Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.10.130.0

First Published: 2020-07-31

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

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 8.10.130.0

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

Support for Cisco Catalyst 9105 Access Points

Support is added for Cisco Catalyst 9105 APs in this release.

- C9105AXI and C9105AXW: VID 03 and earlier

Support for Cisco Catalyst 9130 Series Access Points Tri-Radio (Dynamic) mode

The Cisco Catalyst 9130 Series Access Point is designed keeping high-density deployment in mind. Hence, this AP includes three radios which support the dual radio mode and the radio role assignment functionality. The AP supports radio roles—monitor and client serving roles under Auto and manual modes. You can manage the modes dynamically 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.

This feature enhances the existing Cisco Catalyst 9130 Series Access Points Tri-Radio feature by supporting the radio role.

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

Uplink MU-MIMO in Cisco Catalyst 9130 APs

Uplink Multi-user multiple-input and multiple-output (UL MU MIMO) feature is supported in Cisco Catalyst 9130 APs in this release.

- Conceptually similar to Downlink MU-MIMO, which is already supported in Cisco Catalyst 9130 APs.
- Allows multiple clients to send traffic simultaneously, thus saving air time.
- Controller by AP through triggers sent to clients.
- Supported in 20-MHz, 40-MHz, and 80-MHz bandwidths, but not supported in the 160-MHz bandwidth.
- Supported only in the 5-GHz band.
- Currently limited to support three users. When more than three users are connected, UL MU-MIMO scheduling does not occur, and the AP falls back to single-user (SU) transmission.

Support for Strong Ciphers in Cisco Access Points

This feature enhances access point's security over SSH connections. The weak cipher suites are no longer supported. Any attempt to establish connection using legacy ciphers displays `Unable to negotiate a key exchange method` error message.

The feature is enabled by default.

Cisco Aironet 4800 Access Point Priority for wIPS Mode

In this feature, wIPS scanning is prioritized in Cisco Aironet 4800 APs. The Cisco Hyperlocation feature is disabled when the AP sub-mode is set to **WIPS**.

Strong Credentials for Local User and AP Dot1x User

This feature implements stronger user names and passwords requirements for Controller and AP users.

Cisco Catalyst 9117 AP Image Upgrade Bundle

If you are using Cisco Catalyst 9117 APs, then to upgrade to Release 8.10.130.0, you must download an additional image bundle, ap1g6, which is specific to the Cisco Catalyst 9117 APs. Following are the high-level steps in upgrading to this release:

1. Download the *controller.aes* file from the Cisco software download page and upgrade the controller software with this image.
2. Reboot the controller to load the new image.
3. Download the *apimage.aes* (ap1g6) file from the Cisco software download page and upgrade the controller software with this AP image bundle.
4. Reboot the controller to load the new AP image bundle.

For more information, see **Upgrading Cisco Wireless Release** section of this document.

IoT Features

- **Support reliable WGB downstream broadcast for multiple VLANs.**

  Support to convert downstream broadcast packets to unicast packets in the 4-address format with retransmission to WGB and its wired clients.

  Supported AP platforms

  - Cisco Industrial Wireless 3700 Series Access Points
  - Cisco Aironet 1570 Series Access Points

  Supported WGB platform

  - Cisco Industrial Wireless 3700 Series Access Points

  For more information about the feature, see **Reliable WGB Downstream Broadcast for Multiple VLANs** 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.

- **Support faster detection of missing M1 or M3 message during 4-way handshake**

  Support to configure M1 and M3 timeout value on IOS WGB (IW3700 Series Access Points) to achieve faster detection of missing M1 or M3 message. This enhancement fulfills the requirement for quick roaming to avoid longer outages due to roam. For more information about the feature, see **WGB M1**

and M3 Timeout Enhancement section in the *Cisco Wireless Controller Configuration Guide, Release 8.10*

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

Early Field Trial Features

The following features are in Early Field Trial state:

Note These features are not yet officially supported and there is no assistance from Cisco's Technical Assistance Center.

- **Cisco DNA Center Assurance Wi-Fi 6 Dashboard**

  The Cisco DNA Center Assurance Wi-Fi 6 Dashboard provides a visual representation of your wireless network. The dashboard contains various widgets which show you the efficiency of Wi-Fi 6 networks compared to non-Wi-Fi 6 networks.

