Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.9.100.0

First Published: 2019-04-10

Last Modified: 2019-11-22

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*.

Content Hub

Explore the Content Hub, the all-new product documentation portal in which you can use faceted search to locate content that is most relevant to you, create customized PDFs for ready reference, benefit from context-based recommendations, and much more.

Get started with the Content Hub at https://content.cisco.com/ to craft a personalized documentation experience.

Do provide feedback about your experience with the Content Hub.

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 9115 Access Points

• Cisco Catalyst 9117 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 8.9.100.0

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 9100 Access Points

The Cisco Catalyst 9100 Access Points are IEEE 802.11ax standard compliant APs. The 802.11ax standard allows access points support more clients in dense environments and provides a better experience for typical wireless LAN networks. The 802.11ax standard also provides a more predictable performance for advanced applications such as 4K or 8K video, high-density high-definition collaboration applications, all-wireless offices, and Internet of Things (IoT).

Wi-Fi 6 Features

OFDMA Support for 802.11ax APs: Using the OFDMA technology, the Cisco 9100 APs support eight spatial streams and deliver up to 4800-Mbps throughput at the physical layer. OFDMA-based channel access is backward-compatible with traditional EDCA/CSMA, and Cisco 9100 access points use each channel optimally.

MU-MIMO: Provides concurrent downstream communications to multiple wireless devices for more efficient use of the spectrum.

Target Wake Time (TWT): The TWT feature reduces the network energy consumption through better scheduling and spectrum optimization. Devices enter a doze state until their TWT arrives, thereby significantly increasing battery run time, an important requirement for IoT devices.

1024 Quadrature Amplitude Modulation (QAM): The QAM feature increases throughput in Wi-Fi devices by encoding more data in the same amount of spectrum.

Note For more information about feature support in 802.11ax APs, see Feature Matrix for Cisco Wave 2 Access Points and Wi-Fi 6 (802.11ax) Access Points.

Power Requirements

- We recommend that you pair the Cisco Catalyst 9115 APs with an 802.3at PoE-capable switch to get the best performance from these APs. If the power supply is not 802.3at-capable, there is a drop in performance that is related to Tx power and spatial streams.

  Note Under critically low power conditions, the AP LED might blink in a loop of red, blue, and green color, and the controller GUI summary page might display power supply as medium power.

- We recommend that you pair the Cisco Catalyst 9117 APs with an UPoE switch. This allows the external USB module to be attached to the USB port on the APs.

Models

The following 802.11ax AP models are supported:

- Cisco Catalyst 9115 Access Points

  For more information about Cisco Catalyst 9115 APs, see

  https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/datasheet-c78-741988.html

- Cisco Catalyst 9117 Access Points

  For more information about Cisco Catalyst 9117 APs, see

  https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/datasheet-c78-741989.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 8.9.100.0

Current Software Release	Upgrade Path to Release 8.9.100.0
8.6.x	You can upgrade directly to Release 8.9.100.0.
8.7.x	You can upgrade directly to Release 8.9.100.0.
8.8.x	You can upgrade directly to Release 8.9.100.0.

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 are upgrading from Release 8.0.140.0 or 8.0.15x.0 to a later release and also have the multiple country code feature configured, the feature configuration is corrupted after the upgrade. For more information, see CSCve41740.

- 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

Controller	Link to Download the CIMC Utility Software Image
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.

Caveat ID	Description
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, C9117AXE-B
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	

Client Type and Name	Driver / Software Version
ACER Aspire E 15	Windows 8.1 11.0.0.492
Acer Aspire E 15 E5-573-3870	Windows 10 Pro 11.0.0.492
Apple Macbook Air	OS Sierra v10.12.2
Apple Macbook Air 11 inch	OS Sierra 10.12.6
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
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

Client Type and Name	Driver / Software Version
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
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

Client Type and Name	Driver / Software Version
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
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

Client Type and Name	Driver / Software Version
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
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 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 8: 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 9: 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 10: 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 11: Open Caveats

