>	ME: Internal error, Lock of ipv6_sisf_engine_semaphore failed when IPv6 is disabled globally
<a href="#">CSCvs77557</a>	Cisco Aironet 3802 AP is not able to acknowledge EAP frames (EAP-TLS)
<a href="#">CSCvu22886</a>	C9130: message "unlzma: write: No space left on device" on upgrade to 17.7 Increase max size of /tmp
<a href="#">CSCvu75017</a>	Cisco Wave2 and 802.11AX APs syslog only seen when using "Kern" facility value in AP join profile
<a href="#">CSCvw00282</a>	Cisco 1852 AP: Kernel panic - not syncing: softlockup: hung tasks
<a href="#">CSCvw70285</a>	Cisco Catalyst 9120 APs cannot send acknowledgement over the air during EAP negotiation
<a href="#">CSCvw76804</a>	Cisco Aironet 3802 AP drops Zebra client traffic intermittently after fast transition roams
<a href="#">CSCvw84028</a>	Cisco 9120 AP unexpectedly reloads due to Radio driver
<a href="#">CSCvw93936</a>	Cisco 9115, AP9120 APs: Wireless client SNR value shown as 0 on Client 360 page
<a href="#">CSCvx01028</a>	COS AP does not accept WPA2-PSK password on WGB with special character but works fine in IOS AP
<a href="#">CSCvx37663</a>	Cisco Aironet 1832 AP displays /usr/sbin/capwapd: writing to fd 17 failed!: Input/output error
<a href="#">CSCvx47787</a>	UE does not roam from Macro to Micro Cell on AP2800 with dual 5-GHz radios
<a href="#">CSCvx61201</a>	Clients get incorrect AP VLAN IP with Cisco Aironet 2800 AP in flex mode
<a href="#">CSCvx62287</a>	17.6: WLAN client fails to associate when switching between WLANs on wpa3-sae in flex: local auth
<a href="#">CSCvx84524</a>	Cisco Aironet 1570 AP does not display the RRM neighbors
<a href="#">CSCvx96224</a>	Numerous core dumps are observed in Cisco Aironet 2800 and 3800 APs slot 1 radios
<a href="#">CSCvx98176</a>	Access point with 17.6 image cannot join AireOS controller
<a href="#">CSCvx99197</a>	Cisco Catalyst 9120 AP reloads unexpectedly after an upgrade to 8.10.158.38 failed to add RFIC image
<a href="#">CSCvx99417</a>	C9130AX AP connected client is randomly stuck in IP learning state when BSS coloring is enabled
<a href="#">CSCvy03587</a>	Macbook clients are stuck in IPLEARN_PENDING status
<a href="#">CSCvy03953</a>	Kernel panic crash is observed in Cisco Catalyst 9130 AP
<a href="#">CSCvy10074</a>	Kernel slab memory leaks are observed in Cisco Aironet 3800 AP on flex local switching WLAN

