Release Notes for Cisco Wireless Controllers and Lightweight Access Points for Cisco Wireless Release 8.2.100.0

First Published: December 15, 2015

This release notes document describes what is new in Cisco Wireless Release 8.2.100.0, instructions to upgrade to this release, and open and resolved caveats for this release. Unless otherwise noted, in this document, all Cisco Wireless Controllers are referred to as *Cisco WLCs*, and all Cisco lightweight access points are referred to as *access points* or *Cisco APs*.

Note For information specific to the Cisco Mobility Express solution, see "Cisco Mobility Express Solution Release Notes" section on page 53.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Revision History

Table 1 Revision History

Modification Date	Modification Details
November 22, 2016	• Features Not Supported on Cisco 2504 WLC, page 34 – Added: EoGRE • Features Not Supported on Cisco Virtual WLCs, page 36 – Added: EoGRE (Supported in only local switching mode)
September 27, 2016	• What's new in this Release – Added: Removal of Support for Rx SOP from Mesh Backhaul, page 10
May 17, 2016	• L3 Interfaces for Tunneling Protocols, page 11 – Added note on feature tunnel support. • Upgrading to Cisco WLC Software Release 8.2.100.0, page 21 – Added this statement: "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."
April 22, 2016	• Features Not Supported on Cisco Virtual WLCs, page 36 – Added Lync SDN.
March 21, 2016	• Features Not Supported on Cisco 2504 WLC, page 34 – Added Application Visibility and Control (AVC) for FlexConnect centrally switched access points to the list of not supported features.
March 16, 2016	• What's New in this Release, page 5 – Added a Note on Release 8.2 related interface restrictions
March 8, 2016	• Resolved Caveats, page 41 – Added CSCuw03323 to the Resolved Caveats list.
March 4, 2016	• Upgrading to Cisco WLC Software Release 8.2.100.0, page 21 – Documented CSCux75436 kernel route issue.
March 3, 2016	• Mobility Express Features, page 54 – Added information about Cisco CMX support.
March 2, 2016	• Upgrading to Cisco WLC Software Release 8.2.100.0, page 21 – Added a statement that Cisco Aironet 3600 Series APs cannot recognize the **reload** command.
February 21, 2016	• 2.4-GHz Mesh, page 10 – Rephrased the statements made in this section.
February 18, 2016	• Features Not Supported on Cisco Aironet 1830 and 1850 APs, page 37 – Added Telnet to the list of unsupported features

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 (5508 and 5520 Wireless Controllers)
- Cisco Flex 7500 Series Wireless Controllers (Cisco Flex 7510 Wireless Controller)
- Cisco 8500 Series Wireless Controllers (8510 and 8540 Wireless Controllers)
- Cisco Virtual Wireless Controllers on the Cisco Services-Ready Engine (Cisco SRE) or the Cisco Wireless LAN Controller Module for Cisco Integrated Services Routers G2 (UCS-E)

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

For information about features that are not supported on the Cisco WLC platforms, see "Features Not Supported on Cisco WLC Platforms" section on page 34.

Supported Access Point Platforms

The following access point platforms are supported in this release:

- Cisco Aironet 1040 Series Access Points
- Cisco Aironet 1140 Series Access Points
- Cisco Aironet 1260 Series Access Points

- Cisco Aironet 1600 Series Access Points
- Cisco Aironet 1700 Series Access Points
- Cisco Aironet 1830 Series Access Points
- Cisco Aironet 1850 Series Access Points
- Cisco Aironet 2600 Series Access Points
- Cisco Aironet 2700 Series Access Points
- Cisco Aironet 3500 Series Access Points
- Cisco Aironet 3600 Series Access Points
- Cisco Aironet 3700 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.

For information about features that are not supported on some access point platforms, see Features Not Supported on Access Point Platforms, page 37.

Note Cisco AP802 is an integrated access point on the Cisco 800 Series Integrated Services Routers (ISRs). For more information about the stock-keeping units (SKUs) for the AP802s and the Cisco ISRs, see the following data sheets:

- AP860:

  http://www.cisco.com/c/en/us/products/collateral/routers/800-series-routers/data_sheet_c78_461543.html

- AP880:

  http://www.cisco.com/c/en/us/products/collateral/routers/887-integrated-services-router-isr/data_sheet_c78_459542.html

  http://www.cisco.com/c/en/us/products/collateral/routers/800-series-routers/data_sheet_c78-613481.html

  http://www.cisco.com/c/en/us/products/collateral/routers/880-3g-integrated-services-router-isr/data_sheet_c78_498096.html

http://www.cisco.com/c/en/us/products/collateral/routers/880g-integrated-services-router-isr/data_sheet_c78-682548.html

- AP890:

  http://www.cisco.com/c/en/us/products/collateral/routers/800-series-routers/data_sheet_c78-519930.html

  Before you use a Cisco AP802 series lightweight access point with Cisco Wireless Release 8.2.100.0, you must upgrade the software in the Cisco 880 Series ISRs to Cisco IOS 15.1(4)M or later releases.

Unsupported Cisco Wireless Controller Platforms

The following Cisco Wireless Controller platforms are not supported:

- Cisco 4400 Series Wireless LAN Controller
- Cisco 2100 Series Wireless LAN Controller
- Cisco Catalyst 3750G Integrated Wireless LAN Controller
- Cisco Wireless Controller software for Cisco SRE Internal Services Module (ISM) 300, Cisco SRE Service Module (SM) 700, Cisco SRE Service Module (SM) 710, Cisco SRE Service Module (SM) 900, and Cisco SRE Service Module (SM) 910.
- Cisco Catalyst 6500 Series and 7600 Series WiSM
- Cisco Wireless LAN Controller Module (NM/NME)

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 53.

Note Release 8.2 does not support multiple non-AP Manager dynamic interfaces, untagged management interfaces, management interfaces mapped to physical ports, and non-LAG scenarios.

Cisco Smart Software Licensing

Cisco started the initiative of simplifying customer license management by building a Cisco Smart Software Manager portal. It helps the customers understand what licenses they have purchased and what licenses they are using. Various other Cisco products are already Smart Enabled and with the introduction of this release Cisco Smart Software Licensing will now be available on the following platforms:

- Cisco 5520 WLC (AIR-CT5520-K9)
- Cisco 8540 WLC (AIR-CT8540-K9)
- Cisco vWLC (L-AIR-CTVM-5-K9)

For more information, see the following:

- *Cisco Smart Software Licensing Overview*
- Cisco Smart Software Licensing section in the *Cisco Wireless Controller Configuration Guide*.

