Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.8.111.0

First Published: 2018-10-10

Last Modified: 2019-05-16

About the Release Notes

This release notes document describes what is new or changed in this release, instructions to upgrade to this release, and provides information about the open and resolved caveats for this release. Unless otherwise noted, in this document, Cisco Wireless Controllers are referred to as *controllers*, and Cisco lightweight access points are referred to as *access points* or *APs*.

Revison History

Table 1: Revision History

Modification Date	Modification Details
January 30, 2019	Added a note about issues related to Cisco Wave 1 AP flash and the solution to address them in the Upgrading Cisco Wireless Release section.

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 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 8.8.111.0

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 8.8, see the Documentation Roadmap:

https://www.cisco.com/c/en/us/td/docs/wireless/doc-roadmap/doc-roadmap-release-88.html

Cisco Intelligent Capture

The Intelligent Capture feature provides support to have a direct communication link between Cisco DNA Center and access points (APs), so each of the APs can communicate with Cisco DNA Center directly. Using this channel, the Cisco DNA Center can receive packet capture data, AP and client statistics, and spectrum data.

For more information about configuring Intelligent Capture feature, see the applicable *Cisco DNA Center Assurance User Guide* at

https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-user-guide-list.html

Cisco 1800s Sensor

For more information about configuring the Cisco 1800s Sensor, see the applicable *Cisco Digital Network Architecture Center User Guide, Release 1.2.5* at:

https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-user-guide-list.html

IPSK Flex Mode Local Switching based P2P Blocking

In this release, this feature is enhanced to support FlexConnect mode Local Switching-based IPSK P2P blocking.

Sleeping Client Management in L2+L3 Authentication Mode

In this release, this feature is enhanced to function with L2+L3 enabled WLANs. This enhancement can be enabled only with dot1x+Webauth security setup.

Inter-Release Controller Mobility (IRCM) with Cisco Catalyst 9800 Series Wireless Controllers

In this release, Inter-Release Controller Mobility (IRCM) with Cisco Catalyst 9800 Series Wireless Controllers is supported.

For more information about IRCM, see the *Cisco Catalyst 9800 Wireless Controller-Aireos IRCM Deployment Guide* at:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b_c9800_wireless_controller-aireos_ircm_dg.html

Early Field Trial Features

The Cisco Wave 2 APs as Workgroup Bridges feature is in Early Field Trial state.

Note This feature is not yet officially supported and there will be no assistance from Cisco's Technical Assistance Center.

Software Release Types and Recommendations

Table 2: Release Types

Release Type	Description	Benefit
Maintenance Deployment (MD)	Software releases that provide bug-fix support and ongoing software maintenance. These releases are categorized as Maintenance Deployment (MD). These releases are long-living releases with ongoing software maintenance.	Provides you with a software release that offers stability and long support duration with periodic maintenance releases (MRs).
Early Deployment (ED)	Software releases that provide new features and new hardware platform support in addition to bug fixes. These releases are categorized as Early Deployment (ED). These releases are short-lived releases.	Allows you to deploy the latest features and new hardware platforms or modules.

For detailed release recommendations, see the *Guidelines for Cisco Wireless Software Release Migration Bulletin* at:

http://www.cisco.com/c/en/us/products/collateral/wireless/8500-series-wireless-controllers/bulletin-c25-730741.html.

Table 3: Upgrade Path to Cisco Wireless Release 8.8.x

Current Software Release	Upgrade Path to Release 8.8.x
8.2.x	You must upgrade to an 8.5.x release and then upgrade to Release 8.8.x.
8.3.x	You must upgrade to an 8.5.x release and then upgrade to Release 8.8.x.
8.4.x	You must upgrade to an 8.5.x release and then upgrade to Release 8.8.x.
8.5.x	You can upgrade directly to Release 8.8.x.
8.6.x	You can upgrade directly to Release 8.8.x.
8.7.x	You can upgrade directly to Release 8.8.x.

Upgrading Cisco Wireless Release

This section describes the guidelines and limitations that you must be aware of when you are upgrading the Cisco Wireless release and the procedure to upgrade.



