Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.3.121.0 and 8.3.122.0

First Published: 2017-07-21

Last Modified: 2018-08-30

About the Release Notes

This release notes document describes what is new or changed in this release, instructions to upgrade to this release, and 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
August 23, 2018	Open Caveat—Added CSCvk44249
January 29, 2018	Key Features Not Supported on Cisco Virtual WLCs section—Modified information about FlexConnect central switching.
October 16, 2017	Key Features Not Supported on Cisco Aironet 1810 OEAP, 1810W, 1815, 1830, 1850, 2800, and 3800 Series APs section—Added SIP snooping with FlexConnect in local switching mode
October 10, 2017	Key Features Not Supported on Cisco Virtual WLCs section—Added Wired Guest and FlexConnect central switching
August 08, 2017	Added Release 8.3.122.0 information.
July 21, 2017	What's New in Release 8.3.121.0 section—Updated Upgrade Warning for Deployments with TSPEC and CAC Enabled section.

Modification Date	Modification Details
June 28, 2017	What's New in Release 8.3.121.0 section—Added Upgrade Warning for Deployments with TSPEC and CAC Enabled section.

Cisco Wireless Controller and Access Point Platforms

Supported Cisco Wireless Controller Platforms

The following Cisco Wireless Controller Platforms are supported in this release:

- Cisco 2500 Series Wireless Controllers (Cisco 2504 Wireless Controller)
- Cisco 5500 Series Wireless Controllers (Cisco 5508 and 5520 Wireless Controllers)
- Cisco Flex 7500 Series Wireless Controllers (Cisco Flex 7510 Wireless Controller)
- Cisco 8500 Series Wireless Controllers (Cisco 8510 and 8540 Wireless Controllers)
- Cisco Virtual Wireless Controllers on VMware ESXi and Kernel-based virtual machine (KVM) systems.

  Note Kernel-based virtual machine (KVM) is supported in Cisco Wireless Release 8.1 and later releases. 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 2504 WLC, Cisco 5508 WLC, Cisco 5520 WLC, Cisco Wireless Services Module 2 (Cisco WiSM2), Cisco Flex 7510 WLC, Cisco 8510 WLC, and Cisco 8540 WLC.

  Note AP Stateful switchover (SSO) is not supported on Cisco 2504 WLCs.

- Cisco WiSM2 for Catalyst 6500 Series Switches
- Cisco Mobility Express Solution

Supported Access Point Platforms

The following access point platforms are supported in this release:

- Cisco Aironet 1040 Series Access Points
- Cisco Aironet 1140 Series Access Points
- Cisco Aironet 1260 Series Access Points
- Cisco Aironet 1600 Series Access Points
- Cisco Aironet 1700 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 2600 Series Access Points
- Cisco Aironet 2700 Series Access Points
- Cisco Aironet 2800 Series Access Points
- Cisco Aironet 3500 Series Access Points
- Cisco Aironet 3600 Series Access Points
- Cisco Aironet 3700 Series Access Points
- Cisco Aironet 3800 Series Access Points
- Cisco Aironet 600 Series OfficeExtend Access Points
- Cisco Aironet 700 Series Access Points
- Cisco Aironet 700W Series Access Points
- Cisco AP802 Integrated Access Point
- Cisco AP803 Integrated Access Point
- Cisco ASA 5506W-AP702
- Cisco Aironet 1530 Series Access Points
- Cisco Aironet 1550 Series Access Points
- Cisco Aironet 1560 Series Access Points
- Cisco Aironet 1570 Series Access Points
- Cisco Industrial Wireless 3700 Series Access Points

Note The Cisco 1040 Series, 1140 Series, and 1260 Series access points have feature parity with Cisco Wireless Release 8.0. Features introduced in Cisco Wireless Release 8.1 and later are not supported on these access points.

Note Before you associate Cisco Aironet 1830 Series and 1850 Series APs with Cisco vWLC running Cisco 8.3.112.0 release software, you must upgrade the APs to Cisco 8.3.112.0 release.

Note Cisco AP802 and AP803 are integrated access points on the Cisco 800 Series Integrated Services Routers (ISRs). For more information about the stock-keeping units (SKUs) for the AP802s and AP803s Cisco ISRs, see http://www.cisco.com/c/en/us/products/routers/800-series-routers/brochure-listing.html. Before you use a Cisco AP802 series lightweight access point with Cisco Wireless Release 8.4, you must upgrade the software in the Cisco 800 Series ISRs to Cisco IOS 15.1(4)M or later releases.

Note 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 https://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html.

What's New in Release 8.3.122.0

Release 8.3.122.0 is a repost of Release 8.3.121.0 with the inclusion of three caveats in the Resolved caveats list.

There are no other updates in this release, all resolved and open caveats in addition to three resolved bugs apply to this release.

Table 2: Resolved Caveats in Release 8.3.122.0

Caveat ID Number	Description
CSCvd27398	WLC management access stops working while WLAN services are still up
CSCve77722	WLAN in FlexConnect local switching drops NAC+802.1X and WPA2-PSK-WebAuth traffic on MAC filter fail
CSCvf31894	Backout changes - CSCvc78546 that leads to CSCve20123

What's New in Release 8.3.121.0

Multicast-to-Unicast Support for Passive Client ARPs

This feature enables the Cisco 5520 WLC to work along with Non-Cisco WGBs in Multicast-to-unicast mode to route ARP traffic from the wired clients behind the Non-Cisco WGBs to all the APs.

For more information, see the Multicast-to-Unicast Support for Passive Client ARPs section in the configuration guide.

AVC Based Selective Reanchoring

This feature is designed to reanchor clients when they roam from one Cisco WLC to another Cisco WLC. Reanchoring of Apple clients prevents depletion of IP addresses available for new clients in Cisco WLC.

Note Some Apple clients roaming to another Cisco WLC fails to reassociate with the new Cisco WLC with the new IP address. These clients do not release the old IP address and therefore do not re-associate with the current Cisco WLC.

For more information, see the AVC Based Reanchoring section in the configuration guide.

Upgrade Warning for Deployments with TSPEC and CAC Enabled

If your network uses TSPEC (VoWLAN clients such as 792x, 882x, Spectralink) protocols, then do not upgrade to 8.3.121.0 if TSPEC and CAC are enabled. You can refer to the bug under open caveats—CSCve20123 for more information.

We recommend you to contact Cisco TAC for further support if you must upgrade to this release.

Important Upgrade Information for Cisco 2500 Series WLCs

If you are using a Cisco 2500 Series WLC and want to upgrade to Release 8.3.121.0, install the Cisco Wireless LAN Controller Field Upgrade Software, Release 1.9.0.0, or a later release. For more information, see http://www.cisco.com/c/en/us/support/wireless/2500-series-wireless-controllers/products-release-notes-list.html#anchor512.

Download the Cisco Wireless LAN Controller Field Upgrade Software for Cisco 2500 Series WLC from the Download Software page.

For other Cisco WLC platforms, see the respective Cisco Wireless LAN Controller Field Upgrade Software release notes for recommended FUS images.

Software Release Types and Recommendations

Table 3: 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: https://www.cisco.com/c/en/us/products/collateral/wireless/8500-series-wireless-controllers/bulletin-c25-738147.html.

Upgrading the Cisco WLC Software Release

Guidelines and Limitations

- We recommend that you install Release 1.9.0.0 of Cisco Wireless LAN 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/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, see https://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/fus_rn_OL-31390-01.html.

  

  Note If you are using a Cisco 2500 Series controller, you must install Release 1.9.0.0 or higher of Cisco Wireless LAN Controller FUS. This is not required if you are using other controller hardware models.

  

  Note The FUS image installation process reboots the Cisco WLC several times and reboots the runtime image. The entire process takes approximately 30 minutes. We recommend that you install the FUS image in a planned outage window.

- Release 8.3 supports additional configuration options for 802.11r FT enable and disable. The additional configuration option is not valid for older releases. If you downgrade from Release 8.3.x 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 8.3.122.0 to a 7.x release, the trap configuration is lost and must be reconfigured.
- If you downgrade from Release 8.3.122.0 to Release 8.1, the Cisco Aironet 1850 Series AP, whose mode prior to the downgrade was Sensor is shown to be in unknown mode after the downgrade. This is because the Sensor mode is not supported in Release 8.1.
- If you have an IPv6-only network and are upgrading to Release 8.3.122.0 or a later release, ensure that the following is done:
  - Enable IPv4 and DHCPv4 on the network—Load a new Cisco WLC software image on all Cisco WLCs plus Supplementary AP Bundle images on the Cisco 2504 WLC, 5508 WLC, and WiSM2 or perform a predownload of AP images on the required Cisco WLCs.
  - Reboot Cisco WLC immediately or at the preset time.
  - Ensure that all Cisco APs are associated with Cisco WLC.

- Disable IPv4 and DHCPv4 on the network.

- After downloading new software to the Cisco APs, it is possible that a Cisco AP may get stuck in an "upgrading image" state. In such a case of a stranded Cisco AP, it may be necessary to forcefully reboot the Cisco WLC to download a new image or to reboot the Cisco WLC after the download of the new image. You can forcefully reboot the Cisco WLC by entering the **reset system forced** command.
- It is not possible to download some of the older configurations from the Cisco WLC because of the Multicast and IP address validations. See the *Restrictions on Configuring Multicast Mode* section in the 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 have ACL configurations in a Cisco WLC, and downgrade from a 7.4 or later release to a 7.3 or earlier release, you might experience XML errors on rebooting the Cisco WLC. However, these errors do not have any impact on any of the functionalities or configurations.
- 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 FlexConnect APs (known as H-REAP APs in the 7.0.x releases) that are associated with a Cisco WLC that has all the 7.0.x software releases prior to Release 7.0.240.0, upgrade to Release 8.3.122.0, the APs lose the enabled VLAN support configuration. The VLAN mappings revert to the default values of the VLAN of the associated interface. The workaround is to upgrade from Release 7.0.240.0 and later 7.0.x releases to Release 8.3.122.0.