Increased AP and Client Scale for Cisco Virtual Wireless Controller

The capacity of Cisco Virtual Wireless Controllers (vWLCs) is increased with the introduction of a Large Scale vWLC.

Two new SKUs with two types of scaling configurations are available. During installation or upgrade, you can choose between Small Scale vWLC and Large Scale vWLC.

This table lists the two types of Cisco vWLCs, their requirements and capacity:

Table 2 Cisco vWLC Types, their Requirements and Capacity

vWLC Type	Virtual CPU	Memory	Number of APs Supported	Number of Clients Supported
Small Scale vWLC	1	2 GB	200	6000
Large Scale vWLC	2	8 GB	3000	32000

Access Point Provisioning using Plug-n-Play (PnP)

The Access Point Provisioning using Plug-n-Play (AP PnP) solution provides staging parameters to an AP before it is associated with a Cisco WLC. Using this staging configuration, the AP gets the run-time configuration when it associates with a Cisco WLC. PnP is supported only on AP recovery images and is activated only for the zero-day deployment. PnP can no longer be initiated after the AP associates with a Cisco WLC for the first time.

The following AP scenario is supported:

- On-premise redirection—Customers hosting the PnP server in their network

The AP PnP solution is supported on the following APs:

- Cisco 702i AP
- Cisco 702W Series APs
- Cisco Aironet 1600 Series APs
- Cisco Aironet 1700 Series APs
- Cisco Aironet 2600 Series APs
- Cisco Aironet 2700 Series APs
- Cisco Aironet 3600 Series APs
- Cisco Aironet 3700 Series APs

NetFlow Export 2.0

The following are the template enhancements in NetFlow Version 9:

- New features can be added to NetFlow quickly, without breaking existing implementations.
- NetFlow is *future-proofed* against new or developing protocols, because NetFlow Version 9 can be adapted to provide support for those protocols.
- NetFlow Version 9 is the IETF standard mechanism for information export.
- Third-party business partners who produce applications that provide collector or display services for NetFlow are not required to recompile their applications each time a new NetFlow feature is added.

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

AVC Enhancements

In Release 8.2, the following features are available on Cisco WLCs:

- Protocol Pack 14.0
- NBAR Engine Release 3.16(23)

Features

- NBAR2 Engine Version 23 is tightly coupled with Cisco Wireless Release 8.2 and aligns with Protocol Pack 14.0.

- Faster upgrade and downgrade process—Downgrading from Release 8.2 to Release 8.1 changes the protocol pack to the previously installed protocol pack version, which is Protocol Pack 11.0.
- Traffic is classified instantly upon Cisco WLC bootup.
- Support for 1536 applications.

Note Newer protocol packs are tied with Network-Based Application Recognition (NBAR) Engine Version 14 and later. Protocol packs that are earlier than Version 14 do not work with the new engine.

For more information, see the *Release Notes for NBAR2 Protocol Pack 14.0.0 for Cisco Wireless Controllers*.

Bonjour Gateway with Googlecast Support

Googlecast Service that uses the service key, *_googlecast._tcp.local*, is supported on the existing implementation of Bonjour gateway on Cisco WLC.

Enhanced wIPS Support for Hyperlocation Module with Advanced Security

wIPS support for the 40 MHz to 80 MHz range using Hyperlocation module is introduced. This feature detects alarms in the 40 MHz to 80 MHz range (if RRM channel scanning is selected) and provides information to Cisco Prime Infrastructure (PI). Channel width information is derived from the packet data rate and sent to the wIPS module, which stores channel width per alarm. Using the **show capwap am alarm** *alarm-id* command, you can view the channel width in which the attack has occurred.

The wIPS alarm report contains the channel width of the attack and device capability (802.11a/b/g/n/ac). No wIPS-specific configuration is required to enable this feature. The only prerequisite is that RRM scanning must be enabled for this feature to work as expected.

Cisco Air Time Fairness: Client Fair Sharing

In Release 8.2, Cisco Air Time Fairness can be enforced on clients that are associated with an SSID/WLAN. This ensures that all clients within an SSID/WLAN are treated equally based on their utilization of the radio air time. This feature is useful in scenarios where one or a few clients could use the total air time available for an SSID/WLAN, thereby depriving Wi-Fi experience for other clients associated with the same SSID/WLAN.

For more information, see the Cisco Air Time Fairness section in the *Cisco Wireless Controller Configuration Guide*.

Cisco WLAN Express Enhancements

- New best practices added in Release 8.2. For details, see the "Complete List of Best Practices in Release 8.2" section on page 9.
- You have the option to ignore a recommended best practice by clicking the **Ignore** button. The **Ignore** button is visible (only for some best practices) when you click the + icon to select a recommended best practice. These best practices are added to the ignored list.

- The best practices information displayed when you click the **Learn More** button is integrated with the Cisco WLC software. The **Learn More** button is visible (only for some best practices) when you click the + icon to select a recommended best practice. Previously, this document was accessible on Cisco.com.
- Updates have been made to the Main Dashboard with the addition of new dashlets. For more information, see the *Cisco Wireless Controller Online Help*.

Complete List of Best Practices in Release 8.2

Note The best practices introduced in Release 8.2 are listed below in bold.

- Infrastructure
  - AVC Visibility
  - **Band Select**
  - Controller High Availability
  - Disable Aironet IE
  - **Disable Internal DHCP**
  - Disable Management over Wireless
  - Fast SSID
  - **HTTPS for Management**
  - Load Balancing
  - **Load Balancing Window**
  - Local Profiling
  - mDNS Gateway
  - Multicast Forwarding
  - Multicast Mobility
  - **Multicast VLAN**
  - NTP
  - **Tagged Management VLAN**
  - **Virtual Gateway IP**
  - **WLAN not on Management VLAN**
- Security
  - **802.1X on AP**
  - CPU ACLs
  - Client Exclusion
  - Legacy IDS
  - Local Management Password Policies
  - Min Rogue RSSI Threshold
  - **Peer to Peer**

  - Rogue Policies
  - SSH/Telnet Access
  - User Login Policies
  - WLAN with 802.1X
  - **WLAN with WPA2 and AES Policy**
- RF Management
  - Auto Coverage Hole Detection
  - Auto Dynamic Channel Assignment
  - Auto Transmit Power Control
  - **Best Channel Width**
  - CleanAir Detection
  - Client Band Select
  - **DCA Cisco AP Load**
  - Event Driven RRM
  - **High SSID Counts**
  - **Wi-Fi Interference**

Note The 40-MHz Channel Width best practice is not available in Release 8.2.

