Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.10.112.0 and 8.10.113.0

First Published: 2020-03-03

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
May 28, 2020	Included Release 8.10.113.0 • Added: Resolved Caveats • Updated: Open Caveats
March 03, 2020	Whats New section • Added: Access Points Specific SSH Setting

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
  - 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 8.10.113.0

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 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 8.10.112.0

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

If you are using Cisco Aironet 2800, 3800, and 4800 series APs with FIPS in enabled state, we recommend that you do not upgrade to Release 8.10.112.0 because of the issue described in CSCvt17801, where the APs go into a loop after trying to join the controller. This issue will require manual recovery of APs using Mode button to factory reset the APs. Therefore, we advise the FIPS customers to use Release 8.5.161.0. 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

New Access Point Support

In this release, support is introduced for the following new access point:

- Cisco Catalyst 9130E Access Points (C9130AXE-x) with Digital Analog Radio Termination (DART) Antenna Support
  - C9130AXE: VID 02 or earlier

Cisco Catalyst 9130 Access Points

Cisco Catalyst 9130E Access Points (C9130AXE-x) support the following features:

- 1x1 mode is supported when the AP is powered by 802.3af PoE
- 2x2, 3x3, and 4x4 antenna configurations for the 2.4-GHz radio

- 2x2, 3x3, 4x4, 6x6, and 8x8 antenna configurations for the 5-GHz radio
- Self-Identifiable Antennas (SIA) using 8-port Digital Analog Radio Termination (DART) plug
- 8-port DART Smart Antenna connector

Note If you configure the 9130 AP to operate in 160-MHz channel width, only 2x2, 3x3, and 4x4 antenna configurations are supported.

The Cisco Catalyst 9130E Access Points have 3 dBm less Tx power range than the Cisco Catalyst 9130I Access Points.

Enhanced CLI Command Outputs for Cisco Catalyst 9130 Series Access Points

Existing controller and access point commands are enhanced to display additional information related to Cisco Catalyst 9130 Series Access Points. The following is the list of commands:

For Cisco Controller

- **show ap config** {**802.11a** | **802.11b**} *ap-name*

  The following is a sample output for DART-RPTNC antenna connected to the AP:

```
cisco-wlc#show ap config 802.11a ap9130332
Attributes for Slot  1
     ……..……
      Legacy Tx Beamforming Configuration ....... AUTOMATIC
      Legacy Tx Beamforming ..................... DISABLED
   Antenna Type.............................. EXTERNAL_ANTENNA
      SIA Status................................ Present(RPTNC)
      External Antenna Gain (in .5 dBi units).... 12
```

- **show ap config slot** *slot-idap-name*

For Cisco Access Points

- **show controllers Dot11Radio** *dot11-interface-no* **antenna**

  The following is a sample output for SIA antenna connected to the AP:

```
cisco-ap#show controllers Dot11Radio 1 antenna
Antenna:        RX [ a b c d e f g h ]
                TX [ a b c d e f g h ]
                External
                Antenna Gain:   1. 4dBi  2. 4dBi  3. 4dBi  4. 4dBi  5. 4dBi  6. 4dBi
7. 4dBi  8. 4dBi
DART connector capable:CAPABLE
DART connector status :PRESENT

SIA RPTNC: NOT_SUPPORTED
SIA DART : Present: 1, Gain: 4
SIA PID:         C-ANT9103=
SIA Description: 8-port Directional
```

Basic Service Set Coloring

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

For more information on BSS Coloring, see https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/managing_aps.html#bss_coloring

Cisco FastLocate on 802.11ax Access Points

The Cisco FastLocate feature enables higher location refresh rates by collecting RSSI or location information through data packets received by the APs. Using these data packets, location-based service (LBS) updates are initiated by the network, and these data packets are available more frequently.

For more information about FastLocate on 802.11ax APs, see https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/location_services.html#fast-locate_9100ap

Access Point Antenna Monitoring and Failure Detection

Having multiple antennas at the transmitter and receiver ends of access points results in greater performance and reliability of the APs. Multiple antennas improve reception through the selection of the stronger signal or a combination of individual signals at the receiver end. Therefore, detection of physical breakage of antennas is critical to the reliability of APs.

