Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.10.121.0 and 8.10.122.0

First Published: 2020-04-04

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*.

Revision History

Table 1: Revision History

Modification Date	Modification Details
August 30, 2022	Added: Supported VIDs for Cisco Catalyst 9120 Access Points and Cisco Catalyst 9130 Access Points
June 05, 2020	Included Release 8.10.122.0 • Added: Resolved Caveats

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 9130 Access Points
  - 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

Note

- 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 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 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 8.10.122.0

There are no new features that are introduced in this release. For more information about updates in this release, see the Caveats section in this document.

Note We recommend that you use the controller GUI on a browser loaded with webadmin certificate (third-party certificate). We also recommend that you do not use the controller GUI on a browser loaded with self-signed certificate. Some rendering issues have been observed on Google Chrome (73.0.3675.0 or a later version) with self-signed certificates. For more information, see CSCvp80151.

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

What's New in Release 8.10.121.0

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

Important Upgrade Information

Cisco Wave 2 APs with FIPS in enabled state add an additional 10-minute delay to complete the FIPS checks on the APs before they can join the controller. Follow the software guidance for FIPS customers at:

https://www.cisco.com/c/en/us/products/collateral/wireless/8500-series-wireless-controllers/bulletin-c25-738147.html

Configuration Based Support for Cisco Catalyst 9130 Series Access Points Tri-Radio

The Cisco Catalyst 9130 Series Access Point is designed keeping high-density deployment in mind. Hence, this AP includes three radios all of which support the radio role assignment functionality. The AP supports radio roles—monitor and client serving roles.. You can manage the modes automatically by using the Flexible Radio Assignment(FRA) feature for 2.4-GHz radio and Dynamic Channel Assignment (DCA) feature for the two 5-GHz radios or manually using the CLI

Note For this release, the Tri-radio function for the Cisco Catalyst 9130AXE External AP is enabled only when using the DART adapter cables AIR-CAB-002-D8-R= (RP-TNC antennas) or AIR-CAB-003-D8-N= (“N” style antennas) with the AP.

For more information about configuring a tri-radio AP, see https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/managing_aps.html#info_tri_radio

Profile Name Matching for Mobility Anchor

Using this feature, you can prevent the anchor controller from picking the wrong WLAN which corresponds to the SSID name received from the foreign controller. This results in roaming and client association failures. This situation can occur because currently AireOS controllers can have two or more different WLANs with the same SSID. With the feature enabled, profile name associated with the SSID will be used in place of SSID as profile name is unique across the controllers.

The feature is disabled by default.

For more information about configuring profile name matching, see https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/mobility_groups.html#info_profile_match_mob_anchor

IP-MAC Context Distribution for FlexConnect Local Switching Clients

Using this feature, you can prevent IP theft and ARP spoofing within the same FlexConnect group. The controller distributes the client IP:MAC context to all the APs in the same FlexConnect group. When the client roams to a new AP, the AP uses the IP:MAC context to validate the client data.

You need to enable the DHCP Addr. Assignment and the FlexConnect Local Switching option in the controller settings for this feature to function.

For more information about configuring the IP-MAC feature, see https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/flexconnect.html#info_ip-mac_contenxt_flex_local_switching

Support for RLAN Local Switching with CAPWAP Down

Using this feature, you can create a redundancy data path for the client traffic when the controller not available. To achieve this functionality, when the controller is not available, the RLAN wired port is locally switched and the AP automatically switches to Local mode.

You may configure the network based on the following procedure:

1. Create three RLANs with different VLANs to isolate the network
2. Map these RLANs to each AP port
3. Enable POE to provide power to the IP Phone
4. AP switches over to Local Mode

Federal Information Processing Standard Support on Cisco Catalyst 9115, 9120, and 9130 Series Access Points

Federal Information Processing Standard (FIPS) mode support extends to Cisco Catalyst 9115, 9120, and 9130 Series Access Points.

IoT Features

- RAP Ethernet Daisy Chain STP Redundancy: Provides network redundancy over the existing daisy chain via STP ring topology.

