Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.6.101.0

First Published: 2017-12-14

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 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.

Revision History

Table 1: Revision History

Modification Date	Modification Details
October 30, 2018	Open Caveats—Added CSCvh65876, CSCvi97023, CSCvj95336, CSCvi49059, CSCvh21953 Resolved Caveats—Added CSCvf66680, CSCvf66696, CSCve64652, CSCvf66723
July 24, 2018	Added the CIMC Utility Upgrade for 5520 and 8540 Controllers section.
March 13, 2018	Supported Cisco Access Point Platforms section—Added information about support for Integrated Access Point on Cisco 1100 Integrated Services Router.
January 29, 2018	Key Features Not Supported in Cisco Virtual WLC—Modified information about FlexConnect central switching.

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

    Note Support introduced in Release 8.4.

  - Kernel-based virtual machine (KVM)

    Note 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 Integrated Services Router
- 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 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 AP803s 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 at 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 8.6.101.0

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

Note For complete listing of all the documentation published for Cisco Wireless Release 8.6, see the Documentation Roadmap: https://www.cisco.com/c/en/us/td/docs/wireless/doc-roadmap/doc-roadmap-release-86.html

Note From this release onwards, the following controllers and APs are not supported:

- controllers not supported:
  - Cisco 2504 Wireless Controller
  - Cisco 5508 Wireless Controller
  - Cisco Flex 7510 Wireless Controller
  - Cisco 8510 Wireless Controller
  - Cisco WiSM2
- Cisco Aironet APs not supported:
  - Cisco Aironet 1600 Series AP
  - Cisco Aironet 2600 Series AP
  - Cisco Aironet 3500 Series AP
  - Cisco 3600 Series AP
  - AP802 Integrated AP
  - Cisco Aironet 1550 Series AP

Note The New Mobility feature is not supported in Release 8.6 and later releases.

Cisco Wave 2 AP Features

- **AP 802.1X supplicant feature supported in Cisco Wave 2 APs**—In the 802.1X authentication scenario between an AP and a Cisco switch, the AP acts as an 802.1X supplicant and is authenticated by the switch using Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) with anonymous Protected Access Credentials (PAC) provisioning. From this release, this feature is available in Cisco Wave 2 APs too.

  For more information, see the "AP 802.1X Supplicant" section in the *Cisco Wireless Controller Configuration Guide*.

  For more information about IEEE 802.1X port-based authentication, see the "Configuring IEEE 802.1X Port-Based Authentication" chapter in the *802.1X Authentication Services Configuration Guide, Cisco IOS Release 15E*.

- **Upgrade Cisco AP and WLC software using Rolling AP Upgrade**—In Cisco Prime Infrastructure 3.3, you can upgrade Cisco AP and WLC software using the Rolling AP Upgrade feature. To prevent APs from rebooting simultaneously, you can instead add APs to upgrade groups. The AP upgrade groups reboot sequentially in the order of your preference.

  For more information, see the "Upgrade Controller Software using Rolling AP Upgrade" section in the *Cisco Prime Infrastructure 3.3 User Guide*.

- **Spectrum Intelligence on Cisco Aironet 18x0 and 1540 Series APs**—In this release, Spectrum Intelligence is supported in Cisco Aironet 18x0 and 1540 Series APs.

  For more information, see the "Configuring Spectrum Intelligence" section in the *Cisco Wireless Controller Configuration Guide*.

- **CMX FastLocate on Cisco Aironet 2800 and 3800 Series APs**—In this release, CMX FastLocate is supported in Cisco Aironet 2800 and 3800 Series APs. For more information about CMX FastLocate, see the CMX FastLocate Deployment Guide.

Custom NAS-ID for RADIUS Accounting Using Downloadable RADIUS AVP

Prior to this release, the NAS-ID field contained the configured NAS-ID or system name if they are not set on WLAN for inclusion in RADIUS accounting messages. In this release, the NAS-ID field is enhanced so that you can configure some key parameters such as the AP name and AP IP address for the RADIUS accounting messages.

In the controller GUI, choose **Security** > **AAA** > **RADIUS** > **Downloaded AVP** > **Acct AVP** to view the downloaded new RADIUS attribute.

This enhancement has the following advantages:

- Flexibility per WLAN to choose NAS ID field subtypes
- Easy to configure, store, upload, and download
- Download when a new WLAN is created; controller reboot is not required
- RADIUS AVP file in the controller can be uploaded and is persistent across reboot

For more information, see the "Custom NAS-ID for RADIUS Accounting Using Downloadable RADIUS AVP" section in the *Cisco Wireless Controller Configuration Guide*.

Multisession ID Support

Prior to this release, audit-session-id was shared across mobility peers along with pairwise master key (PMK). Whenever PMK cache is not created, for example for client security such as open authentication or web authentication, the audit-session-id is not shared. In central web authentication (CWA), the AAA server depends on the audit-session-id to identify the authenticated clients. If controller uses a new audit-session-id for authentication, the AAA server forces the client for reauthentication. In this release, a multisession ID is introduced to be used in the RADIUS server, to support intercontroller client roaming in case of open + MAC filtering with CWA.

For more information, see the "Multisession ID" section in the *Cisco Wireless Controller Configuration Guide*.

Minimum Interval Setting for Volume Metering

Prior to this release, the minimum RADIUS accounting interval that you could configure was 180 seconds. In this release, the minimum interval that you can configure is 60 seconds. controller honors the Acct-Interim-Interval AVP from RADIUS and sends the accounting interim update at the configured interim interval.

For more information, see the "Timers" chapter in the *Cisco Wireless Controller Configuration Guide*.

Securing Network Protocols

- **Securing the password fields**—The maximum number of characters that you can use for the password fields of the following is now set to 127:
  - Administrator user
  - Local network user
  - Local management user
  - RADIUS (authentication, accounting, and DNS) shared secret
  - TACACS+ (authentication, accounting, authorization, and DNS) shared secret
  - IPSec shared secret
  - LDAP bind
  - Local EAP
  - SXP

  Note If you want to downgrade from Release 8.6 to Release 8.5 or an earlier release, ensure that you have a management user account password that is less than or equal to 24 characters to be compatible with the earlier releases. Else, during the downgrade and before you can reboot the controller, you will be prompted with the following message:

  ```
  "Warning!!! Please Configure Mgmt user compatible with older release"
  ```

- **NTP Version 4**—NTP Version 4 is supported in this release. NTP Version 4 supports both IPv4 and IPv6 servers. For more information, see the "Network Time Protocol Setup" chapter in the *Cisco Wireless Controller Configuration Guide*.
- **SSH vulnerability addressed**—Prior to this release, connections were allowed without requiring a username and password. After a connection is set up, a Telnet connection to the local host is initiated. In this release, this vulnerability is addressed, wherein a username and a password are required to allow a connection.

EoGRE Enhancements

- **EoGRE deployment with multiple TGW**—Prior to this release, controller used to send keepalive pings to all the tunnel gateways (TGWs) configured on controller. In this release, keepalive pings are sent only to those TGWs that are mapped to the WLANs that are in enabled state.

