Release Notes for Cisco Wireless Controllers and Lightweight Access Points for Cisco Wireless Release 8.3.102.0

First Published: July 31, 2016

This release notes document describes what is new in Cisco Wireless Release 8.3.102.0, 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 *Cisco WLCs*, and Cisco lightweight access points are referred to as *access points* or *Cisco APs*.

Note For Cisco wireless solution software compatibility information, see the *Cisco Wireless Solutions Software Compatibility Matrix* at http://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html.

Note For information specific to the Cisco Mobility Express solution, see the "Cisco Mobility Express Solution Release Notes" section on page 45.

Cisco Systems, Inc.
www.cisco.com

Revision History

Table 1 Revision History

Modification Date	Modification Details
August 23, 2018	• Open Caveats, page 36 – Added: CSCvk44249
January 29, 2018	• Key Features Not Supported on Cisco Virtual WLCs, page 31 – Modified information about FlexConnect central switching.
October 16, 2017	• Key Features Not Supported on Cisco Aironet 1810 OEAP, 1810W, 1830, 1850, 2800, and 3800 Series APs, page 33 – Added SIP snooping with FlexConnect in local switching mode
October 10, 2017	• Key Features Not Supported on Cisco Virtual WLCs, page 31 – Added Wired Guest and FlexConnect central switching.
May 26, 2017	• What's New in this Release, page 5 – Added information that GLC-TE is supported in Cisco 5508 WLCs.
May 16, 2017	• Important Note on Interoperability Issue Between Release 8.3, SpectraLink Phones, and Other Third-Party Clients, page 15 – Updated this section by adding procedures to disable 802.11k and 802.11v features. • Key Features Not Supported on Cisco Aironet 1810 OEAP, 1810W, 1830, 1850, 2800, and 3800 Series APs, page 33 – Removed Proxy ARP from the list of unsupported FlexConnect features • Guidelines and Limitations, page 16 – Added a restriction recommending that < or > special character should not be present in the backed up configuration file; else the download of the configuration file fails.
March 22, 2017	• Key Features Not Supported on Cisco Flex 7510 WLCs, page 30 – Removed Cisco TrustSec SXP
February 13, 2017	• Open Caveats – Added: CSCvd06463
January 11, 2017	• Key Features Not Supported on Cisco Aironet 1810 OEAP and 1810W Series APs, page 34 – Added: Local AP Authentication under FlexConnect Features • Key Features Not Supported on Cisco Aironet 1830 and 1850 Series APs, page 34 – Added: Local AP Authentication under FlexConnect Features
December 5, 2016	• Added information about change in WLAN-AP group association functionality to the "Upgrading to Cisco WLC Software Release 8.3.102.0" section on page 16

Table 1 Revision History

Modification Date	Modification Details
November 22, 2016	• Key Features Not Supported on Cisco 2504 WLC, page 29 – Added: EoGRE • Key Features Not Supported on Cisco Virtual WLCs, page 31 – Added: EoGRE (Supported in only local switching mode)
October 13, 2016	• Key Features Not Supported on Cisco Aironet 1810 OEAP, 1810W, 1830, 1850, 2800, and 3800 Series APs, page 33 – Added: Telnet
September 30, 2016	• Moved CSCuz45296 and CSCuz79869 to Open Caveats list.
September 27, 2016	• Cisco CMX Cloud Connector, page 9 – Added: Note to state TCP/TLS connection limitation
September 22, 2016	• Key Features Not Supported on Cisco Aironet 1810 OEAP, 1810W, 1830, 1850, 2800, and 3800 Series APs, page 33 – Removed: Enhanced Local Mode (ELM)
September 20, 2016	• Important Note on Interoperability Issue Between Release 8.3, SpectraLink Phones, and Other Third-Party Clients, page 15 – Updated support information for this section.
September 13, 2016	• Key Features Not Supported on Cisco WLC Platforms, page 29 – Added Not Supported Feature list on Cisco WLC platforms • Key Features Not Supported on Cisco Access Point Platforms, page 32 – Added Not Supported Features list on Cisco APs platforms

Cisco Wireless Controller and Cisco Lightweight Access Point Platforms

The section contains the following subsections:

Supported Cisco Wireless Controller Platforms

The following Cisco WLC 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 Cisco Lightweight 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 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 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 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 8.3.102.0, 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 features that are not supported on some access point platforms, see the "Key Features Not Supported on Cisco Access Point Platforms" section on page 32.

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 the *Cisco Wireless Solutions Software Compatibility Matrix* document.

What's New in this Release

Note For information specific to the Cisco Mobility Express solution, see "Cisco Mobility Express Solution Release Notes" section on page 45.

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 8.3.102.0 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 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 8.3.102.0 for the applicable Cisco WLC platforms.

Table 2 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-K9-8-3-102-0.aes	AIR-CT2500-AP_BUNDLE-K9-8-3-102-0.aes
Cisco 5508 WLC	AIR-CT5500-K9-8-3-102-0.aes	AIR-CT5500-AP_BUNDLE-K9-8-3-102-0.aes
	AIR-CT5500-LDPE-K9-8-3-102-0.aes	AIR-CT5500-LDPE-AP_BUNDLE-K9-8-3-102-0.aes
Cisco WiSM2	AIR-WISM2-K9-8-3-102-0.aes	AIR-WISM2-AP_BUNDLE-K9-8-3-102-0.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.

Important Restrictions

- If you do not reboot the Cisco WLC in between installing the Base Install image and the Supplementary AP Bundle image, the active image pointer does not point to the backup image. Therefore, any new Cisco AP that associates with the Cisco WLC prior to a reboot and requests for an image download, does not get the image. The workaround is to reboot the Cisco WLC.
- After you upgrade to Release 8.3.102.0, any upgrade or downgrade that you perform thereafter, results in the backup image getting deleted before starting the upgrade or downgrade process.
- If one of the images in Cisco WLC is Release 8.3.102.0, and the current active image is Release 8.2 or an earlier release, it is not possible to upgrade to another release of the Release 8.3.102.0 train while the non-Release 8.3.102.0 image is still running. You must ensure that the Release 8.3.102.0 image is the active image to perform another upgrade.

High-Level Upgrade Procedure

Follow these high-level steps to upgrade from Release 8.2 or an earlier release to Release 8.3.102.0:

Step 1 Install the Base Install image of Release 8.3.102.0, for example, *AIR-CT5500-K9-8-3-102-0.aes*.

Step 2 (Optional) Install the Supplementary AP Bundle image of Release 8.3, for example, *AIR-CT5500-AP_BUNDLE-K9-8-3-102-0.aes*.

Install the Supplementary AP Bundle image only if you are using the following APs:

- AP802
- Cisco Aironet 1550 Series AP (with 64-MB memory)
- Cisco Aironet 1550 Series AP (with 128-MB memory)
- Cisco Aironet 1570 Series APs

For detailed instructions on installing the Base Install image and the Supplementary AP Bundle image, see the "Upgrading to Cisco WLC Software Release 8.3.102.0 (GUI)" section on page 23.

Step 3 Predownload AP images.

For detailed instructions on predownloading AP images, see the *Predownloading an Image to an Access Point* section in the *Cisco Wireless Controller Configuration Guide*.

Step 4 Reboot the Cisco WLC.

Note There is no change in the downgrade procedure.