Caution Before you upgrade to this release, we recommend that you go through the following documents to understand various issues related to Cisco Wave 1 AP flash and the solution to address them:

- Field Notice: https://www.cisco.com/c/en/us/support/docs/field-notices/703/fn70330.html
- Understanding Various AP-IOS Flash Corruption Issues: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/213317-understanding-various-ap-ios-flash-corru.html

Guidelines and Limitations

- Legacy clients that require RC4 or 3DES encryption types are not supported in Local EAP authentication.
- If you downgrade from Release 8.8.x to Release 8.7, FlexConnect IPv6 ACLs are shown to be in their FlexConnect group.
- If you have an AVC profile with *default-class* setting and you downgrade from Release 8.8.x to an earlier release, the *default-class* setting is still present in the controller, although the earlier releases do not support this setting.
- If you want to downgrade from Release 8.8.x to Release 8.6.101.0 and if you have Wave 2 APs in Flex+Bridge mode, ensure that these APs are changed to Bridge mode before you perform the downgrade; else, the APs will have incorrect configuration after the downgrade process.

- If you downgrade to Release 8.0.140.0 or 8.0.15x.0, and later upgrade to a later release and and also have the multiple country code feature configured, then the configuration file could get corrupted. When you try to upgrade to a later release, special characters are added in the country list causing issues when loading the configuation. For more information, see CSCve41740.



Note Upgrade and downgrade between other releases does not result in this issue.

- After downloading the new software to the Cisco APs, it is possible that a Cisco AP may get stuck in an upgrading image state. In such a scenario, it might be necessary to forcefully reboot the controller to download a new controller software image or to reboot the controller after the download of the new controller software image. You can forcefully reboot the controller by entering the **reset system forced** command.
- It is not possible to download some of the older configurations from the controller because of the Multicast and IP address validations. See the "Restrictions on Configuring Multicast Mode" section in the *Cisco Wireless Controller Configuration Guide* for detailed information about platform support for global multicast and multicast mode.
- When a client sends an HTTP request, the controller intercepts it for redirection to the login page. If the HTTP GET request that is intercepted by the controller is longer than 2000 bytes, the controller drops the packet. Track the Caveat ID CSCuy81133 for a possible enhancement to address this restriction.
- When downgrading from one release to an earlier release, you might lose the configuration from your current release. The workaround is to reload the previous controller configuration files that are saved in the backup server, or to reconfigure the controller.
- When you upgrade 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 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 controller or any AP during the upgrade process. If you do this, the software image might get corrupted. Upgrading 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 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.

- From Release 8.3 or a later release, ensure that the configuration file that you back up does not contain the < or > special characters. If either of the special characters is present, the download of the backed up configuration file fails.

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, or SFTP 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**, or **SFTP**.

Step 8 In the **IP Address** field, enter the IP address of the TFTP, FTP, or SFTP server.

Step 9 If you are using a TFTP server, the default value of 10 retries for the **Maximum Retries** field, and 6 seconds for the **Timeout** field should work correctly without any adjustment. However, you can change these values, if required. To do so, enter the maximum number of times the TFTP server attempts to download the software in the **Maximum Retries** field and the amount of time (in seconds) for which the TFTP server attempts to download the software, in the **Timeout** field.

Step 10 In the **File Path** field, enter the directory path of the software.

Step 11 In the **File Name** field, enter the name of the software file <*filename.aes*>.

Step 12 If you are using an FTP server, perform these steps:

a) In the **Server Login Username** field, enter the username with which to log on to the FTP server.
b) In the **Server Login Password** field, enter the password with which to log on to the FTP server.
c) In the **Server Port Number** field, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 13 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 14 After the download is complete, click **Reboot**.

Step 15 If you are prompted to save your changes, click **Save and Reboot**.

Step 16 Click **OK** to confirm your decision to reboot the controller.

Step 17 If you have disabled the 802.11 networks, reenable them.

Step 18 (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 4: 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 5: 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 6: 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 used for testing the client devices.