  When a WLAN is disabled or deleted in controller, periodic keepalive pings are stopped to the TGW that is mapped to the WLAN.
- **DHCP Option 82 for EoGRE Tunnel in Cisco Wave 2 APs**—In this release, DHCP Option 82 for EoGRE Tunnel is supported in Cisco Wave 2 APs.

Diagnostic Support Bundle

Some commonly collected diagnostic information of various types can be made available in a single bundle that you can upload from controller. The diagnostic information that can you can include in the bundle are core files, crash files, **show run-config** and **config** commands, msglog, and traplog.

For more information, see the "Uploading Diagnostic Support Bundle" section in the *Cisco Wireless Controller Configuration Guide*.

Mesh Leaf Node Support on IR829 AP803 and IW3700 Series APs

Support is added to IR829 AP803 and IW3700 Series APs to configure mesh APs with lower performance to work only as a leaf node, to prevent the wireless backhaul performance from being downgraded.

For more information, see the "Configuring Mesh Leaf Node" section in the *Cisco Wireless Controller Configuration Guide*.

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 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 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 WLC Software Release 8.6.101.0

Current Software Release	Upgrade Path to 8.6.101.0 Software
8.4.100.0	You need to upgrade to Release 8.5.105.0 prior to upgrading to Release 8.6.101.0 or later.
8.5.x.0	You can upgrade directly to Release 8.6.101.0

Upgrading Cisco WLC Software Release

This section describes the guidelines and limitations that you need to be aware of when you are upgrading the Cisco WLC software and the procedure to upgrade to this release.

Guidelines and Limitations

- In Release 8.6, FlexConnect local switching ARP cache is enabled by default. Therefore, if you upgrade to Release 8.6 from an earlier release, FlexConnect local switching ARP cache, if disabled, is enabled automatically.

  If you downgrade from Release 8.6 to an earlier release, FlexConnect local switching ARP cache is disabled. If required, you must manually enable the feature on the corresponding earlier release.

- In Release 8.6, the maximum number of characters for a management user account password is changed to 127 characters. If you want to downgrade from Release 8.6 to Release 8.5 or an earlier release, ensure that your management user account password is less than or equal to 24 characters to be compatible with the earlier releases. Else, during the downgrade, before you can reboot Cisco WLC, you will be prompted with the following message:

  ```
  "Warning!!! Please Configure Mgmt user compatible with older release"
  ```

- In Release 8.6 and later releases, legacy clients that require RC4 or 3DES encryption types are not supported in Local EAP authentication.

- If you are using Release 8.4 and want to upgrade to a later release, it is necessary that you upgrade to Release 8.5.105.0 and then move to a later release.

  Note This restriction is applicable only to Release 8.4 and not any other release.

- The filenames of Cisco Aironet 1700, 2700, 3700, and IW3702 AP software images have been changed from ap3g2-x to c3700-x format. Therefore, if you are upgrading to Release 8.5 or a later release from Release 8.3 or an earlier release, these APs will download the image twice and reboot twice.

- The AAA database size is increased from 2048 entries to 12000 entries for these Cisco WLCs: Cisco 5520 and 8540. Therefore, if you downgrade from Release 8.6 to an earlier release that does not include this enhancement, you might lose most of the AAA database configuration, including management user information. To retain at least 2048 entries, including management user information, we recommend that you follow these downgrade instructions and back up the configuration file before proceeding with the downgrade:

  1. From Release 8.6, downgrade to one of the following releases, which support 2048 database size and include the enhancement.
     - Release 8.5.105.0 or a later 8.5 release
     - Release 8.4
     - Release 8.3.102.0 or a later 8.3 release
     - Release 8.2.130.0 or a later 8.2 release
     - Release 8.0.140.0 or a later 8.0 release

2. Downgrade to a release of your choice.

- This release supports additional configuration options for 802.11r FT enable and disable. The additional configuration option is not valid for releases earlier than Release 8.4. If you downgrade from Release 8.6 to Release 8.2 or an earlier release, the additional configuration option is invalidated and defaulted to FT disable. When you reboot Cisco WLC with the downgraded image, invalid configurations are printed on the console. We recommend that you ignore this because there is no functional impact, and the configuration defaults to FT disable.
- If you downgrade from Release 8.6 to a 7.x release, the trap configuration is lost and must be reconfigured.
- If you have an IPv6-only network and are upgrading to Release 8.4 or a later release, ensure that you perform the following activities:
  - Enable IPv4 and DHCPv4 on the network—Load a new Cisco WLC software image on all the Cisco WLCs or perform a predownload of AP images on the corresponding Cisco WLCs.
  - Reboot Cisco WLC immediately or at a preset time.
  - Ensure that all Cisco APs are associated with Cisco WLC.
  - Disable IPv4 and DHCPv4 on the network.
- 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 Cisco WLC to download a new image or to reboot Cisco WLC after the download of the new image. You can forcefully reboot Cisco WLC by entering the **reset system forced** command.
- It is not possible to download some of the older configurations from Cisco WLC 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 upgrade from Release 8.0.110.0 to a later release, the **config redundancy mobilitymac** *mac-addr* command's setting is removed. You must manually reconfigure the mobility MAC address after the upgrade.
- 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.
- If you are upgrading from a 7.4.x or an earlier release to a release later than 7.4, the Called Station ID type information is mapped to the RADIUS Accounting Called Station ID type, which, by default, is set to apradio-mac-ssid. You can configure the RADIUS Authentication Called Station ID type information by using the **config radius auth callStationIdType** command.
- When a client sends an HTTP request, the Cisco WLC intercepts it for redirection to the login page. If the HTTP GET request that is intercepted by the Cisco WLC is longer than 2000 bytes, the Cisco WLC drops the packet. Track CSCuy81133 for a possible enhancement to address this restriction.
- We recommend that you install Cisco Wireless Controller Field Upgrade Software (FUS), which is a special AES package that contains several system-related component upgrades. These include the bootloader, field recovery image, and FPGA or MCU firmware. Installing the FUS image requires special attention because it installs some critical firmware. The FUS image is independent of the runtime image.

For more information about FUS and the applicable Cisco WLC platforms, see the Field Upgrade Software release notes listing.

- When downgrading from one release to another, you might lose the configuration from your current release. The workaround is to reload the previous Cisco WLC configuration files that are saved in the backup server, or to reconfigure Cisco WLC.
- It is not possible to directly upgrade to this release from a release that is earlier than Release 7.0.98.0.
- When you upgrade Cisco WLC to an intermediate release, wait until all the APs that are associated with Cisco WLC are upgraded to the intermediate release before you install the latest Cisco WLC 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 Cisco WLC 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 Cisco WLC is also automatically upgraded. When an AP is loading software, each of its LEDs blinks in succession.
- We recommend that you access the Cisco WLC GUI using Microsoft Internet Explorer 11 or a later version, or Mozilla Firefox 32 or a later version.
- Cisco WLCs support standard SNMP MIB files. MIBs can be downloaded from the software download page on Cisco.com.
- The Cisco WLC software is factory installed on your Cisco WLC and is automatically downloaded to the APs after a release upgrade and whenever an AP joins a Cisco WLC. 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 Cisco WLC 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 Cisco WLC 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 Cisco WLC 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, choose **Option 2: Run Backup Image** from the **Boot Options** menu to boot from the backup image. Then, upgrade with a known working image and reboot Cisco WLC.
- 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 Cisco WLC.