This feature is based on the signal strength delta across the antennas in the receiver. If the delta is more than the defined limit for a specific duration, the antenna is considered to have issues.

For instructions on how to configure this feature, see https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/managing_aps.html#ap-antenna-monitoring

Auto Enrollment of Certificate for Cisco Wave 2 Access Points in WGB Mode

From this release onwards, Cisco Wave 2 access points in WGB mode can auto enroll CA certificates.

For instructions on how to configure this feature, see https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/workgroup_bridges.html#cisco-wave2-ap-as-wgb.

Secure Unique Device Identification Certificate for Cisco Access Points

From release 8.10.112.0 onwards, supporting Cisco Access Points switch to using High Availability RSA (HARSA) certificate to join the controller. This new certificate has a validity up to year 2099.

If the AP is migrated from 8.10.112.0 release to an older release or to Cisco Catalyst 9800 Series Wireless Controllers, the AP attempts to join using the HARSA certificate and fails, then the AP loads the RSA certificate and join the controller.

Note Cisco Catalyst 9800 Series Wireless Controllers and Controllers running 8.10.100.0 and earlier release software do not support HARSA certificate.

Cisco Access Points supporting HARSA certificate are:

- Cisco Catalyst 9100 Series Access Points

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

TLS 1.2 Support for EAP-FAST Authentication Protocol

In this release, TLS v1.2 support extends to EAP-FAST authentication protocol. The authentication behavior changes are as follows:

- Cisco Wave 1 Mesh APs continue to use TLS v1.0. If it is disabled, these APs fail to authenticate and do not join the network.
- Cisco Wave 2 Mesh APs authenticate using TLS v1.2 and join the network.

Note Cisco Identity Services Engine (ISE) requires an update to support controllers with TLS v1.2.

To enable controllers to support Cisco TrustSec with TLS v1.2, ensure that you validate and apply the fix available for Cisco ISE in CSCvm03681.

Changes to Cisco Access Point Functionality

- From release 8.10.112.0 onwards, the console access to the AP using the default username and password is not supported. You must explicitly configure the controller AP global credentials with non-default username and password to get access to the AP console.
- From release 8.10.112.0 onwards, sensor mode in Cisco AP is not supported. When an AP in sensor mode is upgraded to 8.10.112.0, the AP is switched to local or bridge mode depending on the AP platform type.

Note To continue using the sensor functionality, we recommend that you use the Cisco 1800S dedicated sensor with its supported APs.

- After you upgrade to Release 8.10.112.0, the AP-specific SSH setting changes to disabled state. However, the APs that have global SSH settings are not impacted.

  If you want to retain AP-specific SSH setting, you must explicitly enable SSH on those APs.
- From this release, a new gateway reachability check is introduced. The APs send periodic ICMP echo requests (ping) to the default gateway to check for connectivity. You need to ensure traffic filtering between the APs and the default gateway (like ACLs) allow ICMP pings between the AP and the default gateway. If these pings are blocked, even if the connectivity between the controller and the AP is active, the APs will reload at 4 hours interval.

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

Upgrading 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

- For Cisco Aironet 2800, 3800, and 4800 APs with FIPS in enabled state, see the important upgrade advisory in the *Important Upgrade Information* section.
- 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 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.
  - If you want to upgrade from Release 8.5 to 8.10 and have WPA1 configured with none of the WPA1 AKM that are valid for Release 8.10, the WPA1 configuration is disabled after the upgrade because it impacts the status of the WLAN. Valid AKM for WPA1 in Release 8.5 are 802.1X, PSK, and CCKM.
- 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 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
CSCvh21912	Access point broadcasts a disabled or deleted SSID
CSCvk60956	AP does not move to custom flex group when AP gets configuration with new flexgroup name
CSCvr94407	DHCP Traffic is not being tagged with CMD header by WLC
CSCvs01600	Controller buffer overflow is caused by %SAFEC-3-SAFEC_ERROR constantly appearing in syslogs
CSCvs05669	Clients connected to same SSID using different autonomous Cisco 2702 APs can not ping each other
CSCvs28965	Cannot change some configuration via GUI
CSCvs30363	Cisco 1852 AP: AP radio hangs causing packets drops
CSCvs31212	Cisco 3800 APs in 9800: MIC errors observed for CCKM roams in FlexConnect local switch mode
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