Note In case of FlexConnect VLAN mapping deployment, we recommend that the deployment be done using FlexConnect groups. This allows you to recover VLAN mapping after an AP rejoins the Cisco WLC without having to manually reassign the VLAN mappings.

- 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.
- After you upgrade to Release 7.4, networks that were not affected by the existing preauthentication access control lists might not work because the rules are now enforced. That is, networks with clients configured with static DNS servers might not work unless the static server is defined in the preauthentication ACL.
- On the Cisco Flex 7500 Series WLCs, if FIPS is enabled, the reduced boot options are displayed only after a bootloader upgrade.

Note Bootloader upgrade is not required if FIPS is disabled.

- If you have to downgrade 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 saved on the backup server, or to reconfigure the Cisco WLC.
- It is not possible to directly upgrade to Release 8.3.122.0 release from a release that is earlier than Release 7.0.98.0.
- You can upgrade or downgrade the Cisco WLC software only between certain releases. In some instances, you must first install an intermediate release prior to upgrading to Release 8.3.122.0. The following table shows the upgrade path that you must follow before downloading Release 8.3.122.0.

Note If you upgrade directly to 7.6.x or a later release from a release that is earlier than 7.5, the predownload functionality on Cisco Aironet 2600 and 3600 APs fails. The predownload functionality failure is only a one-time failure. After the upgrade to 7.6.x or a later release, the new image is loaded on the said Cisco APs, and the predownload functionality works as expected.

For detailed release recommendations, see the *Guidelines for Cisco Wireless Software Release Migration Bulletin* at: https://www.cisco.com/c/en/us/products/collateral/wireless/8500-series-wireless-controllers/bulletin-c25-738147.html

Table 4: Upgrade Path to Cisco WLC Software Release 8.3.122.0

Current Software Release	Upgrade Path to 8.3.122.0 Software
8.0.x	You can upgrade directly to 8.3.122.0.
8.2.x	You can upgrade directly to 8.3.122.0. See the "Changes in Images and Installation Procedure for Cisco 2504 WLC, Cisco 5508 WLC, and Cisco WiSM2" section about special upgrade instructions for Cisco 2504 WLC, 5508 WLC, and WiSM2.
8.3.x	You can upgrade directly to 8.3.122.0.

- When you upgrade the Cisco WLC to an intermediate software release, you must wait until all of the access points that are associated with the 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 access point.
- You can upgrade to a new release of the Cisco WLC software or downgrade to an earlier release even if Federal Information Processing Standard (FIPS) is enabled.
- When you upgrade to the latest software release, the software on the access points associated with the Cisco WLC is also automatically upgraded. When an access point is loading software, each of its LEDs blinks in succession.

- We recommend that you access the Cisco WLC GUI using Microsoft Internet Explorer 10 or a later version or Mozilla Firefox 32 or a later version.

  Note Microsoft Internet Explorer 8 might fail to connect over HTTPS because of compatibility issues. In such cases, you can explicitly enable SSLv3 by entering the **config network secureweb sslv3 enable** command.

- Cisco WLCs support standard SNMP MIB files. MIBs can be downloaded from the Software Center on Cisco.com.
- The Cisco WLC software is factory installed on your Cisco WLC and is automatically downloaded to the access points after a release upgrade and whenever an access point joins a Cisco WLC. We recommend that you install the latest software version available for maximum operational benefit.
- Ensure that you have a TFTP, 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 Release 8.3.122.0. Some TFTP servers that support files of this size are tftpd32 and the TFTP server within the Prime Infrastructure. If you attempt to download the 8.3.122.0 Cisco WLC software 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.
- When you plug a Cisco WLC into an AC power source, the bootup script and power-on self test is run to initialize the system. During this time, press Esc to display the bootloader Boot Options menu. The menu options for the Cisco 5500 Series WLC differ from the menu options for the other Cisco WLC platforms.

  Bootloader menu for Cisco 5500 Series WLC:

  ```
  Boot Options
  Please choose an option from below:
  1. Run primary image
  2. Run backup image
  3. Change active boot image
  4. Clear Configuration
  5. Format FLASH Drive
  6. Manually update images
  Please enter your choice:
  ```

  Bootloader menu for other Cisco WLC platforms:

  ```
  Boot Options
  Please choose an option from below:
  1. Run primary image
  2. Run backup image
  3. Manually update images
  4. Change active boot image
  5. Clear Configuration
  Please enter your choice:
  ```

  Enter 1 to run the current software, enter 2 to run the previous software, enter 4 (on Cisco 5508 WLC), or enter 5 (on Cisco WLC platforms other than 5508 WLC) to run the current software and set the Cisco WLC configuration to factory defaults. Do not choose the other options unless directed to do so.

Note See the Installation Guide or the Quick Start Guide pertaining to your Cisco WLC platform for more details on running the bootup script and power-on self test.

- 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 menu to boot from the backup image. Then, upgrade with a known working image and reboot the 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}

  Here:

  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 for the config network ap-discovery nat-ip-only command. To disable AP link latency, use the config ap link-latency disable all command.

- You can configure 802.1p tagging by using the config qos dot1p-tag {bronze | silver | gold | platinum} command. For Release 7.2.103.0 and later releases, if you tag 802.1p packets, the tagging has an impact on only wired packets. Wireless packets are impacted only by the maximum priority level set for QoS.

- You can reduce the network downtime using the following options:
  - You can predownload the AP image.
  - For FlexConnect access points, use the FlexConnect AP upgrade feature to reduce traffic between the Cisco WLC and the AP (main site and the branch). For more information about the FlexConnect AP upgrade feature, see the Cisco Wireless Controller Configuration Guide.

- Do not power down the Cisco WLC or any access point during the upgrade process; otherwise, you might corrupt the software image. Upgrading a Cisco WLC with a large number of access points can take as long as 30 minutes, depending on the size of your network. However, with the increased number of concurrent access point upgrades supported, the upgrade time should be significantly reduced. The access points must remain powered, and the Cisco WLC must not be reset during this time.

- To downgrade from Release 8.3.122.0 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 the Cisco WLC, reboot the Cisco WLC for the changes to take effect:
  - Enable or disable link aggregation (LAG)
  - Enable a feature that is dependent on certificates (such as HTTPS and web authentication)
  - Add a new license or modify an existing license
  - 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
  - Make changes to TCP MSS settings

Changes in Images and Installation Procedure for Cisco 2504 WLC, Cisco 5508 WLC, and Cisco WiSM2

Due to an increase in the size of the Release 8.3.122.0 Cisco WLC software image, the Cisco 2504 WLC, Cisco 5508 WLC, and Cisco WiSM2 software images are split into the following two images:

- Base Install image, which includes the Cisco WLC image and a subset of AP images (excluding some mesh AP images and AP80x images) that are packaged in the Supplementary AP Bundle image
- Supplementary AP Bundle image, which includes AP images that are excluded from the Base Install image. The APs that feature in the Supplementary AP Bundle image are:
  - AP802
  - Cisco Aironet 1530 Series AP
  - Cisco Aironet 1550 Series AP (with 64-MB memory)
  - Cisco Aironet 1550 Series AP (with 128-MB memory)
  - Cisco Aironet 1570 Series APs

Note There is no change with respect to the rest of the Cisco WLC platforms.

Image Details

The following table lists the Cisco WLC images that you have to download to upgrade to Release 8.3.122.0 for the applicable Cisco WLC platforms:

Table 5: Image Details of Cisco 2504 WLC, 5508 WLC, and WiSM2

Cisco WLC	Base Install Image	Supplementary AP Bundle Image [1]
Cisco 2504 WLC	AIR-CT2500-K9-8-3-122-0.aes	AIR-CT2500-AP_BUNDLE-K9-8-3-122-0.aes
Cisco 5508 WLC	AIR-CT5500-K9-8-3-122-0.aes AIR-CT5500-LDPE-K9-8-3-122-0.aes	AIR-CT5500-AP_BUNDLE-K9-8-3-122-0.aes AIR-CT5500-LDPE-AP_BUNDLE-K9-8-3-122-0.aes
Cisco WiSM2	AIR-WISM2-K9-8-3-122-0.aes	AIR-WISM2-AP_BUNDLE-K9-8-3-122-0.aes

[1] AP_BUNDLE or FUS installation files from Release 8.3 for the incumbent platforms should not be renamed because the filenames are used as indicators to not delete the backup image before starting the download.

If renamed and if they do not contain “AP_BUNDLE” or “FUS” strings in their filenames, the backup image will be cleaned up before starting the file download, anticipating a bigger sized regular base image.

Upgrading to Cisco WLC Software Release 8.3.122.0 (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 Release 8.3.122.0 software:

a) Browse to https://software.cisco.com/download/navigator.html.
b) Choose **Wireless** from the center selection window.
c) Click **Wireless LAN Controllers**. The following options are displayed. Depending on your Cisco WLC platform, select either of these options:

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

d) Select the Cisco WLC model number or name.
The **Download Software** page is displayed.
e) The software releases are labeled as follows 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.

f) Click the filename (filename.aes).

Note In Release 8.3.102.0, for Cisco 2504 WLC, Cisco 5508 WLC, and Cisco WiSM2, the Cisco WLC software image is split into two images: the Base Install image and the Supplementary AP Bundle image. Therefore, to upgrade to Release8.3.122.0, repeat Step 2 through Step 14 to complete the installation of both the Base Install image and the Supplementary AP Bundle image.