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 Cisco WLC or any AP during the upgrade process. If you do this, the software image might get corrupted. Upgrading Cisco WLC 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 Cisco WLC must not be reset during this time.
- To downgrade from this release to Release 6.0 or an earlier release, perform either of these tasks:
  - Delete all the WLANs that are mapped to interface groups, and create new ones.
  - Ensure that all the WLANs are mapped to interfaces rather than interface groups.
- After you perform the following functions on Cisco WLC, 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 WLC Software (GUI)

Procedure

Step 1 Upload your Cisco WLC configuration files to a server to back up the configuration files.

Note We highly recommend that you back up your Cisco WLC configuration files prior to upgrading the Cisco WLC software.

Step 2 Follow these steps to obtain Cisco Wireless software:

a) Browse to Cisco Software Central at: https://software.cisco.com/download/navigator.html.
b) Click **Software Download**.
c) On the **Download Software** page, choose **Wireless** > **Wireless LAN Controller**.

The following options are displayed. Depending on your Cisco WLC platform, select one of these options:

- **Integrated Controllers and Controller Modules**
- **Mobility Express**
- **Standalone Controllers**

d) Select the Cisco WLC model number or name.
e) Click **Wireless LAN Controller Software**.
f) The software releases are labeled as described here to help you determine which release to download. Click a Cisco WLC 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.

g) Click the filename <*filename.aes*>.
h) Click **Download**.
i) Read the Cisco End User Software License Agreement and click **Agree**.
j) Save the file to your hard drive.
k) Repeat steps *a* through *j* to download the remaining file.

Step 3 Copy the Cisco WLC software file <*filename.aes*> to the default directory on your TFTP, FTP, or SFTP server.

Step 4 (Optional) Disable the Cisco WLC 802.11 networks.

Note For busy networks, Cisco WLCs on high utilization, and small Cisco WLC 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 Cisco WLC.

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 Cisco WLC.

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

Step 18 To verify that the Cisco WLC software is installed on your Cisco WLC, on the Cisco WLC 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.
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 Cisco WLC 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/Software Parameter	Hardware/Software Configuration Type
Release	8.6.101.0
Cisco WLC	Cisco 5520 Wireless Controller
Access Points	AIR-CAP3802E-B-K9, AIR-AP1852E-B-K9, AIR-CAP3602E-A-K9

Hardware/Software Parameter	Hardware/Software Configuration Type
Radio	802.11ac, 802.11a, 802.11g, 802.11n (2.4 GHz / 5.0 GHz)
Security	Open, PSK (WPA-TKIP-WPA2-AES), 802.1X (WPA-TKIP-WPA2-AES) (EAP-FAST, EAP-TLS)
RADIUS	ACS 5.3, ISE 2.2, 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	Version
Laptop	
Intel 6300	15.16.0.2
Intel 6205	15.16.0.2
Intel 7260	18.33.3.2
Intel 7265	19.10.1.2
Intel 3160	18.40.0.9
Intel 8260	19.10.1.2
Broadcom 4360	6.30.163.2005
Dell 1520/Broadcom 43224HMS	5.60.48.18
Dell 1530 (Broadcom BCM4359)	5.100.235.12
Dell 1560	6.30.223.262
Dell 1540	6.30.223.215
Samsung Chromebook	55.0.2883.103
HP Chromebook	55.0.2883.103
MacBook Pro	OSX 10.11.6
MacBook Air old	OSX 10.11.5
MacBook Air new	OSX 10.11.5
Macbook Pro with Retina Display	OSX 10.12
Macbook New 2015	OSX 10.12.4
Printers	
HP Color LaserJet Pro M452nw	2.4.0.125

Client Type and Name	Version
Tablets	
Apple iPad2	iOS 10
Apple iPad3	iOS 10
Apple iPad mini with Retina display	iOS 10
Apple iPad Air	iOS 10
Apple iPad Air 2	iOS 11
Apple iPad Pro	iOS 11
Samsung Galaxy Tab Pro SM-T320	Android 4.4.2
Samsung Galaxy Tab 10.1- 2014 SM-P600	Android 4.4.2
Samsung Galaxy Note 3 - SM-N900	Android 5.0
Microsoft Surface Pro 3	Windows 8.1
	Driver: 15.68.3093.197
Microsoft Surface Pro 2	Windows 8.1
	Driver: 14.69.24039.134
Microsoft Surface Pro 4	Windows 10
	Driver: 15.68.9040.67
Google Nexus 9	Android 6.0.1
Google 10.2" Pixel C	Andriod 7.1.1
Toshiba Thrive AT105	Android 4.0.4
Mobile Phones	
Cisco 7926G	CP7925G-1.4.5.3.LOADS
Cisco 7925G-EX	CP7925G-1.4.8.4.LOADS
Cisco 8861	Sip88xx.10-2-1-16
Cisco-9971	sip9971.9-4-1-9
Cisco-8821	sip8821.11-0-3ES2-1
Apple iPhone 4S	iOS 10.2.1
Apple iPhone 5	iOS 10.2.1
Apple iPhone 5s	iOS 10.2.1
Apple iPhone 5c	iOS 10.3.1
Apple iPhone 6	iOS 10.3.1
Apple iPhone 6 Plus	iOS 10.3.1
Apple iPhone 6s	iOS 10.2.1

Client Type and Name	Version
Apple iPhone 7	iOS 11.0.3
Apple iPhone X	iOS 11.1.2
HTC One	Android 5.0
OnePlusOne	Android 4.3
OnePlus3	Android 6.0.1
Samsung Galaxy S4 T-I9500	Android 5.0.1
Sony Xperia Z Ultra	Android 4.4.2
Nokia Lumia 1520	Windows Phone 8.10.14219.341
Google Nexus 5	Android 6.0.1
Google Nexus 5X	Android 8.0.0
Google Pixcel	Android 7.1.1
Samsung Galaxy S5-SM-G900A	Android 4.4.2
Samsung Galaxy S III	Android 4.3
Samsung Galaxy S4	Android 5.0.1
Samsung Galaxy S5	Android 4.4.2
Samsung Galaxy S6	Android 7.0
Samsung Galaxy S7	Android 7.0
Samsung Galaxy Nexus GTI9200	Android 4.4.2
Samsung Galaxy Mega SM900	Android 4.4.2
LG G4	Android 5.1
Xiaomi Mi 4c	Android 5.1
Xiaomi Mi 4i	Android 6.0.1

Key Features Not Supported in Controller Platforms

This section lists the features that are not supported on the different 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
- Domain-based ACLs
- Internal DHCP server
- Cisco TrustSec
- Access points in local mode
- Mobility/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 in only 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

Key Features Not Supported in Cisco Aironet 1540, 1560, 1800i, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800, and 3800 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/8-6/b_feature_matrix_for_802_11ac_wave2_access_points.html.