2.4-GHz Mesh

Mesh functionality in 2.4 GHz is supported on all APs that support Mesh.

In addition, while both 2.4 GHz and 5 GHz can be used outdoor across the globe, in Israel, only 2.4 GHz can be used outdoor. Therefore, a new regulatory domain, –I, and country code, IO, is introduced to support the use of 2.4 GHz as outdoor mesh backhaul on Cisco Aironet 1530 and 1570 APs.

Removal of Support for Rx SOP from Mesh Backhaul

From Cisco Wireless Release 8.2, the Rx SOP feature in bridge mode is not supported in the mesh backhaul 5-GHz interface to improve backhaul stability.

Pre-Shared Key Provisioning Support for Mesh Networks

Support is added for the pre-shared key (PSK) functionality that can be provisioned from Cisco WLC and can help make a controlled mesh deployment and enhance mesh access point (MAP) security beyond the currently used default *cisco* PSK.

With this new feature, MAPs, which are not preset yet with a valid PSK can connect to Cisco WLC using the default *cisco* PSK, during the provisioning window controlled by the Administrator. However, it will then receive a new PSK from the Cisco WLC, and from that point on, will only be able to connect with that PSK, and no longer with the default passphrase *cisco*.

Caution If you want to downgrade from Release 8.2 to an earlier release, we recommend that you change the security method to EAP and then perform the downgrade operation.

Dynamic Management User Login via AAA Server

Management users who are logged in when external servers are not available must reauthenticate when the external RADIUS servers are available. Failing to do so will lead to termination of the user session to prevent potential operational and security risks. When RADIUS servers are not available, management users are authenticated locally. After the RADIUS servers are back online, management users are prompted to log in again within a specific timeframe.

For more information, see the Setting up TACACS+ section in the *Cisco Wireless Controller Configuration Guide*.

Test AAA Command for RADIUS

To troubleshoot AAA RADIUS interactions for WLAN authentication, **test aaa** commands are introduced:

- Test AAA RADIUS interactions for WLAN authentication by entering this command:

  test aaa radius username *username* **password** *password* **wlan-id** *wlan-id* [**apgroup** *apgroupname* **server-index** *server-index*]

  The **test** command sends an access request the RADIUS server for client authentication. Access request exchange takes place between Cisco WLC and the AAA server, and the registered RADIUS callback handles the response.

  The response includes authentication status, number of retries, and RADIUS attributes.

- View the RADIUS response to test the RADIUS request by entering this command:

  test aaa show radius

For more information, see the Troubleshooting AAA RADIUS Interactions for WLAN Authentication section in the *Cisco Wireless Controller Configuration Guide*.

Custom HTTP Port for Profiling

WLC can now send HTTP user agent information to ISE for devices that use custom port (not only port 80).

L3 Interfaces for Tunneling Protocols

Prior to Release 8.2, the management IP address was used as the tunnel endpoint. Release 8.2 has allowed the specification of any L3 dynamic interface as a tunnel endpoint, other than the management interface, if need be.

Note This feature currently supports EoGRE and PMIPv6 types of tunnels for mobility tunnel termination.

Cisco 5520, 8510, and 8540 WLC Updates

- Out-of-Band Management Support—Prior to Cisco Wireless Release 8.2, we recommended that you do not use the service port for continuous SNMP polling and management functions, except when the management interface of the Cisco WLC is unreachable. In Cisco Wireless Release 8.2, this restriction is removed.

  In Release 8.2, the following are supported on the Cisco 5520, 8510, and 8540 WLCs:

  - SNMP polling v2 and v3
  - Syslog messaging towards external server
  - Any form of file transfer, including FTP, TFTP, and SFTP, to/from external server
  - HTTP and HTTPS access to Cisco WLC
  - SSH and Telnet
- Local EAP is supported
- Wired Guest Access is supported

Support for Wi-Fi Certified Passpoint Release 2.0

In order to support Passpoint Release 2.0 certification, the technical specification of HotSpot 2.0 Release 2 has been implemented, which allows an end user, upon reaching a Passpoint 2.0 WLAN, to sign up online, on the fly, to that WLAN, in the case where no previously known or preferred WLANs were available to allow secure connection.

This is made possible by adding configuration capability to a Cisco WLC to allow clients to connect to an Online Sign-Up (OSU) server and obtain WPA2-Enterprise credentials to perform their subsequent authentication with the secure Passpoint 2.0 WLAN.

For more information, see the Configuring Mobile Concierge chapter in the *Cisco Wireless Controller Configuration Guide*.

Bonjour Gateway on Cisco 2504 WLC

Limited Bonjour gateway is supported on Cisco 2504 WLC with support for up to 200 instance services.

Increased Channel and Tx Power Support for Various Countries

To maximize the amount of channels supported and transmit power that is specified in the wireless regulations, the following changes are made in the regulatory domains:

Table 3 Regulatory Domain Change

Domain Change	Country	AP Type	Details	
–E to –S	Thailand Vietnam	Indoor and Outdoor	**–E Indoor**	**–S Indoor**
			2412-2472 MHz, 20 dBm EIRP	2412-2472 MHz, 20 dBm EIRP
			5180-5320 MHz, 23 dBm EIRP	5180-5320 MHz, 23 dBm EIRP
			5500-5700 MHz, 30 dBm EIRP	5500-5700 MHz, 30 dBm EIRP
				5745-5825 MHz, 30 dBm EIRP
			–E Outdoor	**–S Outdoor**
			2412-2472 MHz, 20 dBm EIRP	2412-2472 MHz, 20 dBm EIRP
			5500-5700 MHz, 30 dBm EIRP	5500-5700 MHz, 30 dBm EIRP
				5745-5825 MHz, 30 dBm EIRP
–C to –S	Macau	Indoor	**–C Indoor**	**–S Indoor**
			5745-5825 MHz, 30 dBm EIRP	2412-2472 MHz, 20 dBm EIRP
				5180-5320 MHz, 23 dBm EIRP
				5500-5700 MHz, 30 dBm EIRP
				5745-5825 MHz, 30 dBm EIRP
–N to –S[1]	Hong Kong	Outdoor	**–N Outdoor**	**–S Outdoor**
			2412-2472 MHz, 36 dBm EIRP	2412-2472 MHz, 20 dBm EIRP
			5745-5825 MHz, 36 dBm EIRP	5500-5700 MHz, 30 dBm EIRP
				5745-5825 MHz, 30 dBm EIRP

1. –S APs will work with the lower Tx power; –N will continue to use the higher power

Platforms Supported

- Indoor
  - Cisco Aironet 3700 Series Access Points
  - Cisco Aironet 2700 Series Access Points
  - Cisco Aironet 1830 and 1850 Access Points

Note The 1830 and 1850 APs already support the domain change for Thailand and Vietnam. In Release 8.2, the APs support the domain change for Macau.