Access Point Provisioning Using Plug-n-Play

Plug and play (PnP) to configure Cisco APs using Cisco Application Policy Infrastructure Controller (APIC) Enterprise Module (Cisco APIC-EM) is supported on the following Cisco APs in FlexConnect mode and Local mode:

- Cisco Aironet 702i AP
- Cisco Aironet 702W Series AP
- Cisco Aironet 1600 Series AP
- Cisco Aironet 2600 Series AP
- Cisco Aironet 3600 Series AP
- Cisco Aironet 1700 Series AP
- Cisco Aironet 2700 Series AP
- Cisco Aironet 3700 Series AP
- Cisco Aironet 1800 Series AP
- Cisco Aironet 2800 Series AP
- Cisco Aironet 3800 Series AP

This feature helps you to provision in advance, the AP details from a central service (APIC-EM) and eases the steps that are to be performed by a local installer.

Optimized Wi-Fi Connectivity and Prioritized Business Applications in Cisco and Apple Environments

At the center of Apple and Cisco collaboration is a unique handshake between Cisco WLAN and iOS 10 beta Apple devices. This handshake enables Cisco WLAN to provide an optimal Wi-Fi roaming experience to Apple devices. Additionally, Cisco WLAN trusts Apple devices and gives priority treatment for business-critical applications specified by the Apple device.

This feature is supported on all Cisco WLC platforms.

For more information, see the following sections in the *Cisco Wireless Controller Configuration Guide*:

- Configuring FastLane QoS
- Configuring 802.11r Fast Transition
- Configuring 802.11v BSS Transition Support
- Configuring Assisted Roaming
- Configuring EDCA Parameters

Benefits

The Apple and Cisco collaboration positively impacts Apple device users and IT administrators:

- Higher reliability for real-time applications—66 times decrease in probability of poor audio quality experience
- Improved quality of experience—10 times more successful web browsing experience
- Enhanced network performance—86 percent reduction in network message load from the device during roaming
- Ease of management—Up to 50 percent reduction in network overhead due to SSIDs

Unsupported Platforms

The following Cisco APs do not support this feature:

- Cisco Aironet 1810 Series OEAPs
- Cisco Aironet 1810W Series APs
- Cisco Aironet 1830 Series APs
- Cisco Aironet 1850 Series APs
- Cisco Aironet 2800 Series APs
- Cisco Aironet 3800 Series APs

Cisco CMX Cloud Connector

Cisco CMX Cloud Connector provides the ability to send NMSP data seamlessly and securely from Cisco WLC to Cisco CMX Cloud over HTTPS. This enables the delivery of Wi-Fi location-based services including Analytics, from cloud without the need to install and manage Cisco CMX Cloud proxy on the premises. For more information about Cisco CMX Cloud, go to http://support.cmxcisco.com/.

Note To avoid duplication of data, the maximum number of NMSP connections on the Cisco WLC are limited to three connections. There are a maximum of two incoming TCP/TLS connections from MSE and CMX to WLC, and one outgoing HTTPs connection to CMX Cloud.

For more information, see the CMX Cloud Connector section in the *Cisco Wireless Controller Configuration Guide*.

Client Troubleshooting Tool

The Client Troubleshooting tool on Cisco WLC helps a network administrator to troubleshoot clients and get insights into client behavior in real time. This is an on-demand tool that provides features such as packet captures, ping test, connection analysis, and event log.

URL Filtering for Domains

Domain Filtering allows network administrators to define HTTP URL-based Access Control Lists (ACL) in order to allow or disallow traffic.

The URL Filtering feature helps optimize network bandwidth utilization by restricting access to websites. This feature gives you control to build URL ACLs using which you can either permit or deny access to websites. These ACLs can be applied to locations, AP groups, WLAN profiles, and trusted and non-trusted clients within the same SSID.

For information, see the Configuring URL Filtering section in the *Cisco Wireless Controller Configuration Guide*.

Default FlexConnect Group

Default FlexConnect Group is a container where FlexConnect APs, which are not part of an administrator-configured FlexConnect group, are added automatically when they associate with Cisco WLC. It is not possible to manually add or delete the default FlexConnect group. It is also not possible to manually add or delete APs to the default FlexConnect group.

For more information, see the Default FlexGroup section in the *Cisco Wireless Controller Configuration Guide*.

IPv6 Support for EoGRE Tunnels

Support is added for client IPv6 traffic and IPv6 address format for the EoGRE tunnel gateway. Client IPv6 traffic is supported on both IPv4 and IPv6 EoGRE tunnels. A maximum of eight different client IPv6 addresses are supported. Cisco WLCs send all the client IPv6 addresses that they have learned to the Accounting server in the accounting update message. All RADIUS or Accounting messages that are exchanged between Cisco WLCs and tunnel gateways or RADIUS servers are outside the EoGRE tunnel.

Note IPv6 is not supported on the FlexConnect-to-WAG EoGRE tunnel.

For more information, see the Ethernet over GRE Tunnels section in the *Cisco Wireless Controller Configuration Guide.*

Mesh Off-Channel Background Scanning

Mesh APs will periodically go off channel and scan all the channels to update neighbor lists.

Support is added for permanent off-channel background scanning for mesh APs (MAPs) when fast or very fast convergence is configured, to take advantage of the presence of neighboring MAPs that have been heard outside the Subset Channel list.

Support for NBAR2 Protocol Pack 19.1.0

Support is added for NBAR2 Protocol Pack 19.1.0 for Cisco WLCs, which will be the default protocol pack PP for Release 8.3. The AP protocol pack is upgraded to NBAR2 Protocol Pack 14.

For more information, see *Release Notes for NBAR2 Protocol Pack 19.1.0 for Cisco Wireless Controllers*.

OfficeExtend Support for Wave 2 802.11ac Access Points

OfficeExtend mode allows remote AP to connect to home or remote site broadband Internet access and establish a secure tunnel to the corporate network. This enables remote employees to access data, voice, video, and cloud services for a mobility experience that is consistent with the experience in a corporate office.

Enabling RADIUS NAC on a WPA and WPA2-PSK WLAN

It is possible to enable both RADIUS NAC and WPA/WPA2-PSK on a WLAN. Prior to Release 8.3, it was not possible to enable both of these configurations on the same WLAN.

Use Case

To have web redirect with PSK on Cisco WLCs for device onboarding. For example, onboard devices using an SSID with a PSK, send the MAC address to Cisco ISE using central web authentication (CWA), and determine if it is registered.

For more information, see the Enabling RADIUS NAC on a WPA and WPA2-PSK WLAN section in the *Cisco Wireless Controller Configuration Guide.*

Link Layer Discovery Protocol in Recovery Image

Link Layer Discovery Protocol (LLDP) is added to the recovery image of Cisco IOS APs. LLDP is a vendor-neutral data-link-layer protocol, used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 LAN, mainly wired Ethernet. As protocol runs over the data-link layer, it allows two systems running different network layer protocols to learn about each other. Therefore, the protocol allows interoperability between Cisco devices and non-Cisco devices.

EoGRE Enhancements

It is now possible to assign EoGRE tunnel profiles to WLANs configured for Internal WebAuth and WPA2-PSK. WLANs configured with WPA2-PSK/WPA2-802.1X and Internal WebAuth are also supported. Prior to Release 8.3.102.0, only WLANs configured for Open and WPA2-802.1X were supported.