Table 9: Key Features Not Supported in Cisco Aironet 1540, 1560, 1800i, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800, and 3800 Series APs

Operational Modes	• Autonomous Bridge and Workgroup Bridge (WGB) mode • Mesh mode **Note** Supported on 1540 and 1560 APs. • Flex + Mesh • 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	• Bidirectional Rate Limiting
	• Split Tunneling
	• PPPoE
	• Multicast to Unicast (MC2UC)
	• Traffic Specification (TSpec)
	  • Cisco Compatible Extensions (CCX)
	  • Call Admission Control (CAC)
	• VSA/Realm Match Authentication
	• Link aggregation (LAG)
	• 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
- Flex+Mesh

Key Features Not Supported on Cisco Aironet 1560 Mesh APs

- Noise Tolerant Fast Convergence
- Flex+Mesh

Caveats

Open Caveats

Table 12: Open Caveats

Caveat ID Number	Description
CSCuy61155	802.11b inconsistent probe response; band select enabled; 2.4 GHz
CSCvd91152	3700 APs in FlexConnect mode stop working
CSCve70752	SNMP issue: Txpowerlevel returns null with Cisco WLC Version 8.3.13x.0 and 8.4 at times (including 8.2.161)
CSCve79470	Cisco Wave 2 AP sends RADIUS message directly even if Local Authentication is disabled
CSCvf12011	Webauth logout fails after standalone; connected
CSCvf16153	Active Cisco WLC stopped working with Task Name: SNMPTask
CSCvf21673	Cisco 2800 and 3800 APs send block ACK packets using disabled data rates
CSCvf51131	DHCPv6 stateless not working

Caveat ID Number	Description
CSCvf52731	New Mobility member status shows as Unknown when editing mobility member IP address
CSCvf65133	Dynamic interface template fails to apply on WLC with opt82 setting
CSCvf74377	3800 AP in Sniffer mode: 802.11 acks, RTS, CTS, QoS Null packets do not get captured
CSCvf74406	3800 AP in Sniffer mode: AP does not fill BAR Request Type, BAR Control, SSC, FCS in BAR and BA packets
CSCvf76148	1700 AP continuous radio reset due to incorrect tx inprog
CSCvf80409	1815 AP does not send all traffic after period under load
CSCvf84806	FIQ/NMI Reset AP2800 PC __pci_bus_size_bridges+0x274/0x768 LR warn_slowpath_common+0x58/0x94
CSCvf91228	Cisco WLC unable to timeout clients; stale client entries
CSCvf91434	EoGRE domain: not able to edit from GUI
CSCvf93914	3702 AP: 5-GHz radio constantly flapping
CSCvf94574	Not able to create IPSec profile
CSCvf96532	Cisco WLC anchor commands are missing from the backup
CSCvg03741	SXP connection stay off after disable/enable SXP
CSCvg06111	WLC "in sync" with NTP while authentication is ignored with invalid keys
CSCvg06372	1532I AP fails to receive DHCP address randomly
CSCvg07617	1810W AP Kernel Panic crash is at _ZN17ContentHashFilter11clear_staleEv+0x1ac/0x1d0 [elts_meraki]
CSCvg08001	Cisco WiSM2 stops working for task name spamApTask3 8.2.151.0
CSCvg18543	3700 AP Tx jammed radio unresponsive
CSCvg19117	EoGRE client de-autheenticated when AP moved from Standalone to Connected Mode
CSCvg19242	Cisco Aironet 1700, 2700, and 3700 AP log incorrect PHY in sniffer mode for 11ac
CSCvg21910	Deleting one SSID will affect another SSID created on the same radio interface
CSCvg23810	PMTU change to 1500 from a lesser value is not reflected in AP
CSCvg24476	2802 XOR Operational State is Down/Admin Enabled while 802.11a is Up
CSCvg24737	tb20-vWlc-esxl-80—Clients lost the right override VLAN after AP moves from Standalone mode
CSCvg24833	1530 AP WGB stops working on associating with root

Caveat ID Number	Description
CSCvg25773	Cisco 7510 WLC running Release 8.2.151.0 stops working with TaskName:spamApTask7
CSCvg25902	Cisco 3504 WLC: AP cannot join controller when directly connected to GigE Port 1
CSCvg26841	SNMP walk on bsnMeshNodeTable returns no data for IW3700 AP in Flex+Bridge Mode
CSCvg27361	Adding "switchport voice vlan x" causes wired phone not to pull an IP address
CSCvg27599	Cisco WLC stops working sometime when client switches between FT-enabled SSID and CCKM SSIDs
CSCvg27613	DHCP Proxy enabled and removing DHCP Server Info from Dynamic interface disables WLAN
CSCvg28378	AP: cmd timeout AP radio unresponsive in due to rxHang
CSCvg29325	FTP download fails on Cisco WLC when using untagged interfaces on different ports
CSCvg32087	5520 WLC stops working: Task Name: nmspTxServerTask
CSCvg32924	SNMPTask (module:k_mib_cisco_lwapp_local) causing memory leak in 16B buffer
CSCvg33308	3800 AP unresponsive, Kernel panic - not syncing: Fatal exception in interrupt
CSCvg34444	IW3702 WGB one way broadcast traffic on 5 GHz (but good in 2.4 GHz) in a mesh network 1572 AP
CSCvg34502	1542 AP not joining WLC with Costa Rica (CR) Country
CSCvg37474	3802 AP not forwarding client traffic
CSCvg38669	ERROR-MeshSecurity: Processing EAPOL from CAWAWP, Mesh mode is not started
CSCvg38681	FlexConnect AP's WLAN-VLAN mapping's inheritance is lost when a WLAN is deleted from AP group
CSCvg39960	Cisco WLC stops working on task: sntpReceiveTask
CSCvg40792	Client global IPv6 not correctly mapped to MAC address under certain condition
CSCvg43654	Cisco Wave 2 APs in FlexConnect do not forward DHCP NAK to wireless client
CSCvg44078	Cisco WLC unable to timeout clients; stale client entries
CSCvg44450	2800 AP is not able to process the ARP response
CSCvg45550	1530 LAP drop EAP identity packets sent by Cisco WLC random and cause EAP negotiation to fail
CSCvg46125	Cisco WLC stops working multiple times