  Supported AP platforms: Cisco Catalyst IW6300 Heavy Duty Series Access Points and Cisco 6300 Series Embedded Services Access Points.

For more information about the feature, see the *Cisco Catalyst IW6300 Heavy Duty Series Access Point Software Configuration Guide* at:

https://www.cisco.com/c/en/us/td/docs/wireless/outdoor_industrial/iw6300/software/config/guide/b_iw6300_scg.html

- Reliable WGB downstream multicast and broadcast for multiple VLANs.

  Supported AP platforms:

  - Cisco Catalyst IW6300 Heavy Duty Series Access Points
  - Cisco 6300 Series Embedded Services Access Points

- Supported WGB platforms

  - Cisco Catalyst Industrial Wireless 6300 Series Access Points
  - Cisco 6300 Series Embedded Services Access Points
  - Cisco Industrial Wireless 3700 Series Access Points

  For more information about the feature, see the **Reliable Transmission of Downstream Broadcast and Multicast with Multiple VLAN Support** section in the *Cisco Wireless Controller Configuration Guide, Release 8.10* at:

  https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/workgroup_bridges.html#id_135186

What's Changed in Release 8.10.121.0

This section provides information about the changes and enhancements that are introduced in this release.

Removed SNMP Default Credentials

To enhance security on the controller, the SNMPv2 community strings and SNMPv3 user credentials are no longer created by default. We recommend that you create the required credentials manually. A warning message is displayed if you have not configured the basic SNMP setup.

Configuring SNMP with Strong Passwords

Weak passwords are no longer allowed for SNMPv2 community strings and SNMPv3 user credentials. Strong password mode is enabled by default.

For more information about strong password policy, see https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/managing_users.html#ID1404

Configuring Over the Distribution System on a WLAN

When you create a WLAN, the **Over the DS** functionality, by default, is set to disabled state. The behavior during upgrade or downgrade procedure is as follows:

- During an upgrade from a previous release which does not include the fix, the **over-the-DS** value is set to disabled for all WLANs
- During a downgrade to a previous release which does not include the fix, the **over-the-DS** value is set to enabled for all WLANs

Software Release Types and Recommendations

Table 2: 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 3: Upgrade Path to Cisco Wireless Release 8.10.x

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

Current Software Release	Upgrade Path to Release 8.10.x
8.9.x	You can upgrade directly to Release 8.10.x.

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 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 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 configuation. 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:

a) Browse to the Software Download portal at: https://software.cisco.com/download/home.
b) Search for the controller model.
c) Click **Wireless LAN Controller Software**.
d) 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.

e) Click the filename <*filename.aes*>.
f) Click **Download**.
g) Read the Cisco End User Software License Agreement and click **Agree**.
h) Save the file to your hard drive.
i) 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, reenable 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 4: 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)	https://software.cisco.com/download/home/286281345/type/283850974/release/3.0(4r) **Note** 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)	https://software.cisco.com/download/home/286281345/type/283850974/release/3.0(4r)
Cisco 5520 Wireless Controller Cisco 8540 Wireless Controller	4.0(1a)	4.0(2n)	https://software.cisco.com/download/home/286281345/type/283850974/release/4.0(2n)

Table 5: 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 CIMS 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

  For information about upgrading the CIMS 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.

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

- **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

  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

Table 6: 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 7: Resolved Caveats for Release 3.0(4l)

Caveat ID	Description
CSCvp41543	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 8: 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	C9130, C9120
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 2.3, Cisco ISE 2.2
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 9: Client Types

Client Type and Name	Driver / Software Version
Wi-Fi 6 Devices (Mobile Phone and Laptop)	
Samsung Galaxy S10+	Android 9.0
Samsung S10 (SM-G973U1)	Android 9.0 (One UI 1.1)
Samsung S10e (SM-G970U1)	Android 9.0 (One UI 1.1)
Apple iPhone 11	iOS 13.2.1
DELL Latitude 5491 (Intel AX200)	Windows 10 Pro (21.40.2)
Laptops	

