Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.9.111.0

First Published: 2019-06-06

Last Modified: 2022-08-30

About the Release Notes

We recommend that you use this software release only in networks deployed with Cisco Catalyst 9100 Series Access Points.

This release notes document describes what is new or changed in this release, instructions to upgrade to this release, and 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 Cisco Wireless 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 Servers 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 WLC, Cisco 5520 WLC, and Cisco 8540 WLC.
- Cisco Mobility Express Solution

Supported Cisco Access Point Platforms

The following Cisco AP platforms are supported in this release:

- Cisco Catalyst 9120 Access Points
  - C9120AXI: VID 06 and earlier
- 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 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

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 8.9.111.0

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

Note For complete listing of all the documentation published for Cisco Wireless Release 8.9, see the Documentation Roadmap:

https://www.cisco.com/c/en/us/td/docs/wireless/doc-roadmap/doc-roadmap-release-89.html

Cisco Catalyst 9120 Access Points

Cisco Catalyst 9120 Access Points provide a seamless wireless experience anywhere and goes beyond the Wi-Fi 6 (802.11ax) standard. The access points provide integrated security, resiliency, and operational flexibility as well as increased network intelligence.

In the Cisco's intent-based networks of all sizes, the Cisco Catalyst 9120 APs scale to the growing demands of IoT devices while fully supporting the latest innovations and new technologies.

Note The following C9120 model VIDs are supported in this release:

- C9120AXI: VID06 and earlier

For more information about Cisco Catalyst 9120 APs, see

https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9120ax-series-access-points/datasheet-c78-742115.html

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 8.9.110.0

Current Software Release	Upgrade Path to Release 8.9.111.0
8.6.x	You can upgrade directly to Release 8.9.111.0.
8.7.x	You can upgrade directly to Release 8.9.111.0.
8.8.x	You can upgrade directly to Release 8.9.111.0.

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

- 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.

- On executing the **show tech-support** command on a Cisco 9100 AP, if the displayed result is empty, as a workaround, logout and relogin to the same access point using SSH and run the command. For more information, see CSCvo28881.
- 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.
- If you are downgrading from Release 8.9 to an earlier release, any local policy to WLAN ID mapping wherein the local policy ID is greater than 255 is lost after the downgrade. If necessary, you can modify the policy mapping so that a local policy whose ID is greater than 255 is not used.

  You can check for the local policy ID in either of the following ways:

  - CLI: Enter the **show policy summary** command.
  - GUI: Navigate to **Security** > **Local Policies**. On the **Policy List** page, the policy ID is displayed along with the policy name.

- 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 Version 3.0(4d) 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 CIMC 3.0(4d) images are available at the following locations:

Table 3: CIMC Utility Software Image Information

Controller	Link to Download the CIMC Utility Software Image
Cisco 5520 Wireless Controller	https://software.cisco.com/download/home/286281345/type/283850974/release/3.0%25284d%2529
Cisco 8540 Wireless Controller	https://software.cisco.com/download/home/286281356/type/283850974/release/3.0%25284d%2529

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

Table 4: Open Caveats for Release 3.0(4d)

Caveat ID	Description
CSCvj80941	After upgrading CIMC to 3.04d, only after power reset, UCS-based controller is coming up.
CSCvj80915	Not able to logon to the CIMC GUI with the username and password that are configured from the controller.

Table 5: Resolved Caveats for Release 3.0(4d)

Caveat ID	Description
CSCvd86049	**Symptom**: The system will stop working or reboot during OS operation with PROCHOT, MEMHOT, and DMI Timeout-related events reported in the System Event Log (SEL). **Conditions**: C220-M4 or C240-M4 **Workaround**: No workaround is available. This bug fix changes the default BIOS option for ASPM (Active State Power Management) from 'L1 only' to 'Disabled', and the ASPM setting can no longer be modified. This change was made to help increase system stability and eliminate some system crash scenarios.
CSCvf78458	**Symptom**: The system will stop working or reboot during OS operation with PROCHOT, MEMHOT, and DMI Timeout-related events reported in the System Event Log (SEL). **Conditions**: C220-M4 or C240-M4 **Workaround**: No workaround is available. This bug fix changes the BIOS option "Package C-State limit" default value from C6 Retention to C0/C1 to help increase system stability and eliminate some crash scenarios. Once upgraded, reset the BIOS settings to default or manually change Package C-State limit to C0/C1.