Caveat ID Number	Description
CSCvg47269	**debug disable-all** command does not disable debugs for FlexConnect group client debugging
CSCvg48395	TrustSec not workingEnvironment Data download failing with 3504 WLC
CSCvg49532	HA—**config service statistics** command is not synced
CSCvg53640	1830 AP triggered FW assert for radio failure (beacons stuck)
CSCvg56184	Wave 1 APs in sniffer mode show incorrect TID in captured traffic
CSCvg59338	NMSP drops seen with high density deployments
CSCvg60452	aIOS and FlexConnect standalone failure on FT-dot1x authentication or M3 RSN IE
CSCvg60758	Cisco Wave 2 AP drops TCP retransmit from server
CSCvg62039	False radar detection on AP1832 with 40-MHz CW
CSCvg62560	3800 AP not handling DSCP tags properly
CSCvg63216	WLC RFID queue breached with more than 4000 tags.
CSCvg64621	1852/1832 SI: WLC config file does not contain the SI/CleanAir enable/disable state for network/AP
CSCvg64750	HA osapi_file.c:1030 Failed to open the file, %OSAPI-3-SOCK_SEND_FAILED: [SA]osapi_support
CSCvg64892	FIQ-NMI related Kernel Panic on 3802E AP
CSCvg64993	Cisco WLC mDNS secure printer service response missing TXT record with mdns snooping enabled
CSCvg66702	Cisco WLC stops working endlessly when updating OUI file
CSCvg67318	**run-config** commands do not include TPC version
CSCvg67509	1810W AP stops working with kernel panic
CSCvg70352	AP 1832/1852 Kernel Panic at __kmalloc_poolid+0xb8/0x16c
CSCvg70903	WLAN session timeout does not default to dot1x reauth timeout when WebAuth is enabled via GUI
CSCvg73797	CAP 2800/3800: command timeout at 0x8000 in FW
CSCvg74107	Cisco WiSM2 stops working on Dot1x_NW_MsgTask due to Dynamic VLAN feature handling for AP702W
CSCvg74780	AP syslog and AP mgmtuser configs lost on reordered config download
CSCvg75583	Server status in the **show cloud-services cmx summary** command shown as "Server Error"

Caveat ID Number	Description
CSCvg77711	System unresponsive randomly on running mesh commands
CSCvg78101	Local EAP profiles changed not retained after apply
CSCvg79115	Cisco WLC suggested to 5 GHz for Cisco Wave 2 APs but they are staying on 2.4 GHz without auto alignment
CSCvg82156	2802E AP with Radio1 unresponsive
CSCvg82215	Cisco 3504 WLC unresponsive when using mGig port
CSCvg83600	The SPAM QUEUES of the WLC are getting breached.
CSCvg86324	Cisco WLC stops working with SNMP operation with FlexConnect ACL
CSCvg90217	IPv6 rogue clients are shown as unknown
CSCvg91108	WQE size constantly increasing, error messages
CSCvg91708	Cisco WLC emweb unresponsive at commandConfigSpamApAntennaMonitor
CSCvg91734	1852 and 1832 AP—AP data traffic stall in HD environment
CSCvg93023	1562 AP reports incorrect power level to WLC
CSCvg94522	smr4: TxFSM stuck on Radio 0 with new signature
CSCvg94720	AP: Sending EAP packets unencrypted at session timeout
CSCvg96533	3800 and 2800 AP: FIQ/NMI reset seen on .98 image and .102
CSCvg96852	CAP 1815W Sniffer Mode AP beacons allows clients to join and blackhole traffic
CSCvg96857	WLC SSH/Telnet exits with 1542D Mesh AP with **show mesh neigh summary** command.
CSCvh01089	COS AP: false beacon stuck issue due to no beacon updates in wcp message Host Triggered Radio Crash
CSCvh03148	COS AP: Client shows as connected but unable to pass any traffic
CSCvh21953	Cisco Aironet 1560, 1800, 2800 and 3800 Series Access Point Denial of Service Vulnerability
CSCvh65876	Cisco Wireless LAN Controller Software GUI Privilege Escalation Vulnerability
CSCvi49059	[FALL WLC BUNDLE] NO CVE Cisco Wireless LAN Controller Privilege Escalation Vulnerability
CSCvi97023	Cisco Wireless LAN Controller Cross-Site Scripting Vulnerability
CSCvj95336	Cisco Wireless LAN Controller Software Information Disclosure Vulnerability

Resolved Caveats

Table 13: Resolved Caveats

Caveat ID Number	Description
CSCuz60197	Cisco Wave 2 APs - "CAPWAP preferred mode" gets displayed as "Not configured"
CSCva89294	AP803 failed to send auth/reasso to new AP while roaming
CSCvc58294	WLC Monitoring Gui: Unable to clear top WLANs statistics
CSCvd09394	AP3700: Tx util values are not changed
CSCvd12313	Wireless client fails to receive Multicast traffic when 802.1X is enabled
CSCvd15449	FRA Probe suppression does not work for pre-association client
CSCvd42321	Cisco 1832 AP drops the CAC SIP 486 packet
CSCvd64928	System stopped working on PMIPV6_Thread_0 during creation of LMA entry
CSCvd79103	Client CCX version for the same client differs for each of the APs
CSCvd79532	8.5 mgmt gw is not reachable after connecting device on MDA port
CSCvd86206	SNMP trapflag adjchannel-rogueap config not retaining during upload/download
CSCvd90160	AP2800 sending announce as 0 in Reassociation response in FlexConnect Mode in FT and adaptive FT
CSCvd92528	Local policy ACL does not apply when intf group mapped to WLAN and DHCP addr assign is disabled
CSCve00155	3802:Unable to update property /soc/gop/mac0:local-mac-address, err=FDT_ERR_NOSPACE
CSCve09179	CAP 3800 sending deauth to connected clients when CAPWAP flaps.
CSCve12846	1850 Flex mode AP not prioritizing packets based on QoS Map
CSCve13386	Assoc req forwarded to WLC after max clients on ap radio in flex local switching
CSCve13886	WPS signature is getting disabled upon upload or download
CSCve14345	Dashboard UI :- filtering the Accesspoint field with "is Null " and "is not null" is leading to hung
CSCve18213	Foreign WLC leaks IPv6 and IPv4 multicast client traffic out of EoIP tunnel
CSCve18315	WLC allowing blank as avc profile name
CSCve18359	Observed traceback on Cisco 1570 AP when changing AP mode to FlexConnect from Flex+Bridge
CSCve24232	AVC profile showing incorrect characters for an entry after upgrade