Caveat ID Number	Description
CSCvs49476	Cisco 1815W AP on 8.10.105.0 code reloads unexpectedly with radio0FW coredumps
CSCvs49779	HA: 8.8 WLC rebooting due to peer Redundancy Port Keep Alives loss
CSCvs55071	WLC RRM sets all Cisco 9120APs on 2.4-GHz at Channel 1 & power 1
CSCvs55383	Cisco 3700AP reloads unexpectedly with CHUNKBADROOTCHUNKPTR
CSCvs57879	Cisco 1815w after upgrading to 8.8.125.x, RLAN fails to pass 7970G traffic
CSCvs60860	Cisco Wave 2 APs: client stops forwarding traffic
CSCvs63543	AP1800 2800 cannot connect to 802.11b network when use client which can only support 802.11b
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	WLC-AP Primary Controller name and IP address mismatch
CSCvs75832	Cisco 9115 APs: rogue containment in monitor mode not working as expected
CSCvs77557	Cisco 3802 AP is not able to acknowledge EAP frames (EAP-TLS).
CSCvs82411	Cisco 9120 APs unable to see neighbor APs on WLC with FIPS enabled
CSCvt04565	SSH access to the controller is failing, stating protocol error occurred

Resolved Caveats

Table 14: Resolved Caveats for Release 8.10.113.0

Caveat ID Number	Description
CSCvt17801	AP 2800/3800/4800/1560/IW 6300 gets into a loop after attempting to join WLC with FIPS enabled
CSCvu02495	Cisco Wave 2 AP boot faiilure with message saying bad lzma header and AP unable to boot and join WLC.
CSCvs00138	Cisco Wave 2 APs in Flex mode unable to accept new Clients with - AID allocation failed for slot 0 | 1
CSCvs87888	Evaluation of Cisco Catalyst 9100 Series APs for Kr00k attack - CVE-2019-15126
CSCvt47413	IW-6300H/1562/2800/3800/4800 series APs are failing DFS compliance

Table 15: Resolved Caveats for Release 8.10.112.0

Caveat ID Number	Description
CSCvc80047	Cisco AP reloads unexpectedly- dpaa_get_pool_id_from_ios_pool_ptr
CSCvh58917	Cisco controller MAC authentication web redirected URL is broken
CSCvh68195	8.8: 5520 Tracebacks observed 0x135956f 0x135af79 0x1362144 0x12ee263 0x3ba6c07dff 0x7f4ede3a439d
CSCvm68624	Cisco Wave 1 AP console display logs 'DTX DUMP'
CSCvn00847	Cisco 702W AP loses connection to Cisco controller
CSCvo10708	Cisco 2800, 3800 APs do not defer off-channel scanning when multicast transmission is active
CSCvo26193	WLC not sending RADIUS authentication request for MAC auth when other WLAN profile has local entry
CSCvo26217	Fabric Enabled Wireless: Cisco 5520 WLC does not reconnect to CP
CSCvo91229	AP deauth client with reason 7 after success re-association due to 'Unknown Mn,calling delete'
CSCvp00688	Cisco 2800, 3800 AP radio reloads unexpectedly
CSCvp26672	Cisco 702 APs fail to authenticate clients due to decrypt error on the AP
CSCvp30608	Cisco Wave2 AP with data DTLS encryption drop out of order CAPWAP data packets
CSCvp33020	Cisco Wave 1 APs stop forwarding multicast traffic under high load
CSCvp34186	Cisco 9120AP: kernel panic crash at select_task_rq_fair+0x2c/0x7d8
CSCvp38189	Socket from WCPd to CAPWAPd is closed
CSCvp40627	Cisco controller fails to initiate 1x message
CSCvp48157	Cisco 1570 RAP intermittently drops broadcast packets
CSCvp58062	Cisco 1800 series AP Radio core dump due to beacon stuck FW hang
CSCvp59502	Controller reloads unexpectedly during de-authenticating client in multiple times[10-15] on UI page
CSCvp60641	RRM Auto RF grouping has to have the same WLC Leader for both bands or FRA is broken
CSCvp66546	Cisco 702w AP Radio reset due to Tx stuck
CSCvp68494	Cisco 2800 AP reloads unexpectedly due to exception when having MU-MIMO clients in network
CSCvp69474	Access point reloads unexpectedly generating capwapd core dumps