Caveat ID Number	Description
CSCvo28881	AP9115, 9117: show tech-support is empty with only section heading
CSCvo36670	AP9115: LED becoming dark during initial boot-up creating ambiguity on AP state
CSCvo75152	AP9115: Ucode crash @ INCR_OVFL0_DEAD due to Rx hang detection - tracking RX Hangs R0: 0x1ff16c9
CSCvo77090	AP9117: 11ax EFT: Firmware assert at whal_recv_recovery.c:834
CSCvp12679	Cisco 9117 AP: Firmware assert at ar_wal_tx_de.c:50 followed by Kernel Panic - no core files
CSCve42897	Controller unexpectedly reloads with "NMI received for unknown reason 2d on CPU 0" during traffic
CSCvh81618	When adding a member to RF Group with static leader 8510 or 8540, group size exceeded error
CSCvi77141	HA_send_usmDbSpamSetRadSlotBand, ErrType:Apply Config failed on Standby
CSCvj48316	AP3700: process "QoS stats process" causes unexpected reloads
CSCvk42225	Maximum clients reached on AP. Sending association response failure with reason code 17.
CSCvm46237	Cisco 1562 radio1 operational status down for all channels in the blocked list not going back up
CSCvm63736	Erratic multicast throughput
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
CSCvm68624	Cisco Wave 1 AP console display logs 'DTX DUMP'
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
CSCvm95330	Cisco controller ignores DBS Max Best Channel Width Allowed

Caveat ID Number	Description
CSCvn03560	Decrypt errors seen on Cisco 702 AP
CSCvn07126	Cisco FlexConnect - Cisco 2802 AP's lowers the priority UP on QoS on the downlink transmit
CSCvn11713	Cisco AP702w Beacon Stuck
CSCvn15777	Cisco 5508 controller reloads unexpectedly with high CPU util on emWeb process
CSCvn31768	WLC cLWebAuthWlanConfigTable OID is broken when MS-OPEN feature is enabled on one of the SSIDs
CSCvn37957	Cisco controller FTIE not saved sending Association Response FT 802.11r
CSCvn42067	MAPs Client radio (slot 0) chanAutoCfg changes from CONFIG_AUTO to CONFIG_STATIC at random
CSCvn49888	Cisco 702, 1532 AP has tracebacks and beacons stuck with load 8.5.140.0
CSCvn53435	C3702AP on 8.5.140.0: %DOT11-2-RADIO_RX_BUF: 1E72C72C leads to unexpected reloads with reason 44
CSCvn56211	Cisco 702W AP radio resets, tracebacks and other radio buffer errors
CSCvn87656	SJSU 1815 click crash in the context of qca driver @ click_packet_type_event_hook
CSCvn95727	XOR Radio in 5GHz is sending some traffic at disabled data rates
CSCvn98598	FT 802.1X clients cannot authenticate after ME primary AP / N+1 controller failover
CSCvo17872	Cisco 3800 AP running 8.5.140.0: FIQ/NMI reloads unexpectedly
CSCvo25646	Split ACLs not being saved in the APs after they reboot
CSCvo35676	Cisco controller does not send registration request to satellite server
CSCvo48759	AP deauths associated clients with reason code 7, Class 3 frame received from nonassociated STA
CSCvo49625	AP 802 does not complete ARP
CSCvo50532	AP1572 reporting "nokey" errors
CSCvo55603	Cisco 4800 series access points not requesting UPoE power when connected to Cisco 94xx switch.
CSCvo57350	Cisco 1852 AP LED blinks amber even while it's successfully serving clients
CSCvo74306	Cisco 1815W APs: Per-user BW contract not working with web policy
CSCvo79313	FW whal_interrupt.c:341, whal_interrupt.c:347 Assertion on 8.9.4.41 (SF 03923061)
CSCvo85485	5 GHz radio Rx high due to incorrect 802.11ac MCS9 with 1SS/2SS in 20 MHz

Caveat ID Number	Description
CSCvo87382	Central European Time (CET) is not reflected correctly as per Daylight Saving Time (DST)
CSCvo90764	AP4800: AP recurrent unexpected reloads found in multiple places
CSCvp01439	Cisco 1815 AP leaking RLAN VLAN traffic when port looped
CSCvp05117	P-Q domain Wave 2 APs cannot join the controller and the AP reloads unexpectedly