  Note We recommend that you manage this Cisco DNA Center Assurance feature using the Cisco DNA Center UI.

  For more information about Cisco DNA Center Assurance feature, see https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/m_wifi6_assurance_dashboard.html and chapter **Monitor Wi-Fi 6 Readiness** in Cisco DNA Assurance User Guide.

What's Changed in Release 8.10.130.0

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

OFDMA in Cisco Catalyst 9130 APs

In this release, the Cisco Catalyst 9130 APs support both the Uplink and the Downlink Orthogonal frequency-division multiple access (UL OFDMA and DL OFDMA) features.

Currently, the feature is enhanced to support 37 users in a DL OFDMA or UL OFDMA transmission.

Regulatory Domain Rule Changes

In this release, there are regulatory domain changes implemented for Bahrain, Egypt, India, Indonesia, Japan, Russia, and Taiwan. For more information about these regulatory domain changes, see https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/reg-domain/reg-domain-rule-changes-in-810MR3-and-17-3.html

Support for Spectrum Intelligence in Cisco Catalyst 9115 AP

From this release, Spectrum Intelligence feature is supported on Cisco Catalyst 9115 Access Points.

Suppport for Hardware DTLS Encryption in Cisco Catalyst 9115 and 9120 Access Points

From this release, hardware DTLS encryption is supported on Cisco Catalyst 9115 and 9120 Access Points.

Full Certificate Chain for Web Administrator Access

In this feature enhancement, when a web browser is used to access the controller webUI via the HTTPS protocol, the controller sends the full certificate chain to the browser for TLS authentication.

SNMP Support Added to NTP Server for an AP Group

This feature is enhanced to support SNMP for AP group NTP server configuration.

Link Aggregation Group Support Extented to Cisco Aironet 1850 Access Points

From this release, the Link Aggregation Group (LAG) feature is supported on Cisco Aironet 1850 APs in Cisco FlexConnect mode.

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.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.
8.9.x	You can upgrade directly to Release 8.10.x.
8.10.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 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)	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.

Controller	Current CIMC Version	Recommended CIMC Version	Link to Download the CIMC Utility Software Image
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 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 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 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(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 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, 9105 and 3800 APs
Radio	802.11ax (2.4 GHz or 5 GHz), 802.11ac, 802.11a, 802.11g, 802.11n (2.4 GH
Security	Open, WPA3-SAE/OWE (WPA3 Supported Clients), WPA2+WPA3 (Mix (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
Wi-Fi 6 Devices (Mobile Phone and Laptop)	
Samsung S20	Android 10
Samsung S10 (SM-G973U1)	Android 9.0 (One UI 1.1)
Samsung S10e (SM-G970U1)	Android 9.0 (One UI 1.1)
Samsung Galaxy S10+	Android 9.0
Apple iPhone 11	iOS 13.5
DELL LATITUDE 5491 (Intel AX200)	Windows 10 Pro (21.40.2)
Laptops	
Acer Aspire E 15 E5-573-3870 (Qualcomm Atheros QCA9377)	Windows 10 Pro (12.0.0.832)
Apple Macbook Air 11 inch	OS Sierra 10.12.6
Apple Macbook Air 13 inch	OS Catalina 10.15.4
Apple Macbook Air 13 inch	OS High Sierra 10.13.4
Macbook Pro Retina	OS Mojave 10.14.3
Macbook Pro Retina 13 inch early 2015	OS Mojave 10.14.3
DELL 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 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 Pro	iOS 13.5
Apple iPad Air2 MGLW2LL/A	iOS 12.4.1