Client Type and Name	Driver / Software Version
Acer Aspire E 15 E5-573-3870 (Qualcomm Atheros QCA9377)	Windows 10 Pro (12.0.0.832)
Apple Macbook Air	OS Sierra v10.12.2
Apple Macbook Air 11 inch	OS X Yosemite 10.10.5
Apple Macbook Air 11 inch	OS Sierra 10.12.6
Apple Macbook Air 13 inch	OS High Sierra 10.13.4
Apple Macbook Pro	OS X 10.8.5
Macbook Pro Retina	OS Mojave 10.14.3
Macbook Pro Retina 13 inch early 2015	OS Mojave 10.14.3
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 Inspiron 15-7569 (Intel Dual Band Wireless-AC 3165)	Windows 10 Home (18.32.0.5)
DELL Inspiron 13-5368 Signature Edi (Intel Dual Band Wireless AC 3165	Win 10 Home (18.40.0.12)
DELL Latitude E5430 (Intel Centrino Advanced-N 6205)	Windows 7 Professional (15.18.0.1)
DELL Latitude E5540 (Intel Dual Band Wireless AC7260)	Windows 7 Professional (21.10.1)
DELL Latitude E6840 (Broadcom Dell Wireless 1540 802.11 a/g/n)	Windows 7 Professional (6.30.223.215)
DELL Latitude 3480 (Qualcomm DELL wireless 1820)	Win 10 Pro (12.0.0.242)
DELL XPS 12 v9250 (Intel Dual Band Wireless AC 8260)	Windows 10 (19.50.1.6)
DELL XPS 12 9250 (Intel Dual Band Wireless AC 8260)	Windows 10 Home (21.40.0)
FUJITSU Lifebook E556 Intel 8260 (Intel Dual Band Wireless AC 8260)	Windows 8 (19.50.1.6)
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 you to update to the latest Intel wireless drivers if advertised SSIDs are not visible.	
Tablets	
Apple iPad Air MD785LL/A	iOS 11.4.1

Client Type and Name	Driver / Software Version
Apple iPad Air 2 MGLW2LL/A	iOS 10.2.1
Apple iPad Air2 MGLW2LL/A	iOS 12.4.1
Apple iPad MD328LL/A	iOS 9.3.5
Apple iPad MD78LL/A	iOS 11.4.1
Apple iPad MGL12LL/A	iOS 9.1
Apple iPad mini 2 ME279LL/A	iOS 11.4.1
Apple iPad mini 2 ME279LL/A	iOS 12.0
Apple iPad mini 4 9.0.1 MK872LL/A	iOS 11.4.1
Apple iPad 2 MC979LL/A	iOS 9.3.1
Samsung Galaxy Tab A SM T350	Android 5.0.2
Samsung Galaxy Tab GT N5110	Android 4.4.2
Samsung Galaxy Tab SM-P 350	Android 6.0.1
Samsung Tab Pro SM-T320	Android 4.4.2
Toshiba Tab AT100	Android 4.0.4
Mobile Phones	
Apple iPhone 5	iOS 10.3.12
Apple iPhone 5c	iOS 10.3.3
Apple iPhone 7 MN8J2LL/A	iOS 11.2.5
Apple iPhone 8 plus	iOS 12.4.1
Apple iPhone 8 Plus MQ8D2LL/A	iOS 12.4.1
Apple iPhone MD237LL/A	iOS 9.3.5
Apple iPhone SE MLY12LL/A	iOS 11.3
Apple iPhone X MQA52LL/A	iOS 13.1
ASCOM Myco2	Build 2.1
ASCOM Myco2	Build 4.5
ASCOM Myco 3 v1.2.3	Android 8.1
ASUS Nexus 7	Android 6.0
AT100	Android 4.0.4
Drager Delta	VG9.0.2
Drager M300.3	VG2.4
Drager M300.4	VG2.4
Drager M540	DG6.0.2 (1.2.6)