Identifier	Headline
<a href="#">CSCvy11334</a>	The non-Wi-Fi channel utilization shows 41
<a href="#">CSCvy13594</a>	Cisco Catalyst 9130 AP experiences radio firmware crash on Radio 1 multiple times a day
<a href="#">CSCvy17092</a>	CSA event after Radar detection is missed in the driver
<a href="#">CSCvy30091</a>	Cisco Catalyst 9120 AP stops transmitting to Macbook after a session re-authentication
<a href="#">CSCvy34827</a>	Controller not sending "termination request" to the LMA, when client disconnects
<a href="#">CSCvy40772</a>	Smart license configuration is missing from the backup file on Cisco 3504 controllers
<a href="#">CSCvy44800</a>	AP forgets its TAG after a second reboot or CAPWAP restart
<a href="#">CSCvy46806</a>	802.11ax AP BSS Color Global Config push from Controller not applied to AP Groups
<a href="#">CSCvy48763</a>	Cisco 9130AP Kernel panic crash after N+1 failover or fallback
<a href="#">CSCvy52874</a>	Cisco Catalyst 9115 AP reloads unexpectedly after loading the 17.3.3 ES6 image
<a href="#">CSCvy54374</a>	Controller sends Association Response with status 53 for Apple iPhoneXS iPhoneX
<a href="#">CSCvy55727</a>	Cisco Aironet 1832 AP ends abnormally due to "translation fault"
<a href="#">CSCvy59897</a>	Cisco COS APs detects its own BSSID as rogue
<a href="#">CSCvy60772</a>	8.10_stale entry noticed on the controller
<a href="#">CSCvy61021</a>	Controller running 8.5.176.0 image reloads unexpectedly due to memory corruption
<a href="#">CSCvy62022</a>	Roaming client stops receiving IP multicast in a new Cisco Aironet 3800 AP
<a href="#">CSCvy62990</a>	Cisco controller silently reloads unexpectedly due to memory leak.
<a href="#">CSCvy67399</a>	Controller switchover occurs unexpectedly due to memory leak
<a href="#">CSCvy75868</a>	Cisco Wave 2 APs reload unexpectedly due to kernel panic
<a href="#">CSCvy77144</a>	Flex local-sw COS-APs not plumbing preauth ACL for first client connection attempt for CWA and EWA
<a href="#">CSCvy79320</a>	Increased Ping loss after two days of reboot
<a href="#">CSCvy80084</a>	Need to update BCM Tx/Rx error stats
<a href="#">CSCvy81859</a>	Packet drops are observed at device driver level
<a href="#">CSCvy85178</a>	4800 APs in ELM and Local mode on same controller/same RF group are detecting each other as honeypot
<a href="#">CSCvy91441</a>	Cisco Aironet 2802 AP experiences radio crash

Identifier	Headline
<a href="#">CSCvy94725</a>	Cisco Aironet 2800 and 3800 APs experience Kernel Panic Driver crash when PC is at wLRxRingCleanup
<a href="#">CSCvy95264</a>	Workgroup bridge (WGB) cannot associate when PSK password contains special characters
<a href="#">CSCvy95842</a>	Connected AP with non-EWC image undergoes factory reset after reload when DHCP option 43 is set
<a href="#">CSCvz02579</a>	C9130AXI AP cannot connect to the controller after shut or no shut on a C9300-48H switch interface
<a href="#">CSCvz05501</a>	Cisco Aironet 2800 AP FW crash is observed in Radio 0
<a href="#">CSCvz05686</a>	Cisco Aironet 2802 or 3802 AP fails to bring up its radios and continuously logs messages
<a href="#">CSCvz06937</a>	Cisco Catalyst 9120 AP FW crash is observed in Radio 1
<a href="#">CSCvz09846</a>	Cisco Catalyst 9130 AP stale clients in the radio driver table causes associations to fail
<a href="#">CSCvz09942</a>	Cisco Catalyst 9120AXI AP displays kernel panic in Cisco IOS-XE 17.3.4.30
<a href="#">CSCvz16800</a>	AireOS is unable to receive M2 from MAC addresses with 0x888e in the middle octet (central auth)
<a href="#">CSCvz18980</a>	Opportunistic Key Caching (OKC) is not pushed from the controller to AP when applied in CLI
<a href="#">CSCvz21627</a>	Cisco 3800/4800 WIPS AP does not list few BSSIDs in RRM neighbor list causing false honeypot alarms
<a href="#">CSCvz24841</a>	Retried 802.11r auth packet forwarded to controller causes duplicate auth responses sent to client
<a href="#">CSCvz25183</a>	COS AP fragmenting CAPWAP discovery packets are unable to join the controller
<a href="#">CSCvz30883</a>	Cisco 9120 AP running 17.3.4ES2 is facing RX stuck not ACKing any of the received frames
<a href="#">CSCvz34172</a>	Cisco 1832 AP experiences kernel panic while setting client ACL in Cisco IOS XE 17.3.4
<a href="#">CSCvz36463</a>	Cisco Catalyst 9130 AP flashes insufficient power LED when USB is enabled on PoE+ Switch
<a href="#">CSCvz40749</a>	COS AP Probe filter to limit unwanted probes from AP to Controller not working
<a href="#">CSCvz42194</a>	Controller constantly reloading due to switch-driver crash ,(Version: 8.10.162.0)
<a href="#">CSCvz43397</a>	Unexpected string interleaves CLI output on Controller-ME show run-config commands