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 6: Test Bed Configuration for Interoperability

Hardware or Software Parameter	Hardware or Software Configuration Type
Release	8.9.x
Cisco Wireless Controller	Cisco 5520 Wireless Controller
Access Points	C9115AXE-B, C9117AXI-B, C9120AXI-B

Hardware or Software Parameter	Hardware or Software Configuration Type
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, PSK (WPA-TKIP-WPA2-AES), 802.1X (WPA-TKIP-WPA2-AES)(EAP-FAST)
RADIUS	Cisco ACS 5.3, Cisco ISE 2.2, Cisco ISE 2.3
Types of tests	Connectivity, traffic (ICMP), and roaming between two APs

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

Table 7: Client Types

Client Type and Name	Driver / Software Version
Laptops	
ACER Aspire E 15	Windows 8.1
Acer Aspire E 15 E5-573-3870	Windows 10 Pro
Apple Macbook Air	OS Sierra v10.12.2
Apple Macbook Air 11 inch	OS Sierra 10.12.6
Apple Macbook Air 11 inch mid 2013	OS Sierra 10.12.3
Apple Macbook Air 11 inch Mid 2013	OS X Yosemite 10.10.5
Apple Macbook Air 13inch (mid 2011)	OS Sierra 10.12.4
Apple Macbook Pro OS X v10.8.5 mid 2009	OS X 10.8.5
Apple Macbook Pro Retina 13 inch early 2015	OS Sierra 10.12.6
Apple Macbook Pro Retina 13 inch late 2013	OS Sierra 10.12.4
DELL Inspiron 13-5368 Signature Edi	Win 10 Home 18.40.0.12
DELL Inspiron 15-7569	Windows 10 Home 18.32.0.5
DELL Latitude 3480	Win 10 Pro 12.0.0.307
DELL Latitude E5430	Windows 7 Professional 15.1.1.1
DELL Latitude E5430	Windows 7 Professional 15.17.0.1
DELL Latitude E6430 Dekra TB	Windows 7 Professional 6.30.223.60
DELL latitude E6840	Windows 7 Professional 6.30.223.215
DELL Latitude E7450	Windows 7 Professional 6.30.223.245
DELL Latitude Intel Centino N 6205	Win 8.1 Pro 15.18.0.1
DELL XPS 12 9250	Windows 10 Home 18.40.0.9

Client Type and Name	Driver / Software Version
DELL XPS 12 v9250	Windows 10 19.50.1.6
FUJITSU Lifebook E556 Intel 8260	Windows 10 Pro 19.20.0.6
HP Chromebook Chrome OS	Chrome OS 55.028883.103
Lenovo Thinkpad Yoga 460	Windows 10 Pro 20.20.2.2
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	
Amazon Kindle	Ver 6.2.2
Apple iPad 2 MC979LL/A	iOS 9.3.1
Apple iPad Air2 MGLW2LL/A	iOS 11.4.1
Apple iPad Air 2 MGLW2LL/A	iOS 10.2.1
Apple iPad Air MD785LL/A	iOS 11.4.1
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 MK6L2LL/A	iOS 10.2
ET50PE Enterprise Tablet	Ver5.1.1
Google Nexus 9 Tab	Android 6.0.1
Motorola ET1 ENTERPRISE TABLET	ANDROID VERSION: 2.3.4
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 Galaxy TAB SM-P600	Android 4.4.2
Samsung Tab Pro	Samsung Android 4.4.2
Samsung Tab Pro SM-T320	Android 4.4.2
Samsung Tab SM-T520	Android 4.4.2
Toshiba TAB AT100	Android 4.0.4
Mobile Phones	
Apple iPhone 5	iOS 10.3.12