Client Type and Name	Driver / Software Version
Google Pixel	Android 10
Google Pixel 3	Android 10
HTC One 6.0	Android 5.0.2
Huawei Mate 20 pro	Android 8.1
Huawei P20 Pro	Android 8.1
Huawei P7-L10	Android 4.4.2
LG v40 ThinQ	Android 9.0
Moto X 2nd gen	Android 5.0
Samsung Galaxy Mega GT-i9200	Android 4.4.2
Samsung Galaxy S10.P.1.4	Android 9
Samsung Galaxy S4	Android 4.2.2
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 Experia	Android 9.0
Spectralink 8440	Android 5.0.0.1079
Spectralink 8742	Android 5.1.1
Spectralink 8744	Android 5.1.1
Spectralink Versity Phones 9540	Android 8.1
Vocera Badges B3000n	4.3.1.17
Vocera Smart Badges V5000	5.0.2.163
Zebra MC40	Android Ver: 4.4.4
Zebra MC40N0	Android Ver: 4.1.1
Zebra MC55A	Windows 6.5
Zebra MC75A	OEM ver 02.37.0001
Zebra MC9090	Windows Mobile 6.1
Zebra MC92N0	Android Ver: 4.4.4
Zebra TC51	Android Ver: 6.0.1
Zebra TC52	Android Ver: 8.1.0
Zebra TC55	Android Ver: 8.1.0

Client Type and Name	Driver / Software Version
Zebra TC57	Android Ver: 8.1.0
Zebra TC8000	Android Ver: 4.4.3
Printers	
Zebra QLn320 Printer	LINK OS 6.0 v68.20.15Z
Zebra ZD410 Printer	LINK OS 6.0 v84.20.18Z
Zebra ZQ310 Printer	LINK OS 6.0 v68.20.15Z
Zebra ZQ610 Printer	LINK OS 6.0 v84.20.18Z
Zebra ZQ620 Printer	LINK OS 6.0 v85.20.19Z
Zebra ZT230 Printer	LINK OS 6.0 v72_20_18Z
Zebra ZT410 Printer	LINK OS 6.0 v84.20.18Z

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/wave2-ap/feature-matrix/b-wave2-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 10: Key Features Not Supported in Cisco Aironet 1800i, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800, 3800, and 4800 Series APs

Operational Modes	• Autonomous Bridge and Workgroup Bridge (WGB) mode **Note** WGB is supported in Cisco Aironet 2800, 3800 Series APs. • Mesh mode **Note** Mesh mode is supported in Cisco Aironet 1815i, 1815m, 1830, 1850, 2800, 3800, and 4800 Series APs in Release 8.10.x. • LAG behind NAT or PAT environment
Protocols	• Full Cisco Compatible Extensions (CCX) support • Rogue Location Discovery Protocol (RLDP) • Telnet • Internet Group Management Protocol (IGMP)v3
Security	• CKIP, CMIC, and LEAP with Dynamic WEP • Static WEP for CKIP • WPA2 + TKIP **Note** WPA +TKIP and TKIP + AES protocols are supported.
Quality of Service	Cisco Air Time Fairness (ATF) **Note** ATF is supported in Cisco Aironet 2800, 3800, and 4800 Series APs in Release 8.10.
FlexConnect Features	• PPPoE • Multicast to Unicast (MC2UC) **Note** VideoStream is supported • Traffic Specification (TSpec) • Cisco Compatible eXtensions (CCX) • Call Admission Control (CAC) • VSA/Realm Match Authentication • SIP snooping with FlexConnect in local switching mode

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 11: 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 12: 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 13: Open Caveats