Workgroup Bridge (WGB) Downstream Broadcast On Multiple VLANs

Cisco Wireless Release 8.3 provides an enhancement to broadcast traffic support on multiple 802.1Q VLAN workgroup bridge (WGB) deployments that traverse mesh networks and in Local mode; specifically, support for WGB downstream broadcasts over multiple VLANs (to differentiate and prioritize traffic); and, bridging of VLAN traffic to wired clients connected to the WGB. Applications for this functionality are commonly found in the transportation and mining industries. For more information, see CSCub87583.

Supported Platforms

- Access point (AP) and WGB support:
  - IW3700 Series
  - 1552H/SA/SD/WU Series
- Cisco WLC support (systems that support central-switching traffic forwarding):
  - Cisco 2504 WLC
  - Cisco 5508 WLC
  - Cisco WiSM2

For more information, see the Workgroup Bridge (WGB) Downstream Broadcast On Multiple VLANs section in the *Cisco Wireless Controller Configuration Guide*.

Support for –M Regulatory Domain on Cisco Industrial Wireless 3700 Series APs

The –M Regulatory Domain is supported on Cisco Industrial Wireless 3700 Series APs in the following countries:

- Qatar
- Saudi Arabia
- Kuwait

Security Enhancements

- Search results for rogue devices can now be filtered by their MAC address. The filter is available on all the pages under the Rogues section in the Cisco WLC GUI.
- Cisco WLC can itself generate 2048-bit RSA key CSR certificates. This signed certificate can be downloaded and used with the RSA key pair generated by the Cisco WLC.
- SNMP over IPSec and SNMP traps over IPSec are supported over IPv6 interfaces.
- New attributes are added to AAA callStationIdType for Lawful Intercept:
  - **config radius callStationIdType ap-mac-ssid-ap-group**

    Sets the Called Station ID type in the format <*AP MAC address*>:<*SSID*>:<*AP Group*> sent in the RADIUS Accounting messages
  - **config radius auth callStationIdType ap-mac-ssid-ap-group**

    Sets the Called Station ID type in the format <*AP MAC address*>:<*SSID*>:<*AP Group*> sent in the RADIUS Authentication messages.

Cisco Hyperlocation Enhancements

Cisco Hyperlocation Module software has been updated to enhance High Availability and the new –B domain for AP3702-B, along with new code updates:

- Hyperlocation updates do not stop and you do not have to reconfigure Hyperlocation should a Cisco WLC fail switchover occur.
- Higher simultaneous AoA client processing, more location accuracy, more stability.

Cisco TrustSec Capabilities with FlexConnect

Cisco Wireless Release 8.3 extends the capability to simplify access control management using Cisco TrustSec Security Groups to users connected to FlexConnect APs.

Users connected to FlexConnect APs can now be classified with a Security Group Tag (SGT) to simplify policy management. Cisco WLCs can now share Security Group membership information over an SGT eXchange Protocol (SXP) connection with switches, routers, and firewalls to simplify access control list management and firewall rule management elsewhere in the network.

To use this capability, Cisco Identity Services Engine would be required to authorize devices based on attributes such as the role of the user and/or device and assign a Security Group Tag as part of an authorization rule.

Other devices receiving SGT information over SXP can then apply Security Group Access Control Lists and group-based firewall rules, which are more flexible and much easier to manage than using IP address-based controls.

The feature complements existing support for Security Group-based policies for centrally switched user traffic in the earlier Cisco Wireless releases.

Cisco WLC GUI Enhancements

Information Related to Cisco Aironet 2800 Series and 3800 Series APs

Cisco 2800 AP and 3800 AP support the XOR radio slot where the Wi-Fi radio can be switched between 2.4 GHz and 5 GHz and vice versa:

- Network Summary page shows both 2.4 GHz and 5 GHz in slot 0, including information about Active Clients, Rogues, and Interferers.
- AP Detail Performance Summary and RF Troubleshooting reflect both 2.4-GHz data and 5-GHz data for slot 0.
- AP Table view is consistent in 2.4-GHz and 5-GHz tabs.
- Client tabular and detailed views reflect proper operating role of XOR radio
- AP Wireless Dashboard is consistent if operating in 2.4 GHz and 5 GHz or 2 x 5 GHz.

Cisco Aironet 2800 Series and 3800 Series APs Support Channel Width of 160 MHz

- AP Table, AP Detail, and AP Performance reflect the 160-MHz channel width
- Client Table and Client Detail reflect the 160-MHz channel width

mGig Interface Support

- Updated field formatting-<*switch*>, <*port-type*><*port*>
- mGig interface is supported on the Cisco 3800 AP:
  - Port type shows as GigabitEthernet when a Cisco 3800 AP is connected to a legacy Gigabit port
  - Port type shows as TenGigabitEthernet when a Cisco 3800 AP is connected to an mGig port

Event Log

- Raw log events are captured for the client
- You can save the event logs and examine them offline

Client Troubleshooting

- Involves troubleshooting of issues around connectivity, IP, and so on. For more information about client troubleshooting enhancements, see the "Cisco Mobility Express Solution Release Notes" section on page 45.

AP Distribution

- Data in both chart and tabular formats are available and shows the number of APs belonging to each of the PIDs in the network in the Wireless Dashboard view in both 2.4 GHz and 5 GHz.
- Data in both chart and tabular formats are available, and shows the AP count for 2.4 GHz and 5 GHz based on the spatial streams supported by the APs.

Wireless Dashboard

Data based on the 2.4-GHz bands and 5-GHz bands related to an AP and a client is available in pie-chart format.

Miscellaneous

- Top WLANs are displayed on the Network Summary page.
- Color coding is available in the AP Performance summary.
- APs are accessible from the Client view.
- CDP/LLDP neighbor host name is displayed in the AP Detailed view.
- It is possible to clear or reset the Client Failure Reason data on the Client Performance page so that only the new failures are captured from that point of time.

Important Note on Interoperability Issue Between Release 8.3, SpectraLink Phones, and Other Third-Party Clients

After you upgrade to Cisco Wireless Release 8.3.102.0, the 802.11k and 802.11v protocols are enabled by default on all existing WLANs, and new WLANs that you may create, because of improved feature support on Apple iOS 10. Because of these new features, third-party clients such as scanners may have issues connecting to WLAN. This could be due to some of the client types not ignoring the new information element and thereby failing to connect. As per the IEEE standards, if a client does not understand any new information element, it should ignore and still be able to connect. A better solution for this would be to work with client vendor.

The workaround, in Cisco WLC, is to disable these features on the WLAN.

Disabling 802.11k and 802.11v on Cisco WLC (GUI)

Step 1 Choose **WLANs** > WLAN ID.

Step 2 On the **WLANs > Edit** page, click the **Advanced** tab.

Step 3 In the **11k** section, uncheck all the check boxes.

Step 4 In the **11v BSS Transition Support** section, uncheck the **BSS Transition** check box.

Step 5 Save the configuration.

Disabling 802.11k and 802.11v on Cisco WLC (CLI)

Step 1 Disable 802.11k by entering these commands:

config wlan assisted-roaming neighbor-list disable *wlan-id*

config wlan assisted-roaming dual-list disable *wlan-id*

config wlan assisted-roaming prediction disable *wlan-id*

Step 2 Disable 802.11v by entering this command:

config wlan bss-transition disable *wlan-id*

Step 3 Save the configuration by entering this command:

save config

GLC-TE Support in Cisco 5508 WLCs

The GLC-TE 1000BASE-T SFP module is supported in Cisco 5508 WLCs. The Cisco 5508 WLCs that have the GLC-TE SFP module must run Release 8.3 or a later release. The GLC-TE SFP module is a replacement of GLC-T, which has reached its end-of-sale date as of June 1, 2017. For more information about end-of-sale and end-of-life announcement for select Cisco 1000BASE-T SFP modules, see http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/eos-eol-notice-c51-737325.html.