Client Type and Name	Driver / Software Version
Apple iPad Mini 4 9.0.1 MK872LL/A	iOS 11.4.1
Apple iPad Mini 2 ME279LL/A	iOS 12.0
Microsoft Surface Pro 3 – 11ac	Qualcomm Atheros QCA61x4A
Microsoft Surface Pro 3 – 11ax	Intel AX201 chipset. Driver v21.40.1.3
Microsoft Surface Pro 7 – 11ax	Intel Wi-Fi chip (HarrisonPeak AX201) (11ax, WPA3)
Microsoft Surface Pro X – 11ac & WPA3	WCN3998 Wi-Fi Chip (11ac, WPA3)
Mobile Phones	
Apple iPhone 5	iOS 12.4.1
Apple iPhone 6s	iOS 13.5
Apple iPhone 8	iOS 13.5
Apple iPhone X MQA52LL/A	iOS 13.5
Apple iPhone 11	iOS 13.5
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 10
Google Pixel 4	Android 10
Huawei Mate 20 pro	Android 9.0
Huawei P20 Pro	Android 9.0
LG v40 ThinQ	Android 9.0
Samsung Galaxy S7	Andriod 6.0.1
Samsung Galaxy S7 SM - G930F	Android 8.0
Samsung Galaxy S8	Android 8.0
Samsung Galaxy S9+ - G965U1	Android 9.0
Samsung Galaxy SM - G950U	Android 7.0

Client Type and Name	Driver / Software Version
Sony Experia xz3	Android 9.0
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
Printers	
Zebra QLn320 Printer	LINK OS 6.1
Zebra ZT230 Printer	LINK OS 6.1
Zebra ZQ310 Printer	LINK OS 6.1
Zebra ZT410 Printer	LINK OS 6.1
Zebra ZQ610 Printer	LINK OS 6.3
Zebra ZQ620 Printer	LINK OS 6.1
Wireless Module	
Intel 11ax 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/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 9: 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
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 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

Caveat ID Number	Description
CSCvm17365	Cisco Wave 2 APs reloads unexpectedly due to FIQ/NMI reset
CSCvq11556	Cisco Wave 2 APs to not trigger CAC if radio is shutdown less than 16sec in a DFS channel

Caveat ID Number	Description
CSCvt18256	Cisco 9130I WLAN: [0:E:BSSCOLOR] ieee80211_setup_bsscolor failed : not 11AX channel
CSCvt61795	Cisco 3800 AP's advertise RSN PSK in the beacon on WLAN with open MAC filtering authentication
CSCvt82413	WLC - Tracebacks on dot11 auth validation
CSCvt99064	WLC GUI HTTPs stops working after downloading a web auth certificate
CSCvu02448	Cisco 3702 AP unable to join controller. Shows high CPU utilization under NCI Rx.
CSCvu03573	Cisco 9130 AP whal_hwsch.c:2494 Assertion num_proc_entry <= num_peek_entry failed
CSCvu10516	AireOS drops ARP request or reply when local client tries to reach L3 roamed client
CSCvu24138	WPA2 clients with PSK-SHA2 are wrongly shown as WPA3 in client details
CSCvu28462	Tri-Radio: All value in 'RRM Frame Statistics' for Slot 2 is 0
CSCvu47655	WLC DP unexpectedly reloads due to max out IP Flow
CSCvu55303	AP9120 Kernel Panic causes AP to reload unexpectedly due to sockets_in_use
CSCvu58082	3800AP with data DTLS encryption disconnect from 9800 due to CAPWAP keepalive after rx PMTU discover
CSCvu62353	Cisco 1810W AP reloads unexpectedly on AP running 17.3.0.92
CSCvu66043	Cisco 9130 APs not sending DHCP messages over the Air
CSCvu68553	CoA-NAK does not have correct message length to account for Service-Type
CSCvu68859	8.10 MR2: fabric WLC unexpected reload observed @serial8250_poll while removing mobility tunnel
CSCvu74482	WLC on 8.10.121.0 reloads unexpectedly on pmalloc detected memory corruption
CSCvu83242	Several 1852 APs facing different radio failure FW asserts
CSCvv10289	Cisco 9120 AP dropping certain UDP packets over the air
CSCvv10289	MX40 - Cisco 9120 AP dropping certain UDP packets over the air
CSCvv12301	Memory leak seen in nmspMxServerTask and nmspTxServerTask
CSCvv13566	Cisco AP reloads unexpectedly with asserts on wifi txfifo id mismatch
CSCvv22110	9130 AP multicast traffic failures after GTK key index rotation for vocera Clients