Resolved Caveats

Table 12: Resolved Caveats

Caveat ID Number	Description
CSCut85555	APF_HA-3-SYNC_RETRANSMIT_FAIL Messages in show msglog
CSCvd67485	Cisco 3700 AP Tx stop Radio reset due to false radio Tx inprog count
CSCvf57867	Only single IMM / CIMC IP addr configured for both controller active and standby
CSCvf99887	MAP Gigabit port being learnt in Mesh management VLAN instead of client VLAN
CSCvg14610	bsnMeshNeighsTable walk sporadically fails
CSCvg76166	Channel utilization changes to 0% on a certain Cisco Wave 1 APs
CSCvg91770	Cisco 1810W AP stops to send data frame intermittently
CSCvh24354	ME/Flex local - MN_REASSOC_TIMEOUT / EAP negotiation failures
CSCvh83197	Cisco 1560 AP will create a loop when failing over to wireless and wired connection comes back
CSCvi02072	Cisco Wave 2 APs: ETSI 5G adaptive Wi-Fi compliance fix
CSCvi02980	Cisco Controller becomes inaccessible with client rate limiting
CSCvi04556	SSO failover causes mobilty tunnels go down
CSCvi09095	Radio Reset Tx Jammed seen on both 8.3 and 8.5 releases
CSCvi09153	Cisco Wave 1 APs radio reset due FST14 FW: cmd=0x31 seq=6 due to mcast stuck in radio
CSCvi10888	Cisco AP intermittently stops transmitting Beacon for 12 and 85 seconds
CSCvi12046	Cisco 2800 AP: FlexConnect AP WLAN-VLAN Mapped incorrectly
CSCvi13589	Locally generated webadmin certificate shows as 3rd party after upgrade on 8.3 code
CSCvi25532	Standby 8540 controller-reloads unexpectedly with rmgrMain due to IPC timeout

Caveat ID Number	Description
CSCvi25724	Cisco Wave 1 APs unexpectedly reloads due to bad CPQ on 8.5 release code
CSCvi42632	AP generating 'hostapd' core files, does not respond to EAPOL
CSCvi48503	Standby controller continuously reboots with "Reason: XMLs were not transferred from Active to Standby"
CSCvi49126	RSN IE validation fails in M2 (802.11r session timeout) after reassociation causing deauth code 17
CSCvi51536	Access Point is not sending TCP fragments over the air
CSCvi52529	Controller: Unexpected reload occurs due to OsapiBsnTimer increase memory, no crash file is generated
CSCvi57213	Cisco 1832 AP unexpectedly reloads with 'PC is at __napi_complete+0x28/0x60'
CSCvi59432	Creation time of Local Net User set to Jan 1 00:00:00 1970
CSCvi61401	Cisco controller remote access failing after upgrade
CSCvi65222	802.11 arp-cache does not work if BVI VLAN and client VLAN are different
CSCvi67565	TrustSec: AP picks wrong SXP Node ID
CSCvi70783	Wireless Service Assurance WSA DNA Assurance certficate is not upated on controller
CSCvi73013	Cisco Wave 1 AP deauthenticating client due to idle timeout
CSCvi73402	Cisco 1810W AP not giving IPs to cell phones using WPA/TKIP protocol
CSCvi74683	AIR-CT3504 mGig showing FCS errors incrementing
CSCvi80815	Add a warning when FRA is disabled to warn a user that XOR radio will not revert back to 2.4Band
CSCvi82147	Failed to set Country Codes when controller has redundant country codes CA2, KR, PH2, US2, USL, USX
CSCvi82384	Unwanted "Warning: time of day goes back (-240985959us), taking countermeasures." on 1542 AP
CSCvi82746	Cisco controller reloads unexpectedly with Task Name SISF BT Process
CSCvi84511	Cisco 3800 AP with Wired1 (aux) LAN enabled - CDP-4-DUPLEX_MISMATCH messages constantly logged
CSCvi84734	Cisco 702w AP: client intermittently cannot connect- decrypt errors
CSCvi85464	AP specific configuration lost post ap reload - wlan-acl mappings and policies lost
CSCvi85834	New Mobility CAPWAP control keepalive should not plumb keys when receiving unencrypted responses