Table 7: Test Bed Configuration for Interoperability

Hardware or Software Parameter	Hardware or Software Configuration Type
Release	8.8.x.
Cisco Wireless Controller	Cisco 5520 Wireless Controller
Access Points	AIR-CAP3802E-B-K9, AIR-AP1852E-B-K9
Radio	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-AE
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 8: Client Types

Client Type and Name	Driver / Software Version
Laptops	
Acer Aspire 15 Windows 8 Home	Qc Atheros Qca9377 11.0.0.492
Acer Aspire E15 Windows 8	Qc Atheros Qca9377 15.1.1.1
Acer Aspire E 15 Windows 8.1	QC Atheros Qca9377 11.0.0.492
Acer Aspire E15 Windows 8.1 Pro	Qc Atheros Qca9377 11.0.0.492

Client Type and Name	Driver / Software Version
Dell Inspiron 15 7569 Windows 10 Home	Ntel Ac 3165 18.32.0.5
Dell Latitude 6430 Windows 8.1 Pro	Intel 6205w8 15.16.0.2
Dell Latitude E5430 Windows 7	Intel Centrino N 6205 15.17.0.1
Dell Latitude E5450 Windows 7 Professional	Intel 7260 18.33.6.2
Dell Latitude E5540 Windows 7	Intel Dualband Ac7260 1.566.0.0
Dell Latitude E6430 Windows 7 Professional	Intel Centrino Ultn6300 15.9.2.1
Dell Latitude E6430 Windows 7 Professional	Intel 6250 15.11.0.7
Dell Latitude E6430 Windows 7 Professional	Intel 3160 6.30.223.215
Dell Latitude E7450 Windows 7 Professional	Broadcom 1560 15.1.1.1
Dell Latitude Windows 8.1 Pro	Intel Ac7260 18.33.3.2
Fujitsu Lifebook E556 Windows 10 Pro	Intel 8260 11.0.0.492
Lenovo Yoga 460 Windows 10 Pro	Intel Ac8260 19.1.0.4
Macbook Air Mac OS Sierra 10.12.3	Broadcom Bcm43xx 1.0 6.30.225.29.1
Macbook Air Macos Sierra 10.12.6	Broadcom Bcm43xx 1.0 7.21.171.68.1a4
Macbook Air OS X Yosemite (10.10.5)	Broadcom Bcm43xx 1.0 7.15.166.24.3
Macbook Mac OS Sierra 10.12 Beta	Broadcom Bcm43xx 1.0 7.21.149.34.1a7
Macbook Pro Mac OS Sierra 10.12.4	Broadcom Bcm43xx 1.0 7.21.171.68.1a4
Macbook Pro OS X 10.8.5	Broadcom Bcm43xx 1.0 5.106.98.100.17
Macbook Pro Retina Mac OS Sierra 10.12.3	Broadcom Bcm43xx 1.0 7.15.166.24.3
Tablets	
Apple iPad	iOS 9.3.1
Apple iPad mini	iOS 12.0
Apple iPad mini 2	iOS 10.3.1
Apple iPad Air	iOS 10.1.1
Apple iPad Air 2	iOS 10.2.1
Mobile Phones	
Apple iPhone 4S	iOS 8.0
Apple iPhone 5	iOS 10.3.1
Apple iPhone 5C	iOS 9.3.2
Apple iPhone 6 Plus	iOS 12.0
Apple iPhone SE	iOS 10.3.1
AT100	Toshiba Android 4.0.4