Download the Supplementary AP Bundle image only if you are using any of these APs: AP802, Cisco Aironet 1530 Series AP, Cisco Aironet 1550 Series AP (with 64-MB memory), Cisco Aironet 1550 Series AP (with 128-MB memory), and/or Cisco Aironet 1570 Series APs. For more information, see the "Changes in Images and Installation Procedure for Cisco 2504 WLC, Cisco 5508 WLC, and Cisco WiSM2" section.

g) Click **Download**.
h) Read the Cisco End User Software License Agreement and click **Agree**.
i) Save the file to your hard drive.
j) Repeat steps a through *i* 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 802.11a/n and 802.11b/g/n networks.

Note For busy networks, Cisco WLCs on high utilization, and small Cisco WLC platforms, we recommend that you disable the 802.11a/n and 802.11b/g/n 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** text box, 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** text field, and 6 seconds for the Timeout text field should work correctly without any adjustment. However, you can change these values, if desired. To do so, enter the maximum number of times that the TFTP server attempts to download the software in the Maximum Retries text box and the amount of time (in seconds) for which the TFTP server attempts to download the software, in the Timeout text box.

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

Step 11 In the **File Name** text box, 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** text box, enter the username with which to log on to the FTP server.
b) In the **Server Login Password** text box, enter the password with which to log on to the FTP server.
c) In the **Server Port Number** text box, 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 appears indicating the status of the download.

Note In Release 8.3.102.0, for Cisco 2504 WLC, Cisco 5508 WLC, and Cisco WiSM2, the Cisco WLC software image is split into two images: the Base Install image and the Supplementary AP Bundle image. Therefore, to upgrade to Release8.3.122.0, repeat Step 2 through Step 14 to complete the installation of both the Base Install image and the Supplementary AP Bundle image.

Download the Supplementary AP Bundle image only if you are using any of these APs: AP802, Cisco Aironet 1530 Series AP, Cisco Aironet 1550 Series AP (with 64-MB memory), Cisco Aironet 1550 Series AP (with 128-MB memory), and/or Cisco Aironet 1570 Series APs. For more information, see the "Changes in Images and Installation Procedure for Cisco 2504 WLC, Cisco 5508 WLC, and Cisco WiSM2" section.

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 For Cisco WiSM2 on the Catalyst switch, check the port channel and re-enable the port channel if necessary.

Step 18 If you have disabled the 802.11a/n and 802.11b/g/n networks, re-enable them.

Step 19 To verify that the 8.3.122.0 Cisco WLC software is installed on your Cisco WLC, click **Monitor** on the Cisco WLC GUI and view the Software Version field under Controller Summary.

Interoperability With Other Clients in this Release

This section describes the interoperability of Cisco WLC Software, Release 8.3.122.0 with other client devices.

The following table describes the configuration used for testing the client devices.

Table 6: Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	8.3.122.0
Cisco WLC	Cisco 55xx Series Wireless Controller
Access points	AIR-CAP3802E-B-K9, AIR-AP1852E-B-K9
Radio	802.11ac, 802.11a, 802.11g, 802.11n (2.4 GHz / 5.0 GHz)
Security	Open, PSK (WPA-TKIP-WPA2-AES) (WPA-TKIP), 802.1X (WPA-TKIP-WPA2-AES) (LEAP, EAP-FAST)
RADIUS	ACS 5.3, ISE
Types of tests	Connectivity, traffic (ICMP), and roaming between two access points

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

Table 7: Laptops

Client Name	Version Details
Asus AC56(USB)	1027.515.2015
Broadcom 4360	6.30.163.2005
D-Link DWA-182 (USB)	6.30.145.30
Dell 1520/Broadcom 43224HMS	5.60.48.18
Dell 1530 (Broadcom BCM4359)	5.100.235.12
Dell 1540	6.30.223.215
Dell 1560	6.30.223.262
Engenius EUB 1200AC(USB)	1026.5.1118.2013
HP Chromebook	55.0.2883.103
Intel 3160	18.40.0.9
Intel 6205	15.16.0.2
Intel 6300	15.16.0.2
Intel 7260	18.33.3.2
Intel 7265	19.10.1.2
Intel 8260	19.50.1.5
Linksys AE6000 (USB)	5.1.2.0
MacBook Air new	OSX 10.11.5
MacBook Air old	macOS Sierra (10.12.3)
Macbook New 2015	macOS Sierra (10.12.5)
MacBook Pro	macOS Sierra (10.12.2)
Macbook Pro with Retina Display	OSX 10.12
Netgear A6200 (USB)	6.30.145.30
Netgear A6210(USB)	5.1.18.0
Samsung Chromebook	55.0.2883.103

Table 8: Tablets

Client Name	Version Details
Apple iPad Air	iOS 10.2.1
Apple iPad Air 2	iOS 10.2.1
Apple iPad mini with Retina display	iOS 10.2.1
Apple iPad Pro	iOS 10.2.1
Apple iPad2	iOS 10.3
Apple iPad3	iOS 10.2.1
Google 10.2" Pixel C	Andriod 7.1.1
Google Nexus 9	Android 6.0.1
Microsoft Surface Pro 2	Windows 8.1 - Driver: 14.69.24039.134
Microsoft Surface Pro 3	Windows 8.1 - Driver: 15.68.3093.197
Microsoft Surface Pro 4	Windows10 - Driver: 15.68.9040.67
Samsung Galaxy Note 3 - SM-N900	Android 5.0
Samsung Galaxy Tab 10.1- 2014 SM-P600	Android 4.4.2
Samsung Galaxy Tab Pro SM-T320	Android 4.4.2
Toshiba Thrive AT105	Android 4.0.4

Table 9: Mobile Devices and Printers

Client Name	Version Details
Apple iPhone 4S	iOS 10.2.1
Apple iPhone 5	iOS 10.2.1
Apple iPhone 5c	iOS 10
Apple iPhone 5s	iOS 10.2.1
Apple iPhone 6	iOS 10.2.1
Apple iPhone 6 Plus	iOS 10.2.1
Apple iPhone 6s	iOS 10.2.1
Apple iPhone 7	iOS 10.2.1
Cisco 7925G-EX	CP7925G-1.4.8.4.LOADS

Client Name	Version Details
Cisco 7926G	CP7925G-1.4.5.3.LOADS
Cisco-8821	SIP8821.11-0-3ES2-1
Cisco 8861	SIP 88xx.10-2-1-16
Cisco-9971	SIP9971.9-4-1-9
Datamax o'neil RL4e	18.06_0049 0004
Getac F110	Windows 7
Google Nexus 5	Android 6.0.1
Google Nexus 5X	Android 6.0.1
Google Pixel	Android 7.1.1
HP Color LaserJet Pro M452nw Printer	2.4.0.125
HTC One	Android 5.0
LG G4	Android 5.1
MC40N0	Andriod 4.4.4
MC55A	OS 05.02.29344
MC70	05.01.0476
MC9060	Microsoft Pocket PC Version 4.20.0
MC9090-d1cb	OS 5.1.478 (Build 15706.3.5.2)
MC9190G	OS 06.00.000
MC92	Andriod 4.4.4
Motorola MC 75A	OS 5.2.23137 (Build 23137.5.3.9)
Motorola WT41N0	OS 7.00.2824 (OEM Version: 02.46.02) - WLAN Firmware: X_2.01.0.0200
Nokia Lumia 1520	Windows Phone 8.10.14219.341
OnePlusOne	Android 4.3
OnePlus3	Android 6.0.1
Samsung Galaxy Mega SM900	Android 4.4.2
Samsung Galaxy Nexus GTI9200	Android 4.4.2
Samsung Galaxy S III	Android 4.3

Client Name	Version Details
Samsung Galaxy S4	Android 5.0.1
Samsung Galaxy S4 T-I9500	Android 5.0.1
Samsung Galaxy S5	Android 4.4.2
Samsung Galaxy S5-SM-G900A	Android 4.4.2
Samsung Galaxy S6	Android 6.0.1
Samsung Galaxy S7	Android 6.0.1
Sony Xperia Z Ultra	Android 4.4.2
TC55	Andriod 4.1.2
TC70	Andriod 4.4.3
TC75	Andriod 4.4.3
TC8000	Andriod 4.4.3
VC5090	Microsoft Windows CE version 5.00 (Build 1400)
VC70N0	OS 7.00.2864
Xiaomi Mi 4c	Android 5.1
Xiaomi Mi 4i	Android 6.0.1
Zebra CC5000-15	Andriod 4.1.1
Zebra ET1	Andriod 2.3.4
Zebra TC51	Andriod 6.0.1
Zebra ZT230	V72.19.15Z
Zebra ZT410	V72.19.15Z

Key Features Not Supported on Cisco WLC Platforms

This section lists the features that are not supported on the different 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 on Cisco 2504 WLCs

- Autoinstall
- Cisco WLC integration with Lync SDN API
- Application Visibility and Control (AVC) for FlexConnect local switched access points
- Application Visibility and Control (AVC) for FlexConnect centrally switched access points

Note However, AVC for local mode APs is supported. If you are using a Cisco 2500 Series controller and you intend to use the Application Visibility and Control (AVC) and NetFlow protocol features, you must install Release 1.9.0.0 of Cisco Wireless LAN Controller FUS. This is not required if you are using other controller hardware models.

- URL ACL
- Bandwidth Contract
- Service Port
- AppleTalk Bridging
- Right-to-Use Licensing
- PMIPv6
- EoGRE
- AP Stateful Switchover (SSO) and client SSO
- Multicast-to-Unicast
- Cisco Smart Software Licensing

Note The features that are not supported on Cisco WiSM2 and Cisco 5508 WLC are not supported on Cisco 2504 WLCs too.

Note Directly connected APs are supported only in the local mode.