Software Release Types and Recommendations

Table 3 Release Types

Release Type	Description	Benefit
Maintenance Deployment (MD) releases	Software releases that provide bug-fix support and ongoing software maintenance. These releases are categorized as Maintenance Deployment (MD) and may be part of the AssureWave program.[1] These are releases with long life and ongoing software maintenance.	Provides you with a software release that offers stability and long support duration with periodic maintenance releases (MRs).
Early Deployment (ED) releases	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.

1. AssureWave is a Cisco program that focuses on satisfying customer quality requirements in key industry segments in the mobility space. This program links and expands on product testing conducted within development engineering, regression testing, and system test groups within Cisco. The AssureWave program has established partnerships with major device and application vendors to help ensure broader interoperability with our new release. The AssureWave certification marks the successful completion of extensive wireless controller and access point testing in real-world use cases with a variety of mobile client devices applicable in a specific industry.

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

Upgrading to Cisco WLC Software Release 8.3.102.0

Guidelines and Limitations

- WLAN-AP group association functionality:
  - Functionality prior to Release 7.4.130.0—If a WLAN was added to an AP group prior to Release 7.4.130.0, the RF radio policy is set to All after an XML upload/download. This is because the default value of RF policy was not added. This issue was addressed through CSCud37443. However, this corrects only the newly created WLAN-AP group associations and not the previous ones. Therefore, if you have configured a WLAN-AP group association prior to Release 7.4.130.0, you must remove the WLAN from the AP group and add it again in Release 7.4.130.0 or a later release.

    Also, the XML configuration for radio policy was not present in releases prior to 8.0. This issue is addressed through CSCul59089.

  - Change in functionality with Release 7.4.130.0—The RF radio policy is by default set to None for all WLAN-AP group associations created in Release 7.4.130.0. Any previous WLAN-AP group associations that are carried over will continue to be set to All unless a WLAN is removed from the AP group and added again.

    The XML upload/download for AP group RF radio policy is available only from Release 8.0.

- 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 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 to a 7.x release, the trap configuration is lost and must be reconfigured.
- If you downgrade from Release 8.3 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 or a later release, ensure that the following is done:
  a. 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.
  b. Reboot Cisco WLC immediately or at the preset time.
  c. Ensure that all Cisco APs are associated with Cisco WLC.
  d. 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 introduced in this release. The platform support for global multicast and multicast mode are listed in the following table.

Table 4 Platform Support for Global Multicast and Multicast Mode

Platform	Global Multicast	Multicast Mode	Support
Cisco 5520, 8510, and 8540 WLCs	Enabled	Unicast	No
	Enabled	Multicast	Yes
	Disabled	Unicast	Yes
	Disabled	Multicast	No
Cisco Flex 7510 WLC	Multicast is not supported.		
Cisco 5508 WLC	Enabled	Unicast	Yes
	Enabled	Multicast	Yes
	Disabled	Unicast	Yes
	Disabled	Multicast	No

Table 4 Platform Support for Global Multicast and Multicast Mode (continued)

Platform	Global Multicast	Multicast Mode	Support
Cisco 2504 WLC	Only multicast mode is supported.		
Cisco vWLC	Multicast is not supported.		

- The **reload** command is not recognized by Cisco Aironet 3600 Series APs. The workaround is to use the **debug capwap console cli** command.
- 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 8.3.102.0, 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 8.3.102.0.

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.
- 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 http://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/fus_rn_OL-31390-01.html.

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.

Note 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.

- 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 8.3.102.0 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 8.3.102.0. Table 5 shows the upgrade path that you must follow before downloading Release 8.3.102.0.

Caution 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.

Table 5 Upgrade Path to Cisco WLC Software Release 8.3.102.0

Current Software Release	Upgrade Path to 8.3.102.0 Software
8.0.x	You can upgrade directly to 8.3.102.0.
8.2.x	You can upgrade directly to 8.3.102.0. **Note** See "Changes in Images and Installation Procedure for Cisco 2504 WLC, Cisco 5508 WLC, and Cisco WiSM2" section on page 6 about special upgrade instructions for Cisco 2504 WLC, 5508 WLC, and WiSM2.

- 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 8.3.102.0. 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 8.3.102.0 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 5500 Series WLC), or enter **5** (on Cisco WLC platforms other than 5500 series) 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 8.3.102.0 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
- Applicable to Release 8.3 or a later release: Ensure that the configuration file that you back up does not contain < or > special character. If either of the special characters is present, then the download of the backed up configuration file fails.

Upgrading to Cisco WLC Software Release 8.3.102.0 (GUI)

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 8.3.102.0 software:

a. Browse to http://www.cisco.com/cisco/software/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 Release 8.3.102.0, 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 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 on page 6.

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 Release 8.3.102.0, 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 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 on page 6.

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 Re-enable the WLANs.

Step 18 For Cisco WiSM2 on the Catalyst switch, check the port channel and re-enable the port channel if necessary.

Step 19 If you have disabled the 802.11a/n and 802.11b/g/n networks in Step 4, re-enable them.

Step 20 To verify that the 8.3.102.0 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

This section describes the interoperability of Cisco WLC Software, Release 8.3.102.0 with other client devices.

Table 6 describes the configuration used for testing the client devices.

Table 6 Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	8.3.102.0
Cisco WLC	Cisco 55xx Series Wireless Controller
Access points	3802, 3502, 3602, 1602, 2602, 1702, 2702, 3702, 702, 702W, 1852
Radio	802.11ac, 802.11a, 802.11g, 802.11n2, 802.11n5
Security	Open, WEP, PSK (WPA and WPA2), 802.1X (WPA-TKIP and WPA2-AES) (LEAP, PEAP, EAP-FAST, EAP-TLS)
RADIUS	ACS 5.3, ISE 1.4
Types of tests	Connectivity, traffic, and roaming between two access points

Table 7 lists the client types on which the tests were conducted. The clients included laptops, handheld devices, phones, and printers.

Table 7 Client Types

Client Type and Name	Version
Laptop	
Intel 5100/5300	v14.3.2.1
Intel 6200	15.15.0.1
Intel 6300	15.16.0.2
Intel 6205	15.16.0.2
Intel 1000/1030	v14.3.0.6
Intel 7260	18.40.0.9
Intel 7265	18.40.0.9

Table 7 Client Types (continued)

Client Type and Name	Version
Intel 3160	18.40.0.9
Intel 8260	18.40.0.9
Broadcom 4360	6.30.163.2005
Linksys AE6000 (USB)	5.1.2.0
Netgear A6200 (USB)	6.30.145.30
Netgear A6210(USB)	5.1.18.0
D-Link DWA-182 (USB)	6.30.145.30
Engenius EUB 1200AC(USB)	1026.5.1118.2013
Asus AC56(USB)	1027.515.2015
Dell 1395/1397/Broadcom 4312HMG(L)	5.30.21.0
Dell 1501 (Broadcom BCM4313)	v5.60.48.35/v5.60.350.11
Dell 1505/1510/Broadcom 4321MCAG/4322HM	5.60.18.8
Dell 1515(Atheros)	8.0.0.239
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
Cisco CB21	1.3.0.532
Atheros HB92/HB97	8.0.0.320
Atheros HB95	7.7.0.358
MacBook Pro	OSX 10.11.5
MacBook Air old	OSX 10.11.5
MacBook Air new	OSX 10.11.5
Macbook Pro with Retina Display	OSX 10.11.5
Macbook New 2015	OSX 10.11.5
Tablets	
Apple iPad2	iOS 9.3.2(13F69)
Apple iPad3	iOS 9.3.2(13F69)
Apple iPad mini with Retina display	iOS 9.3.2(13F69)
Apple iPad Air	iOS 9.3.2(13F69)
Apple iPad Air 2	iOS 9.3.2(13F69)
Apple iPad Pro	iOS 9.3.2(13F69)
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