Caveat ID Number	Description
CSCvi86276	Cisco controller reloads unexpectedly on emWeb due to too many HTTP buffers received
CSCvi86834	Mesh Ethernet bridging - wired client associated to MAP fails to pass traffic over tagged VLAN
CSCvi90766	Cisco AP with regulatory domain Morocco cannot join the Cisco controller
CSCvi91017	The FlexConnect groups are missing in backup configuration file
CSCvi91285	Install mapping on radio backhaul for Wave 2 APs Flex+Bridge setting is not retained after reboot
CSCvi92170	Cisco 1800 series APs falsely shows 100% channel utilization on 5GHz
CSCvi93045	Cisco 2800 AP CleanAir goes down (sensord died)
CSCvi96066	Cisco Wave2 APs on 8.5MR3:2.4GHz backhaul map will not connect to RAP/Wave2 AP client low throughput
CSCvi96690	Cisco 2800 AP detects Intel Dual Band Wireless-AC 8260 as rogue client/AP
CSCvi96718	Cisco ME (Mobility Express) unexpectedly reloads on DHCP spamSendConfigSync
CSCvi97282	Assigning a NetFlow monitor to the WLAN will internally enable AVC on the Cisco controller
CSCvi98357	Cisco AP1815I : reloads unexpectedly due to 'watchdog reset(sync_log)'
CSCvj01739	Cisco WiSM2 unexpectedly reloads on task name sshpmLscTask after initial config
CSCvj03161	Cisco Wave 1 APs not reporting known interference with disabled WSSI module
CSCvj04401	Client remains stuck in DHCP-REQD state on Anchor side unless ISE NAC is disabled on the anchor side
CSCvj06837	Cisco Wave 1 MAP: Mesh security failures after roaming between 2 parents
CSCvj07190	Cisco 2800 AP not joining the controller if 'Enable NAT Address' feature is enabled
CSCvj07930	Cisco 3802, 2802 AP with DART connectors has a Tx power value of 0
CSCvj08387	Cisco controller reloads unexpectedly while working on spamApTask6
CSCvj11251	Cisco 2802 AP not sending re-association response to Cisco 8821 phone
CSCvj11270	Watchdog reset out of memory on Cisco 3800 AP running 8.3.133.0 code
CSCvj11397	Cisco 3504 Controller - OpenDNS registration failure - Return 77
CSCvj12234	Cisco Wave 2 AP boot up would fail, errmsg "failed execution Repeat wlFwGetHwSpecs"
CSCvj13920	Cisco controller reloads unexpectedly due to task name RRM-MGR-2_4-GRP

Caveat ID Number	Description
CSCvj13958	Cisco Wave 2 3800,2800 APs sending beacon on wrong channels intermittently on 5GHz
CSCvj14729	Upgrading Mobility Express to 8.7.102.0, causes it to reload unexpectedly in a continuous loop
CSCvj17181	Cisco controller's GUI does not allow spaces while creating a webauth CSR certificate
CSCvj18004	Cisco AP on 8.5MR3 Interim code cannot join with NAT address on management interface of controller
CSCvj23106	Cisco Rx SOP global configuration not applied to new Access Points
CSCvj25194	Clean up debug lisp map-server output for AP onboarding
CSCvj25768	Bridge mode Cisco Wave 2 Mesh APs bridging issues
CSCvj25842	Cisco 1815I AP: Kernel panic: PC is at vfs_read+0x14/0x134
CSCvj28658	Cisco 1810wAP kernel panic leads to unexpected reload on PC at ieee80211_node_authorize+0x90/0xb8
CSCvj29270	Flex AP's WLAN-VLAN mapping mismatch in multiple controller scenarios
CSCvj32199	SSH/Management Access of Primary controller is not possible when HA failover occurs in 8.5.120.0
CSCvj32563	Transfer download on Cisco controller fails with error message when no APs are upgrading
CSCvj32624	Cisco 702 AP as WGB keeps getting disconnected from the WLAN due to parent lost: Missed beacons
CSCvj32964	WGB is only allowing 8 MAC addresses pass traffic using 3802 AP [as CAPWAP AP and 3702 AP as WGB]
CSCvj33381	Cisco AP: process wcpd causes unexpected reloads
CSCvj33894	Add 'show advanced hyperlocation summary' to 'show run-config' and 'show tech'
CSCvj35883	Allow Cisco 2800, 3800 APs to be able to convert to sensor mode
CSCvj36633	Cisco Wave 1 APs: fail to boot after upgrade due to file corruption
CSCvj36853	AP name corruption after upgrade
CSCvj36923	Cisco AP name mismatch with controller on join
CSCvj37393	Cisco Wave 2 APs not sending probe response when SSID is not broadcasted
CSCvj38456	Cisco controller is losing its EoGRE configuration after reboot
CSCvj39005	[SDA] Wireless Clients losing L2VNID override when performing Switchover on Cisco 5520 controller