Client Type and Name	Driver / Software Version
Cisco 7925G-EX	CP7925G-1.4.8.4.LOADS
Cisco 7926G	CP7925G-1.4.8.4.LOADS
Cisco 8821	sip8821.11-0-4-14
ET1	Android VERSION 2.3.4
ET5	Android 5.1.1
LG-D855	LG Android 5.0
Mediapad X1 7.0	Huawei Android 4.4.2
Moto X 2nd Gen	Motorola Android 5.0
One Plus One	One Plus Android 4.3
One Plus Three	One Plus Android 6.0.1
Samsung Galaxy S4	Samsung Android 4.2.2
Samsung Galaxy S4	Samsung Android 5.0.1
Samsung Galaxy S6	Samsung Android 7.0
Samsung Galaxy S6	Samsung Android 6.0.1
Samsung Galaxy S8	Samsung Android 7.0
Samsung Tab Pro	Samsung Android 4.4.2
SM-P600	Samsung Android 4.4.2
SM-T520	Samsung Android 4.4.2
TC510K	Zebra Android 6.0.1
TC8000	Zebra Android 4.4.3
8742	Spectralink Android 5.1.1
8744	Spectralink Android 5.1.1 2.5.0

Key Features Not Supported in Cisco WLC Platforms

This section lists the features that are not supported on various Cisco WLC platforms:



Note In a converged access environment that has Cisco WLCs 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 Cisco WLC 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
- Cisco WLC 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 9: Key Features Not Supported in Cisco Aironet 1800i, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800, 3800, and 4800 Series APs

Operational Modes	• Autonomous Bridge and Workgroup Bridge (WGB) mode • 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 10: Key Features Not Supported in Cisco Aironet 1800i, 1810 OEAP and 1810W Series APs

Operational Modes	Mobility Express
FlexConnect Features	Local AP authentication
Location Services	Data RSSI (Fast Locate)

Key Features Not Supported in Cisco Aironet 1830, 1850, and 1815 Series APs

Table 11: Key Features Not Supported in Cisco Aironet 1830, 1850, and 1815 Series APs

Operational Modes	Mobility Express is not supported in Cisco 1815t APs.
FlexConnect Features	Local AP Authentication
Location Services	Data RSSI (Fast Locate)

Key Features Not Supported in Mesh Networks

- Load-based call admission control (CAC). Mesh networks support only bandwidth-based CAC or static CAC
- High availability (Fast heartbeat and primary discovery join timer)
- AP acting as supplicant with EAP-FASTv1 and 802.1X authentication

- AP join priority (Mesh APs have a fixed priority)
- Location-based services

Key Features Not Supported in Cisco Aironet 1540 Mesh APs

- Dynamic Mesh backhaul data rate.

Note We recommend that you keep the Bridge data rate of the AP as auto.

- Background scanning
- Noise-tolerant fast convergence

Key Features Not Supported on Cisco Aironet 1560 APs

- MAC Authentication FlexConnect Local Authentication
- Noise-tolerant fast convergence
- Static WEP

Caveats

Open Caveats

Table 12: Open Caveats

Caveat ID Number	Description
CSCvd91152	Cisco 2700, 3700 series APs reload - %DOT11-2-RADIO_RX_BUF: Corrupt buf
CSCvf57867	Only single IMM / CIMC IP addr configured for both controller active and standby
CSCvi77141	HA_send_usmDbSpamSetRadSlotBand, ErrType:Apply Config failed on Standby
CSCvj80129	Cisco Wave 2 AP uses invalid CAPWAP-Data keep-alive source port
CSCvj81526	AP name is "AP0000.0000.0000" on new/factory reset APs
CSCvk42225	Max client reached on AP. Sending association response failure with reason code 17
CSCvk76386	Reaper Reset due to too much cpu while SW Watchdog is disabled - various processes
CSCvm11861	Cisco Wave 2 AP-COS FIQ/NMI reloads unexpectedly on the radio driver
CSCvm33978	Apple iPad devices are getting profiled as Apple device
CSCvm58235	Cisco 2802E AP with dart connector - custom RF profile not always applied properly to XOR