Caveat ID Number	Description
CSCuy18812	Include SW port channel needed configuration for Cisco 1850AP
CSCvq90572	Cisco 2802AP Client negotiation rate decreases
CSCvq99108	Cisco 3700 AP series reloads unexpectedly due to reason 44
CSCvr07112	Cisco 2800 AP with data DTLS encryption enabled get a low throughput
CSCvr16233	Cisco 2802 AP beacon loss issue
CSCvs12882	Cisco 1850 APs not responding to dot11 authentication or association frames (SF 04358108)
CSCvs30363	Cisco 1852 AP: AP radio hangs causing packets drops, SF 04334576
CSCvs49476	Cisco 1815W AP on 8.10.105.0 code reloads unexpectedly with radio0FW coredumps (SF 04367723)
CSCvs52093	Cisco 2802 AP in Flex mode in only one site HTTPS packets from controller to Client getting drop
CSCvs71672	AP did not attach the VLAN tag on central switching change to FlexConnect local switching
CSCvs73405	Cisco 5508 controller clients profiled as unknown when doing local profiling
CSCvs77557	Cisco 3802 AP is not able to acknowledge EAP frames (EAP-TLS).

Caveat ID Number	Description
CSCvs82411	Cisco 9120 APs unable to see neighbor APs on controller with FIPS enabled
CSCvs90805	FlexConnect local switching AP sends deauthentication when moves from standalone to connected mode
CSCvs98970	Controller Reaper Reset in Process SNMPTask
CSCvt03983	Intel clients experiencing latency / drops connected to Cisco 9120 APs
CSCvt04565	SSH access to controller is failing, stating protocol error occurred
CSCvt10962	Clients cannot connect to Cisco 1800 AP with 2.4 GHz with hidden SSID [SF 04513749]
CSCvt11269	Cisco 9120AXI-E: AP max transmit power is 12 dBm on Radio 0 -E domain
CSCvt13716	Cisco 9120 AP is beaconing to disabled SSIDs
CSCvt15152	4800 APs stopped supporting European weather band 5600-5650MHz- channels 120,124,128 on 8.10 release
CSCvt17006	Cisco 1850AP: /usr/sbin/capwapd: writing to fd 17 failed!: Input/output error
CSCvt18317	Cisco controller reloads unexpectedly in SNMPTask due to Reaper Reset
CSCvt18451	Zebra QLN420 having issues passing traffic with 2700 WAVE 1 AP when printer firmware is upgraded.
CSCvt20213	AireOS controller not enforcing redirect URL/ACL on second CoA from AAA server
CSCvt21068	Cisco 1840 AP transmitting on different channel [SF 04488433]
CSCvt21838	Cisco 1542 MAP failing to join the AP1542 RAP
CSCvt22353	Cisco Wave 2 APs not sending DHCP messages over the air
CSCvt23051	Cisco 9120AX AP: 17.1.1: AP is not using correct datarates
CSCvt26556	FlexConnect AP central RADIUS authentication issues
CSCvt27739	Cisco 1800s Sensor first AP in test always fails for DNS resolution
CSCvt29353	APs using disabled data rates to send ACK/Block ACKs when the client is using disabled rates
CSCvt29399	Throughput degradation observed with Wave 2 APs with Flex Local Switching EoGRE tunnel to Benu WAG
CSCvt29596	Current Tx Rate for 802.11AX clients displayed incorrectly on the 9800 controller
CSCvt31668	8.10: Efficient Join fails because of low memory.
CSCvt37813	ME day zero provision accessing http://mobilityexpress.cisco failure when ME acting as DHCP server

Caveat ID Number	Description
CSCvt39042	Cisco 1815i AP reloads unexpectedly with - PC is at pskb_expand_head+0x44/0x2f4
CSCvt40896	Wave 2 APs using disabled data rates to send ACK/Block ACKs when the client is using disabled rates
CSCvt69211	AP 9120/9115: Interference value jumps to 90-100% when no WLANs are enabled
CSCvt69222	AP: CAPWAP continuously keeps flapping on AP causing controller disconnects
CSCvu00121	Cisco 1840 AP on 8.10 MR3: kernel panic PC is at _raw_spin_lock_bh+0x50/0x64