Key Features Not Supported on WiSM2 and Cisco 5508 WLCs

- Spanning Tree Protocol (STP)
- Port Mirroring
- VPN Termination (such as IPsec and L2TP)
- VPN Passthrough Option

Note You can replicate this functionality on a Cisco 5500 Series WLC by creating an open WLAN using an ACL.

- Configuration of 802.3 bridging, AppleTalk, and Point-to-Point Protocol over Ethernet (PPPoE)
- Fragmented pings on any interface
- Right-to-Use Licensing
- Cisco 5508 WLC cannot function as mobility controller (MC). However, Cisco 5508 WLC can function as guest anchor in a New Mobility environment.
- Cisco Smart Software Licensing

Key Features Not Supported on Cisco Flex 7510 WLCs

- Static AP-manager interface

Note For Cisco Flex 7500 Series WLCs, it is not necessary to configure an AP-manager interface. The management interface acts as an AP-manager interface by default, and the access points can join on this interface.

- IPv6 and Dual Stack client visibility

Note IPv6 client bridging and Router Advertisement Guard are supported.

- Internal DHCP server
- Access points in local mode

Note An AP associated with the Cisco WLC in the local mode should be converted to the FlexConnect mode or monitor mode, either manually or by enabling the autoconvert feature. On the Cisco Flex 7500 WLC CLI, enable the autoconvert feature by entering the config ap autoconvert enable command.

- Mesh (use Flex + Bridge mode for mesh-enabled FlexConnect deployments)
- Spanning Tree Protocol (STP)
- Cisco Flex 7500 Series WLC cannot be configured as a guest anchor Cisco WLC. However, it can be configured as a foreign Cisco WLC to tunnel guest traffic to a guest anchor Cisco WLC in a DMZ.
- Multicast

Note FlexConnect local-switched multicast traffic is bridged transparently for both wired and wireless on the same VLAN. FlexConnect access points do not limit traffic based on Internet Group Management Protocol (IGMP) or MLD snooping.

- PMIPv6
- Cisco Smart Software Licensing
- EoGRE

Key Features Not Supported on Cisco 5520, 8510, and 8540 WLCs

- Internal DHCP Server
- Mobility controller functionality in converged access mode

Note Cisco Smart Software Licensing is not supported on Cisco 8510 WLC.

- Spanning Tree Protocol (STP)
- Port Mirroring
- VPN Termination (such as IPsec and L2TP)
- VPN Passthrough Option

Note You can replicate this functionality by creating an open WLAN using an ACL.

- Configuration of 802.3 bridging, AppleTalk, and Point-to-Point Protocol over Ethernet (PPPoE)
- Fragmented pings on any interface
- Cisco 5520, 8510, and 8540 WLCs cannot function as mobility controller (MC). However, they can function as guest anchor in a New Mobility environment.

Key Features Not Supported on Cisco Virtual WLCs

- Internal DHCP server
- TrustSec SXP
- Access points in local mode
- Mobility/Guest Anchor
- Wired Guest
- Multicast

Note FlexConnect local-switched multicast traffic is bridged transparently for both wired and wireless on the same VLAN. FlexConnect access points 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.

- 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
- Cisco WLC integration with Lync SDN API
- Cisco OfficeExtend Access Points

Key Features Not Supported on Access Point Platforms

Key Features Not Supported on Cisco Aironet 1520 and 1550 APs (with 64 MB memory)

- PPPoE
- PMIPv6

See the amount of memory in a Cisco Aironet 1550 AP by entering this command in Cisco WLC CLI:

show mesh ap summary

Key Features Not Supported on Cisco Aironet 1560, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800, and 3800 Series APs

Table 10: Key Features Not Supported on Cisco Aironet 1560, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800 and 3800 Series APs

Operational Modes	• Spectrum Expert Connect • Autonomous Bridge and Workgroup Bridge (WGB) mode • Mesh mode • Flex plus Mesh • 802.1x supplicant for AP authentication on the wired port • Link aggregation (LAG) behind NAT/PAT environment
Protocols	• 802.11u • Full Cisco Compatible Extensions (CCX) support • Rogue Location Discovery Protocol (RLDP) • Native IPv6 • Internet Group Management Protocol (IGMP) v3
Security	• TrustSec SXP • 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)
Location Services	• Data RSSI (Fast Locate)

FlexConnect Features	• Per Client AAA (QoS Override) • Bidirectional rate-limiting • Split Tunneling • EoGRE • PPPoE • Multicast to Unicast (MC2UC) • Traffic Specification (TSpec) • Cisco Compatible Extensions (CCX) • Call Admission Control (CAC) • DHCP Option 60 • NAT/PAT support • VSA/Realm Match Authentication • Link aggregation (LAG) • MAC Authentication Flex Local Authentication • SIP with FlexConnect in local switching mode

Key Features Not Supported on Cisco Aironet 1810 OEAP and 1810W Series APs

Table 11: Key Features Not Supported on Cisco Aironet 1810 OEAP and 1810W Series APs

Operational Modes	• Monitor Mode • Mobility Express

Key Features Not Supported on Cisco Aironet 1830 and 1850 Series and 1815i APs

Table 12: Key Features Not Supported on Cisco Aironet 1830 and 1850 Series and 1815i APs

Operational Modes	• Monitor Mode

Key Features Not Supported on 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
- Access point join priority (mesh access points have a fixed priority)

- Location-based services

Caveats

Open Caveats

Table 13: Open Caveats for Release 8.3.121.0 and 8.3.122.0

Caveat ID Number	Description
CSCuj27382	AP local auth, PEAP auth fails, with EAP-TLS enabled and no or expired certificate
CSCur89551	LWAPP-3-INVALID_AID: message observed for Flex 1240 APs
CSCus50404	AP Name is mismatched between controller and Cisco AP
CSCut91086	Client associated to MAP does not get AAA override in Flex+Bridge mode
CSCux92335	Cisco 3602 APs losing MAC address 8.0.120.0
CSCuy66962	Roaming fails with WLC not sending Sent 1x initiate message
CSCuy75333	Cisco 2504 WLC config restoration failure due to multicast mode command
CSCuy93000	SC2 Radio Randomly sending Corrupted timestamp BCN on Hidden SSID
CSCuz19004	Radio Resets on Cisco 702w AP
CSCva04984	WebUI displays wrong WLAN ID under AP for FlexConnect AVC mappings at Flex group
CSCva33956	After using SFTP transfer, spurious messages are observed and WLC goes non responsive
CSCva50180	AIR-CAP1602I-E-K9 stopped working
CSCva58323	AP3800 sends out multicast packets with no clients associated
CSCva58429	Cisco 1532i AP low throughput (Flex Local switching + EoGRE)
CSCva82261	Cisco 1532 AP uplink drops when sending heavy upstream traffic
CSCva87833	AIR-CT8510-K9 stopped working; SSO disabled
CSCvb71347	WLC multicast config not coherent for code upload/download
CSCvb86237	Cisco 8510 WLC stopped working Task Name: TempStatus
CSCvb90235	Cisco 3700 AP WGB inconsistently facing joining issues because of no probe response by 3600-802.11ac module root AP
CSCvb91832	Cisco 1810W radio firmware reloads unexpectedly @0x009C30A0/0x0000, memory corruption

Caveat ID Number	Description
CSCvb93124	Cisco WLC stopped working on spamApTask5
CSCvc01761	WLC Continuously Probes Active RADIUS Server
CSCvc06547	AP retransmits packet even though client sends ACK
CSCvc17678	Cisco 8.3.111.0: wrong enable global mDNS snooping message when clicking apply on Cisco 2800, 3800 APs edit page
CSCvc18786	WLC stops working during multiple login sessions either with local user or with TACACS+
CSCvc24917	Defect of msglog corresponding to 'AP Message Timeout: Max retransmissions reached on AP ...'
CSCvc28035	clDLApBootTable shows blank when WLC has 2800I AP
CSCvc30828	AP does not allow world mode to be set via GUI on 15.3(3)JD
CSCvc31268	CISCO-LWAPP-SYS-MIB::clsApTransferEntry isn't provided values for AP primary/ backup images
CSCvc31574	AP_2800 : Kernel Panic PC is at memset+0x74/0xe0
CSCvc35151	AP radio reset happens multiple times without trigger
CSCvc37641	Cisco 700 AP does not provide SSH access in WIPS submode for Cisco FlexConnect
CSCvc45620	Cisco WLC reloads unexpectedly in SNMPTask due to missed software watchdog
CSCvc51637	802.1x CCKM roams fail on WGB at GTK key rotation
CSCvc51666	IOS AP transmits on the disabled 24Mb rate band
CSCvc53441	AP3800 Flex not starting EAPOL process when PMF=Required with HotSpot STA
CSCvc53744	MFPR and MFPC disabled clients is not dissociated as per 8.4.3 (802.11w) specifications
CSCvc55430	WLC HA redundancy management interface not reachable for a short time after failover
CSCvc61795	IP call setup fail after L3 handover happens during call among Cisco 1832AP
CSCvc66547	CPU ACL configured to block access to Virtual IP does not work as expected
CSCvc70819	GUI: Could not configure Global multicast mode for Cisco 7500 WLC image
CSCvc71537	Cisco WLC profiles Cisco Unified Wireless IP Phone 7925 incorrectly
CSCvc72724	Cisco 8510 AP SSO stopped working on portalProcessLogout
CSCvc76969	Silent reboot on Cisco 5508 and WiSM2 WLCs