Caveat ID Number	Description
CSCve25792	GUI shows label as "AVC Based Reanchor" while configuring in Selective-Roam
CSCve31474	WGB HSR 802.11v neighbor report error message when Infrastructure MFP is enabled
CSCve36498	Ascom phones stop transmitting voice durning call
CSCve44977	WLC 8.5.1.138 Dual Band radios showing incorrect suggested mode
CSCve47928	Cisco 8.5 release: AP is not joining the Cisco WLC after image upgrade
CSCve49567	Not able to add TACACS+ server from GUI
CSCve50022	CTS SXP connection flap seen between CAT6K and WLC
CSCve55360	Korean/ Japanese character support in LocalEapProfiles
CSCve56404	Cisco 8.5 release: Cisco XOR radio configured to Sensor mode using GUI has operational state down
CSCve59671	Cisco WLC and ME: RADIUS fail-over does not work when retransmit timeout is not set to default value
CSCve60014	Sleeping client entry not getting created after idle timeout
CSCve64066	AP is not joining the controller when for first time IP is changed from DHCP to static
CSCve64652	Cisco Access Point 802.11r Fast Transition Denial of Service Vulnerability
CSCve65242	Cisco 702w AP radio resets with reason code 71
CSCve72187	Micro-Macro transition configuration should be limited to within the defined range
CSCve73743	Unable to change "Back-up Primary Controller name" from GUI
CSCve75339	Macro to micro transition threshold is not configurable on Mobility Express
CSCve75515	Configuration backup shows the time instead of the NAT IP
CSCve75791	After config upload/download event, netuser start time resets to invalid value.
CSCve78449	Cisco 3700 AP: radio d1 reset: Tx jammed
CSCve80917	IPsec profile should be none on disabling IPsec under SNMP communities and Trap Receiver
CSCve81269	Clients failed to get connected to the Cisco AP in Flex mode with message as AID already in use
CSCve81314	Clients fails to connect to AID with message as All AID are in use when the AP is in Local mode
CSCve83024	WLC power supply issues not showing up on 360 page
CSCve84257	[8.5] show inventory displaying incorrect output for AP802

Caveat ID Number	Description
CSCve84906	Traceback observed in Cisco WLC while something is fetched for Flex ACL with AVC
CSCve85321	WGB traffic disruption on missed beacons and no scan or roam
CSCve86627	Bridging interface mode get reset to 'access' when configure MeshAP from GUI
CSCve87353	Find button goes disable in successive search for AP filter page
CSCve87947	**Show run-config no-ap** is missing AP Group and RF profile configuration
CSCve88358	Cisco Wave 2 APs: Flex standalone mode: EoGRE clients are dropped in Local AP VLAN
CSCve89376	Cisco Wave1 APs sends RA periodically when EoGRE tunnel profile is added to the AP
CSCve90032	WLC FEW: flooding logs with "Updating MS IPv6[1] Addr" logs
CSCve90626	Virtual IP address changes to 0.0.0.0 after rebooting
CSCve95309	'WL_IOCTL_SET_MGMT_SEND failed for apr1v0 error Bad address' messages on AP followed by Radio reset
CSCve97039	Cisco 3800 AP drops P2P information element after adding 802.11u or HotSpot support on a WLAN.
CSCve98440	CONFIG WIZARD: after ap group & rf profile mapping add/del command, not able to execute any command
CSCve98689	Repeated CDP-4-DUPLEX_MISMATCH is observed when 1852 and 3802 APs are connected to Cisco 3850 switch.
CSCvf00877	8.5: cmdtimeout when xor in sensor mode, band mismatch errors
CSCvf01576	Cisco 3504 WLC is not generating a crash file.
CSCvf03702	The Mobility Group Members is not able to modified
CSCvf05391	Cisco WLC not sending delete payload to AP on exclusion client manual deauth
CSCvf05427	Cisco 2800/3800 AP cannot use the RX-SOP
CSCvf05741	Reason for channel change is shown as none and noise/energy/interfere as 0 for the dual band radio
CSCvf05776	Target assert XXXXXXXX WAITING FOR STOP EVENT on Cisco 1810 AP
CSCvf07062	Channel assignment leader shows junk value on standby WLC
CSCvf07189	8.5 Incorrect prompt after executing any CLI with (y/n) option
CSCvf07640	[5520] Setting an IPv6 address for primary-base on an AP from WLC cuts off last characters after ::

Caveat ID Number	Description
CSCvf07968	Cisco Wave 2 AP specific backup RADIUS server configuration lost post CAPWAP reset or AP reload
CSCvf08009	Cisco Wave2 AP reboots with watchdogd-reason CAPWAP on associating avc profile under FlexConnect grp
CSCvf08272	Black-list timer is showing as `blacklist due to be cleared` but still the blocked list timer remaining
CSCvf08351	cLApEthernetIfMacAddress is not showing AP MAC address
CSCvf08808	dca min-metric not getting logged on TACACS+
CSCvf09040	"Missing 802.1X or client control block" Errors in WLC Message Logs
CSCvf10157	Cisco WiSM2 stopped working with emWeb in 8.5.1.183 build
CSCvf10486	Dual band radio on AP2800 does not go down after changing the country code from IN to US on AP
CSCvf10509	GUI does not show the 5-Ghz radio after changing the country code on CAP 2800, 3800 from IN to US
CSCvf10535	"show wlan" command is not working properly
CSCvf10786	CAP 2800, 3800 sniffer mode logs wrong PHY and data rates for 802.11ac
CSCvf11072	ME: SUBNET_MISMATCH_IP_ADD_ON_MSCB mismatches while registering IP address x.x.x.x
CSCvf11782	Invalid domain name after ap reset
CSCvf11909	External Server IP address accepts broadcast and Loopback address
CSCvf12068	Wrong values of coverage exception &coverage level in RF Profile in uploaded config and tech support
CSCvf13943	RF grouping off in WLC respond join command with incorrect reason code: 1
CSCvf16302	Flash on lightweight IOS APs gets corrupted
CSCvf16842	Tunnel Gateway (TGW) in Cisco 3802 AP comes up only after the Heartbeat interval expires
CSCvf16869	AP continuously reboots with "Process sync_log gone"
CSCvf16958	Cisco Wave 2 AP unable to process VLAN NAME ID mapping TLV payload
CSCvf17088	Cisco WLC fails to respond neighbor request for WLAN id greater than 255
CSCvf17133	8.3.133.0:"config dhcp address-pool test 178.1.0.1 178.1.0.100" hits "Invalid scope specified."
CSCvf17294	Cisco 2800, 3800 APs running 8.2.154.61 release: wifi0 resets multiple times

Caveat ID Number	Description
CSCvf17647	Mismatch in enabling IPv6 multicast address in WLC UI and CLI
CSCvf17664	AVC in disabled state under WLAN AVC mapping on enabling from console
CSCvf18363	Kernel panic stopped working in Cisco 1542 AP
CSCvf18505	When WLC adaptive/fastlane is disabled, the CCX IE is missing in probe response Wave 2 APs
CSCvf19306	AP Name is truncated in client detail for Nearby AP statistics attribute
CSCvf19400	Mobility statistics is getting updated wrongly for L3 roam
CSCvf19452	cLApEthernetIfType is shown as other instead of a correct value
CSCvf19557	cLApEthernetIfCdpEnabled shows true when cdp is disabled on the ap interface
CSCvf19677	Member active WLC showing wrong allowed channel list after switchover
CSCvf20006	Duplicate entries allowed as SNMP community entries with read only and read write - HA synch failing
CSCvf20089	AP adder license is taking effect only after a reboot on the Cisco 3504 WLC.
CSCvf20107	WLC shows radio role as NA and channel and power as blank for slot 2 installed modules
CSCvf20148	Error reason is not provided when user try to delete Out of Box AP group
CSCvf20997	Hotspot getting enabled with open security in WLC
CSCvf21657	AP 1850 radar detection in high density client enviornment
CSCvf21763	Limit stations in CAPWAP discovery response is giving wrong data
CSCvf22104	Identity PSK does not work when order of PSK mode and PSK key are interchanged
CSCvf22185	In Cisco 2800/3800 and Cisco 1562 APs, the Watchdog reset is observed (capwapd stopped working)
CSCvf22672	WLC - exit is not working after 'advanced fra revert all auto' command execution in config mode
CSCvf22697	Flooding "Invalid checkpoint client ID (0)" message on Standby WLC
CSCvf23079	CAPWAP_HA-3-AP_TEMP_DB_ADD_ERR in standby WLC when changing CAPWAP mode continuously
CSCvf23817	8.6: 5760 WLC Crash by SNMPTask
CSCvf24716	Redundant MAC address is used by standby-wlc for GW and peer RMI
CSCvf24746	Showing wrong AP model name in Popup message