Resolved Caveats

Table 13: Resolved Caveats

Caveat ID Number	Description
CSCvh21912	Access point broadcasts a disabled or deleted SSID
CSCvj03786	WLC emits error messages: "RRM LOG: No receiver found for IAPP CHD message/AGGR Neigh message"
CSCvk42191	AP3800 advertises RSN IE for an OPEN SSID.
CSCvm63643	With IPv6 TGW on AP, fragmentation for IPv4 packets are not handled
CSCvo83091	8.5 FlexConnect AP in Standalone mode get stranded and does not send CAPWAP Discovery
CSCvp26215	WLC does not present full certificate in web admin
CSCvp54103	Cisco Wave 1 APs reload unexpectedly with 'Unexpected exception to CPU' in logs
CSCvp94841	AP should reply to IGMPv3 Query using IGMPv3 report when CAPWAP multicast is enabled in WLC
CSCvq90572	Receive throughput degrades for Cisco 2800, 3800, 4800, 1560 APs - AP fails to send block ACKs
CSCvq99108	Cisco 3700 AP series reloads unexpectedly due to reason 44
CSCvr72661	FlexConnect peer connectivity breaks after roam with AVC enabled
CSCvs26416	IPTV getting disconnected intermittently
CSCvs48711	Controller shows LAN port Status UP even though the status at the AP side is Down and Protocol UP
CSCvs52093	Cisco 2802 AP in Flex mode in only one site HTTPS packets from WLC to Client getting drop
CSCvs52851	Cisco 9130E APs: Large ping losses, videos stopping etc during auditorium test
CSCvs56849	9120AXI unexpectedly reloads with watchdog or grpc_server tainted - PC at "raw_spin_lock+0x24/0x38"
CSCvs67058	Cisco 1852 AP unexpectedly reloads with GRPC connection timed out
CSCvs67811	AP's acting as MAP's not able to see RAP's
CSCvs71672	AP fails to attach the VLAN tag when client user ID changes from central to local switching
CSCvs72880	Stale client entries getting created in WLC
CSCvs73405	Cisco WLC controller clients profiled as unknown when doing local profiling

Caveat ID Number	Description
CSCvs81190	Cisco 1800,1815,1840,1850,1540AP unexpectedly reload due kernel panic triggered by DFS channel use
CSCvs82411	Cisco 9120 APs unable to see neighbor APs on controller with FIPS enabled
CSCvs86828	C9130 AP RRM: %LWAPP-3-VENDOR_PLD_VALIDATE_ERR: [PA]spam_lrad.c:12307 Validation of RRM_INTERFERENCE
CSCvs89410	Cisco 3602 AP Image corruption issue
CSCvs92867	Client command - 'clear dot11' not deleting client
CSCvs98970	Controller Reaper Reset in Process SNMPTask
CSCvt03401	AVC status is getting disabled while configuring service-policy input from DNA.
CSCvt04565	SSH access to the controller is failing, stating protocol error occurred
CSCvt06414	Cisco 9130 AP Kernel Panic at cisco_wlan_crypto_decap
CSCvt06772	Antenna Monitoring and Failure Detection needs to support AP-3802P
CSCvt07649	WLC uses WLAN interface IP as NAS-IP when per-WLAN RADIUS source support is enabled to AP group
CSCvt08140	Cisco 2800, 3800, 4800 APs: Support for ANQP BSSID broadcast response
CSCvt10962	Clients cannot connect to Cisco 1800 AP with 2.4 GHz with hidden SSID
CSCvt15152	4800 APs stopped supporting European weather band 5600-5650MHz- channels 120,124,128 on 8.10 release
CSCvt16235	Static CAPWAP path MTU configuration for AP-COS
CSCvt17006	Cisco 1850AP: /usr/sbin/capwapd: writing to fd 17 failed!: Input/output error
CSCvt17971	WLC / CMX Telemetry output sending numerous duplicate and erroneous TAG records
CSCvt20213	AireOS controller not enforcing redirect URL/ACL on second CoA from AAA server
CSCvt21084	911x AP models shows incorrect details on Acesspoint view of WLC
CSCvt22353	Cisco 2800, 3800, 4800, 1560 APs are not transmitting data frames over the air
CSCvt24635	CAPWAP DTLS session closed for AP, because the DTLS server session shutdown
CSCvt24946	Cisco 4800 AP: flooding syslogs with "BA session Not established?"
CSCvt25642	WLC reloads unexpectedly while accessing GUI > Monitor > Clients page
CSCvt26140	Client cannot connect to Cisco Wave 1 APs with dot1x-sha256 received assoc-resp 20