Client Type and Name	Driver / Software Version
Apple iPhone 5c	iOS 10.3.3
Apple iPhone 7 MN8J2LL/A	iOS 11.2.5
Apple iPhone 8 plus	iOS 12.0.1
Apple iPhone 8 Plus MQ8D2LL/A	iOS 12.0.1
Apple iPhone MD237LL/A	iOS 9.3.5
Apple iPhone SE MLY12LL/A	iOS 11.3
Apple iPhone X MQA52LL/A	iOS 12
ASCOM Myco2	Build 2.1, Android Version 4.4.2
ASCOM Myco2	Build 4.5, Android Version 4.4.2
ASCOM Myco2	Platform Version 10.1.0
ASUS Nexus 7	Android 6.0
AT100	Android 4.0.4
Cisco CP 7925G-EX	1.4.8.4.LOADS
Cisco CP 7926G	1.4.8.4.LOADS
Cisco CP 7926G	1.4.5.3.LOADS
Cisco CP 8821	rootfs8821.11-0-3ES2-1
Google Pixel	Android 8.1.0
HTC One 6.0	Android 5.0.2
HTC PI39100	Android 7.5
Huawei MATE9 Pro LON-L29	Android 7.0
Huawei MediaPad. X1 7.0	Android 4.4.2
Huawei P7-L10	Android 4.4.2
LG D855	Android 5.0
Motorola ET1 Enterprise Tablet	Android 2.3.4
Motorola ET50PE Enterprise Tablet	Android 5.1.1
Motorola MC75A	OEM ver 02.37.0001
Motorola MC9090	Windows Mobile 6.1
Motorola MC9090G	OEM Ver 1.35
Moto X 2nd gen	Android 5.0
Nokia Lumia 1520 0268	Windows 10
Nokia Lumia 925.5	Windows 8.1
One Plus One	Android 4.3

Client Type and Name	Driver / Software Version
Samsung Galaxy Mega GT-i9200	Android 4.4
Samsung Galaxy Note 3 - SM-N9005	Android 5.0
Samsung Galaxy Note4 edge	Android 6.0.1
Samsung Galaxy S10.P.1.4	Android 9
Samsung Galaxy S4	Android 4.2.2
Samsung Galaxy S4	Android 4.2.2
Samsung Galaxy S4	Android 5.0.1
Samsung Galaxy S4 GT 19500	Android 5.0.1
Samsung Galaxy S6	Android 7.0
Samsung Galaxy S6	Android 6.0.1
Samsung Galaxy S7	Android 6.0.1
Samsung Galaxy S8	Android 7.0
Samsung S7 SM-G930F	Android 7.0
Samsung SM-P600	Android 4.4.2
Samsung SM-T520	Android 4.4.2
Spectralink 8440	Android 5.0.0.1079
Spectralink 8742	Android 5.1.1
Spectralink 8742	Android 5.1.1
Spectralink 8744	Android 5.1.1
Spectralink 9553	Android 8.10.0
Symbol MC40	Android Ver 4.4.4
Symbol MC40N0 EZ	Android ver: 4.1.1
Symbol MC55A	Windows 6.5
Symbol MC 7090	OEM Ver 03.33.0000
Symbol MC92N0	Android Ver 4.4.4
TC510K	Android 6.0.1
TC8000	Android 4.4.3
Zebra TC510K	Android Ver: 6.0.1
Zebra TC520K	Android Ver: 8.1.0
Zebra TC57	Android Ver: 8.1.0
Zebra TC700H	Android Ver:4.4.3
Zebra TC75	Android Ver: 4.4.3