Caveat ID Number	Description
CSCvf25062	Cisco 3802AP on 8.3.124.17 release [cmd mismatch] wifi0: Host Cmd:0x9201 F/W Cmd:0x8001 Last:0x801d
CSCvf25083	8.3MR3: is valid for netflow monitor but not for GUI and error message is incorrectly showing on UI
CSCvf25436	DCA assigns channels out of DCA channel list
CSCvf26013	WLC- Previous AP field is set by the last disassoc frame sent up from the STA not the last roam
CSCvf26065	32 Split Tunnel--char chopped to 31;Edit serves as Add;Error incorrect;Gateway can be removed
CSCvf26207	Cisco 7510 WLC running 8.0.120.36 reloads unexpectedly while running airewave director debug
CSCvf27533	Cisco 3800 AP in a constant reboot loop
CSCvf28003	"FRA Enabled Learn More" navigation link is not working under Best practices
CSCvf29208	Cisco 1560-Mesh: Fixed backhaul rate issues.
CSCvf29426	Implement CCA, RX-SOP thresholds for Marvell autonomous IOS
CSCvf30698	WLC shows COF and Suggested mode as none with FRA enable after HA Failover
CSCvf31054	Continuous FIQ/NMI reloads unexpectedly for 3802 AP when XOR is in sensor mode
CSCvf31090	WLC GUI displays incorrect number of fastlane clients
CSCvf32958	capwapd no heartbeat during waiting for uplink IP address
CSCvf33154	Wireless to Wireless multicast failure on Cisco 2800, 3800 APs with WPA-PSK-TKIP
CSCvf34480	Cisco Wave 2 APs: losing flex-avc-profile config if one out of 2 WLAN disabled
CSCvf34483	CAP 1810 reported timeout communicating to controller on data plane
CSCvf35683	Text view of Dual band radio does not display Rx neighbors
CSCvf37633	Error in mapping QoS role during the creation of local net users
CSCvf37785	On an 1810W AP, multicast fails to pass on the LAN port when switchport configured for 1000M speed
CSCvf38393	NDP on 2800/3800 not transmitting at Correct Power on 802.11b/g/n Channels
CSCvf38544	WLC: Jamaica Country does not add -E Regulatory Domain support for Outdoor APs
CSCvf40071	WIPS engine gets disabled on 2800 after AP reboot
CSCvf41057	Clients QoS level changes automatically to silver from gold during local authentication

Caveat ID Number	Description
CSCvf41342	HA SSO - Apply Config failed on Standby, Reason:5
CSCvf41587	CAP 3800 rebooted after rejoining WLC (upgrade) due to watchdog reset with "wcpd" as reason.
CSCvf42460	WLC pushing truncated wIPS profile to APs
CSCvf43759	Issue 'no bvi-vlanid' on WGB does not cast IAPP message to refresh BVI VLAN id on AP
CSCvf44042	WLC returns extension channels for XOR in 2.4GHz or Monitor Mode
CSCvf44061	SNMP get or walk on device for bsnAPBridgingSupport returns ENABLE for Cisco 2800, 3800 APs
CSCvf45017	Remote LAN with 1810w in FlexConnect mode not showing client IP
CSCvf45989	WLC DP core 0 hung due to RML interrupt handler
CSCvf46178	Cisco 1262 autonomous AP drops ARP requests
CSCvf47198	1542-Mesh: Fixed backhaul rate configuration does not work
CSCvf49632	CAPWAPd reloads unexpectedly after enabling CAPWAP payload debug
CSCvf50387	new Cisco 1562 AP reloads unexpectedly due to: FIQ/NMI reset
CSCvf50487	Enabling DHCP option 82 on EoGRE profile is not updated in GUI
CSCvf51780	Cisco 3504 WLC reloads unexpectedly during external webauth redirection with MAX length URL
CSCvf51951	Hexdump of packet observed in apf task
CSCvf52875	SNMP:Junk characters instead of server IP when image download is initiated from Prime Infrastructure
CSCvf55570	Clients unable to connect when CCKM and FT802.1X are enabled together
CSCvf55741	Cisco 1532 AP cannot use static IP address when configured as mesh AP (MAP)
CSCvf56556	Guest User role cannot be called properly on the Cisco 2504 WLC platform
CSCvf57305	Issues with 1562s MAP taking a long time to join RAP
CSCvf57588	Cisco Wireless LAN Controller - standby WLC reloads unexpectedly at HA Config Sync Task
CSCvf57743	Certain sequence causes Unexpected displays, 32 char name chopped to 31 Interface Group
CSCvf57859	Ceiling not working if DSCP sent is higher than metal policy of WLAN
CSCvf58977	RTU license count taking over Smart Account count

Caveat ID Number	Description
CSCvf59630	XOR radio does not move to 5GHz/Monitor bands after being marked redundant
CSCvf59970	Crete-Mesh: Client not always authorized after reset
CSCvf60009	Ethernet daisy chain IW3702 GE1 1Gbps reload same time when configured speed 100 & duplex full
CSCvf60045	Cisco Controller reloads unexpectedly on "config bleBeaconwhiteList add"
CSCvf60057	8.3MR3:2800/3800 AP cannot handle Probe Limit Interval up to 64000ms required from CSCvb91652
CSCvf61345	SNMPv3 same user adding accepted silently but actually not able in CLI but ok for UI
CSCvf61646	802.11v BSS Transition Preferred Candidate List Not Included with Radio Policy Set to 802.11a Only
CSCvf61962	Cisco WLC reloads unexpectedly due high CPU usage by SNMP task
CSCvf61975	WLC reaper not creating proper crash file
CSCvf62929	WLC randomly marks wireless management frames with DSCP CS0 instead of CS6
CSCvf63464	AP show CLIs seen having previously joined controller CAPWAP tunneled WLAN entries
CSCvf63534	CONTROLLER->PMIPv6->LMA with 128 char shown incorrectly in GUI/CLI, out of range ERROR issue
CSCvf64199	On 1810 APs warning msg throwing while configuring Tx Power for Radio "B"
CSCvf64931	Summary is showing 7500 Interferers on 2.4GHz but Interferers is showing nothing
CSCvf65362	Buff Leak on ap console when in FlexConnect mode
CSCvf65577	"AP 1388 doe not exist anymore on the system" pops when back on Dual band page
CSCvf65687	EoGRE AP bytes and packets stats are vice-versa in AP and WLC with Wave 1 AP on both CLI and GUI
CSCvf66680	Cisco WLC Control And Provisioning of Wireless Access Points Information Disclosure
CSCvf66696	Cisco WLC Control & Provisioning of Wireless Access Points Protocol Denial of Service Vulnerability
CSCvf66723	Cisco Wireless LAN Controller Directory Traversal Vulnerability
CSCvf66887	CLI can provision up to 394 characters while GUI/error help message showing max 63 characters
CSCvf67467	System reloads unexpectedly as Reaper Reset:Task wipsTask taking too much CPU
CSCvf67691	EoGRE DHCP82 "show flexconnect dhcp option82" issues