Caveat ID Number	Description
CSCvj41040	Cisco 1800 APs in Cisco FlexConnect mode, fail FT roam
CSCvj41853	Incorrect Tx power on AP3802P-Q on some channels
CSCvj46554	CONFIGSYNC-3-CONFIG_SYNC_SEM_REL_FAIL & CLEAN_TASK: Reaper cleaning up exited task 'ConfigSync'
CSCvj47445	Cisco controller sending CAPWAP discovery response when it has no available licenses
CSCvj48364	Cisco Controller is generating client traps without a session-id
CSCvj50100	AP free memory leak - downstream frames are dropped before forwarding to radio driver
CSCvj50170	Client coming back within 10 seconds of cleanup time is stopping the DHCP timer on the controller
CSCvj53743	Cisco 1572IC AP: Channels and Maximum Power Settings settings spreadsheet incorrect values for V02
CSCvj54432	Cisco controller unexpectedly reloads on task Dot1x_NW_MsgTask_2
CSCvj60609	Cisco vWLC web authentication not working
CSCvj60738	Beacon Stuck for last 60s on slot 0. Triggering Radio core...
CSCvj62672	Cisco controller sending wrong NAS ID when AAA override is enabled
CSCvj65449	AIR-AP1562D-E-K9 with regulatory domain Kazakhstan does not join the controller
CSCvj70569	Cisco 2800, 3800,4800 APs: Incorrect Tx power on power on till we configure Tx power using Cisco controller
CSCvj70604	Cisco Mesh APs Best-Effort Tx queue stuck
CSCvj72076	Cisco 1800 AP drops a lot of packets
CSCvj72136	Cisco 2800, 3800 APs loose its ability to reach the default gateway
CSCvj72766	UX AP:Primed UX AP reset to UX when SNTP server is configured
CSCvj72890	Cisco 5520 controller reloads unexpectedly when RADIUS server returns invalid value in Airespace-ACL-Name
CSCvj74144	9800:AP keep flap with Failed to receive data keepalive with CAPWAP v6 tunnel having link-encryption
CSCvj76378	Local policy is not applied when foreign controller is running 8.3.141.0
CSCvj77078	Cisco controller unexpectedly reboots on Dot1x_NW_MsgTask_1
CSCvj77328	Cisco 4800 AP does not forward DHCP Offer downstream
CSCvj79841	Cisco 3802 AP reboots unexpectedly

Caveat ID Number	Description
CSCvj80129	Cisco Wave 2 AP uses invalid CAPWAP-Data keep-alive source port
CSCvj80388	Flex-ACL on Wave 2 APs denying host instead of subnet
CSCvj80388	Flex-ACL on Wave 2 APs denying host instead of subnet
CSCvj81101	Cisco 2800, 3800 VAPs/TBTT timers are not enabled properly
CSCvj81526	AP name is "AP0000.0000.0000" on new/factory reset APs
CSCvj83372	Cisco 1852 AP showing irregular data usage
CSCvj86238	Cisco controller stops working as emWeb spikes to 100% CPU usage after executing 'show run-config'
CSCvj90820	SAFEC-3-SAFEC_ERROR: while checking fabric status with show fabric summary
CSCvj91645	Clients not getting exported to anchor on New Mobility
CSCvj95744	Cisco 3700 AP -Downstream ping test fails for WGB wired client with FlexConnect local switching
CSCvj97129	Neighbor packet Tx failure on Cisco 1542, 1562, and 1815 APs
CSCvj97430	Mobility Express AP - Loop detected that causes AP reboot
CSCvj97602	Cisco Controller Client RSSI and SNR values to be updated as part of Assoc & reassoc request processing
CSCvk00884	The controller is replying with the wrong value for the following OID: bsnAPIfProfileParamAssignment
CSCvk00885	In the Controller's GUI, DHCP Address Assignment gets disabled after any sucessive WLAN configuration
CSCvk01283	AP Trustsec: Cisco 1850, 2800, 3800 APs reloading with watchdogd process sxpd gone for 60s
CSCvk02024	Cisco 1850 APs experiencing frequent and unexpected reloads due to memory corruption
CSCvk02153	Wave 1 AP WLAN Client Stats cldcClientDataRetries counter is zero
CSCvk05150	OpenDNS profile keeps being mapped for client when the username changes
CSCvk05965	Cisco controller in HA SSO: standby controller is in a reboot loop
CSCvk09135	Unexpected reload in emWeb while monitoring rogue APs
CSCvk09513	AP is not downloading the controller's 85Mr3 image rather it says image is already in the backup
CSCvk12146	Spurious messages getting printed on Cisco 2800, 3800 APs while enabling or disabling a WLAN