Caveat ID Number	Description
CSCvc78857	AVC profile is not applied on client behind WGB.
CSCvc82559	CIsco 5508 WLC reaper rest stopped working on several tasks.
CSCvc84474	ISE Endpoint purge not working on Foreign-Anchor setup
CSCvc84637	Cisco 1810W APs sending invalid AC_NAME when WLC hostname is 31 bytes long
CSCvc89532	Cisco 1702i AP stopped working with DOT11-2-RADIO_RX_BUF: Corrupt buffer: errors
CSCvc93377	Tracebacks and MFP queue logs filling up the message log on WLC
CSCvc95821	GUI-ping o/p not throwing proper previlege error with read only user
CSCvc96076	Cisco WiSM2 HA - standby stopped working with task name spamApTask2 in ideal state
CSCvd02303	Flex-Bridge AP stopped working while joining to the Cisco WLC
CSCvd07243	Unable to change AP name nor location from the GUI
CSCvd09507	Rogue Rule substring-ssid turns invalid on WLC when user configured SSID is included in PI template
CSCvd16346	Cisco WLC memory corruption when TACACS+ respond with unknown attributes
CSCvd16800	Client associated to MAP does not get AAA override in Flex+Bridge mode. Bug ID CSCut91086 not fixed
CSCvd19417	Single A-MPDU fix TID 0 issues
CSCvd22402	WLAN-VLAN mapping is not removed after deleting WLAN
CSCvd23175	Cisco 2800, 3800 APs WCPD memory leak observed
CSCvd23185	WGB wired clients not seen by WLC.
CSCvd23301	WLC GUI Trapflags for client association with statistics does not display correct config
CSCvd23902	Cisco 1532 AP: Root bridge drops packets from non-root bridge in non-native VLAN
CSCvd26885	Unit of probe suppression hysteresis should be dB
CSCvd27365	Incorrect number of clients reported on Cisco AP by Cisco WLC
CSCvd28374	Cisco 802 AP incorrect base radio MAC assigned not ending with zero causing to only support one BSSID
CSCvd29653	iPhone7 dissociates after session-timeout
CSCvd34785	Mobility multicast ip address reverse in TACACS+ packets

Caveat ID Number	Description
CSCvd36190	Cisco 5520 WLC stopped working with Taskname haSSOServiceTask6
CSCvd37522	show run-config' commands: Incorrect index numbers for RADIUS Accounting Servers
CSCvd40203	Cisco 3700 AP FlexConnect reloads unexpectedly with FT or adaptive FT roaming with Iphone 6s plus + WGB + debugs on
CSCvd40978	COS APs (Cisco AP2800, 3800, 1850 APs) on 8.2 falsely show 100% channel utilization
CSCvd42321	Cisco 1832 APs drop CAC SIP 486 Packet
CSCvd42669	Cisco 2500 WLC stopped working
CSCvd44909	Client traffic dropped in Anchor foreign AirOS setup with new-mobility if foreign is behind NAT
CSCvd45744	Customer reporting that AP reboots after 4 hours while doing Site Survey
CSCvd46374	Client with lower signal strength than RX-SOP threshold can connect radio
CSCvd48852	Audit-Session-ID info is missing after re-authentication
CSCvd50134	Cisco 2600, 3700 APs not showing last reload reason
CSCvd52587	Cisco 1140 AP 2.4GHz radio resets with reason code 71 on event.r0
CSCvd55938	Client fails to pass traffic after 802.11r roaming with 802.11w set to optional
CSCvd56588	Cisco 2800, 3800 APs: Incorrect RSSI Values displayed when client associates to XOR radio
CSCvd62184	SC2: Radio reset /w reason reqsema on 8.3MR2
CSCvd63539	Getting 'max containments reached...:3' on Cisco 1852 AP in monitor mode
CSCvd64928	System stopped working on PMIPV6_Thread_0 during creation of LMA entry
CSCvd65773	Need to extend SC3 WiMAX reg change CSCuz23501 to all non-DFS channels
CSCvd67485	Flex AP reconnect, radio reset during DTLS setup
CSCvd67730	Client fails PSK SSID authentication after master AP reboot (EAPOL M3 not sent on 4-way handshake)
CSCvd68141	WLC stopped working at task nmspRxServerTask
CSCvd68412	Wireless client Rx stats not getting updated
CSCvd68648	cLApWlanStatsOnlineUserNum is not current number of online user
CSCvd72064	GUI does not show which accounting servers are active
CSCvd72117	Pending request Counter increments for acct and auth server to which no acct/auth request being send

Caveat ID Number	Description
CSCvd72131	Cisco 7500 Flex WLC reloads unexpectedly for SNMPTask Reaper reset
CSCvd72499	Cisco 3800APs: sometimes sending 802.11 deauthentication to clients just after a roaming event
CSCvd75965	AP Sends deauth to iphone leading to 11r roaming faliure while doing continous roaming using JFW
CSCvd76743	COS Flex: AP makes all QoS frames as Best Effort on Platinum WLAN
CSCvd76773	Antenna Gain on 2.4 GHz radio resets to default after Cisco 3800 E AP reboot
CSCvd77312	Cisco 3800 AP: Frequent AP radio reloads unexpectedly due to TCQVerify not equal to zero
CSCvd78053	Cisco AP vapID is missing in show CAPWAP reap saved
CSCvd79416	Cisco OEAP1810 GUI: In/Out packet count for LAN Port and Clients connected via switch get reset after few secs
CSCvd79464	APs with WSM module enabled sending RRM Data every 5sec for each radio
CSCvd79511	Radius Admin mode goes into disable state in LTB setup
CSCvd79745	Clients fail to pass auth when using L2 and Web-Auth on MAC failure on same WLAN
CSCvd80508	Cisco 1810W AP at a vWLC: LAN ports stuck on admin-down after modifying RLAN settings
CSCvd84229	Cisco WLC wrongly reporting 4SS rate for HT in 2.4GHz with Cisco 1850 APs
CSCvd84773	Cisco WLC reloads unexpectedly in an loop due to nmspRxServerTask
CSCvd86566	Client with incorrect NAI Realm gets Access-Accept from RADIUS server
CSCvd90110	Cisco 2800 APs sending incorrect AKM in Re-assoc response in Flex Mode with adaptive FT
CSCvd90151	Cisco 2800, 3800 APs: when WLC sends association reject, AP sends deauth with status 0
CSCvd90377	Cisco WLC applying wrong ACL to clients when doing CWA
CSCvd91152	Cisco 3700 APs in FlexConnect running on Cisco 8.3.111.0 release reloads unexpectedly
CSCvd96678	Vocera B3000N badge failing to associate
CSCvd96846	SXP debugs - IP address of client displayed in reverse
CSCve02041	Cisco 2800, 3800APs: AP printing 'radio off due to POE' when it is actually on
CSCve02210	Incorrect SNMP OID issue for FT - 1.3.6.1.4.1.9.9.521.1.1.1.1.10
CSCve02612	HA- Config sync failed on standby when Cisco Flex AP configs modified

Caveat ID Number	Description
CSCve02689	Silent reboot after memory usage goes to 85%
CSCve12254	cLApWlanStatsOnlineUserNum is not current number of online user
CSCve13779	Cisco 2802 AP: rogue detection configuration changed back to Enabled after AP reboot
CSCve15860	Cisco 8540 WLC is not responding to capwap-data keep-alive
CSCve18213	Foreign WLC leaks IPv6 and IPv4 multicast client traffic out of EoIP tunnel
CSCve20123	When client does inter AP roam DP may not plumb tclass while having active call **Note** Do not upgrade to Release 8.3.121.0 if your network deployment uses TSPEC protocols (VoWLAN clients such as 792x, 882x, Spectralink) and if TSPEC and CAC is enabled on it. Contact Cisco TAC for further information if you must upgrade to this release.
CSCve23581	Cisco AP2800, 3800 AP sends multicast with AES when client is TKIP
CSCve24871	Flex ARP responds for wired clients
CSCve26935	Cisco 2800, 3800 AP: IPv4 TCP low throughput with Windows 10 Creator
CSCve26948	Cisco 2800, 3800 AP: CAPWAPd blocked during Cisco AP boot causing watchdog reset (WCPD)
CSCve27052	Cisco APs shows public IP on Cisco WLC GUI but private IP in CLI
CSCve38070	Cisco 2800, 3800 APs false 100% channel utilization observed
CSCvk44249	WLC 5508 - foreign mapping is missing on a WLAN when restoring a backup

Resolved Caveats

Table 14: Resolved Caveats for Release 8.3.121.0 and 8.3.122.0

Caveat ID Number	Description
CSCuq05475	Controller GUI shows AP's NAT IP instead of private IP
CSCuw45964	Mobility Express: While Editing a WLAN in HTTP session, user is getting logged out
CSCux11777	AP1532 non-root bridge high retransmission and latency rate
CSCux83260	"lbs-ssc" and" sha256-lbs-ssc" missing in Cisco WLC web UI
CSCux97132	AP starts CAC timer after rolling back to lower bandwidth
CSCuz03702	New mobility:Wired client behind WGB fails to pass traffic after roaming
CSCuz16883	Address registration issues for mobility scenarios