Resolved Caveats

Table 14: Resolved Caveats for Release 8.10.122.0

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

Table 15: Resolved Caveats for Release 8.10.121.0

Caveat ID Number	Description
CSCuw77959	Cisco IOS and IOS XE Software DHCP Remote Code Execution Vulnerability
CSCux66796	Cisco IOS and IOS XE Software TACACS+ Client Denial of Service Vulnerability
CSCvc99155	Cisco IOS and IOS XE Network Based Application Recognition Denial of Service Vuln
CSCvd13371	Some configuration change on a WLAN causes the radio to reset
CSCve09716	AP radio reloads unexpectedly due to TCQVerify!= 0;beacons stopped for several seconds;false high CU
CSCvf36258	Cisco IOS and IOS XE Software HTTP Client Information Disclosure Vulnerability
CSCvg39082	Cisco IOS and IOS XE Software TCP Denial of Service Vulnerability
CSCvg54267	Cisco IOS and IOS XE Software Cisco Discovery Protocol Denial of Service Vulnerability
CSCvi48253	Self-signed certificates expire on 00:00 1 Jan 2020 UTC, cannot be created after that time

Caveat ID Number	Description
CSCvk60956	AP does not move to custom flex group when AP gets configuration with new flexgroup name
CSCvm66185	During AP Boot the AP sends 3 DHCP releases causing BAD_ADDRESS on Windows Server 2016
CSCvm92998	Cisco IOS and IOS XE Software Change of Authorization Denial of Service Vulnerability
CSCvn00218	Cisco IOS and IOS XE Software Session Initiation Protocol Denial of Service Vulnerability
CSCvq66030	Cisco IOS and Cisco IOS XE Software Web UI Cross-Site Request Forgery Vulnerability
CSCvq83638	Cisco Wave 2 APs: 1562APs does not pass traffic in Ethernet Bridging Mode on 8.5.151
CSCvq98797	Traceroute fails: /bin/sh: /usr/bin/traceroute: not found
CSCvr03652	Cisco Wave 2 APs: - FT dot1x fails in Standalone mode
CSCvr10424	Cisco FlexConnect AP drop UDP packet(port 2598).
CSCvr20539	Controller not assigning correct channel width to Cisco APs.
CSCvr82193	Wave2 AP Flex local RADIUS fallback with FT Enabled -Standalone mode PMKID is seen in Assoc Response
CSCvr82520	Cisco Wave 1 AP Software reloads unexpectedly when configuring a long SNMP-server community string
CSCvr87573	Cisco 2802 AP stops sending broadcast ARP to wireless
CSCvr93760	VLAN bridging problem on Cisco 1810W AP with RLANs
CSCvr94407	DHCP traffic is not being tagged with CMD header by the controller
CSCvs00138	Cisco 2802AP -AID allocation failed for slot 0
CSCvs01600	Controller buffer overflow is caused by %SAFEC-3-SAFEC_ERROR constantly appearing in syslogs
CSCvs02759	Beacon stuck followed by assert; AP radio on channel 36 while controller thinks its on different channel
CSCvs05669	Clients connected to same SSID using different autonomous Cisco 2702 APs can not ping each other
CSCvs16432	Controller reloads unexpectedly on IPv6_Msg_Task
CSCvs17014	Cisco 1832 AP - No Rx Neighbors