Caveat ID Number	Description
CSCvk14267	Observed XML and Invalid config during upload and download of the controller's configuration
CSCvk15043	Wave 1 APs - AP radio FW image install failure in the bootup loop
CSCvk15068	Cisco Wave 1 APs recovery logic for failure on primary image
CSCvk15165	Cisco Controller reloads unexpectedly after modifying SNMP trap controls via GUI
CSCvk18752	Cisco 1815AP: Incorrect VCI string of DHCP option 60
CSCvk20484	IPC timeout and tracebacks reported on HA pair running 8.5.131.0 (8.5MR3)
CSCvk20801	MAC OUI database not getting updated
CSCvk21816	Downstream traffic marking traffic with UP3 in Wave 2 APs,same policy working fine in IOS-APs 16.3.X
CSCvk22312	Hotspot 2.0 OSU SSID is picking profile name
CSCvk23508	No legacy rates; default to lowest CCK/OFDM rate
CSCvk23577	Client is unable to connect due to the 'Failed to create a timer' error
CSCvk24360	Cisco controller's power supply status is incorrect when there is no power supply
CSCvk25593	Cisco 1542, 1815I APs - Ethernet interface flapping when connected to 100Mbit switchports
CSCvk25644	Cisco controller HA standby reboots reaching maintenance mode due to missing NaServCaCert_p12.pem on Active
CSCvk26519	Cisco 1562 MAP stops sending Block ACK once the Cisco 1572 RAP moves to another controller
CSCvk26563	Cisco 1810W AP running 8.2.170.4 code: 5G radio FW resets @0x009A4F9F
CSCvk26732	New Flash recovery logic
CSCvk27093	NAS-ID in WLAN cannot be changed in the startup-command after you saved once
CSCvk27250	System not operational with task apfRogueTask_3
CSCvk29178	Cisco 1550 AP: BVI interface uses a different MAC-Address than the Gigabit interface
CSCvk35047	Cisco controller stops working when LAG mode is enabled on the AP
CSCvk36463	Support Bundle output only genertaes WSA core bundle when WSA is enabled
CSCvk36887	Some clients cannot associate because their entry is not getting deleted at the controller
CSCvk38453	AP does not initiate the CAPWAP discovery process, it gets stuck during the PNP discovery process

Caveat ID Number	Description
CSCvk39197	SSH session closes abruptly
CSCvk39704	Wave 2 APs not sending discovery request to Multicast address resulting AP join Failure in IPv6 n/w
CSCvk39841	Change SSID name with SNMP fails with commitFailed
CSCvk39948	Cisco controller is not returning the expected prompt when logging in via SSH
CSCvk41068	Advance IPMI is not set and causing fan noise
CSCvk41249	Controller on 8.7 code does not present full certificate chain on web authentication guest portal
CSCvk41512	Cisco Wave 2 APs in sniffer mode not sending frames with AMSDU 1500 Bytes to destination
CSCvk41603	Controller -Unable to add or delete DCA channels in RF-Profile while Channel width configured as 80 MHz
CSCvk43936	Cisco 2800, 3800 AP with LAG enabled would bridge BPDU packets
CSCvk44959	Cisco controller reloads unexpectedly on Taskname 'emWeb'
CSCvk45006	Cisco Mesh Ethernet bridging:-unable to configure more than 12 allowed VLANs on Mesh APs
CSCvk46817	AIR-AP2802I not sending beacons with both radios in 5GHz
CSCvk47740	Unable to configure Pre-auth ACLs for RLAN in the Cisco Mobility Express UI
CSCvk51634	Wave 2 Flex Efficient Upgrade fails as primary AP sends empty image_str to controller
CSCvk53499	Cisco APs do not reconnect, error log: System reached max concurrent DTLS Handshakes
CSCvk53743	8.5_New mobility:UI throws wrong error message while adding used public IP
CSCvk53883	ME GUI: preauth ACL rules disappear when VLAN tagging is enabled on WLAN
CSCvk55651	Cisco 1852 AP failure of association due to set CAPWAP tunnel failed
CSCvk56651	BSSID/Client Rate Limit prevent clients to pass traffic on Mobility Express
CSCvk56753	8.8 - Cisco Wave 2 APs not working with 802.1x port security
CSCvk59498	Cisco 3702 AP: High CPU utilization under NCI Rx. Unable to join the controller
CSCvk59536	Unable to upgrade to 8.8+ ME from 8.7 release
CSCvk61078	VLAN priority tag inside the EoGRE packet set to non-zero when 802.1p set to none in LOCAL mode
CSCvk62055	Cisco Wave 2 APs preimage download fails after 64 retries with poor WAN link