Caveat ID Number	Description
CSCuz45986	CWA not working on Cisco 8500 WLC as guest anchor with accounting enabled
CSCuz47559	Error saving config file happens on multiple Cisco 2702 APs
CSCuz70879	MAP reloads on hitting 40 mins timer even when it is downloading image
CSCva06617	Globally configured ATF mode not applied to newly joined AP2700
CSCva14667	GET on AP groups table after set - response missing
CSCva17630	WLC sends warm-start trap instead of cold-start during autoprovisioning
CSCva26821	Auto Anchor Deployment: scheduling deletion of mobile station fails
CSCva31890	MIB table bsnMobileStationPerRadioPerVapTable has no data
CSCva33212	Reintroduce auto provisioning feature on WLC 2504 running 8.0 release
CSCva39537	802.11h configuration not saved after restoring config backup
CSCva40580	BulkSync on active WLC never completes and is stuck in 'in-progress'
CSCva44397	WLC gateway not reachable after disabling LAG
CSCva46506	Flexgroup RADIUS configurations are not pushed to AP
CSCva49263	802.11r re-auth failure after roaming
CSCva64515	%SPECTRUM-3-CA_LOGMSG: SPECTRUM LOG: invalid radio type
CSCva66176	AP drop of from Network due to large set of Mobility groups in down/down
CSCva66489	802.11r session timeout after reassocition causing deauthentication 17 mismatch FTIE
CSCva68921	Cisco WiSM2 reaperWatcher got stuck on DP0 while retriving crash and reloads unexpectedly
CSCva77707	AIR-CT5508 SSO ARP request out redundancy management sent with wrong MAC
CSCva81406	WLC - Unmap deauth reason code 16 from reason code 15 exclusively
CSCva83802	HA: SSH on redundancy management interface rejected
CSCva85361	WLC losing IPv6 connectivity
CSCva90265	iPAD PRO with IOS10 is getting deauthenticated at times due to M3 timer
CSCva91483	AP2700 failing co-channel fairness with Samsung S5
CSCva92917	Observed Traceback logs in show msglog and logging

Caveat ID Number	Description
CSCva95121	Stale IP route left on Flex AP config if booting up in standalone mode
CSCva99052	Configuring 1810W to OEAP does not enable DHCP on Local port LAN3
CSCva99545	Invalid information displayed in show cert webauth/webadmin
CSCvb03237	ME contacting CCO byitself
CSCvb05067	Local EAP fails after wrong username login
CSCvb05494	Wrong format of SNMP trap - mobility flap alarm
CSCvb11778	Cisco WLC running 8.1.x release reloads unexpectedly on sisfSwitcherTask
CSCvb12026	Client Load Balance export to anchors fails with new mobility enabled
CSCvb12565	WLC stops working when running 'show run-config' command with no APs
CSCvb13666	WiSM2 stopped working with Task Name 'IPv6_Msg_Task'
CSCvb15871	aIOS does not forward broadcast multicast frames with dynamic VLAN
CSCvb16806	Cisco 5500 MC showing stale connections from MA clients
CSCvb20553	CoA for session timeout not working using free RADIUS server
CSCvb29996	Cisco 1810W AP hardware Watchdog reloads unexpectedly PC=0xc03b3ffc, LR=0xc008af24
CSCvb33076	WLC: GUI does not allow to change sniffer channel
CSCvb35865	AP2800 reloads unexpectedly for FlexConnect-Sensor-FlexConnect
CSCvb44979	WLC Local EAP with Cisco Unified Wireless IP Phone 7925 handshake failure
CSCvb45130	Part of ATF config is not pushed to uploaded config
CSCvb46044	Standby reboots continuously with reason XMLs were not transferred from Active to Standby
CSCvb48354	RRM Not updating as per configured on WLC
CSCvb51570	WISM 2 reloads unexpectedly on upgrade to 8.3.102.0 with Task Name: spamApTask6
CSCvb53368	Validate rogue clients against AAA not work
CSCvb54306	Cisco 1815 AP: LED blikning green - light green even at full power and clients connected
CSCvb57350	SNMP trap for AP interface Up/down traps not getting generated

Caveat ID Number	Description
CSCvb57779	APs unable to join WLC in different subnet through gateways with proxy-arp disabled
CSCvb61023	DHCP Option 82(remote-id) not present is some AP
CSCvb62874	Radio interface input queue gets filled on Autonomous APs
CSCvb64042	WLC HA transfer download failure with legitimate network latency
CSCvb64560	CISCO-LWAPP-AAA-MIB: DEFVAL format incorrect for some objects
CSCvb67724	Cisco 5508 WLC is going out of memory
CSCvb69962	Client traps not showing session ID's
CSCvb70551	COS AP's rebooted due to Kernel Panic-Not Syncing: Out of Memory
CSCvb71600	Cisco WLC stopped woking after applyng CPU ACL
CSCvb74948	AVC - CISCO-JABBER-IM application is getting misclassified as SSL
CSCvb77390	WLC stopped working accessing MAC Address Database
CSCvb81940	VLAN tagging for external module removed from Cisco AP after upgrade to 8.3.102.0 release
CSCvb86157	Clients cannot connect anymore to vWLC- Instrumented code added
CSCvb88777	ME:Console lockup due to unwanted rsync failure messages
CSCvb89781	Cisco 2700-B AP unable to join WLC: Unable to create temp dir "flash:/update"
CSCvb91652	WLC sluggishness due to flooding probe, need probe throttling configs
CSCvb93189	AP drops Retransmitted M3 from WLC
CSCvb93365	WLC msglog showing a lot of traceback
CSCvb94413	Cisco 2800, 3800 APs: low Tx power observed in certain RF conditions
CSCvb96009	Cisco WLC running 8.3.102 reloads unexpectedly on emweb task
CSCvb97383	WLC deauthenticating roaming client with idle timeout
CSCvb97656	Unexpected reload: Task Name: mmListen on 8.3.102.0
CSCvb98859	AP in local sw/local auth disconnect EAP-SIM client idle for more than 0.5 second
CSCvb99468	AirOS WLC reloads unexpectedly in emWeb when serving an EmWebForm exclusion-list
CSCvc04089	Cisco 2700 series AP radio resets reason code 71 RADIO_RC_NO_REPORT

Caveat ID Number	Description
CSCvc07184	Media streaming behavior different between 1560/3800 and 3700
CSCvc07521	AP3800 sends A-MSDU larger than client can handle
CSCvc08052	DFS false detection on AP2700
CSCvc09824	AP2800 band select stats counter show zero
CSCvc11630	Radio reset in switching to connected mode from standalone
CSCvc12594	Controller fails to send SNMP when using untagged interfaces on different ports
CSCvc18670	WLC: Client stops passing traffic on DHCP Reqd. WLAN after sending a Reassoc request but no DHCP pkt
CSCvc23724	Cisco WLC reloads unexpectedly with EoGRE Heartbeat and skip count configured with value 0 which makes tunnel dead
CSCvc24485	#APF-3-UNKNOWN_RADIO_TYPE: [SS] apf_utils.c:571 Unknown Radio Type 0 from Standby flooding syslog
CSCvc28168	WLC set ZERO 802.11e QoS UP for part of the downstream voice packets and APs trust it
CSCvc33793	WLC tears down connected AP due to unequal loadbalance between SPAM queues high load
CSCvc39231	SNMP GETBULK on cLIpsecProfileTable returns with No response from controller
CSCvc40267	WLC sends wrong VLAN for AAA overriden client re-associating to AP belonging to FlexConnect Group
CSCvc40852	Active controller in HA pair shows different socket errors
CSCvc41438	WGB running 15.3(3)JD WGB takes ~500ms longer to scan DFS channels vs JBB
CSCvc41484	Cisco 1850 APs: high failure rate in off-channel operation
CSCvc44293	ME UI - Changing Transmit power on UI does not work
CSCvc49492	AP1852 detects high noise level on 5-GHz radio
CSCvc49713	AP generates flood of Received and decoded a DMS client request payload successfully
CSCvc50436	WGB wired client randomly stuck in the DHCP_REQD state after layer 2 roaming between the controllers
CSCvc52093	WLC send deauth 17 to phone in 4-way handshake
CSCvc55328	Cisco AP reloads unexpectedly due to kernel panic at WlLoadRateGrp
CSCvc61652	m25/1.0 is shown in client info

Caveat ID Number	Description
CSCvc62277	Cisco 5520 WC reloads unexpectedly on running RRM commands on task emWeb
CSCvc63169	Flex AP specific WLAN-VLAN Mapping lost on rebooting the AP
CSCvc65568	Cisco Wireless IP Phne 8821 fails 802.11r FT roam with invalid FTIE MIC
CSCvc65641	WLC reports tracebacks reported very frequently but no unexpected reloads
CSCvc65675	WLC: Constantly increasing memory consumption by SNMPTask
CSCvc66352	Cisco 5500 WLC reloads unexpectedly with taskname emweb
CSCvc67005	2802 AP drops client ARP packets after web authentication
CSCvc67465	Flex AP loses VLAN mapping if VLAN tagging is enabled
CSCvc68156	Full support for distance on AP1572
CSCvc74507	Fix incorrect commit of CSCuu59589
CSCvc74515	WLC Data plane stopped working due to fragmentation
CSCvc74876	Cisco 2800, 3800 APs runing 8.2.145.21 release: CAPWAP disconnect then stuck in discovery loop
CSCvc78510	Cisco 2702 AP aux port goes to disabled after the AP is rebooted
CSCvc78546	WLC sets Zero 802.11e QoS for downstream voice traffic when CAC is disabled
CSCvc79811	When adding or removing country codes 2.4-GHz channels change
CSCvc81929	ME reloads unexpectedly when DHCP screen is accessed
CSCvc82053	The NMSP info or probe notification queue is saturating
CSCvc82376	EAP-TLS certs and PMK cache are missing on Flex AP after reload
CSCvc82845	WLC returns nothing for SNMP get WEB ACL - cldcClientAaaOverrideAclName
CSCvc83175	vWLC does not learn client IP / Client stuck in DHCP_REQD
CSCvc83465	Cisco 3800 AP sometime stops sniffing on DFS channel
CSCvc83490	Redundancy Mobility MAC does not stay, Primary WLC's MAC is always set instead
CSCvc83583	Cisco 5520 WLC reloads unexpectedly with taskname apfProbeThread
CSCvc85164	802.11k: WNM neighbor report is empty in when WLAN ID is greater than 1