  - Cisco Aironet 1700 Series Access Points
  - Cisco Aironet 700i and 700w Access Points
- Outdoor

- Cisco Aironet 1570 Series Access Points
- Cisco Aironet 1530 Series Access Points

Universal PIDs Supported

- Indoor
  - Cisco Aironet 3700 Series Access Points
  - Cisco Aironet 2700 Series Access Points
  - Cisco Aironet 1830 and 1850 Access Points

Note Supports Macau changes from –C to –S domain.

  - Cisco Aironet 700i and 700w Access Points
- Outdoor
  - Cisco Aironet 1530 Series Access Points

Legacy APs

- Changes made in Cisco WLC to support –S domain for Hong Kong, Macau, Thailand, and Vietnam.
- Changes made in Cisco WLC to support –I domain for Algeria
- Previously supported domains can continue to associate with Cisco WLC and be supported in addition to the new domain APs.

Upgrade and Downgrade Scenarios

- When you upgrade to Release 8.2, the regular SKU APs will continue to associate with the Cisco WLC and be operational with both the radios.
- If a Cisco WLC is downgraded from Release 8.2, the indoor APs deployed in Hong Kong, Thailand, Vietnam, and Macau with –S domain and APs deployed in Algeria with –I domain will continue to associate with Cisco WLCs. However, the 802.11a radio will not be operational.

Increased Country Code Support

In Release 8.2, you can configure up to 110 country codes per Cisco WLC. Prior to Release 8.2, you could configure up to 20 country codes per Cisco WLC.

Security Update

Support for Transport Layer Security (TLS) v1.2 is added in Release 8.2.

The following are supported for web authentication and WebAdmin based on the configuration:

- TLSv1.2
- TLSv1.0
- SSLv3
- SSLv2

Note DTLSv1.2 for CAPWAP is not supported.

QoS Mapping

The QoS Mapping feature maintains the QoS policies in situations where appropriate QoS markings that match the application type are not marked by clients or applications. The administrator maps the differentiated services code point (DSCP) to user-priority values in a Cisco WLC, which in turn provides better experience to users while using certain applications, such as voice or video applications.

For more information, see the Configuring QoS Mapping section in the *Cisco Wireless Controller Configuration Guide*.

Cisco Industrial Wireless 3702 Access Point Updates

- Flexible Antenna Port Support—The Cisco IW 3702 AP model with external antennas can operate in the 2.4-GHz and 5.0-GHz band in one of two antenna band modes.

  In the single-band mode:

  - the 5-GHz radio uses antenna ports C and D, each with a single band antenna
  - the 2.4-GHz radio uses antenna ports A and B, each with a single band antenna

  In the dual-band mode, four dual-band antennas are used and both the radios share these antennas.
- Daisy chaining is supported (support introduced in Release 8.1.111.0)

Software Release Support for Access Points

Table 4 lists the Cisco WLC software releases that support specific Cisco access points. The First Support column lists the earliest Cisco WLC software release that supports the corresponding access point. For APs that are not supported in ongoing releases, the Last Support column lists the last release that supports the corresponding APs.

Note Third-party antennas are not supported with Cisco indoor APs.

Table 4 Software Support for Access Points

Access Points		First Support	Last Support
700 Series	AIR-CAP702I-x-K9	7.5.102.0	—
	AIR-CAP702I-xK910	7.5.102.0	—
700W Series	AIR-CAP702Wx-K9	7.6.120.0	—
	AIR-CAP702W-xK910	7.6.120.0	—

Table 4 Software Support for Access Points (continued)

Access Points		First Support	Last Support
1000 Series	AIR-AP1010	3.0.100.0	4.2.209.0
	AIR-AP1020	3.0.100.0	4.2.209.0
	AIR-AP1030	3.0.100.0	4.2.209.0
	Airespace AS1200	—	4.0
	AIR-LAP1041N	7.0.98.0	—
	AIR-LAP1042N	7.0.98.0	—
1100 Series	AIR-LAP1121	4.0.155.0	7.0.x
1130 Series	AIR-LAP1131	3.1.59.24	8.0.x
1140 Series	AIR-LAP1141N	5.2.157.0	—
	AIR-LAP1142N	5.2.157.0	—
1220 Series	AIR-AP1220A	3.1.59.24	7.0.x
	AIR-AP1220B	3.1.59.24	7.0.x
1230 Series	AIR-AP1230A	3.1.59.24	7.0.x
	AIR-AP1230B	3.1.59.24	7.0.x
	AIR-LAP1231G	3.1.59.24	7.0.x
	AIR-LAP1232AG	3.1.59.24	7.0.x
1240 Series	AIR-LAP1242G	3.1.59.24	8.0.x
	AIR-LAP1242AG	3.1.59.24	8.0.x
1250 Series	AIR-LAP1250	4.2.61.0	8.0.x
	AIR-LAP1252G	4.2.61.0	8.0.x
	AIR-LAP1252AG	4.2.61.0	8.0.x
1260 Series	AIR-LAP1261N	7.0.116.0	—
	AIR-LAP1262N	7.0.98.0	—
1300 Series	AIR-BR1310G	4.0.155.0	7.0.x
1400 Series	Standalone Only	—	—
1600 Series	AIR-CAP1602I-x-K9	7.4.100.0	—
	AIR-CAP1602I-xK910	7.4.100.0	—
	AIR-SAP1602I-x-K9	7.4.100.0	—
	AIR-SAP1602I-xK9-5	7.4.100.0	—
	AIR-CAP1602E-x-K9	7.4.100.0	—
	AIR-SAP1602E-xK9-5	7.4.100.0	—
1700 Series	AIR-CAP1702I-x-K9	8.0.100.0	—
	AIR-CAP1702I-xK910	8.0.100.0	—
1830 Series	AIR-AP1832I-UXK9	8.1.120.0	—
	AIR-AP1832I-x-K9	8.1.120.0	—

Table 4 Software Support for Access Points (continued)