Table 7 Client Types (continued)

Client Type and Name	Version
Microsoft Surface Pro 3	Windows 8.1 Driver: 15.68.3093.197
Microsoft Surface Pro 2	Windows 8.1 Driver: 14.69.24039.134
Google Nexus 9	Android 6.0.1
Google Nexus 7 2nd Gen	Android 5.0
Intermec CK70	Windows Mobile 6.5 / 2.01.06.0355
Intermec CN50	Windows Mobile 6.1 / 2.01.06.0333
Symbol MC5590	Windows Mobile 6.5 / 3.00.0.0.051R
Symbol MC70	Windows Mobile 6.5 / 3.00.2.0.006R
Phones and Printers	
Cisco 7921G	1.4.5.3.LOADS
Cisco 7925G	1.4.5.3.LOADS
Cisco 8861	Sip88xx.10-2-1-16
Apple iPhone 4S	iOS 9.3.2(13F69)
Apple iPhone 5	iOS 9.3.2(13F69)
Apple iPhone 5s	iOS 9.3.2(13F69)
Apple iPhone 5c	iOS 9.3.2(13F69)
Apple iPhone 6	iOS 9.3.2(13F69)
Apple iPhone 6 Plus	iOS 9.3.2(13F69)
Apple iPhone 6s	iOS 9.3.2(13F69)
HTC One	Android 5.0
OnePlusOne	Android 4.3
Samsung Galaxy S4 T-I9500	Android 5.0.1
Sony Xperia Z Ultra	Android 4.4.2
Nokia Lumia 1520	Windows Phone 8.1
Google Nexus 5	Android 5.1
Google Nexus 6	Android 5.1.1
Samsung Galaxy S5-SM-G900A	Android 4.4.2
Huawei Ascend P7	Android 4.4.2
Samsung Galaxy S III	Android 4.3
Samsung Galaxy Nexus GTI9200	Android 4.4.2
Samsung Galaxy Mega SM900	Android 4.4.2
Samsung Galaxy S6	Android 6.0.1
Samsung Galaxy S7	Android 6.0.1
LG G4	Android 5.1

Table 7 Client Types (continued)

Client Type and Name	Version
Google Nexus 5X	Android 6.0.1
Xiaomi Mi 4c	Android 5.1.1
Xiaomi Mi 4i	Android 5.1.1

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 WLC

- 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.

- 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 Cisco WiSM2 and Cisco 5508 WLC

- 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

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.

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
- 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 Cisco Access Point Platforms

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

Table 8 Key Features Not Supported on Cisco Aironet 1810 OEAP, 1810W, 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
Protocols	• 802.11u • Full Cisco Compatible Extensions (CCX) support • Rogue Location Discovery Protocol (RLDP) • Native IPv6 • Telnet • Internet Group Management Protocol (IGMP)v3
Security	• Encryption – Temporal Key Integrity Protocol (TKIP) • Locally Significant Certificate (LSC) • TrustSec SXP • CKIP, CMIC, and LEAP with Dynamic WEP • Static WEP key for TKIP or CKIP [1] • WPA2 + TKIP **Note** WPA +TKIP and TKIP + AES protocols are supported.
Quality of Service	• Cisco Air Time Fairness (ATF)

Table 8 Key Features Not Supported on Cisco Aironet 1810 OEAP, 1810W, 1830, 1850, 2800 and 3800 Series APs (continued)

Location Services	• Data RSSI (Fast Locate) • Wi-Fi Tag
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 • SIP snooping with FlexConnect in local switching mode

1. For more details, see the *Wi-Fi Alliance Technical Note TKIP* document in the Wi-Fi Organization's website.

Note For Cisco Aironet1850 Series AP technical specifications with details on currently supported features, see the *Cisco Aironet 1850 Series Access Points Data Sheet*.

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

Table 9 Key Features Not Supported on Cisco Aironet 1810 OEAP and 1810W Series APs

Operational Modes	• Monitor Mode • Multiple client on wired ports
FlexConnect Features	• Local AP Authentication

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

Table 10 Key Features Not Supported on Cisco Aironet 1830 OEAP and 1850 Series APs

Operational Modes	• Monitor Mode
FlexConnect Features	• Local AP Authentication

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

Caveats describe unexpected behavior in a product. The Open Caveats section lists open caveats that apply to the current release and may apply to previous releases. A caveat that is open for a prior release and is still unresolved applies to all future releases until it is resolved.

To view the details of the software bugs pertaining to your product, perform the following task:

Click the Caveat ID/Bug ID number in the table.

The corresponding Bug Search Tool page is displayed with details of the Caveat ID/Bug ID.

The Bug Search Tool (BST), which is the online successor to the Bug Toolkit, is designed to improve the effectiveness in network risk management and device troubleshooting. The BST allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data, such as bug details, product, and version. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of a caveat whose ID you do not have, perform the following procedure:

1. Access the BST using your Cisco user ID and password:

   https://bst.cloudapps.cisco.com/bugsearch/

2. In the Bug Search window that is displayed, enter the necessary information in the corresponding fields.

For more information about how to use the Cisco Bug Search Tool effectively, including how to set email alerts for bugs and to save bugs and searches, see the Bug Search Tool Help & FAQ page.

Open Caveats

Table 11 Open Caveats for Release 8.3.102.0

Caveat ID Number	Headline
CSCuy21335	Filters are not working for table view in client performance
CSCuy89039	While roaming, static IP client from Export foreign to Export anchor client state changes from run to WebAuth request state
CSCuz45296	Cisco WLC sends acct-update multiple times in the same millisecond
CSCuz45986	CWA not working on Cisco 8500 WLC as Guest anchor with Accounting enabled
CSCuz46892	Cisco External AP rebooted because it detected another Cisco WLC
CSCuz52457	clshLtResultsTable is empty for IW-3700 AP
CSCuz55191	No events seen for DHCP Release/Renew from the client
CSCuz61571	Cisco 3802 AP SMP: Failed to stop secondary CPUs&of_i2c: modalias failure on
CSCuz65145	Previous WebAuth logout reasonType is logged only in the subsequent WebAuth login
CSCuz65175	Cisco 1852 AP: HTTP profiling causes CPU spikes and degraded performance
CSCuz70879	MAP reloads on hitting 40 minutes even when it is downloading image
CSCuz74953	Console messages after image download terminated on the GUI
CSCuz77434	APW5100 web GUI supports image downloading when AP configured –B domain
CSCuz78490	DHCP: Usage indicator will not show 100 percent usage even if all IP addresses are in use
CSCuz78638	DHCP: Default router IP address is also assigned to the client from the scope
CSCuz79869	Cisco 8510 WLC stopped working
CSCuz80349	Cisco AP GUI: some radio interface attributes' default values are set to none
CSCuz81089	Upgrade failure observed with ME using Release 8.3 and external Cisco 1850 AP with Release 8.2.x or 8.3
CSCuz89436	Cisco 3800 AP disconnects from Cisco WLC when local switching is enabled
CSCuz98344	Cisco 1810W and 3802 AP: Incorrect predownload status
CSCuz98904	Cisco 2800/3800 AP: **show advanced** FRA should show disabled radios in the network
CSCva00336	Cisco 3800 AP: SSID for XOR 5-GHz radio is not getting scanned in 160-MHz STA
CSCva01258	Logout operation becomes unresponsive for some time (5 to 10 seconds) on Mozilla Firefox browser for a scenario
CSCva01681	IP address shown incorrectly in WGB
CSCva04984	Cisco WLC GUI displays incorrect WLAN ID under AP for FlexConnect AVC mappings at FlexConnect group
CSCva07357	Cisco 1810 AP: Association traps are not observed in traplogs