Caveat ID Number	Description
CSCvm62619	Cisco controller reloads unexpectedly with task emweb after 'debug flexconnect' command is typed
CSCvm65411	Cisco 2700 AP radio resets with FC71 code
CSCvm68341	Cisco controller is sending duplicate interim accounting packets to ISE
CSCvm69246	Cisco controller applying wrong interface policy to re-associated client after SSO
CSCvm84145	Multiple Vulnerabilities in OpenSSL
CSCvm89668	Cisco 1542 AP reloads unexpectedly due to kernel panic-cascade+0x60/0x88
CSCvn04046	Cisco 2800,3800 AP does not map the DSCP to the correct WMM UP Value for FlexConnect Local Switching
CSCvn10187	IOS Flex LSLA AP Client VLAN issue, clients getting IP from incorrect VLAN
CSCvn15777	Cisco 5508 WLC reloads unexpectedly with high cpu util on emWeb process
CSCvn17267	702AP: WGB is disconnectig from root AP 'parent lost: Too many retries' RTS when root AP is offchanl
CSCvn18259	Cisoc 1702 AP did not recognize association request, ACK from wireless client
CSCvn23565	Cisco 702w AP enables POE in LAN 4 before joining Cisoc WLC after reboot
CSCvn26130	Cisco 3702 AP reloads unexpectedly due to Encryption Engine Stuck
CSCvn35621	Cisco Wave 1 AP sends multiple control subtype frames on very low RSSI
CSCvn36636	Cisco IOS FlexConnect AP changes VLAN ID for SSID
CSCvn37291	Cisco 819: AP group name on AP module is missing after router reload
CSCvn37957	WLC FTIE not saved sending Association Response FT 802.11r
CSCvn38028	8.5 MAP - IOS_PKI_SHIM: PKI_SignMessage PostHashEncrypt ret 1 Error
CSCvn40052	SC2/SC3 not recognising the ACK from the client at Cell Edges
CSCvn41324	Standby WLC keeps unjoined AP Stats entry even if Stats is cleared on Active WLC
CSCvn41371	[Cisco 1832i AP/8.8.100] TKIP first M5 not encrypted immediately after M1-M4
CSCvn43971	AAA override pmk-cache can result in unwanted L3 inter-controller roaming
CSCvn46394	Unable to do PAC provisioning if Auth server shared secret is changed
CSCvn47094	CLI not taking all the commands sent via "paste"
CSCvn47628	Cisco 3700 AP Slot 2 module reloads unexpectedly
CSCvn48626	CAP1552H 15.3(3)JD6 Autonomous Status LED not lighting. It is unlit (Off).

Caveat ID Number	Description
CSCvn48931	Cisco 2800 ME controller reloads unexpectedly with FIQ/NMI reset on 8.5.135.73.
CSCvn49888	Cisco 702W AP has tracebacks and beacons stuck with load 8.5.140.0
CSCvn50968	Invalid web-auth https-redirect command in startup-config
CSCvn53435	C3702AP on 8.5.140.0: %DOT11-2-RADIO_RX_BUF: 1E72C72C leads to unexpected reloads with reason 44
CSCvn53514	AP Syslog Facility does not work on IOS AP
CSCvn54514	Client usage counters not reset with Accounting stop
CSCvn54535	DCA assigning channel not allowed via RF profile to Cisco Wave 2 APs.
CSCvn55904	WLC modified FlexACLs rules are not populated on the Flex AP
CSCvn56211	Cisco 702W AP radio resets, tracebacks and other radio buffer errors
CSCvn57308	WLC/AP do not send M1 message to clients
CSCvn59061	Cisco 8510 controller on on 8.3.141.10 DP crash at broffu_fp_dapi_cmd.c:4588
CSCvn59160	WLC logs "NMSP cloud service update. Received CMX service Link Check" even when CMX is not used
CSCvn59720	Cisco 702w AP on 8.5.135.5: Client not getting DHCP IP
CSCvn60018	Wireless clients getting IP from wrong VLAN using VLAN Based Central Switching.
CSCvn60681	Dynamic AP Manager does not work when LAG enabled on WLC
CSCvn61436	Cisco 5520 controller reloads unexpectedly on taskname : NFV9_Task
CSCvn62160	Multicast Packet drop on Cisco 2800, 3800 AP series
CSCvn62176	Cisco 3802 series APs unable to associate clients when using UNII-1 Channels
CSCvn63678	Cisco 702w AP fails to broadcast beacons on BI