Access Points		First Support	Last Support
1850 Series	AIR-AP1852I-UXK9	8.1.111.0	—
	AIR-AP1852I-UXK910	8.1.111.0	—
	AIR-AP1852I-UXK9C	8.1.111.0	—
	AIRAP1852I-UXK910C	8.1.111.0	—
	AIR-AP1852E-UXK9	8.1.111.0	—
	AIR-AP1852E-UXK910	8.1.111.0	—
	AIR-AP1852E-UXK9C	8.1.111.0	—
	AIRAP1852E-UXK910C	8.1.111.0	—
	AIR-AP1852E-x-K9	8.1.111.0	—
	AIR-AP1852E-x-K9C	8.1.111.0	—
	AIR-AP1852I-x-K9	8.1.111.0	—
	AIR-AP1852I-x-K9C	8.1.111.0	—
AP801	—	5.1.151.0	8.0.x
AP802	—	7.0.98.0	—
AP802H	—	7.3.101.0	—
AP803	—	8.1.120.0	—
ASA5506W-AP702	—	8.1.120.0	—
2600 Series	AIR-CAP2602I-x-K9	7.2.110.0	—
	AIR-CAP2602I-xK910	7.2.110.0	—
	AIR-SAP2602I-x-K9	7.2.110.0	—
	AIR-SAP2602I-x-K95	7.2.110.0	—
	AIR-CAP2602E-x-K9	7.2.110.0	—
	AIR-CAP2602E-xK910	7.2.110.0	—
	AIR-SAP2602E-x-K9	7.2.110.0	—
	AIR-SAP2602E-x-K95	7.2.110.0	—
2700 Series	AIR-CAP2702I-x-K9	7.6.120.0	—
	AIR-CAP2702I-xK910	7.6.120.0	—
	AIR-CAP2702E-x-K9	7.6.120.0	—
	AIR-CAP2702E-xK910	7.6.120.0	—
	AIR-AP2702I-UXK9	8.0.110.0	—
3500 Series	AIR-CAP3501E	7.0.98.0	—
	AIR-CAP3501I	7.0.98.0	—
	AIR-CAP3502E	7.0.98.0	—
	AIR-CAP3502I	7.0.98.0	—
	AIR-CAP3502P	7.0.116.0	—

Table 4 Software Support for Access Points (continued)

Access Points		First Support	Last Support
3600 Series[1]	AIR-CAP3602I-x-K9	7.1.91.0	—
	AIR-CAP3602I-xK910	7.1.91.0	—
	AIR-CAP3602E-x-K9	7.1.91.0	—
	AIR-CAP3602E-xK910	7.1.91.0	—
	USC5101-AI-AIR-K9	7.6	—
3700 Series	AIR-CAP3702I	7.6	—
	AIR-CAP3702E	7.6	—
	AIR-CAP3702P	7.6	—
600 Series	AIR-OEAP602I	7.0.116.0	—
1500 Mesh Series	AIR-LAP-150	3.1.59.24	4.2.207.54M
	AIR-LAP-1510	3.1.59.24	4.2.207.54M

Table 4 Software Support for Access Points (continued)

Access Points		First Support	Last Support
1520 Mesh Series	AIR-LAP1522AG	-A and N: 4.1.190.1 or 5.2 or later[2]	8.0.x
		All other reg. domains: 4.1.191.24M or 5.2 or later[1]	8.0.x
	AIR-LAP1522HZ	-A and N: 4.1.190.1 or 5.2 or later[1]	8.0.x
		All other reg. domains: 4.1.191.24M or 5.2 or later[1]	8.0.x
	AIR-LAP1522PC	-A and N: 4.1.190.1 or 5.2 or later[1]	8.0.x
		All other reg. domains: 4.1.191.24M or 5.2 or later[1]	8.0.x
	AIR-LAP1522CM	7.0.116.0 or later.	8.0.x
	AIR-LAP1524SB	-A, C and N: 6.0 or later	8.0.x
		All other reg. domains: 7.0.116.0 or later.	8.0.x
	AIR-LAP1524PS	-A: 4.1.192.22M or 5.2 or later[1]	8.0.x
1530	AIR-CAP1532I-x-K9	7.6	—
	AIR-CAP1532E-x-K9	7.6	—
1550	AIR-CAP1552C-x-K9	7.0.116.0	—
	AIR-CAP1552E-x-K9	7.0.116.0	—
	AIR-CAP1552H-x-K9	7.0.116.0	—
	AIR-CAP1552I-x-K9	7.0.116.0	—
	AIR-CAP1552EU-x-K9	7.3.101.0	—
	AIR-CAP1552CU-x-K9	7.3.101.0	—
	AIR-CAP1552WU-x-K9	8.0.100.0	—

Table 4 Software Support for Access Points (continued)

Access Points		First Support	Last Support
1552S	AIR-CAP1552SA-x-K9	7.0.220.0	—
	AIR-CAP1552SD-x-K9	7.0.220.0	—
1570	AIR-AP1572EAC-x-K9	8.0.110.0	—
	AIR-AP1572ICy[3]-x-K9	8.0.110.0	—
	AIR-AP1572ECy-x-K9	8.0.110.0	—
IW3700	IW3702-2E-UXK9	8.0.120.0	—
	IW3702-4E-UXK9	8.0.120.0	—

1. The Cisco 3600 AP was introduced in Cisco Wireless Release 7.1.91.0. If your network deployment uses Cisco 3600 APs with Cisco Wireless Release 7.1.91.0, we highly recommend that you upgrade to Cisco Wireless Release 7.2.115.2 or a later release.
2. These access points are supported in a separate 4.1.19x.x mesh software release and in Release 5.2 or later releases. These access points are not supported in the 4.2, 5.0, and 5.1 releases.
3. y—Country DOCSIS Compliance, see ordering guide for details.

Software Release Types and Recommendations

This section contains the following topics:

Release Types

Table 5 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 LAN controller and access point testing in real-world use cases with a variety of mobile client devices applicable in a specific industry.

Software Release Recommendations

Table 6 Software Release Recommendations

Type of Release	Deployed Release	Recommended Release
Maintenance Deployment (MD) releases	7.0 MD release train (latest release: 7.0.252.0)	7.4 MD release train (7.4.140.0 is the MD release)
Early Deployment (ED) releases for pre-802.11ac deployments	7.2 ED releases 7.3 ED releases	7.4 MD release train (7.4.140.0 is the MD release)
Early Deployment (ED) releases for 802.11ac deployments	7.5 ED release 7.6 ED release	8.0 ED release (8.0.121.0 is 8.0MR2 on the 8.0 release train)

For detailed release recommendations, see the software release bulletin:

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

For more information about the Cisco Wireless solution compatibility matrix, see http://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html.