Caveat ID Number	Description
CSCvp70358	Cisco 2802 AP reloads unexpectedly with watchdog process sxpd
CSCvp72309	Cisco 3800 AP stops passing traffic under client load Intel NIC 8260/8265 load in MU-MIMO deployment
CSCvp73800	AP wrongly set 'Channel Center Segment 0' to '42' in Assoc Resp while it's operating on CH144/80MHz
CSCvp76453	Traceback : APF-3-NO_FRAMED_IP_ADDRESS: on Acct Start and Interim while running scale test
CSCvp78698	Cisco WLC reloads unexpectedly during mesh tree update
CSCvp82616	Cisco 3800 AP transmitting 802.11n with WMM disabled on 2.4GHz after manualy FRA switch
CSCvp86151	Cisco Wave1 APs radio reset with code 44, mostly seen on 2.4GHz radio
CSCvp86251	WLC does not forward or bridge DHCP REQUEST or DISCOVER for WLAN inherited Central DHCP clients
CSCvp88088	AP9117: FW crash @whal_recv_recovery.c:834 (RX_BACKPRESSURE_MONITOR_BUF_EMPTY) (SF 04035754)
CSCvp91790	Cisco Wave2 AP WGB - Uplink does not get established when Wave2 AP root-ap is rebooted
CSCvp91931	702 AP as WGB keeps sending a new association req every 7 seconds when connected to 2800, 3800 APs
CSCvp92098	Cisco Wireless LAN Controller HTTP Parsing Engine Denial of Service Vulnerability
CSCvp96611	WLC generating client traps without a session-id
CSCvq00175	Regarding "config rf-profile max-client-trap-threshold "and"config rf-profile trap-threshold clients
CSCvq00695	Cisco 3700 AP does not perform DFS CAC after radio is admin down for over a minute
CSCvq00819	SNMP set on Cisco 3802 AP fails when assigning AP HA Pri/Sec on 8.5.144.0
CSCvq01837	Fabric Interface Name might not be shown on GUI
CSCvq04108	64-character RADIUS server Shared Secret in WLC gets corrupted after power cycle
CSCvq07516	Cisco 9120 AP: CAPWAPd core generated
CSCvq09845	AP9115/9120 CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on AP connected port
CSCvq09953	WLAN configuration not applied on the correct WLAN id
CSCvq10242	Client obtains IPv6 link local address with IPv6 disabled

Caveat ID Number	Description
CSCvq14112	Cisco 1832 AP showing up as "low power" when using a PWRINJ5
CSCvq22269	APs stuck in downloading state
CSCvq25317	PMIPv6 - WLC as MAG sends DHCP ACK with subnet mask 0.0.0.0 and router addr 0.0.0.0 on DHCP renewal
CSCvq25654	Cisco 2702 AP sent deauthentication to multicast MAC address
CSCvq26161	Update (1815M/1542) POE power request to match HW spec.
CSCvq26205	8.10 (WLC:3504): system reloads unexpectedly with task dx_sync_task
CSCvq26208	Tx complete not happening for all frames [Tx stuck after 2 mins for 10 seconds]
CSCvq27679	Cisco 1572AP: Radio reset due to pak count mismatch, false detection
CSCvq28024	Cisco 3802I AP 2.4GHz band did not show correct noise Information
CSCvq36007	Cisco 2800, 3800 APs: unable send proper sequence# and burst rate upstream breaking RFID
CSCvq39469	Kernel panic: coredump: process ntp_proc; 9120AX AP SW reloads unexpectedly on Process capwap_brain
CSCvq42724	WLC sends clients DHCP DISCOVER or REQUEST packets via wrong destination port UDP 68
CSCvq44627	ME : Efficient upgrade failed with http download
CSCvq49277	Cisco 8540 controller reloads unexpectedly on Task name: emWeb
CSCvq52834	AP2800/3800/4800 doing CAC after radio up/down on DFS channel in Local Mode
CSCvq53705	ME UI not operational due to "error in setting port number"
CSCvq54695	Traffic from home network is seen by client on Cisco 1815t RLAN port
CSCvq59233	Cisco 2802AP: Kernel panic crash: PC is at _Z27clickps_atomic_dec_and_testP8atomic_t
CSCvq59683	Cisco Wireless LAN Controller Path Traversal Vulnerability
CSCvq60744	HA SSO active WLC reloads unexpectedly due to apfReceiveTask
CSCvq63117	Client can not send the traffic, when two clients in different VNID joins the network
CSCvq64828	Radio stopped working on AP2800 and rcore was created
CSCvq66811	Cisco Wave 1 AP goes out of memory and fails to reply to assoc/reassoc from clients
CSCvq67649	WLC - certain AP Airewave Director Configuration is not listed in 'show run-config'
CSCvq69068	Cisco Wave 1 AP drops M2 when client is roaming