Caveat ID Number	Description
CSCvs19137	Authentication failure EAP timeout on a Cisco 1852 AP with data DTLS encryption enabled
CSCvs29874	802.11v DMS not shown as supported within beacon of Cisco 1852 AP on 8.10 release software
CSCvs31212	Cisco 3800 APs in 9800: MIC errors observed for CCKM roams in FlexConnect local switch mode
CSCvs31857	4800 series AP causes duplex mismatch log on mGig when speed is set to auto on 9400 Catalyst switch
CSCvs32307	Cisco Wave 2 APs with FT Standalone mode Roam traffic is blackholed when PMK is present
CSCvs36123	Cisco Wave 2 APs - Client traffic blackholed in Standalone with 802.11r
CSCvs36177	Cisco Wave 2 APs - AP sending the EAP identity req with incorrect BSSID
CSCvs37305	Secondary controller continuously rebooting while attempting to reform HA (after failover occurs)
CSCvs39989	Controller on 8.10.105.0 resets due to unexpected reloading of the switch-driver
CSCvs40887	Cisco AP4800/3800/2800/1562 stuck in "BootROM: Image checksum verification FAILED"
CSCvs41893	Cisco 3702 AP running 8.5.151.0 release software reloads unexpectedly
CSCvs42820	Mobility Express Macfilter change to none in case add RADIUS server in Controller
CSCvs47177	Removal of default "Thanks Page" for Web PassThrough Captive portal feature
CSCvs49779	HA: controller on 8.8 software rebooting due to peer Redundancy Port Keep Alives loss
CSCvs50731	Cisco 9130I/1852 APs "{watchdogd} Process syslogd gone for 60s" & " can't open '3410/maps'"
CSCvs52266	9800-CL displaying wrong AVC data on GUI page.
CSCvs52402	MnM-Test: AP9120 - Kernel panic seen at at _raw_spin_lock_bh
CSCvs55071	Controller RRM sets all Cisco 9120APs on 2.4-GHz at Channel 1 & power 1
CSCvs55109	AP Ethernet link flaps at 5G speed due to Fast Retrain failure
CSCvs59018	AP disjoins Mobility Express primary after configuring RADIUS server with non-default port
CSCvs59125	Cisco 9120AP: 802.11bgn UDP downlink throughput is lower than expected
CSCvs63478	Cisco 3504 controller: webauth unexpectedly reloaded on ewsContextSendRedirect

Caveat ID Number	Description
CSCvs63593	AP3802-P-k9 Transmit Power Adjustment with AIR-ANT2513P4M-N (13dBi) W52 Japan Outdoor
CSCvs66107	Cisco 9115AX AP: Rogue containment not working if AP in monitor mode
CSCvs66411	Flex AP sending RADIUS packets to AAA server when in local auth mode
CSCvs67441	Flex 9120 AP not allowing authentication to clients for SSIDs with special characters
CSCvs68187	Controller-AP Primary Controller name and IP address mismatch
CSCvs70502	Cisco Wave 1 AP reloads unexpectedly which relates to fast roaming state machine
CSCvs72354	Cisco 9130E AP: NSS reloads unexpectedly causes AP to be stuck in continuous loop
CSCvs74755	PRP:WGB BVI IP is not reachable from default gateway with ARP entry timeout on core switch
CSCvs75832	Cisco 9115 APs: rogue containment in monitor mode not working as expected
CSCvs78454	Controller reset due to switch-driver unexpectedly reloads on 8.10.128.20
CSCvs87888	Evaluation of Cisco Catalyst 9100 Series APs for Kr00k attack - CVE-2019-15126
CSCvs88238	FEW client ARP/DHCP failures after roaming among Cisco Wave 1 APs
CSCvs89401	Cisco Wave 2 AP beacons disabled SSID
CSCvs89702	Controller reset due to switch-driver unexpectedly reloads on 8.5.151.0
CSCvs97706	Controller reloads unexpectedly on emWeb task
CSCvs97942	ME GUI : cannot change order of ACL rules
CSCvs98107	ANQP responses not sent over the air
CSCvt01409	C9800: Dual-band static channel configuration switches to DCA after AP rejoin
CSCvt06414	Cisco 9130 AP Kernel Panic at cisco_wlan_crypto_decap
CSCvt08458	Cisco 9130 AP Serviceability NSS-Coredump copy cores does not work
CSCvt09218	Flex connected mode: after continuous roam, client takes longer time to reconnect
CSCvt24200	Macbook running Catalina does not connect to 9130 AP after toggling WiFi
CSCvt25898	Anchor IRCM controller is changing VLAN between webauth and run in CWA scenario without AAA VLAN change
CSCvt35811	AP9130 Channel/Mode Mismatch between WCP and WLAN driver (SF #04498730)

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

- 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 Mobility Services Engine

Cisco Mobility Services Engine 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.