Client Type and Name	Driver / Software Version
Zebra TC8000	Android Ver: 4.4.3
Zebra TC8000	Android Ver: 5.1.1
Zebra WT6000	Android Ver 5.1.1
Drager M300	
Drager Delta	
Printers	
Zebra QLn320 Printer	Ver: V 68.20.15ZP41800
Zebra ZQ620 Printer	V85.20.15

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 WLC

- 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 WLCs

- 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 WLC

- 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 features that are not supported on various Cisco Aironet AP platforms:

Key Features Not Supported in Cisco Catalyst 9120 APs

Table 8: Key Features Not Supported in Cisco Catalyst 9120 Series APs

Operational Modes	• Downlink High Efficiency MU-MIMO • Uplink MU-MIMO • Downlink OFDMA • Uplink OFDMA • BSS coloring • Workgroup Bridge (WGB) mode • Mesh mode • Mobility Express • Web Security Appliance (WSA) Sensor • Target Wake Time (TWT)

Key Features Not Supported in Cisco Catalyst 9117 APs

Table 9: Key Features Not Supported in Cisco Catalyst 9117 APs

Operational Modes	• Downlink High Efficiency MU-MIMO • Uplink MU-MIMO • Downlink OFDMA • Uplink OFDMA • BSS coloring • Mobility Express • Target Wake Time (TWT)

Key Features Not Supported in Cisco Catalyst 9115 APs

Table 10: Key Features Not Supported in Cisco Catalyst 9115 Series APs

Operational Modes	• Downlink High Efficiency MU-MIMO • Uplink MU-MIMO • Downlink OFDMA • Uplink OFDMA • BSS coloring • Mobility Express • RF channel width 80+80 MHz

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

For detailed information about feature support on Cisco Aironet Wave 2 APs, see:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-7/b_feature_matrix_for_802_11ac_wave2_access_points.html.

Table 11: 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 • Mesh mode • 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)

FlexConnect Features	• Split Tunneling
	• 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 12: 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 13: 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

Caveats

Open Caveats

Table 14: Open Caveats

Caveat ID Number	Description
CSCvb70551	Cisco Wave 2 APs reboot due to kernel panic-not syncing: Out of Memory
CSCvj48316	AP3700: process "QoS stats process" causes unexpected reloads
CSCvj61869	20-30 Mbps downlink speed on 702w AP with WPA2+802.1x SSID
CSCvm63975	Cisco controller loses config if specific countries are enabled together
CSCvm65411	Cisco 2700 AP radio resets with FC71 code
CSCvm68341	Cisco controller is sending duplicate interim accounting packets to ISE
CSCvm81901	Cisco 3800 AP does not acknowledge the client frames
CSCvm93785	Cisco 2800, 3800 AP reloads unexpectedly on Click: Client update cache from write handler
CSCvn03560	Decrypt errors seen on Cisco 702 AP
CSCvn15777	Cisco 5508 controller reloads unexpectedly with high CPU util on emWeb process