Caveat ID Number	Description
CSCvq70602	CAPWAPd experiences watchdog timeout while trying to connect to cleanaird IPC socket
CSCvq71200	WLC Sent RST after TACACS+ authentication request cause login failed.
CSCvq71817	WLC OUI file incompatibility
CSCvq72812	Cisco Wave 2 APs dropping CAPWAP keepalive and unable to join 9800 WLC
CSCvq72831	Cisco Wave 1 APs: Cisco FlexConnect LS marks CS3 trafic to BE priority while connected to 9800 WLC
CSCvq80582	Cisco 9120, 9115 APs: low throughput issues, legacy rates with PMF Required
CSCvq81315	Cisco 2700 AP PCI0 reloads unexpectedly with Cisco CleanAir enabled
CSCvq81388	Wave1 AP resetting 5GHz radio often with radio reset code 44, messages with "DTX marked with poison"
CSCvq82562	Cisco Wave 1 Access points not passing BPDUs in flex+bridge mode when connected to eWLC
CSCvq83205	After AP-SSO failover, WLC fails to send EAPOL M1
CSCvq84949	Cisco 9120 AP on DFS Channels not responding to probe request causing client join problems
CSCvq84965	Cisco 9120 AP: click has the client stale entries in client IP table
CSCvq86217	Cisco 9120 AP: show controller dot11 1 shows QBSS as 100% with 13 clients connected
CSCvq88525	Cisco 2800 AP: radio stopped working in newdp-dma-thread-stuck
CSCvq92184	Clients unable to connect to AP with data encryption enabled
CSCvq92379	AP9120 dual_dfs rmmod causes kernel crash
CSCvq92443	AP9120 Flooding "chatter: our own containing BSSID"
CSCvq92716	GUI display - version info is impacted by config
CSCvq95330	Cisco Wave 2 APs: WGB does not send IAPP message in static IP config
CSCvr01310	AireOS 8.x || MN country code Regulatory domain (-E) for Outdoor missing on WLC
CSCvr01652	CWA broken for SDA in 8.9
CSCvr01892	Cisco 2800 AP SW reloads unexpectedly on process hostapd
CSCvr02462	Cisco 9120 AXE: AP continuously reboot when connected to 8.9.1 or 16.12.1 release build
CSCvr07053	Lot of aptraced cores seen on production network with 16.12.1

Caveat ID Number	Description
CSCvr09722	Cisco 1832 APs: Association denied because AP is unable to handle additional associated STAs
CSCvr11240	Cisco 1815T AP leaking client MAC from LAN3 to WAN port
CSCvr14071	Cisco 3802 AP when CAPWAP resets, it does not send disassociate
CSCvr14081	Cisco 3802 AP: No Rx packets seen for 5-GHz radio
CSCvr14946	Cisco 1815t AP: CDP is not sent over WAN interface even after being enabled.
CSCvr18534	Cisco 8540 WLC stopped working - "Crash function not supported by this task: RRM-MGR-2_4-GRP"
CSCvr22918	Cisco 9115AX, 9120AX APs: When non-broadcasted SSID is configured, beacons are corrupted
CSCvr23173	Cisco 9117 AP: invalid radar detection on non-serving channel, SF 04205492
CSCvr27788	5GHz radio on 1562E-G APs Operationally Down - Regulatory Domain Failure when Pakistan is Configured
CSCvr28017	Cisco WLC does not show -A regulatory domain for 5 GHz radio with country code PA (Panama)
CSCvr29590	Cisco Controller local EAP does not send access-reject on auth failure
CSCvr33340	Wave 2 APs in FlexConnect mode sending Auth Request to AAA without Local Auth Enabled
CSCvr34339	Cisco AP unexpectedly reloads with "watchdog reset(wcpd)"
CSCvr34683	WLC resets its config to factory default after power-cycle
CSCvr35607	WLC displays login banner after login, not before login like in older codes
CSCvr35679	Flex LS, Central Authentication and Local Association - CCKM, roaming failure due to RN mis-match
CSCvr36185	Cisco 2800 series APs are using 802.11n rates with WPA+TKIP only WLAN
CSCvr36693	WLC 8540 OID returns small number than actual traffic size
CSCvr37120	HTTPS traffic to SP of WLC always allowed even if CPU ACL is configured in 8.5 and above
CSCvr38675	Client connectivity failure seen after LAN link flap
CSCvr39587	MAPs failing mesh_sec_auth and excluding Parent upon RAP failure
CSCvr40133	Add support in AP for checking supported controller versions for 16.12 and 17.1 branches
CSCvr43311	Unable to set syslog login level to all the APs "Unable to set the Log Trap level"