Caveat ID Number	Description
CSCvc85328	AP1832/1852 APs: Power injector/Normal mode inspite of power supply by AIR-PWR-C
CSCvc86170	ClickAP FlexConnect Local Auth doesn't work on WLAN with CCKM security
CSCvc86951	Cisco 1850 AP beacon missing or corrupted during downstream traffic test
CSCvc86979	2800 AP silent reboot with NUL print every 10 mins continuously
CSCvc87433	Webauth with proxy does not work after 8.2
CSCvc88997	FRA probe suppression config not saved after WLC reboot
CSCvc93398	AP2800/AP3800 MU-MIMO forms MU groups with 2SS clients
CSCvc94524	Cisco 2800, 3800 APs iphone and android phones are not getting IPv6 addresses
CSCvc94648	Evaluation of WLC for OpenSSL Jan 2017
CSCvc95222	Cisco 1810w AP LAN port dropping IPTV packets when wired device is 100M
CSCvc98310	AP 1830: 2.4-GHz radio stopped working @0x009915D7
CSCvd00067	Wired WGB client is removed from parent AP's association table
CSCvd00289	Cisco 2800, 3800 APs CAPWAPd init unsuccessful creating 2 CAPWAPd causing WCPD watchdogd reset
CSCvd01586	Cisco WLC reloads unexpectedly on task name: RRM-DCLNT-2_4 | rrmClientCoverageHoleAlgorithm
CSCvd06463	AMSDU packets Tx cause 5sec gap of packet Tx to Cisco Wireless IP Phone 8821 from IOS AP
CSCvd06848	WLC stopped working on SNMPTask
CSCvd06993	Upgrade to 8.3 requires to reconfigure DNS server IP
CSCvd07215	AP1810/2800 doesn't learn DHCP lease time from DHCP server and defaults to 24hr.
CSCvd07423	AP firmware corrupt after power cycle bad mzip file, unknown zip method reboot loop
CSCvd09240	Local-auth EAP-TLS win10 not working
CSCvd10363	Config uploads and downloads are not allowed in Cisco Mobility Express after flash error message
CSCvd12057	Flex AVC : Downstream QoS marking not working - 8.3
CSCvd14806	APs randomly not showing any neighbors on both radios

Caveat ID Number	Description
CSCvd15394	3800 AP will reject login for login credentials with childer ~ in password
CSCvd15404	Rule creation with CLRuleConfigEntry stops the controller from working
CSCvd15742	Cisco AP reloads unexpectedly with %ENTROPY-0-ENTROPY_ERROR: Unable to collect sufficient entropy
CSCvd18025	Anchor1 WLC does not free client sessions after client roaming to Anchor2 WLC-client entries stale
CSCvd18535	ROKH id inconsistent for 802.11r roaming in Flex - NAT setup
CSCvd18732	Cisco 1810 AP radio firmware assert @0x0099B2DA in overnight multi-client test
CSCvd18773	8.2 clients unable to authenticate for extra 3 seconds post 1 sec cleanup timeout
CSCvd19354	Cisco WLC reloads unexpectedly while editing config rf-profile hsr-mode disable | enable config rf-profile 11b
CSCvd20251	DP stopped working on Cisco 5508 WLC running 8.0.140.0 release
CSCvd20271	AP 3800 stopped working in Monitor mode with wIPS submode
CSCvd20843	Beacon stuck due to off-channel stuck
CSCvd21051	AP3800: Kernel crash at wlTxDone+0x190/0x688 [ap8x]
CSCvd21155	WLC stopped working when multicasting traffic and accessing WLC GUI
CSCvd21969	AAA AVC Override - AVC profile retained after roaming
CSCvd24540	SNMP System stopped working when tried to create tunnel with clGatewayTunnelEntry MiB
CSCvd25231	Collect stack info for silent reboot of 2800/3800 APs
CSCvd27065	EAP-FAST EAP-Chaining on wired Cisco 1810WAP port does not work
CSCvd27285	ME_1852E : CCO image download re-initiated on the APs on which the download was already completed
CSCvd27398	WLC management access stops working while WLAN services are still up
CSCvd28645	Cisco AP sending RTS at 6 data rate when data rate 6 is disabled
CSCvd29564	Layer 2 Packet Drop Of CDP Packets for COS APs
CSCvd30952	RM3010L-B-K9 Hyperlocation Module stopped working
CSCvd32632	Standby Controller stopped working @rmgrReboot

Caveat ID Number	Description
CSCvd33140	Constant increase in WLC Memory reaching 90% and above
CSCvd33219	AP 3800: FW hang detected - chatter: wl1: fwHangDetect(357): FTR!
CSCvd35231	AP1810W: Reload Reason: 0: Unknown aka Silent Reboot
CSCvd35988	8.5 5520WLC-HA causing DENY rule on WLC and Telnet&Gui access down
CSCvd36259	ME Controller intermittently Flaps with external AP.
CSCvd36736	AP in local sw/local auth disconnect EAP-SIM client idle for more than 0.5 second
CSCvd37808	Cisco 8510 WLC stopped working - iappSocketTask
CSCvd37960	Clients getting re-anchored if critical application is present on client
CSCvd39346	Cisco 2800, 3800 APs WCPD slow memory leak
CSCvd40646	AP2802 - Kernel Panic - Dot11Classifier: Mgmt frame not supported 0
CSCvd42348	Standby WLC stopped working on performing SNMP Set on bsnDot11QosProfileEntry
CSCvd44446	Retried EAP Response Dropped as a duplicate while First EAP Response was not even received on the AP
CSCvd46216	AP1832/AP1852 sometimes does not send authentication response
CSCvd48333	Controller stopped working : emWeb
CSCvd49909	Kernel panic @ ClientCapabilitiesTracker virtual address invalid band select
CSCvd50044	System stopped working multiple times on ping Rx task
CSCvd51674	AP1810W: Silent reboot : revert highest power table value
CSCvd53205	DCA lists in RF profiles are broken after backup/restore the WLC's config
CSCvd53765	After restarting WLC NMSP goes down on CMX
CSCvd54154	All AP1850 connected to master AP reloads unexpectedly in a loop due to watchdog reset
CSCvd56064	Flex local switching, local auth not supported when PMF is enabled in 8.3.114.22
CSCvd56422	Error cause 403 generated for 'RFC-3576 Disconnect-Request'
CSCvd56581	Client not getting IP address when moving between SSID
CSCvd56671	802.11r FT roaming across WLCs: WLC reloads unexpectedly in 'apfMsConnTask_0' in 8.3 MR2

Caveat ID Number	Description
CSCvd58113	Cisco WLC allowing telnet and SSH over IPv6 on global telnet and SSH disabled
CSCvd58664	AP dropping EAP packets on Radio which is seen on wired uplink
CSCvd61701	SSH to Standby RMI or Service port Fails
CSCvd61747	AP3800: Radio reloads unexpectedly due to off channel stuck due to defer_chchange_flag always set to TRUE
CSCvd61977	2800/3800 APs-radio coredump generation may stuck ca_status leading to IPC call function failures
CSCvd63242	Click AP not associating with 802.11r client in CiFlexConnect mode
CSCvd66657	AP 3802: SensorD stuck in offchannel causing radio stops working
CSCvd67178	Anchor not deleting webauth req client beyond webauth timeout
CSCvd69782	Roaming L3 test was failed with 50% in Talwar and Pata WLC
CSCvd69992	AP: 2800/3800 unable send proper sequence# and burst rate upstream
CSCvd70755	AIR-AP3802I reloads unexpectedly due to kernel panic
CSCvd72432	LocalEAP LDAP request With incorrect password lockout users
CSCvd72664	Mobility Express AP sometimes tags 802.1q VLAN for native WLAN, causing ARP packet drop
CSCvd74063	AP1832 reloads unexpectedly due to watchdog reset(wcpd no heartbeat)
CSCvd77037	AP1832 sending instant ACK after CTS that block data from client
CSCvd79597	Smart License 5520/8540 WLC : Unable to reset HTTP-Proxy on Call home configuration from GUI
CSCvd80962	LWAPP-3-AP_LOCK_ERR traceback observed on WLC for Cisco 2800, 3800 APs
CSCvd81303	Cisco 2800, 3800 APs: Limit 'best' DCA to 80 MHz also for RF profiles
CSCvd81926	CCX Proxy arp flag not set in IOS APs
CSCvd83741	AP: 1850 unable send proper sequence# and burst rate upstream from AP to MSE
CSCvd85995	AP3800: AP deauth client after roaming and does not send deauth when client sends QoS null
CSCvd86274	Cisco 1800/2800/3800 Series AP does not send the Platform value via CDP when it is brand new
CSCvd87065	Cisco WLC reloads unexpectedly due to task nmspTxServerTask
CSCvd88630	Cisco 3800 AP reloads unexpectedly due to 'WCPD' in 8.4 release

Caveat ID Number	Description
CSCvd90117	AP3800 - Radio unexpectedly reloads frequently due to beacon stuck
CSCvd90669	Need support for AAA override with MAC filtering on RLAN
CSCvd90707	Command mismatch traceback observed on 2.4 GHz radio
CSCvd91770	Trust-DSCP-Upstream broken on 8.2.151.0 release
CSCvd91894	Cisco 3800/2800 APs kernel panic unexpectedl reload on PC is at mv_dev_kfree_skb+0xc/0xa4 [ap8x]
CSCvd97103	IPv4 CPU ACL - IP-Address with netmask other than 255.255.255.255 does not work
CSCvd98548	Kernel panic inside ForwardFrame function!
CSCvd99909	Cisco 3800 AP- 5-GHz radio reloads unexpectedly - when SI enabled
CSCve00464	AP1852 detects high noise level on 5-GHz radio for every channel except the serving one
CSCve01109	SXP connection on WLC stays off
CSCve01552	Unknown Username when switching from open to 802.1x SSID
CSCve01859	With FIPS enabled on 5520WLC, 3802AP shows no 5-GHz neighbors
CSCve06701	Client stuck in DHCP_REQD on flex AP after changing native VLAN
CSCve07524	In GUI 802.11ac configuration behavior mismatch with CLI for different AP mode
CSCve10751	Clients cannot assocate with AP after changing from DFS to non-DFS channels during CAC, QCA 02910240
CSCve13183	Cisco 2800, 3800, 1800 APs WCPD reloads unexpectedly due to double-free in RRM Off-channel element
CSCve14081	AireOS: Same channel has been assigned to both the 5-GHz Radios after CAPWAP restart
CSCve14710	ME_3800 : Observed an EMWEB device unexpected reload
CSCve17355	Upgrade to Cisco WLC - 8.3 software enables 802.11k and 802.11v by default on all WLANs
CSCve21379	During Auto Provisioning feature, RADIUS server templates are getting applied but staying disabled.
CSCve23737	AP 3800: FIQ/NMI reloads unexpectedly with FIQ stack corruption for CPU1 and showing all zero
CSCve23874	Cisco 2800, 3800 APs:Client associates even if CAC timer start on AP log, when DFS channel is set
CSCve24313	ME internal AP loses timezone (in ssh) after reboot