Resolved Caveats

Table 13: 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

Caveat ID Number	Description
CSCvg76166	Channel utilization changes to 0% on Marvell chipset based Cisco Wave 1 APs
CSCvh24354	ME: 1800 AP disconnects the client during EAP negotiation by reason: MN_REASSOC_TIMEOUT
CSCvh87451	Cisco 1832 AP Rx not working with AP not responding to probe requests
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
CSCvi09153	Cisco Wave 1 APs radio reset due FST14 FW: cmd=0x31 seq=6 due to mcast stuck in radio
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 WLC-reloads unexpectedly with rmgrMain due to IPC timeout
CSCvi25724	Cisco IOS APs unexpectedly reloads due to bad CPQ on 8.5 release code
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
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	WLC 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
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 WLC has redundant country codes CA2, KR, PH2, US2, USL, USX
CSCvi85834	New Mobility CAPWAP control keepalive should not plumb keys when receiving unencrypted responses

Caveat ID Number	Description
CSCvi86276	Cisco WLC reloads unexpectedly on emWeb due to too many HTTP buffers received
CSCvi90766	Cisco AP with regulatory domain Morocco cannot join the Cisco WLC
CSCvi91017	The FlexConnect groups are missing in backup configuration file
CSCvi92170	Cisco 1800 series APs falsely shows 100% channel utilization on 5GHz
CSCvi93045	Cisco 2800 AP CleanAir goes down (sensord died)
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 WLC
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 WLC if 'Enable NAT Address' feature is enabled
CSCvj07930	Cisco 3802, 2802 AP with DART connectors has a Tx power value of 0
CSCvj08387	WLC 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
CSCvj13920	WLC system reloads unexpectedly due to task name RRM-MGR-2_4-GRP
CSCvj14729	Upgrading Mobility Express to 8.7.102.0 causes it to reloads unexpectedly in a continuous loop
CSCvj17181	Creating a webauth CSR certificate on the WLC GUI does not allow spaces
CSCvj18004	8.5MR3 Interim AP 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

Caveat ID Number	Description
CSCvj28658	Cisco 1810wAP kernel panic leads to unexpected reload on PC at ieee80211_node_authorize+0x90/0xb8
CSCvj32199	SSH/Management Access of Primary WLC not possible when HA failover occurs in 8.5.120.0
CSCvj32624	702 AP as WGB keeps being 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]
CSCvj33894	Add 'show advanced hyperlocation summary' to 'show run-config' and 'show tech'
CSCvj36853	AP name corruption after upgrade
CSCvj36923	Cisco AP name mismatch with controller on join
CSCvj37393	Cisco Wav 2 APs not sending probe response when SSID is not broadcasted
CSCvj38456	WLC is losing its EoGRE configuration after reboot
CSCvj39005	[SDA] Wireless Clients losing L2VNID override when performing Switchover on Cisco 5520 WLC
CSCvj41853	Incorrect Tx power on AP3802P-Q on some channels
CSCvj44533	SSH CBC ciphers are present from 8.6 and onwards releases
CSCvj46554	CONFIGSYNC-3-CONFIG_SYNC_SEM_REL_FAIL & CLEAN_TASK: Reaper cleaning up exited task 'ConfigSync'
CSCvj47445	Cisco WLC sending CAPWAP discovery response when it has no available licenses
CSCvj47460	Cisco WiSM2 reloads unexpectedly on SNMP task
CSCvj48364	Cisco Controller is generating client traps without a session-id
CSCvj50170	Client coming back within 10 seconds of cleanup time is stopping the DHCP timer on the WLC
CSCvj54432	Cisco WLC unexpectedly reloads on task Dot1x_NW_MsgTask_2
CSCvj60609	Cisco vWLC web authentication not working
CSCvj62672	WLC sending wrong NAS ID when AAA override is enabled
CSCvj65449	AIR-AP1562D-E-K9 with regulatory domain Kazakhstan does not join the WLC
CSCvj70569	Cisco 2800, 3800,4800 APs: Incorrect Tx power on power on till we configure Tx power using Cisco WLC
CSCvj70604	Cisco Mesh APs Best-Effort Tx queue stuck