Caveat ID Number	Description
CSCvr46272	Web Auth is required when client move to another AP during 4-way handshake
CSCvr50556	Cisco 9120 AP Half Duplex Mismatch messages seen on mGig port of 9300, 9400 controller
CSCvr50874	Cisco 3800 AP running]release 8.5.144.49: kernel panic crash
CSCvr54605	9115 sending 2 reassoc-resp with different SN and size for FlexConnect local sw central auth roam
CSCvr55000	Cisco 9120ax unable to pass traffic during throughput test
CSCvr57817	Cisco Wave 1APs are adding C0 to the AID in assoc-resp when configured as flexconnect central assoc.
CSCvr59946	WLC sent the wrong VLAN tag to the AP when local switching change to Central Switching VLAN
CSCvr63068	Cisco Controller RADIUS or TACACS+ servers in disabled state after multiple reboots
CSCvr71272	Cisco 3504 wlc: Free Timer Depletion leads to wlc unexpectedly reloading and clients cannot connect
CSCvr72088	SJSU: Memory leak in NMSP connection
CSCvr75831	Few Cisco Wave 1 AP client is loosing connectivity on roaming
CSCvr82181	WLC reloads unexpectedly while accessing GUI > Monitor > Clients page
CSCvr82193	Wave2 AP Flex local RADIUS fallback with FT Enabled -Standalone mode PMKID is seen in Assoc Response
CSCvr85760	Cisco Wave 2 APs sending - Invalid AID 0 received
CSCvr86159	Primary Controller 5520 in 8.9.111.0 rebooted unexpectedly
CSCvr88965	Cisco 3800 AP adding extra padding to EAP-ID-REQ
CSCvr95403	Client ARP entry remains even if the client is disconnected
CSCvr96406	Cisco 9120 AP sending wrong client statistics to controller
CSCvr97368	HTTPS and SSH traffic dead slow with CTS inline tagging enabled
CSCvr98813	Cisco 9120 AP flash write error: No space left on device with 250M available
CSCvs01333	Cisco Controller sending incorrect certificate password for Cisco FlexConnect local auth EAP-TLS
CSCvs14548	Trustpoint Configuration Fails on Wave 2 APs in WGB
CSCvs19446	Cisco 9115 AP flex local auth clients stuck on dot1x on 16.12.1sES1
CSCvs22775	Cisco 2800, 3800 AP running 8.10.105.0: Deauth frame not sent for contained clients

Caveat ID Number	Description
CSCvs22835	Cisco AP with SHA2 MIC certificate fails to join WLC with config ap cert-expiry-ignore mic enable
CSCvs27550	Cisco 1815 AP Kernel Panic pointing to Ethernet driver with large size packet traffic
CSCvs29183	WLC still shows weak SSH encryption algorithms with encryption high enabled
CSCvs39989	Cisco controller on 8.10.105.0 resets due to unexpected reloading of the switch-driver
CSCvs59018	AP disjoins Mobility Express primary after configuring RADIUS server with non-default port
CSCvs63593	AP3802-P-k9 Transmit Power Adjustment with AIR-ANT2513P4M-N (13dBi) W52 Japan Outdoor

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.