Upgrading to Cisco WLC Software Release 8.2.100.0

Guidelines and Limitations

- After upgrading to Release 8.2, the Cisco WLC might lose all IPv4 connectivity. The Cisco WLC can no longer service incoming SSH/Web sessions and is unable to ping other IPv4 stations. However, the default router is able to ping the Cisco WLC's management interface.

  Every 10 seconds, a message similar to the following is sent to the msglog:

  ```
  *dtlArpTask: Jan 06 23:50:37.312: %OSAPI-4-GW_ADD_FAILED: osapi_net.c:1032 Unable to add the gateway 192.168.145.1. System command returned failure. Errorcode:256
  ```

  This occurs in the following conditions:

  a. LAG is not configured.

  b. The management interface is untagged and is mapped to one physical port.

  c. When an untagged dynamic interface is added and mapped to port 2, the default route for the management interface is lost.

  The workaround is to configure all interfaces with VLANs.

  You can track this issue via CSCux75436.

- Effective with Release 8.2.100.0, you cannot 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 7 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
Cisco 2504 WLC	Only multicast mode is supported.		
Cisco vWLC	Multicast is not supported.		

- In Release 8.2, the **reload** command is not recognized by Cisco Aironet 3600 Series APs. The workaround is to use the **debug capwap console cli** command.
- Cisco WLC Release 7.3.112.0, which is configured for new mobility, might revert to old mobility after upgrading to Release 7.6, even though Release 7.6 supports new mobility. This issue occurs when new mobility, which is compatible with the Cisco 5760 Wireless LAN Controller and the Cisco Catalyst 3850 Series Switch, are in use. However, old mobility is not affected.

  The workaround is as follows:

  a. Enter the following commands:

  ```
  config boot backup
  show boot

  Primary Boot Image.................. 7.6.100.0
  Backup Boot Image................... 7.3.112.0 (default) (active)
  ```

  b. After the reboot, press **Esc** on the console, and use the boot menu to select **Release 7.6**.

  c. After booting on Release 7.6, set back the primary boot, and save the configuration by entering the following command:

  config boot primary

Note The epings are not available in the Cisco 5500 Series WLC when New Mobility is enabled.

Note If you downgrade from a Cisco WLC release that supports new mobility to a Cisco WLC release that does not support new mobility, for example, Cisco Wireless Release 7.6 to Release 7.3.x and you download the 7.6 configuration file with new mobility in enabled state, the release that does not support new mobility will have the new mobility feature in enabled state.

- If you downgrade from Release 8.2.100.0 to a 7.x release, the trap configuration is lost and must be reconfigured.
- 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 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 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 8.2.100.0, 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 8.2.100.0.

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 request that is intercepted by the Cisco WLC is fragmented, the Cisco WLC drops the packet because the HTTP request does not contain enough information required for redirection.
- 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 8.2.100.0 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 8.2.100.0. Table 8 shows the upgrade path that you must follow before downloading Release 8.2.100.0.

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 8 Upgrade Path to Cisco WLC Software Release 8.2.100.0

Current Software Release	Upgrade Path to 8.2.100.0 Software
7.0.x releases	You can upgrade directly to 8.2.100.0. **Note** If you have VLAN support and VLAN mappings defined on H-REAP access points and are currently using a 7.0.x Cisco WLC software release that is earlier than 7.0.240.0, we recommend that you upgrade to the 7.0.240.0 release and then upgrade to 8.2.100.0 to avoid losing those VLAN settings. **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.
7.1.91.0	You can upgrade directly to 8.2.100.0.

Table 8 Upgrade Path to Cisco WLC Software Release 8.2.100.0 (continued)

Current Software Release	Upgrade Path to 8.2.100.0 Software
7.2.x releases	You can upgrade directly to 8.2.100.0. **Note** If you have an 802.11u HotSpot configuration on the WLANs, we recommend that you first upgrade to the 7.3.101.0 Cisco WLC software release and then to the 8.2.100.0 Cisco WLC software release. You must downgrade from the 8.2.100.0 Cisco WLC software release to a 7.2.x Cisco WLC software release if you have an 802.11u HotSpot configuration on the WLANs that are not supported.
7.3.x releases	You can upgrade directly to 8.2.100.0.
7.4.x releases	You can upgrade directly to 8.2.100.0.
7.5.x releases	You can upgrade directly to 8.2.100.0.
7.6.x	You can upgrade directly to 8.2.100.0.
8.0.x	You can upgrade directly to 8.2.100.0.
8.1.x	You can upgrade directly to 8.2.100.0.

- When you upgrade the Cisco WLC to an intermediate software release, you must wait until all of the access points that are associated with the Cisco WLC are upgraded to the intermediate release before you install the latest Cisco WLC software. In large networks, it can take some time to download the software on each access point.
- You can upgrade to a new release of the Cisco WLC software or downgrade to an earlier release even if Federal Information Processing Standard (FIPS) is enabled.
- When you upgrade to the latest software release, the software on the access points associated with the Cisco WLC is also automatically upgraded. When an access point is loading software, each of its LEDs blinks in succession.
- We recommend that you access the Cisco WLC GUI using Microsoft Internet Explorer 10 or a later version or Mozilla Firefox 32 or a later version.

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

- Cisco WLCs support standard SNMP MIB files. MIBs can be downloaded from the Software Center on Cisco.com.

- The Cisco WLC software is factory installed on your Cisco WLC and is automatically downloaded to the access points after a release upgrade and whenever an access point joins a Cisco WLC. We recommend that you install the latest software version available for maximum operational benefit.
- Ensure that you have a TFTP, FTP, or SFTP server available for the software upgrade. Follow these guidelines when setting up a server:
  - Ensure that your TFTP server supports files that are larger than the size of Cisco WLC software Release 8.2.100.0. 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 8.2.100.0 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*.

Note Predownloading Release 8.2.100.0 on a Cisco Aironet 1240 access point is not supported when upgrading from a previous Cisco WLC release. If predownloading is attempted on a Cisco Aironet 1240 access point, an AP disconnect will occur momentarily.

- 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 8.2.100.0 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

Upgrading to Cisco WLC Software Release 8.2.100.0 (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 8.2.100.0 software:

a. Click this URL to go to the Software Center:

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
- 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).