Caveat ID Number	Description
CSCvj71373	Ping command does not use management interface as source interface
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 WLC reloads unexpectedly when RADIUS server returns invalid value in Airespace-ACL-Name
CSCvj73077	Cisco 1810W APs may have power denied from older PoE 802.3af switches
CSCvj76378	Local policy is not applied when foreign WLC is running 8.3.141.0
CSCvj77078	WLC unexpectedly reboots on Dot1x_NW_MsgTask_1
CSCvj86238	Cisco controller stops working as emWeb spikes to 100% CPU usage after executing 'show run-config'
CSCvj97602	WLC Client RSSI and SNR values to be updated as part of Assoc & reassoc request processing
CSCvk00884	The WLC is replying with the wrong value for the following OID: bsnAPIfProfileParamAssignment
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
CSCvk09135	Cisco 5520 Controller reloads unexpectedly for emweb in 8.6.101.0 release
CSCvk09513	AP is not downloading the WLC 85Mr3 image rather it says image is already in the backup
CSCvk15043	Wave 1 APs - AP radio FW image install failure in the bootup loop
CSCvk15068	IOS 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)
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	WLC power supply status is incorrect when there is no power supply

Caveat ID Number	Description
CSCvk25593	Cisco 1542, 1815I APs - Ethernet interface flapping when connected to 100Mbit switchports
CSCvk25644	WLC 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
CSCvk27093	NAS-ID in WLAN cannot be changed in the startup-command after you saved once
CSCvk35047	Cisco WLC stops working when LAG mode is enabled on the AP
CSCvk36463	Support Bundle output only genertaes WSA core bundle when WSA is enabled
CSCvk38453	AP does not initiate the CAPWAP discovery process, it gets stuck during the PNP discovery process
CSCvk39948	WLC is not returning the expected prompt when logging in via SSH
CSCvk41068	Advance IPMI is not set and causing fan noise
CSCvk41249	WLC 8.7 does not present full certificate chain on web authentication guest portal
CSCvk41512	APX800 sniffer mode not sending frames with AMSDU 1500 Bytes to destination
CSCvk43025	Local Split and Central path traffic stops after some time with Cisco 2800 APs
CSCvk44959	Cisco controller reloads unexpectedly on Taskname 'emWeb'
CSCvk46817	AIR-AP2802I not sending beacons with both radios in 5GHz
CSCvk47740	Pre-auth ACLs are not configuring for RLAN in ME UI
CSCvk51634	Wave 2 Flex Efficient Upgrade fails as primary AP sends empty image_str to WLC
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
CSCvk59498	Cisco 3702 AP: High CPU utilization under NCI Rx. Unable to join the controller
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
CSCvk62355	CAP2800 on ME image 8.6.101.0, 8.7.106.0 reloads unexpectedly in ewsContexSendRedirect200->ewaDate

Caveat ID Number	Description
CSCvk62680	Cisco WiSM2 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
CSCvk70185	WLC Smart License : Smart license registration failing for ProductInstance not valid in switchover
CSCvk72075	WLC is sending incorrect counter value for the broadcast and multicast throgh SNMP
CSCvk73639	Cisco controller to support OUI based Client Profiling
CSCvk76043	Unable to Associate clients with PSK/dot1x security in Flexconnect Standalone Mode.
CSCvm00214	Cisco WiSM2 memory leak due to hotspot_anqp
CSCvm04245	Cisco 1810W AP reports low power after requesting and receiving 14.2W after upgrading to 8.5.131.0
CSCvm04408	Cheetah WGB - Fast Roaming PSK with/without over the DS. FT Auth-Response is not received
CSCvm05695	AAA override for native VLAN with flexlocal switching not applied to client on Cisco 1562 AP
CSCvm10519	Intergrated Management Module (IMM) summary shows a username which is multiple usernames merged
CSCvm11060	WLC: After soft-roam of client, client is not able to see new Apple TV from associated AP-Grp VLAN
CSCvm15625	DCA channel assignment on XOR radio is broken while static 5G assignment
CSCvm18273	Cisco 702W AP: Runs out of memory and reloads
CSCvm21666	Cisco 4800 series AP takes pre-download of unsupported code
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
CSCvm33617	Configuration file should not be modified due to low flash memory
CSCvm34641	Cisco controller is sending packets out to Gateway with DF =1 when inside header is set DF =0 -EoGRE
CSCvm37510	Controller crashing due to SNMP memory corruption