Table 11 Open Caveats for Release 8.3.102.0 (continued)

Caveat ID Number	Headline
CSCva08567	Unable to hide the help text: Click on Help button and then click elsewhere
CSCva12999	The Cisco WLC is not setting the Operational Mode Notification bit in the Extended Capabilities IE for an Association Response
CSCva19606	Response time for SSH is in minutes instead of milliseconds
CSCva21300	OEAP: MAC filter does not work
CSCva22440	Cisco 3800 AP: QBSS STA Count keeps incrementing with STA associating again
CSCva25497	IOS sensor connects NA server but it restarts back from first interface
CSCva28475	Sensors do not associate if Aironet IE is disabled
CSCva30466	Cisco 1850 AP as sensor reporting incorrect operation status to Cisco WLC
CSCva30680	With Cisco 2800 AP as ME and 100 clients passing UDP traffic on Cisco internal AP, with internal DHCP server, **sh dhcp lease** command is unresponsive and takes more than 2 minutes to respond
CSCva30763	**show dot11** generic command does not work as expected
CSCva31890	MIB table bsnMobileStationPerRadioPerVapTable has no data
CSCva34187	After terminate, message for schedule later is incorrect
CSCva34228	Day0: All the details should be overwritten in an error scenario
CSCva34776	Cisco 3800 AP: When channel is global, moving band throws generic SNMP exception
CSCva35909	ME controller reloading while APs are downloading image on the current controller
CSCva38508	No NMSP response when Cisco 1850 AP is within half-duplex mode
CSCva38821	Cisco 1852 AP in FlexConnect mode converts back to Local after sensor test
CSCva38941	Clients are redirected to internal LWA URL instead of CMX cloud URL
CSCva39815	ME UI: Set Update time needs to change as Set Reboot time for HTTP mode
CSCva39994	Cisco 1852 AP: Client display error
CSCva40167	Only 62 characters for second label and error popped incorrectly
CSCva40580	BulkSync on active Cisco WLC never completes and is stuck in ‘in-progress’
CSCva40800	Meaningful Reason Type for DHCP and EAP Timeouts
CSCva40923	ME: Proper warning message while changing txPower for internal Cisco 3800 AP
CSCva41259	Cisco WLC showing WLAN-specific client IP address for group-specific WLAN-VLAN mapping
CSCva42290	The Cisco WLC is not setting the QoS Map Set bit or the WNM Notification bit in the Extnded Capabilities IE of an Association Response
CSCva42582	XOR radio admin status disabled when AP mode changed to sniffer
CSCva42917	Same AP image shows up on primary and backup side
CSCva43211	Unable to import configuration file because other Cisco AP is becoming the primary AP

Table 11 Open Caveats for Release 8.3.102.0 (continued)

Caveat ID Number	Headline
CSCva43331	Some ATF client statistics are missing on a Cisco AP after multiple roams
CSCva45543	SNMP Null was returned for class com.cisco.server.managedobjects
CSCva70440	AP801 is rebooting continuously
CSCvd06463	IOS AP doing AMSDU aggregation for voice traffic in queue 0 despite BA request declined by Cisco Wireless IP Phone 8821
CSCvk44249	WLC 5508 - foreign mapping is missing on a WLAN when restoring a backup

Resolved Caveats

Table 12 Resolved Caveats for 8.3.102.0

Caveat ID Number	Headline
CSCuy37478	Cisco 1850 AP static IP configuration does not apply DNS information
CSCuw70789	Cisco AP using a reserved port to join the Cisco WLC
CSCux34439	802.11ac clients cannot connect to CAP3600 Radio slot2 — 802.11ac module
CSCux72176	Need way to keep Cisco AP from reloading when it cannot join a Cisco WLC
CSCux63218	Upgrade to Release 8.0 moved Cisco APs to EAP-MD5 authentication on wired 802.1x
CSCux45077	Cisco 3500 AP stopped working due to “LWAPP CLIENT” process
CSCux62529	Cisco AP stopped working at disc_client_txq_dump
CSCuz59419	Cisco AP reuses the same channel without waiting for 30 minutes after DFS reset
CSCuy45955	DFS scan causes beacon transmission to be stuck on AP
CSCuy63094	Cisco 1572CM AP not sending Option 60
CSCuv61271	Window DHCP BAD_ADDRESS for Cisco APs
CSCux84256	Cisco 1850 AP stops working on radio failure: check_tx_beacon_stuck beacons stuck
CSCuz89662	Cisco 1852 AP reject clients association due to “suppRates statusCode is 18”
CSCux86366	Cisco 2700 universal mode AP shows AP name as 3600 on web interface
CSCuy13549	FlexConnect group push eap-md5 supplicant config to Cisco APs
CSCuy83736	Cisco AP: LED status changed after installing WSSI (RM3000) blinking blue 24x7
CSCuy46033	MAP fails to rejoin the RAP after it loses connection on Release 8.0.121.0
CSCva37881	Cisco 2800 and 3800 APs configured as mDNS APs do not forward mDNS and report the services to Cisco WLC
CSCuz29774	Cisco 1852 APs losing connectivity to ME controller with AVC in enabled state
CSCuy27190	Cisco 1850 AP and 1830 AP draw 24.8 Watts

Table 12 Resolved Caveats for 8.3.102.0 (continued)