Caveat ID Number	Description
CSCvt28616	Flexconnect reap count for current users not getting decremented causing new Wi-Fi client disconnect
CSCvt29550	AireOS GUI: Current TX Rate for 11AX clients is displayed incorrectly
CSCvt29946	Cisco 9120 AP alpha: DHCP packets to be sent to the clients are dropped by AP
CSCvt37863	Rate limiting not working for downstream traffic when ACL is pushed from ISE
CSCvt38277	Cisco 9130 unexpectedly reloads at __qdf_nbuf_is_tso Kernel panic
CSCvt38486	Cisco Wave 2 APs: EAP-PEAP flex auth fails occasionally because of low EAP-timeout
CSCvt40272	Clients connected to 2 different autonomous APs with ISE VLAN Override cannot ping in 5GHz radio
CSCvt43995	Client MAC address is learned from controller interface in SDA fabric
CSCvt44296	Organization name truncated to less than 64 characters while generating CSR on WLC
CSCvt44832	9115 AP flash getting 100% utilised.
CSCvt45502	SDA Wireless: IPv6: Router Advertisement from incorrect VN/pool
CSCvt46341	Unexpected reload in Task Name: Client Profiler Task
CSCvt47529	In SDA solution, Multicast stream pauses periodically_mroute state pruning
CSCvt51471	802.11ax client is displayed as 802.11ac(5 GHz) or 802.11n(2.4 GHz) on Standby WLC
CSCvt51979	AP1840 consistently running a High Channel Utilization only in 5 GHz without any clients connected.
CSCvt53637	EWC conversion fails for 9115AX AP with -T domain
CSCvt53819	CPU increases to 90+% with high volume traffic.
CSCvt55612	Cisco 9120 power is lower than 2800, 3800 with CCK rates disabled (2.4-GHz)
CSCvt56201	AP coverage hole with 0 clients
CSCvt58675	Cisco 9117AX, 9130 AP unexpectedly reloads OOM "handle_mm_fault+ x538/0x1230"
CSCvt62980	%SAFEC-3-SAFEC_ERROR: safecWrapper.c:57 DATA INCONSISTENCY: (22) strncpy_s: when syncing from Prime
CSCvt63250	Cisco 9120 AP watchdog_status reason: 14 no crash was generated.
CSCvt63822	AP sends lower bytes of packets while performing PMTU negotiations.
CSCvt64308	OEAP config does not get saved to AP flash
CSCvt66702	1800, 1815, 1840, 1850, 1540 - ERP Field from AP appears to be incorrect

Caveat ID Number	Description
CSCvt68068	Cisco Wave 2 APs: Reports itself as a Threat and logs "AP Impersonation" alerts
CSCvt70070	WLC reset on task name: apfRogueTask_2
CSCvt71646	WLC reloads unexpectedly on ATF stats decode
CSCvt72136	Wave 2 AP:IPv4 network is unreachable due to Gateway deleted on AP after configuring static IPv6 add
CSCvt73463	Cisco 18xx APs: Software unexpectedly reloads on Process hostapd
CSCvt74430	Cisco Wave 1 APs: Inconsistent AP logging level config behavior
CSCvt75359	85mr6 & later release: Cisco Wave 1 APs not sending deauth rc 7 after Rx frame from non assoc client
CSCvt76571	Cisco DNA Center 1.3.3: Cisco DNA Center stalls on Rogue Management page
CSCvt81606	Cisco 1832 AP kernel panic unexpected reload (PC is at vfp_reload_hw)
CSCvt84649	Cisco 2800, 3800 APs: dropping ARP_REPLY packet post fix for CSCvm07536
CSCvt86786	8.10 ME: ME/RAP transmit beacon on backhaul universal Client Access disabled and Mapping enabled
CSCvt87401	Cisco 9120 APs: is not applying trust-dscp-upstream and CAPWAP traffic marked with UP to DSCP
CSCvt87904	Cisco 9115/9120 APs: 2.4-GHz throughput does not change based on the number of streams
CSCvt89481	AC Wave 1 AP not sending Cisco NDP Packets on the 2.4GHz band
CSCvt89970	Cisco Wave 2 APs: Adding ARP entry check to Gateway reachability
CSCvt89989	Mesh AP: With ACL blocks ping to GW, AP can't join controller if it doesn't complete within 45sec
CSCvt92754	1532 AP ethernet interface lost packet
CSCvt96416	DCA sets channel width to 20MHz although 40MHz is set on RF Profile
CSCvt99526	[AP] Fabric SDA - Fabric APs not taking static-ip address
CSCvu02096	Not able to download NSP app for pre-auth from google store using DNS based ACLs
CSCvu03384	Wave 2 APs silver UP 00 to DSCP upstream mapping not capped by bronze profile
CSCvu04311	WLC should not send client IPv6 packets to switch in CAPWAP or IP
CSCvu07193	External Webauth URL : ? character is not allowed in this field
CSCvu08514	Controller reporting incorrect channels for Interferers on NMSP.