Identifier	Headline
<a href="#">CSCvz44787</a>	Cisco Catalyst 9120AXE AP displays incorrect PID and description for Self Identifying Antenna
<a href="#">CSCvz46237</a>	Cisco Catalyst 9130 AP reloads unexpectedly on 17.3.4 CCO version
<a href="#">CSCvz49187</a>	Cisco Catalyst 9120 Series AP sends packets with QoS TID when WMM is disabled on WLAN
<a href="#">CSCvz55681</a>	Unexpected system reload is observed in C9120AXI-B APs joined to C9800-CL running Cisco 17.6.1
<a href="#">CSCvz56061</a>	Mobility Express can't input WLAN user information CSV file on GUI
<a href="#">CSCvz57427</a>	AP reports disassoc reason of 'Link failure' as AP reloads unexpectedly
<a href="#">CSCvz58365</a>	Cisco Catalyst 9130 APs unexpectedly reboot due to kernel panic
<a href="#">CSCvz58499</a>	Cisco Catalyst 9120 AP reloads unexpectedly due to kernel panic on 2.4-GHz band
<a href="#">CSCvz59574</a>	Cisco Catalyst 9130 AP: Radio operates in channel 128 and publishes in channel 56
<a href="#">CSCvz62197</a>	Controller reloads unexpectedly in spamApTask process with NtpServerSyncPayload
<a href="#">CSCvz64239</a>	Cisco Aironet 1815 APs reloads unexpectedly and radio would not come up
<a href="#">CSCvz64295</a>	17.3.4 - 1815 - FW assert issue
<a href="#">CSCvz66798</a>	C9120 AP FlexConnect drops ARP request from client to gateway after a WLAN change (local to central)
<a href="#">CSCvz69441</a>	Cisco Catalyst 9115 AP reloads unexpectedly due to kernel panic PC
<a href="#">CSCvz75232</a>	Cisco 8540 HA reloads unexpectedly due to pmalloc double free (capwap_ac_sm.c)
<a href="#">CSCvz79327</a>	AP 1832 reloads unexpectedly due to radio failure - Beacon Stuck - reset radio for recovery
<a href="#">CSCvz87088</a>	Cisco Catalyst 9120 APs in monitor mode cannot update neighbor-list causing false honeypot alarms
<a href="#">CSCvz89108</a>	9120 -NDP Received frames from neighbour AP with RSSI lower than configured RxSOP
<a href="#">CSCvz94267</a>	Cisco Catalyst 9130 APs reloads unexpectedly after upgrading to 17.3.4 and applying the ESW7 image
<a href="#">CSCvz94692</a>	AP reloads unexpectedly due to: radio failure(too many radio failures)
<a href="#">CSCvz95465</a>	Cisco 9117 AP reloads unexpectedly due to kernel panic dp_rx_process
<a href="#">CSCvz95929</a>	[HCA] PSM microcode watchdog with Cisco 9120 APs
<a href="#">CSCvz96432</a>	Cisco 8540 HA controller resets due to unexpected system reload (spamApTask)