Caveat ID Number	Headline
CSCuz02444	Cisco AP stuck in low-power when CDP/LLDP is not negotiated during bootup
CSCuy94534	Cisco 3700/2700 AP on DFS does not see Cisco 3700/2700 AP as neighbor when RxSOP is high, medium, or low.
CSCuy48983	AIR-CAP2702 radio reset due to Encryption Engine STUCK BZ738[BZ1180]
CSCut29345	**show controllers dot11Radio** showing incorrect information about rates
CSCuy31962	Cisco APs detect different WPA Support value from Rogue AP
CSCuw23023	Cisco 3700 AP Sniffer Mode not capturing on 5-GHz radio with RxSOP set
CSCux38644	Cisco 3700 AP, 1600 AP, 1532 Autonomous AP decrease power after reboot
CSCuw41092	Cisco AP does not send traffic indication in beacon for power-save client after FT
CSCux68014	Cisco 1572 EAC AP fallback shutdown not working
CSCux71803	AP802 autonomous unable to configure EoGRE
CSCux22620	Cisco 8510 WLC stopped working in radiusTransportThread system task
CSCuw91763	AES Key Wrap feature does not work as expected
CSCuy34175	Unable to create local net users with spaces between first and last name
CSCuy75241	Cisco 5508 WLC stops working with task mmMobility
CSCur53041	DTLS connection failure
CSCux75330	Mismatch AP count and unable to add more APs to WLC
CSCuy50490	Unknown AP type. Using Controller Version!!
CSCuw06127	Cisco WLC stopped working on Release 8.0.120 due to memory leak in CDP Main
CSCuy58091	Evaluation of Cisco WLC for OpenSSL March 2016
CSCuz52435	Evaluation of Cisco WLC for OpenSSL May 2016
CSCux55307	AIR-CT5520 stopped working in dtlArpTask
CSCuw09545	Incorrect DHCP “Pool Usage” on the Cisco WLC when queried via SNMP
CSCuy70039	Cisco WLC should not forward DHCPINFORM when client is in DHCP_REQD
CSCuz72460	Cisco 1852 ME AP unable to add space to SSID via GUI or CLI after initial config
CSCuz17680	Cisco Flex 7510 WLC stopped working after enabling the enhanced client traps
CSCux44685	Disallow configuration of WLAN Local and RADIUS client profiling
CSCur90555	Cisco WLC on Release 8.0 keeps ghost client entry
CSCuz24986	Cisco WLC sends NAK to a valid CoA due to unrecognized Session-ID
CSCuy30583	Cisco 5520 WLC: The **show imm chassis** shows no results; and then the Cisco WLC stops working
CSCuy12943	Cisco WLC on Release 8.1: Unknown emWeb error message

Table 12 Resolved Caveats for 8.3.102.0 (continued)

Caveat ID Number	Headline
CSCuu80484	Cisco 5520 DP WLC stopped working on Release 8.1.102.0
CSCuw24476	Increased ping latency and reduced traffic on Cisco 8510 WLC with QoS rate limiting
CSCuw12544	Rate-limiting is causing 500-ms gap of traffic when roaming
CSCuu20256	Traffic drop on Cisco WLCs on Release 7.6.130.x and with PMIPv6
CSCuv03963	Cisco WLC dataplane issue: “fatal condition at broffu_fp_dapi_cmd.c”
CSCuw44480	802.11r client fails authentication if self reset before user idle timeout expires
CSCuv37613	Apple devices failing 802.11r FT roam
CSCuy20175	Windows client: User authentication failing when doing inter-WLC roaming
CSCuw89581	Cisco WLC stopped working on apfReceiveTask
CSCuv30948	Local net users not saved in config backup
CSCux08557	Reaper reset because of SNMPTASK: VALIDATE_GUEST_SESSION_FAILED
CSCuz78555	Bulk sync status “In-progress” after standby boots up
CSCuy14547	HA Config Sync failed
CSCuy57978	Standby Cisco WLC sending LLC frames from wireless clients when Standby Hot
CSCux85357	Cisco WLC sends GARP for FlexConnect local switching clients after HA switch-over
CSCuy29143	ARP not forwarded when FlexConnect ARP caching enabled
CSCuy91543	Only locally switched FlexConnect APs should not join CAPWAP multicast group
CSCuz71587	Unable to push the FlexConnect template from Cisco Prime Infrastructure to Cisco WLC
CSCux95319	Roaming central to local authentication causes in FlexConnect-caused 802.1x table failures
CSCuy71261	VLAN mapping has incorrect VLAN number after Cisco AP moved to AP group
CSCuz56479	Cisco WLC cLReapApVlanInheritance object not taking WLAN-specific value (3)
CSCuz57472	Cisco 8510 WLC on Release 8.0.120.0: IPv6 not getting disabled causing Multicast queue to be full
CSCua43558	Cisco WLC stopped working on Task:sisfSwitcherTask with IPv6 traffic
CSCuw13264	Cisco 702W AP: Missing interface information about the AP on Cisco WLC after HA failover
CSCuw30129	Debugging logging quickly falls behind real-time
CSCux51833	Client fails on RAP with AAA override ACL when Cisco AP is in Flex+Bridge Mode
CSCuz07287	The **show mesh per-stats summary** command shows negative values

Table 12 Resolved Caveats for 8.3.102.0 (continued)

Caveat ID Number	Headline
CSCux59359	Cisco 8510 WLC behind NAT on New Mobility and client stuck in DHCP_REQD state
CSCuv09655	Cisco WLC as Anchor stopped working on Release 8.0.110.x with New Mobility apf_msDeleteTblEntry
CSCux13032	Anchor not appending client MAC address in external WebAuth redirect with HTTPS
CSCuz38059	Anchor WLC does not free client sessions; client entries are stale
CSCux82955	Anchor WLC does not forward DHCP request to server as VLAN set as 0
CSCut76824	Anchor WLC will not forward DHCP request to the DHCP server
CSCut27598	Client unable to get IP when switching WLAN on New mobility
CSCuu97761	Foreign WLC upgraded to Release 8.1 fails to export clients to Anchor WLC
CSCuv85747	Mobility Member entries going stale
CSCut16170	Mobility tunnel down after switchover on Release 7.6
CSCux00803	New Mobility clients stuck in DHCP_REQD state with NAT IP on Foreign WLC
CSCuu21625	Session not cleared on Cisco 5508 anchor WLC with Cisco Catalyst 3850 Switch as foreign WLC causing authentication issues
CSCuu72366	System stopped working or memory leak on mmListen process
CSCuv34277	Wireless client unable to get IP address on Cisco Catalyst 3650 Switch acting as MA from Cisco 5508 WLC as anchor
CSCut39118	Cisco 8510 WLC failure to collect feature MobilityExtGroupMember on PI 2.2
CSCuz22985	BCAST Queue full, causing clients to stay Multicast-direct Pending status
CSCuz79764	Download configuration failed even if it should be supported
CSCuz23006	Global Multicast cannot be enabled
CSCux69221	HP printer not seen by Apple iOS devices after returning from sleep mode
CSCuv22052	Link local multicast control traffic sent by APs with IGMP Snooping enabled
CSCur91936	mDNS discovery issue with Cisco WLC on Release 8.0.100.x
CSCuz63274	mDNS snooping drops IPv6 mDNS traffic
CSCuy44880	MTU is not retrieved
CSCux96500	Cisco WiSM2/WLC stopped working on bcastReceiveTask
CSCuz60441	Same AVC profile is applied once switched to new WLAN
CSCuy43365	Cisco 5520/8540 WLC on Release 8.2.100.0 stopped working in Reaper Reset: Task ”apfReceiveTask”
CSCuv86494	Cisco WLC clears AP MAC address before deleting client, sends NetFlow with Zero AP MAC address
CSCuw28246	Cisco 8540/5520 WLC does not detect power supply cable failure
CSCux58741	Cisco 8540 WLC does not show proper RAID volume status
CSCuu86587	Cisco 8540 WLC DN1/DN2: Need closed loop Cavium fan control

Table 12 Resolved Caveats for 8.3.102.0 (continued)