Caveat ID Number	Description
CSCvf68049	IOS AP should send Flex client del instead of MN delete for Flex local auth clients delete
CSCvf68619	3702 NOS Dual-Band setting for CleanAir back silently, many 1601336064s shown in Detail page
CSCvf68648	Dataplane reloads unexpectedly when using EoGRE tunnel
CSCvf68674	Node ptr_meshFileCfg.cfg.convMethod value = 3 is out of range for min = 0 and max = 2 upgrade
CSCvf69070	Aironet2802 marking upstream client traffic with incorrect DSCP values when WMM is disabled
CSCvf69071	Cisco 3504 WLC factory default license issue
CSCvf69955	Kernel Panic seen on 1542 Mesh APs
CSCvf71136	Infra IPv6 AP drops off from the WLC every 4 to 12 hours
CSCvf71893	AP not blocking all channels in set to WLC when radar is detected on one of the channels in 80MHz
CSCvf72352	Rogue APs getting contained or containment pending automatically on the WLC
CSCvf72497	CAP 3600 dropping over DTLS tunnel with Cisco 8540 WLC
CSCvf72997	CAP 1832 kernel panic
CSCvf75869	Cisco 2800, 3800 APs: radio0 reloads unexpectedly in longevity due to 3rd party FW issue(s)
CSCvf76245	"debug client" sometimes reports wrong BSSID in (Re)association message
CSCvf76274	APs can no longer join the WLC; CAPWAP-3-DTLS_DB_ERR
CSCvf76429	INTERFERERS Table loading issue for 2.4 GHz,5 GHz
CSCvf76739	Cisco 2800/3800 AAA override VLAN does not work for native VLAN.
CSCvf77787	AP LAG fails using LACP with non-Cisco switches
CSCvf77798	Trapflags do not sync for HA SSO
CSCvf81919	CAP 3800 stops working: selipc causing double free
CSCvf82065	CAP 1562 unable to pass multicast joins from RAP to MAPs
CSCvf82117	WLC fails to send complete IPv6 client information to Prime Infrastructure
CSCvf83251	WLC debug client, flooding logs with " iapp ipv6" logs
CSCvf83404	VLAN override on RLAN with FlexConnect Local Switching does not work

Caveat ID Number	Description
CSCvf83594	Client moving to RUN state from webauth reqd after reassoc request
CSCvf83733	WLC detects IDS Signature attack even if Signature Processing is disabled
CSCvf84540	Cisco 3700 AP: radio d1 reset: Tx jammed, probably beacon was not really sent by Hw
CSCvf84715	AP loses config and NAND disk error messages are seen on console
CSCvf84816	Cisco 1810WAP: Kernel Panic- crash files shows PC is at 0x4 LR is at ieee80211_free_node+0x264/0x4b4
CSCvf85960	Primary Secondary Tertiary controller IPV6 address not retain post reload
CSCvf86007	Buff Leak on AP when AP changes channel
CSCvf86035	1815w Kernel Panic PC wlan_channel_frequency+0x10/0x18 LR acfg_get_client_info+0x84/0x264
CSCvf86148	Cisco 3800 AP reloads unexpectedly while running 8.3.124.40 code
CSCvf87646	Cisco 2800,3800 APs in Sniffer mode - frequent kernel panics observed
CSCvf87731	Cisco 5508 WLC reloads unexpectedly during AP join failure
CSCvf88091	Clients behind 3rd Party WGB fail DHCP post upgrade to 8.0.150.0
CSCvf88518	CAP 1832 reloads unexpectedly due to kernel panic
CSCvf89334	OpenDNS information is lost when primary AP fails over to the new one
CSCvf92627	AP3802E- on 8.5.107.34 reloads unexpectedly due to watchdog reset(with reason: out to reboot with r)
CSCvf95036	Cisco 1850 radio firmware reloads unexpectedly at 0x009A4859
CSCvf95264	CAP 1800 kernel panic pc @Kfree
CSCvf98138	AP1532 stops working on client connection to WLAN profile with EoGRE tunnel
CSCvf99003	3802 chatter: IOCTL_SET_MGMT_SEND failed for apr0v0 error Operat
CSCvg01352	IPv4 traffic drops with "Packet needs to be fragmented but DF bit is set" and MTU mismatch
CSCvg01740	Deauth reason pulled from association response code wrongly
CSCvg01874	Unable to add LSC CA Certificate on Cisco WLC GUI
CSCvg07115	Debug fastpath command cause the 8540/8510 WLCs to stop working
CSCvg07438	AP3800: Low throughput due to packet drops in AP in both fragmented and non-fragmented packets

Caveat ID Number	Description
CSCvg08398	Observed "buf leak" message on corsica FlexConnect mode APs
CSCvg14346	WLC- is flagging Misc_Reason 0x9 as an Invalid Apple Reason Code but displays proprietary failure
CSCvg15820	AP MAC:SSID:AP Group attribute is not present in Accounting called station ID GUI list
CSCvg20439	CAP 1562 is dropping downlink unicast messages, making connectivity difficult across mesh link
CSCvg20743	The client RSSI/SNR is shown as unavailable when connected to 2800/3800 APs.
CSCvg21263	CIAM Alert: GNU dnsmasq DNS Reply Heap Buffer Overflow Vulnerability
CSCvg21614	"show ap network-diagnostics" does not work for 1815 AP when in FlexConnect OEAP mode
CSCvg22483	Rogue client on friendly rogue contained with 'valid client on rogue AP' auto contain enabled
CSCvg24597	WLC management VLAN zero in kernel causing reachability issues
CSCvg31499	AP 3800,2800 8.5.107.57 and .61 when AP is in flex mode, AP reloads unexpectedly due hostapd process
CSCvg35226	Unable to change Antenna Band Mode to 1562E AP
CSCvg41678	8.6: 2802 Kernel panic PC@AccumulateScanResults
CSCvg46620	Dataplane watchdog timeout due to NBAR max flows exceeded
CSCvg48786	Cisco 1815T AP LAN3 not coming up when a client is directly connected
CSCvg62163	Cisco 3504 WLC not communicating to Smart Licensing Cloud Server
CSCvg87547	AP: Client disconnected due to idle timeout wrongly kicking in when client is going to power save

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