Caveat ID Number	Description
CSCvm43028	8.8MR1:Number of DX messages in sync Queue ... 440001[805520.362884] Controller crashed ....Queue
CSCvm46810	Cisco controller reloads unexpectedly in Dot1x_NW_MsgTask_7 due to validateWpaKeyStateSTART
CSCvm46823	DNAC Wireless Assurance does not respond to POST causing WLC to timeout & eventually drop data
CSCvm51362	Cisco controller reloads unexpectedly due to data plane crash
CSCvm60915	Cisco 3800 AP stops passing traffic under client load in MU-MIMO deployment
CSCvm62202	Cisco 1852 AP Kernel Panic at ClientCapabilitiesTracker
CSCvm62803	WLC allows to configure OEAP ACLs in software version that do not support them
CSCvm65360	Cisco controller redirects to internal webauth login page after successful external webauth login
CSCvm69246	WLC applying wrong interface policy to re-associated client after SSO
CSCvm71487	Cisco 2800, 3800 APs: dropping the Neighbor Advertisement for Global IPv6 address
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 Clients are not able to authenticate to COS AP after HA Failover
CSCvm90337	Cisco 18xx APs unexpectedly reload due to 'radio failure(radio recovery failed)'
CSCvn05881	Phone 8821 has roaming issues with 2802/3802 access points MIC mismatch
CSCvm90580	Cisco Wave 2 APs: AP not able to join the controller when NAT is enabled
CSCvm97915	WLC includes NULL Bytes within the JSON it posts
CSCvn03560	Decrypt errors seen on Cisco 702 AP
CSCvn11947	Cisco 1815w:RLAN port'traffic will get stuck at TX direction after end device restarts several times
CSCvn14292	Cisco 3800 AP reloads unexpectedly on 8.2.170.2
CSCvn27902	'%SAFEC-3-SAFEC_ERROR' observed while decoding iPSK key from radius

Related Documentation

Wireless Products Comparison

- Use this tool to compare the specifications of Cisco wireless access points and controllers:

  https://www.cisco.com/c/en/us/products/wireless/wireless-lan-controller/product-comparison.html

- Product Approval Status:

  https://prdapp.cloudapps.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL_SEARCH

- Wireless LAN Compliance Lookup:

  https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html

Cisco Wireless Controller

For more information about the controllers, lightweight APs, and mesh APs, see these documents:

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

For all controller software related documentation, see:

http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/tsd-products-support-series-home.html

Cisco Mobility Express

- *Cisco Mobility Express Release Notes*
- *Cisco Mobility Express User Guide*
- *Cisco Aironet Universal AP Priming and Cisco AirProvision User Guide*

Cisco Aironet Access Points for Cisco IOS Releases

- *Release Notes for Cisco Aironet Access Points for Cisco IOS Releases*
- *Cisco IOS Configuration Guides for Autonomous Aironet Access Points*
- *Cisco IOS Command References for Autonomous Aironet Access Points*

Open Source Used in Controller and Access Point Software

Click this link to access the documents that describe the open source used in controller and access point software:

https://www.cisco.com/c/en/us/about/legal/open-source-documentation-responsive.html

Cisco Prime Infrastructure

Cisco Prime Infrastructure Documentation

Cisco Mobility Services Engine

Cisco Mobility Services Engine Documentation

Cisco Connected Mobile Experiences

Cisco Connected Mobile Experiences Documentation

Cisco Digital Network Architecture

https://www.cisco.com/c/en/us/support/wireless/dna-spaces/series.html

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2018–2019 Cisco Systems, Inc. All rights reserved.