Caveat ID Number	Description
CSCvu10591	Mesh backhual sharing SSIDs still showing state UP after RAP/MAP flexconnect backhual-WLAN disabled
CSCvu11239	OEAP AP Local configs missing after reload
CSCvu13199	WLC is triggering too many LRAD delete events for the APs
CSCvu18039	WLC 8.10 sends mobility packets with MTU greater than 1500 bytes
CSCvu18085	AP9117: AP not forwarding Server Hello downstream - EAP type PEAP
CSCvu23186	WLC on 8.10.121.0 reloads unexpectedly with reason "reset due to switch-driver crash"
CSCvu23563	Cisco 9130 AP does not forward EAP-TLS packets intermittently. drop_memfail counter increasing
CSCvu24770	Various Android 10 phones fail to associate
CSCvu25264	AIR-AP2802I-H-K9 WCPd reloads unexpectedly on 8.5.135.0 lick-install/include/click/vector.hh:291
CSCvu27015	Swaping pri or secon controller from WLC GUI HA tab, the name not apply to AP CLI config
CSCvu32113	1562 MAP does not create or keep adjacency with RAP from Mobility Express WLC
CSCvu36206	Configuration changed after upgrade to 8.10.112 release
CSCvu37470	WLC reloads unexpectedly on RF profile config change
CSCvu39140	AP9120 and AP9130 have their radio slot 0 changed to monitor mode after enabling fast locate
CSCvu39206	Cisco 9130 AP: MTU mismatch between NSS and CAPWAP
CSCvu40287	Cisco 9120 AP reloads unexpectedly with watchdog_last.status reason:14
CSCvu43631	AP PnP doesn't try sync time with public NTP server
CSCvu44130	802.11AX clients not listed in the Active Clients filter from the Main Dashboard
CSCvu46237	5520 model running s/w 8.8.125 sending WSA data with s/w version as 8.6.161
CSCvu46244	WLC not updating fastpath table after a GW GARP failover
CSCvu48396	[SDA] With post-auth IPv6 flex ACL traffic breaks for client
CSCvu57562	Out of box 9130 does not try to discover WLC using IP address returned in DHCP option 43 or DNS
CSCvu61194	Cisco 2800, 3800 APs sends burst of RTS and BAR randomly leading to low client data rates
CSCvu61306	WLC shows low power PoE status for 1830 APs with USB port disabled.

Caveat ID Number	Description
CSCvu66823	WLC reloads unexpectedly due to memory leak & AVC is enabled
CSCvu67221	9120AXI 17.1.1 reloads unexpectedly on "NMI watchdog: BUG: soft lockup - CPU#1 stuck for 23s!
CSCvu83817	WLC reloads unexpectedly on DHCP socket task
CSCvu91002	AireOS controllers unexpectedly reloads randomly at tunnelProfileGwRadiusProxyGetSafe task
CSCvu95312	OEAP: LAN port 3 (Local Port) client cannot access AP Web GUI
CSCvv03650	WP OEAP: Client connected to dedicated local port on AP cannot access AP Web GUI

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.