Caveat ID Number	Description
CSCvn17267	702AP: WGB disconnects from root AP 'parent lost: Too many retries' RTS when root AP is offchanl
CSCvn27144	Unable to restore 802.11ac MCS parameter
CSCvn37957	Cisco controller FTIE not saved sending Association Response FT 802.11r
CSCvn56211	Cisco 702W AP radio resets, tracebacks and other radio buffer errors
CSCvn62176	Cisco 3802 series APs unable to associate clients when using UNII-1 Channels
CSCvn69015	Cisco Wave 2 APs in local mode forwards layer 2 multicast control traffic from their wired interface
CSCvn99809	Handling PAK scheduler during AID plumbing
CSCvo28881	AP9115, 9117: show tech-support is empty with only section heading.
CSCvo50532	Cisco 1572 AP reporting "nokey" errors
CSCvo55603	Cisco 4800 series access points not requesting UPoE power when connected to Cisco 94xx switch.
CSCvo71753	AP side: Multicast Traffic stops working when enabling Inline Tagging on CTS
CSCvo74306	Cisco 1815W APs: Per-user BW contract not working with web policy
CSCvo87937	"FW crashed" reload on 2800/3800/4800/1560 AP, with ATF + MU-MIMO
CSCvp00688	EFT <TUD> : Cisco 2800, 3800 AP radio reloads unexpectedly
CSCvp03798	Wave1 APs: FlexConnect local EoGRE reloads unexpectedly due to Memory fragmentation "Net Background"
CSCvp11765	Wireless client fail to associate to Cisco 1830 APs until reboot
CSCvp18422	Cisco controller running 8.5.135.0 reloads unexpectedly with taskname spamApTask6
CSCvp21915	RSN IE length mismatch between assoc and EAPOL-M2 frame
CSCvp58062	Cisco 1815 AP Radio core dump due to beacon stuck FW hang
CSCvp88088	AP9117: FW crash @whal_recv_recovery.c:834 (RX_BACKPRESSURE_MONITOR_BUF_EMPTY) (SF 04035754)

Resolved Caveats

Table 15: Resolved Caveats

Caveat ID Number	Description
CSCvj69298	Data Plane reloads unexpectedly due to RPE/Double bit errors

Caveat ID Number	Description
CSCvk70379	8.5_ Stale clients exist in Cisco controller
CSCvk79765	apstatEngineMsgQ MSGQ_RUNNING_HIGH or MSGQ_SEND_FAILED Queue Utilization Issues
CSCvm65360	Cisco controller redirects to internal webauth login page after successful external webauth login
CSCvm90337	Cisco 18xx APs unexpectedly reload due to 'radio failure(radio recovery failed)'
CSCvm91854	Cisco 8540 controller becomes inaccessible with systemDb corruption
CSCvn74948	Cisco APs reloads unexpectedly with watchdog process sxpd
CSCvn87656	Cisco Wave 2 APs reloads unexpectedly in the context of QCA driver @ click_packet_type_event_hook
CSCvn98214	Cisco 1830 AP: core-radio1FW found during WGB association, WGB did not join
CSCvn98598	FT 802.1X clients cannot authenticate after ME primary AP / N+1 controller failover
CSCvo26556	WLC reloads unexpectedly on the command "config network ssh host-key use-device-certificate-key"
CSCvo28124	Local switching WLANs is changed to central switching in some scenarios
CSCvo48363	Cisco controller reloads unexpectedly when viewing multicast MGID in GUI
CSCvo48759	AP deauths associated clients with reason code 7, Class 3 frame received from nonassociated STA
CSCvo90764	AP4800: AP recurrent unexpected reloads found in multiple places
CSCvo98569	Cisco Wave 1 AP: EoGRE upstream/downstream packet drops observed for flex local EoGRE
CSCvp07442	Cisco controller reloads unexpectedly on task 'tplusTransportThread'
CSCvp07829	On Toggling the CDP state of the 4800 AP, The AP turns off and shows as Ieee PD on the switch.
CSCvp26465	AireOS HA: The mobility hash keys are not getting synced UP in AireOS
CSCvp36496	The beamforming configuration gets back to the default after AP reload and rejoined to controller
CSCvp41629	Regulatory domains of 802.11bg changes to -A after slot 0 switches 5 GHz
CSCvp52994	WLC fails to learn AAA VLAN, fails to send Central Switched VLAN on second Add mobile
CSCvp57188	Cisco 4800 AP memory leak in kmalloc-512 and kmalloc-1024 in 8.8.X.X code

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 Cisco WLCs, lightweight APs, and mesh APs, see these documents:

- The quick start guide or installation guide for your particular Cisco WLC or access point
- Cisco Wireless Solutions Software Compatibility Matrix
- *Cisco Wireless Controller Configuration Guide*
- *Cisco Wireless Controller Command Reference*
- *Cisco Wireless Controller System Message Guide*

For all Cisco WLC 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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.