Caveat ID Number	Description
CSCve26592	Cisco ME running 8.2.151.0 Master/Internal AP not able to join Controller
CSCve27955	Config upload failing due to WLANs having special or invalid characters
CSCve30199	CCKM PMK (Version 2) message flooding 8.3.x release
CSCve30922	Cisco 8540 WLC modifies IP Header 'Router Alert' to 'End of Option List' when IGMP snooping enabled
CSCve34143	WLAN-VLAN mapping not working sometime when AP is removed and added back in flex group
CSCve77722	WLAN in FlexConnect local switching drops NAC+802.1X and WPA2-PSK-WebAuth traffic on MAC filter fail
CSCvf31894	Backout changes - CSCvc78546 that leads to CSCve20123

Cisco Mobility Express Solution Release Notes

Overview

Note The Cisco Mobility Express wireless network solution is available starting from Cisco Wireless Release 8.1.122.0.

The Cisco Mobility Express wireless network solution provides a wireless controller functionality bundled into the Cisco Aironet 1560, 1815, 1830, 1850, 2800, and 3800 Series access points.

In the Cisco Mobility Express wireless network solution, one AP, which runs the Cisco Mobility Express wireless controller, is designated as the Master AP. Other access points, referred to as Subordinate APs, associate to this Master AP.

The Master AP operates as a wireless controller, to manage and control the subordinate APs. It also operates as an AP to serve clients. The subordinate APs behave as normal lightweight APs to serve clients.

For more information about the solution, including the setup and configuration, see the *Cisco Mobility Express User Guide for Release 8.3*, at http://www.cisco.com/c/en/us/td/docs/wireless/access_point/mob_exp/83/user_guide/b_ME_User_Guide_83.html

Supported Cisco Aironet Access Points

APs Supported as Master (Support Integrated Wireless Controller Capability)	APs Supported as Subordinate
Cisco Aironet 1560 Series Cisco Aironet 1830 Series Cisco Aironet 1850 Series Cisco Aironet 2800 Series Cisco Aironet 3800 Series	In addition to the following, all the APs that are supported as Master APs are also supported as subordinate APs: Cisco Aironet 700i Series Cisco Aironet 700w Series Cisco Aironet 1600 Series Cisco Aironet 1700 Series Cisco Aironet 1810W Series Cisco Aironet 2600 Series Cisco Aironet 2700 Series Cisco Aironet 3500 Series Cisco Aironet 3600 Series Cisco Aironet 3700 Series

Cisco Mobility Express Features

The following new features and functionalities have been introduced in this release:

- Support for the following access points:
  - Cisco Aironet 1560 Series
  - Cisco Aironet 2800 Series
  - Cisco Aironet 3800 Series
- Simple Network Management Protocol (SNMP) Version 3 polling; configurable through the GUI.
- Support for the Flexible Radio Assignment (FRA) functionality for the radio in slot 0 on Cisco Aironet 3800 Series access points. FRA automatically detects when a high number of devices are connected to a network, and changes the dual radios in an access point from 2.4GHz/5GHz to 5GHz/5GHz to serve more clients.
- Improvements in software update and access point image management with direct download from Cisco.com.
- Integration with Cisco CMX Cloud for both guest services and presence analytics. This is enabled by the integrated cloud connector on the Cisco Mobility Express controller for seamless integration and easier provisioning.
- Localization to Japanese and Korean for the Cisco Mobility Express controller GUI.
- Setting up and managing an internal DHCP server through the GUI.
- Importing a customized guest login page.

- Forced failover to a specified AP as master.

The following are existing features, with continued support in the current release:

Note Even if the Cisco AP is 802.3ad (LACP)-compliant, link aggregation groups (LAG) are not supported on the AP while it has a Cisco Mobility Express software image.

- Scalability:
  - Up to 25 APs
  - Up to 16 WLANs
  - Up to 100 rogue APs
  - Up to 1000 rogue clients
- License—Does not require any licenses (Cisco Right-To-Use License or Swift) for APs.
- Operation— The Master AP can concurrently function as controller (to manage APs) and as an AP (to serve clients).
- GUI and CLI-based initial configuration wizards.
- Up to three Network Time Protocol (NTP) servers, with support for FQDN names.
- Simple Network Management Protocol (SNMP) Version 3 polling, configurable through the CLI.
- IEEE 802.11r with support for Over-the-Air Fast BSS transition method, Over-the-DS Fast BSS transition method, and Fast Transition PSK authentication. Fast BSS transition methods are supported via CLI only.
- CCKM, supported via CLI only.
- Client ping test
- Changing the country code on the controller and APs on the network, via the controller GUI.
- Syslog messaging towards external server.
- Software image download using TFTP and HTTP.
- Priming at distribution site.
- Default Service Set Identifier (SSID), set from factory. Available for initial provisioning only.
- Management through the web interface Monitoring Dashboard.
- Cisco Wireless Controller Best Practices.
- Quality of Service (QoS).
- Multicast with default settings.
- Application Visibility and Control (AVC)—Limited HTTP, with only Application Visibility and not Control. Deep Packet inspection with 1,500+ signatures.
- WLAN access control lists (ACLs).

- Roaming—Layer 2 roaming without mobility groups.
- IPv6—For client bridging only.
- High Density Experience (HDX)—Supported when managing APs that support HDX.
- Radio Resource Management (RRM)—Supported within AP group only.
- WPA2 Security.
- WLAN-VLAN mapping.
- Guest WLAN login with Web Authorization.
- Local EAP Authentication (local RADIUS server).
- Local profile.
- Network Time Protocol (NTP) Server.
- Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP).
- Clean Air.
- Simple Network Management Protocol—SNMPv1, by default, and SNMPv2c.
- Management—SSH, Telnet, Admin users.
- Reset to factory defaults.
- Serviceability—Core file and core options, Logging and syslog.
- Cisco Prime Infrastructure.
- BYOD—Onboarding only.
- UX regulatory domain.
- Authentication, Authorization, Accounting (AAA) Override.
- IEEE 802.11k
- IEEE 802.11r
- Supported—Over-the-Air Fast BSS transition method
- Not Supported—Over-the-DS Fast BSS transition and Fast Transition PSK authentication
- Passive Client
- Voice with Call Admission Control (CAC), with Traffic Specification (TSpec)
- Fast SSID Changing
- Terminal Access Controller Access Control System (TACACS)
- Management over wireless
- High Availability and Redundancy—Built-in redundancy mechanism to self-select a Master AP and to select a new AP as Master in case of a failure. Supported using VRRP.
- Software upgrade with preimage download

- Migration to controller-based deployment.

Compatibility with Other Cisco Wireless Solutions

See the Cisco Wireless Solutions Software Compatibility Matrix, at: http://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html

Software Release Information

The following table lists the Cisco Mobility Express software for Cisco Wireless 8.3.133.0.

Access Points Supported As Master	Software to be Used only for Conversion from Unified Wireless Network Lightweight AP Software To Cisco Mobility Express Software	AP Software Image Bundle, to be Used for Software Update, or Supported Access Point Images, or Both
1560	AIR-AP1560-K9-8-3-130-0.tar	AIR-AP1560-K9-ME-8-3-130-0.zip
1830	AIR-AP1830-K9-8-3-130-0.tar	AIR-AP1830-K9-ME-8-3-130-0.zip
1850	AIR-AP1850-K9-8-3-130-0.tar	AIR-AP1850-K9-ME-8-3-130-0.zip
2800	AIR-AP2800-K9-8-3-130-0.tar	AIR-AP2800-K9-ME-8-3-130-0.zip
3800	AIR-AP3800-K9-8-3-130-0.tar	AIR-AP3800-K9-ME-8-3-130-0.zip

Installing Mobility Express Software

See the "Getting Started" section in the *Mobility Express User Guide* at http://www.cisco.com/c/en/us/td/docs/wireless/access_point/mob_exp/83/user_guide/b_ME_User_Guide_83.html

Caveats

The open caveats applicable to the Cisco Mobility Express solution are listed under the Open Caveats section. All caveats associated with the Cisco Mobility Express solution have *Cisco Mobility Express* specified in the headline.

Related Documentation

Wireless Products Comparison

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

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

- Product Approval Status:

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

- Wireless LAN Compliance Lookup:

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

Cisco Wireless Controller

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

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

For all Cisco WLC software related documentation, see:

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

Cisco Mobility Express

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

Cisco Aironet Access Points for Cisco IOS Releases

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

Open Source Used in Controller and Access Point Software

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

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

Cisco Prime Infrastructure

Cisco Prime Infrastructure Documentation

Cisco Mobility Services Engine

Cisco Mobility Services Engine Documentation

Cisco Connected Mobile Experiences

Cisco Connected Mobile Experiences Documentation