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 Disable the WLANs on the Cisco WLC.

Step 6 Choose **Commands** > **Download File** to open the Download File to Controller page.

Step 7 From the **File Type** drop-down list, choose **Code**.

Step 8 From the **Transfer Mode** drop-down list, choose **TFTP**, **FTP**, or **SFTP**.

Step 9 In the **IP Address** text box, enter the IP address of the TFTP, FTP, or SFTP server.

Step 10 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 11 In the **File Path** text box, enter the directory path of the software.

Step 12 In the **File Name** text box, enter the name of the software file (*filename*.aes).

Step 13 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 14 Click **Download** to download the software to the Cisco WLC.

A message appears indicating the status of the download.

Step 15 After the download is complete, click **Reboot**.

Step 16 If you are prompted to save your changes, click **Save and Reboot**.

Step 17 Click **OK** to confirm your decision to reboot the Cisco WLC.

Step 18 Re-enable the WLANs.

Step 19 For Cisco WiSM2 on the Catalyst switch, check the port channel and re-enable the port channel if necessary.

Step 20 If you have disabled the 802.11a/n and 802.11b/g/n networks in Step 4, re-enable them.

Step 21 To verify that the 8.2.100.0 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.

Special Notes for Licensed Data Payload Encryption on Cisco Wireless LAN Controllers

Datagram Transport Layer Security (DTLS) is required for all Cisco 600 Series OfficeExtend Access Point deployments to encrypt data plane traffic between the APs and the Cisco WLC. You can purchase Cisco Wireless LAN Controllers with either DTLS that is enabled (non-LDPE) or disabled (LDPE). If DTLS is disabled, you must install a DTLS license to enable DTLS encryption. The DTLS license is available for download on Cisco.com.

Important Note for Customers in Russia

If you plan to install a Cisco Wireless LAN Controller in Russia, you must get a Paper PAK, and not download the license from Cisco.com. The DTLS Paper PAK license is for customers who purchase a Cisco WLC with DTLS that is disabled due to import restrictions, but have authorization from local regulators to add DTLS support after the initial purchase. Refer to your local government regulations to ensure that DTLS encryption is permitted.

Note Paper PAKs and electronic licenses that are available are outlined in the respective Cisco WLC platform data sheets.

Downloading and Installing a DTLS License for an LDPE Cisco WLC

Step 1 To download the Cisco DTLS license:

a. Go to the Cisco Software Center at this URL:

https://tools.cisco.com/SWIFT/LicensingUI/Home

b. From the Product License Registration page from the **Get Other Licenses** drop-down list, click **IPS, Crypto, Other ...**.

c. In the **Wireless** section, click **Cisco Wireless Controllers (2500/5500/7500/WiSM2) DTLS License** and click **Next**.

d. Follow the on-screen instructions to generate the license file. The license file information will be sent to you in an e-mail.

Step 2 Copy the license file to your TFTP server.

Step 3 Install the DTLS license either by using the Cisco WLC web GUI interface or the CLI:

- To install the license using the WLC web GUI, choose:

  Management > Software Activation > Commands > Action: **Install License**

- To install the license using the CLI, enter this command:

  license install tftp:*//ipaddress /path /extracted-file*

  After the installation of the DTLS license, reboot the system. Ensure that the DTLS license that is installed is active.

Upgrading from an LDPE to a Non-LDPE Cisco WLC

Step 1 Download the non-LDPE software release:

a. Go to the Cisco Software Center at:

http://www.cisco.com/cisco/software/navigator.html?mdfid=282585015&i=rm

b. Choose the Cisco WLC model.

c. Click **Wireless LAN Controller Software**.

d. In the left navigation pane, click the software release number for which you want to install the non-LDPE software.

e. Choose the non-LDPE software release: AIR-X-K9-X-X.X.aes

f. Click **Download**.

g. Read the Cisco End User Software License Agreement and then click **Agree**.

h. Save the file to your hard drive.

Step 2 Copy the Cisco WLC software file (*filename*.aes) to the default directory on your TFTP server or FTP server.

Step 3 Upgrade the Cisco WLC with this version by performing Step 3 through Step 21 detailed in the "Upgrading to Cisco WLC Software Release 8.2.100.0" section on page 21.

Interoperability with Other Clients

This section describes the interoperability of Cisco WLC Software, Release 8.2.100.0 with other client devices.

Table 9 describes the configuration used for testing the client devices.

Table 9 Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	8.2.100.0
Cisco WLC	Cisco 55xx Series Controller
Access points	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 4.2, ACS 5.2
Types of tests	Connectivity, traffic, and roaming between two access points

Table 10 lists the client types on which the tests were conducted, including laptops, handheld devices, phones, and printers.

Table 10 Client Types

Client Type and Name	Version
Laptop	
Intel 4965	v13.4
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	17.16.0.4
Intel 7265	17.16.0.4
Intel 3160	17.16.0.4
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)	
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 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 10.11.1
MacBook Air old	OSX 10.11.1
MacBook Air new	OSX 10.11.1
Macbook Pro with Retina Display	OSX 10.11.1
Macbook New 2015	OSX 10.11.1
Tablets	
Apple iPad2	iOS 9.1(13B143)

Table 10 Client Types (continued)

Client Type and Name	Version
Apple iPad3	iOS 9.1(13B143)
Apple iPad mini with Retina display	iOS 9.1(13B143)
Apple iPad Air	iOS 9.1(13B143)
Apple iPad Air 2	iOS 9.1(13B143)
Samsung Galaxy Tab Pro SM-T320	Android 4.4.2
Samsung Galaxy Tab 10.1- 2014 SM-P600	Android 4.4.2
Samsung Galaxy Note 3 - SM-N900	Android 5.0
Microsoft Surface Pro 3	Windows 8.1 Driver: 15.68.3073.151
Microsoft Surface Pro 2	Windows 8.1 Driver: 14.69.24039.134
Google Nexus 9	Android 6.0
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 MC75	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
Ascom i75	1.8.0
Spectralink 8030	119.081/131.030/132.030
Apple iPhone 4S	iOS 9.1(13B143)
Apple iPhone 5	iOS 9.1(13B143)
Apple iPhone 5s	iOS 9.1(13B143)
Apple iPhone 5c	iOS 9.1(13B143)
Apple iPhone 6	iOS 9.1(13B143)
Apple iPhone 6 Plus	iOS 9.1(13B143)
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
Nexus 6	Android 5.1.1