Caveat ID Number	Headline
CSCuy36572	Evaluation of Cisco WLC for glibc_feb_2016
CSCuu82416	Evaluation of Cisco WLC for OpenSSL June 2015
CSCut31679	Unhandled kernel unaligned access
CSCuy18037	Cisco WLC stopped working in emWeb while accessing the **show client details** command.
CSCuv79793	Cisco WLC is leaking packets from virtual IP onto LAN
CSCuz50774	Cisco WLC will lose pings against its own IP address using small packet size less than 20 or would not lose them but show next log
CSCuy04572	Incorrect timestamp sent on rogue traps when delta value set on Cisco WLC
CSCux74970	MAG with PMIPv6 does not assign secondary DNS to clients via DHCP
CSCux60873	RADIUS interface overwrite does not work when choosing “ap group” interface
CSCux61747	Cisco WLC stops working when configuring DNS-based ACL
CSCuy95327	802.1x frames are not marked with DSCP CS4
CSCuw28141	Reaper Reset: Task "SNMPTask" missed software watchdog
CSCux32328	Token Bucket leak with QoS Roles and with WebAuth on Release 8.0.120.x
CSCuv88984	The **show ap universal summary** command dos not exist
CSCtu45614	Spectrum management bit should be set to 1 all the time
CSCuw38795	Cisco 5508 WLC stopped working upon pushing RF calibration template from PI
CSCuw38022	Cisco 8510 SNMP agent reverses octet order of clrRrmPakRssiNtp object
CSCuy33247	Cisco AP sends disassociation frames twice and optimized roaming goes wrong
CSCuy91177	Client MSCB removed on Optimized Roam
CSCuv67144	Algeria local authorities are not allowing WLAN AP(s) to be imported if they are –E; –I domain is allowed to be imported
CSCuw36069	Threshold MIBs incorrectly set for WSSI modules
CSCuw79951	Unable to disable Assisted Roaming or Load Balancing via CLI
CSCuw62850	Cisco WiSM2 on Release 8.0.120.x stopped working on mwar_ms_deadlock.crash
CSCuz67766	Cisco WLC stopped working due to software watchdog for apfMsConnTask_0
CSCuu52140	Cisco WLC stopped working on RRM data read
CSCut87326	Cisco WLC generates SNMP traps to PI 2.2 for AIR-3702 PoE+ getting low power
CSCuw66299	Cisco WLC message log is showing NMSP Transmit Failure even when there is no MSE
CSCux84074	Cisco WLC should not allow unsupported gain values for given AP

Table 12 Resolved Caveats for 8.3.102.0 (continued)

Caveat ID Number	Headline
CSCuw13322	Cisco 8540 WLC: Unable to re-enable or remove RADIUS Authentication Servers
CSCuw29419	Cisco WLC RADIUS Packet of Disconnect Vulnerability
CSCux37498	CoA with Cisco WLC on Release 8.1.131.0 shows error message on ISE server
CSCux41354	Evaluation of Cisco WLC for OpenSSL December 2015 vulnerabilities
CSCux38853	**grep** command unavailable for Cisco WLC local read-only management user
CSCux58488	Traps received are showing incorrect values or positions
CSCuw90625	Rogue rules are not applied correctly after upgrade to Release 7.6.130.x
CSCut96026	SGT remains for client when moving between WLANs with Fast SSID change
CSCuv97793	Cisco WiSM2 stopped working when AP_DB_CREATE_ERR Message queue MFP-Q is near full
CSCuv82711	Cisco 5508 WLC on Release 8.1.111.0L: RFC-3576 Disconnect-Request not heard from port 3799
CSCux39187	Cisco WLC throws AAA-3-ACCTREQ_SEND_FAILED error message when AAA disabled
CSCuw26629	MIB message of Power supply Status on Cisco Flex 7510 WLC is incorrect
CSCuz86679	Cisco WLC stopped working on SNMPTask
CSCuw34565	Cisco Flex 7510 WLC stopped working after deleting AP crash logs from GUI
CSCuz74146	Unable to edit dynamic interface if WLAN is enabled and mapped to management interface
CSCux56652	Local profile shows incorrect statistics and percentage information
CSCuv96333	Read-only user is able to change “Telnet Capability” setting
CSCuw73215	RF profile > coverage,exception clients range differs in WLC GUI and CLI
CSCuw02258	Severity filter to monitor CleanAir Interferers does not work
CSCuv92719	Cisco vWLC stopped working on Release 8.1.111.0 serving the RF dashboard web page
CSCuz79051	Cisco WiSM2 on Release 8.1.131.0 stopped working in ewaFormServe_multicast_detail
CSCuz74637	Cisco WLC login banner is not displayed on GUI; when using CLI, it works as expected
CSCuw81123	CMCC web portal need to open UDP port 2000
CSCux88967	On MAC Filter failure, client has a session timeout and cannot associate back
CSCux87082	Cisco WLC HA Pair cannot sync WebAuth Messages with more than 255 characters
CSCuy76838	Failed to enable CIDS sensor
CSCuy08363	Rogue detector not working on Release 8.0.120.0
CSCuy37694	Cisco WLC stopped working on Release 8.0.120.0 at task apfRogueTask_1
CSCuw31595	Incorrect information shown in the output of the **show run-config** command

Table 12 Resolved Caveats for 8.3.102.0 (continued)

Caveat ID Number	Headline
CSCuy73679	Cisco 1852 AP as Mobility Express Controller does not send traplog
CSCuy27099	ME: Import/Download config broken for ap-image commands
CSCuy12650	Tracebacks on Autonomous WGB IW3702s
CSCux82914	Cisco WLC message log shows NMSP Transmit Failure even when there is no MSE
CSCut31468	System stopped working or memory leak in mmListen process
CSCuv85891	DFS scan causes beacon transmission to be stuck on AP
CSCut44415	Release 8.1 does not allow zero value for RADIUS ACCT Interim update
CSCuy34975	AIR-CAP2702 radio reset due to Encryption Engine STUCK BZ738[BZ1180]
CSCuz95527	1852 Mobility Express Controller Sends Trap Log with Dst Port 41472

Cisco Mobility Express Solution Release Notes

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 1830, 1850, 2800, and 3800 Series access points. This functionality provides a simplified Wi-Fi architecture with limited enterprise-level WLAN capability to small and medium deployments.

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

The primary 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 Primary (Support Integrated Wireless Controller Capability)	APs Supported as Subordinate
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 primary 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 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 primary.

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 500 clients
  - 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 primary 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 primary AP and to select a new AP as primary 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 Release 8.3.102.0.

Access Points Supported As Primary	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
1830	AIR-AP1830-K9-8-3-102-0.tar	AIR-AP1830-K9-ME-8-3-102-0.zip
1850	AIR-AP1850-K9-8-3-102-0.tar	AIR-AP1850-K9-ME-8-3-102-0.zip
2800	AIR-AP2800-K9-8-3-102-0.tar	AIR-AP2800-K9-ME-8-3-102-0.zip
3800	AIR-AP3800-K9-8-3-102-0.tar	AIR-AP3800-K9-ME-8-3-102-0.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 "Caveats" section on page 35. All caveats associated with the Cisco Mobility Express solution have *Cisco Mobility Express* specified in the headline.

Service and Support

For all Support related information, see http://www.cisco.com/c/en/us/support/index.html.

Related Documentation

Cisco Wireless Controller

For more information about the Cisco WLCs, lightweight access points, and mesh access points, 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 User Guide*

  http://www.cisco.com/c/en/us/td/docs/wireless/access_point/mob_exp/83/user_guide/b_ME_User_Guide_83.html
- *Cisco Aironet Universal AP Priming and Cisco AirProvision User Guide*

  http://www.cisco.com/c/en/us/td/docs/wireless/access_point/ux-ap/guide/uxap-mobapp-g.html

Wireless Products Comparison

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

http://www.cisco.com/c/dam/assets/prod/wireless/cisco-wireless-products-comparison-tool/index.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2016 Cisco Systems, Inc. All rights reserved.