Caveat ID Number	Description
CSCvk62240	Controller Smart license 8.8: The license summary(information) is not syncing in after switchover
CSCvk62355	CAP2800 on ME image 8.6.101.0, 8.7.106.0 reloads unexpectedly in ewsContexSendRedirect200->ewaDate
CSCvk62680	Cisco controller not releasing licenses after reboot
CSCvk63215	Cisco 1852 series APs Kernel Panic due to NSS memory corruption
CSCvk63459	Cisco 3802, 4800 AP drops packets larger than 1426 (inner IP) with VxLAN
CSCvk64247	Cisco controller sends Link up trap when LAG member link down on standby controller
CSCvk64674	Cisco Wave 1 APs advertise Adaptive FT MDIE on probe response for open SSID
CSCvk65908	Cisco 5520 controller reloads unexpectedly with taskname emWeb when checking "show tech-support"
CSCvk66975	AP as a sensor reports all configured tests status as onboarding failure
CSCvk70185	Controller Smart License: Smart license registration failing for ProductInstance not valid in switchover
CSCvk70980	Cisco 2800 APs drop packets resulting in low throughput
CSCvk72075	Cisco controller is sending incorrect counter value for the broadcast and multicast throgh SNMP
CSCvk75036	Broadkey Key Renewal shown as 4-Way key handshake failure instead of 2-way key handshake failure
CSCvk76043	Unable to associate clients with PSK/dot1x security in FlexConnect standalone mode
CSCvk79597	Frequent DFS detection
CSCvm00214	Cisco WiSM2 memory leak due to hotspot_anqp
CSCvm01723	Sensor: Sensor functionality broken when Domain name used for DNA
CSCvm04245	Cisco 1810W AP reports low power after requesting and receiving 14.2W after upgrading to 8.5.131.0
CSCvm05695	AAA override for native VLAN with flexlocal switching not applied to client on Cisco 1562 AP
CSCvm10326	Default Virtual AP IP address is wrong
CSCvm10519	Intergrated Management Module (IMM) summary shows a username which is multiple usernames merged
CSCvm10538	Intergrated Management Module (IMM) username command changes password of second user always

Caveat ID Number	Description
CSCvm10544	Cannot disable some SNMP traps
CSCvm11060	After soft-roam of client, client is not able to see new Apple TV from associated AP-Grp VLAN
CSCvm11861	Cisco Wave 2 APs FIQ/NMI reloads unexpectedly on the radio driver
CSCvm13837	vWLC reloads unexpectedly while fetching memory statistics during longevity run
CSCvm15167	MSCB are not cleared, when client joins a WLAN, reassociates, and joins 2 different WLANs
CSCvm15625	DCA channel assignment on XOR radio is broken while static 5G assignment
CSCvm18273	Handling of Cisco 702W AP reloads due to memory limitation from 8.5release and other memleak fixes
CSCvm21666	Cisco 4800 series AP takes pre-download of unsupported code
CSCvm22144	sensord repeatedly asserts after radio reloads until cleanair is disabled
CSCvm22760	dot1x Supplicant config is not removed from Cisco Wave 1 AP after it is disabled globally on the controller
CSCvm23672	Cisco Wave 2 APs sometimes do not send IAPP update after client address change
CSCvm25082	EoGRE clients ARP Response inside CAPWAP gets corrupted
CSCvm26277	Cisco 1815w AP: RLAN multicast does not work with local mode local switch
CSCvm32197	Cisco controller reloads unexpectedly on webauth_redirect_main task
CSCvm33978	Apple iPad devices are getting profiled as Apple device
CSCvm34641	Cisco controller is sending packets out to Gateway with DF =1 when inside header is set DF =0 -EoGRE
CSCvm37510	Cisco controller reloads unexpectedly due to SNMP memory corruption
CSCvm37979	AP Heatmap does not display Mesh Link SNR
CSCvm40443	Cisco 2702e AP: Reset to Defaults (Except IP) Button does not work correctly from GUI
CSCvm41626	Assoc/Disso stat trap on GUI enables enhanced Assoc/Disso stat trap but does not generate stat traps
CSCvm41771	Cisco controller allows RF-profile with all rates disabled
CSCvm43028	Number of DX messages in sync Queue ... 440001[805520.362884] Controller reloads unexpectedly..Queue
CSCvm46810	Cisco controller reloads unexpectedly in Dot1x_NW_MsgTask_7 due to validateWpaKeyStateSTART