Identifier	Headline
<a href="#">CSCvz99449</a>	APs make too many connections to Identitymgmt causing Identitymgmt to crash
<a href="#">CSCvz99492</a>	Cisco Catalyst 9130 AP unexpectedly reloads with a kernel panic
<a href="#">CSCwa01142</a>	Cisco 9120 APs not responding to client association requests
<a href="#">CSCwa06321</a>	Cisco 9120 AP: Change parameter under WLAN will reset 9120 AP radio
<a href="#">CSCwa08875</a>	Cisco Aironet 3800 series AP crash due to kernel panic (PC is at vfp_reload_hw+0x30/0x44)
<a href="#">CSCwa12204</a>	Cisco 9800 not sending the right AID causing AP's to not accept new clients
<a href="#">CSCwa12278</a>	Cisco 9115 AP reload unexpectedly due to Kernel panic - not syncing: Fatal exception
<a href="#">CSCwa18545</a>	Cisco 9120AP PS Pretend changng client to be in PS mode evn whn client is replying to QoS Null
<a href="#">CSCwa20219</a>	Cisco 9120 radio 1 gets stuck in Tx
<a href="#">CSCwa20827</a>	Cisco controller shows all 802.11AX clients are connected on 1 spatial stream
<a href="#">CSCwa24080</a>	Client cannot connect to tri-radio (slot 2)
<a href="#">CSCwa24962</a>	AireOS Controller Umbrella token name should be restricted to 25 characters
<a href="#">CSCwa26257</a>	Cisco 9120 AP Kernal crash
<a href="#">CSCwa30802</a>	MU sounding errors leading to TCQ stuck issue
<a href="#">CSCwa34136</a>	Cisco 3802 FQI/NMI reset at rb_next+0xc
<a href="#">CSCwa35428</a>	Cisco 9120 AP drops CAPWAP connection when running debug client
<a href="#">CSCwa36877</a>	Client fabric de-registration sent 10 seconds before the client is deleted, causing 10 sec outage
<a href="#">CSCwa38125</a>	Cisco 9130 AP Kernel Panic Crash __dma_inv_range in monitor path
<a href="#">CSCwa44403</a>	Cisco 5520 controller reloads unexpectedly on 8.10.51 in SSO mode
<a href="#">CSCwa45075</a>	AP reloads unexpectedly at FW assert at ar_wal_peer.c:1553
<a href="#">CSCwa45081</a>	Cisco 9130 AP reloads unexpectedly on KP at dp_rx_frag_handle+0x8c/0x8e0 [wifi_3_0]
<a href="#">CSCwa50159</a>	Cisco 9120 APs High Client Count while neighboring APs have very few clients associated
<a href="#">CSCwa53266</a>	Cisco 9120 AP: Randomly retains 802.11w client though it is deleted from the Controller
<a href="#">CSCwa57967</a>	Cisco 9130 AP Slot 2 Mode is changed to local when AP is working on FlexConnect mode

Identifier	Headline
<a href="#">CSCwa73245</a>	MU sounding errors leading to TCQ stuck issue
<a href="#">CSCwa73462</a>	Cisco 1832 AP Indonesia is not beaconing as expected causing client performance issue
<a href="#">CSCwa76198</a>	Kernel panic : PC is at txq_hw_fill+0x36c/0x1018 on 17.3.5EFT
<a href="#">CSCwa82660</a>	AP2800/AP3800 with CAC configured only updating QBSS_AAC sent by WLC after radio reset

## Related Documentation

### Wireless Products Comparison

- Use this tool to compare the specifications of Cisco wireless access points and controllers:  
<https://www.cisco.com/c/en/us/products/wireless/wireless-lan-controller/product-comparison.html>
- Product Approval Status:  
[https://prdapp.cloudapps.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL\\_SEARCH](https://prdapp.cloudapps.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL_SEARCH)
- Wireless LAN Compliance Lookup:  
<https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html>

### Cisco Wireless Controller

For more information about the controllers, lightweight APs, and mesh APs, see these documents:

- The quick start guide or the installation guide for your particular controller or access point
- [Cisco Wireless Solutions Software Compatibility Matrix](#)
- [Cisco Legacy Wireless Solutions Software Compatibility Matrix](#)
- [Cisco Wireless Controller Configuration Guide](#)
- [Cisco Wireless Controller Command Reference](#)
- [Cisco Wireless Controller System Message Guide](#)

For all controller software related documentation, see:

<http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/tsd-products-support-series-home.html>

### Cisco Mobility Express

- [Cisco Mobility Express Release Notes](#)
- [Cisco Mobility Express User Guide](#)
- [Cisco Aironet Universal AP Priming and Cisco AirProvision User Guide](#)

### Cisco Aironet Access Points for Cisco IOS Releases

- [Release Notes for Cisco Aironet Access Points for Cisco IOS Releases](#)
- [Cisco IOS Configuration Guides for Autonomous Aironet Access Points](#)
- [Cisco IOS Command References for Autonomous Aironet Access Points](#)

### Open Source Used in Controller and Access Point Software

Click this link to access the documents that describe the open source used in controller and access point software:

<https://www.cisco.com/c/en/us/about/legal/open-source-documentation-responsive.html>

### Cisco Prime Infrastructure

[Cisco Prime Infrastructure Documentation](#)

### Cisco Connected Mobile Experiences

[Cisco Connected Mobile Experiences Documentation](#)

### Cisco Digital Network Architecture

<https://www.cisco.com/c/en/us/support/wireless/dna-spaces/series.html>

## 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 DevNet](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

### Cisco Bug Search Tool

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

### Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

---

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)

© 2022 Cisco Systems, Inc. All rights reserved.