Caveat ID Number	Description
CSCvm46823	DNAC Wireless Assurance does not respond to POST causing controller to timeout & eventually drop data
CSCvm48446	Unexpected reload in "Dot1x_NW_MsgTask_*"
CSCvm51362	Cisco controller reloads unexpectedly due to data plane crash
CSCvm51648	Controller's open auth guest clients unable to pass traffic and PEM state struck in STATICIP_NOL3SEC
CSCvm52509	When a Cisco 2800 -E AP has both radios on 5 GHz, one radio turns -A
CSCvm58235	Cisco 2802E AP with DART connector - custom RF profile not always applied properly to XOR
CSCvm59899	Cisco 1532 non-root does not learn the distance from the root
CSCvm62202	Cisco 1852 AP Kernel Panic at ClientCapabilitiesTracker
CSCvm62619	Cisco controller reloads unexpectedly with task emweb after 'debug flexconnect' command is typed
CSCvm62803	Cisco controller allows to configure OEAP ACLs in software version that do not support them
CSCvm65774	Cisco controller allows to configure OEAP ACLs via CLI in software version that do not support them
CSCvm65858	Cisco 2800 APs using Flexible Radio Assignment has admin status and clean air status down
CSCvm69246	Cisco controller applying wrong interface policy to re-associated client after SSO
CSCvm71487	Cisco 2800, 3800 APs: dropping the Neighbor Advertisement for Global IPv6 address
CSCvm72007	Incorrect VLAN mapping when using MAC filtering and PSK
CSCvm73244	Cisco 3800AP in sniffer mode not capturing ACK,RTS in 8.7 and 8.8 CSCvf74377
CSCvm78368	Leak in I/O memory - middle buffers - due to LWAPP IPv6
CSCvm80592	Cisco 2800 AP reloads unexpectedly with ERROR TAMD device 'ap-tam' heartbeat failure
CSCvm82471	FT 802.1x/PSK Clients are not able to authenticate to Flexconnect Wave 2 AP after HA Failover
CSCvm83223	Cisco 1832AP: Kernel panic: PC is at _raw_spin_lock+0x44/0x84
CSCvm84941	Cisco 1600, 1700 APs: memory leak due to packets accumulation
CSCvm97915	Cisco controller includes NULL Bytes within the JSON it posts
CSCvn03915	After controller upgrades it reloads unexpectedly due to kernel panic

Caveat ID Number	Description
CSCvn04046	Cisco 2800,3800 AP does not map the DSCP to the correct WMM UP Value for FlexConnect Local Switching
CSCvn11947	Cisco 1815w:RLAN port traffic will get stuck at TX direction after end device restarts several times
CSCvn13314	Cisco 2802, 3802 APs: Default SSID "IP Cheetah" broadcasted during AP boot up
CSCvn14292	Cisco 3800 AP running 8.2.170.2 code reloads unexpectedly
CSCvn18615	APs could not authenticate with ISE 2.5.0.311 when EAP method is set as EAP-FAST
CSCvn20446	Wireless client moves from local switching SSID to central switching SSID DHCP traffic gets dropped
CSCvn27111	Controller on 8.8.114.54 reloads unexpectedly due "pmalloc detected memory corruption spamAP Task4"
CSCvn27902	%SAFEC-3-SAFEC_ERROR observed while decoding iPSK key from RADIUS
CSCvn32314	Cisco 2800 AP on 8.8.114.54 reloads unexpectedly due to WCPD
CSCvn54782	IGMP snooping needs to be enabled for Local Mode Local switching RLAN
CSCvn66293	Cisco 3802 AP relays CDP Packets from wireless devices using Cisco IP Communicator to the switch
CSCvn66715	Cisco 3800 AP stops passing traffic under client with Intel NIC 8260/8265 load in MU-MIMO deployment
CSCvn71004	Cisco controller Mbuf allocation problem / Mbuf Max reached
CSCvo05093	Cisco controller reloads unexpectedly with task name radiusTransportThread

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 Connected Mobile Experiences

Cisco Connected Mobile Experiences Documentation

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.