Table 10 Client Types (continued)

Client Type and Name	Version
Samsung Galaxy S5-SM-G900A	Android 4.4.2
Huawei Ascend P7	Android 4.4.2
Samsung Galaxy S III	Android 4.3
SpectraLink 8450	3.0.2.6098/5.0.0.8774
Samsung Galaxy Nexus GTI9200	Android 4.4.2
Samsung Galaxy Mega SM900	Android 4.4.2
Samsung Galaxy S6	Android 5.1.1

Features Not Supported on Cisco WLC Platforms

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

- Features Not Supported on Cisco 2504 WLC, page 34
- Features Not Supported on Cisco WiSM2 and Cisco 5508 WLC, page 35
- Features Not Supported on Cisco Flex 7510 WLCs, page 35
- Features Not Supported on Cisco 5520, 8510, and 8540 WLCs, page 36
- Features Not Supported on Cisco Virtual WLCs, page 36
- Features Not Supported on Mesh Networks, page 37

Note In a converged access environment that has Cisco WLCs running AireOS code, High Availability Client SSO and native IPv6 are not supported.

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.

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

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.

- TrustSec SXP
- 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

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.

Features Not Supported on Cisco Virtual WLCs

- Cisco Aironet 1850 and 1830 Series APs
- Internal DHCP server
- TrustSec SXP
- Access points in local mode
- Mobility/Guest Anchor
- 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.

- 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

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

Features Not Supported on Access Point Platforms

- Features Not Supported on Cisco Aironet 1830 and 1850 APs, page 37
- Features Not Supported on Cisco Aironet 1550 APs (with 64-MB Memory), page 38

Features Not Supported on Cisco Aironet 1830 and 1850 APs

- Cisco Virtual Wireless Controller
- Mesh mode
- Flex mode
- Monitor mode
- Workgroup Bridge (WGB) mode
- OfficeExtend mode
- Enhanced Local Mode (ELM)
- Integrated BLE
- Basic spectrum analysis
- USB-based Bluetooth Low Energy (BLE) device support
- Cisco CleanAir
- Cisco Wireless ClientLink 3.0
- Rogue Location Discovery Protocol (RLDP)
- Cisco Compatible eXtensions (CCX) Specification
- 802.1x supplicant for AP authentication on the wired port
- Static WEP key for TKIP or CKIP

- Dynamic Transmit Power Control (DTPC)
- Federal Information Processing Standard (FIPS) and Common Criteria
- 40-MHz Rogue detection
- Native IPv6
- Telnet

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

Features Not Supported on Cisco Aironet 1550 APs (with 64-MB Memory)

- PPPoE
- PMIPv6

Note To see the amount of memory in a Cisco Aironet 1550 AP, enter the following command:

```
(Cisco Controller) >show mesh ap summary
```

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://tools.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

Identifier	Description
CSCux59615	8.2.100.0 has incorrect Build Name
CSCux15561	Cisco 3500 AP/Cisco 1260 AP gets into “ap:” mode after power cycle
CSCux21159	Autonomous Bridge—PSK corruption after non-root Bridge reboots
CSCux14242	HTTP profiling support for Cisco 1850 AP
CSCuv51142	SCTG ST: Module reboots after sending LTE data of more than 1300 bytes
CSCux20138	Cisco 3602 AP memory leak at processor pool. Needs reboot to join Cisco WLC
CSCuw36523	AP crashdump validate_memory during Cisco WLC upgrade or downgrade operation
CSCuu63964	02044802: Apple clients cannot reconnect Cisco 1850i AP on forceful deauthentication
CSCux28011	DNS-ACL feature not working with Cisco 1850 AP
CSCuv61089	Cisco AP is duplicating packets to wireless clients and Cisco WLC
CSCur68316	Cisco 802AP-891 in FlexConnect mode are losing VLAN mapping after power cycle
CSCux17645	Mobility Express: Radio failure (firmware stopped responding) during upgrade from Cisco Wireless Release 8.1.131.0 to Cisco Wireless Release 8.2
CSCux02417	OTA and OTDS roaming performance does not meet 50-millisecond benchmark
CSCuw84036	LWAP FlexConnect mode generates traffic blackholing upon WGB PMC cache timeout
CSCux31277	Missing Carrier set on 2.4-Ghz radio for AP803H-AGN-Z-K9
CSCut80914	SC3 mesh: Low uplink throughput from MAP1 with 80-MHz client [BZ1142]
CSCux12825	Cisco 1850 AP is doing ping to 8.8.8.8
CSCux12878	Cisco 1850 AP is trying to contact Meraki server
CSCuq76115	WGB clients with DSCP marking to QoS queue mapping does not work on ISR819
CSCux11777	Cisco 1532 AP non-root bridge high retransmission and latency rate
CSCuw30644	Cisco 702W AP 2.4-GHz radio showing low to no throughput at random times
CSCuw65706	Cisco 1530 AP WGB drops Tx used with other 1530 WGB in the same MAC address range
CSCuw29564	Cisco APs show 0 neighbors on the 5-GHz band and client 802.11 packets are ignored
CSCuv32179	Low throughput with 3700 WGB 80 MHz
CSCuu11133	Wi-Fi TCP downlink degraded with SCTP module traffic
CSCux07090	AP CRASH watchdog reset (wcpd no heartbeat) coredump: process wcpd
CSCuw41092	Cisco AP does not send traffic indication in beacon for power-save client after FT
CSCux06806	ATF EnforcementConfig for network radio is not pushed to uploaded config
CSCux21420	Cisco WiSM2 stops responding under Task name: redXmlTransferMain
CSCux18548	Inter-WLC roaming is not successful for EoGRE tunnel

Table 11 Open Caveats (continued)

Identifier	Description
CSCuw97966	10G link down after reboot on Cisco 8510 WLC on Nexus 5k
CSCuv03963	Multiple Cisco 8510 WLCs using Cisco Wireless Release 8.0110.x DP stopped responding
CSCux28505	Cisco 8510 WLC stopped responding with "fp_main_task" on a Cisco Wireless Release 8.2.x image
CSCuw43910	Local switching/local authentication clients drop when latency is introduced
CSCux21803	Client does not receive broadcast ARP request after AP failover
CSCux26911	Cisco WLC stopped responding on the **config flexconnect arp-caching** command
CSCux00531	Cisco 2504 and 5508 WLCs have partial collection failure file transfer config
CSCux13657	Roaming of Mesh AP via backhaul is no longer working on 2.4-GHz client
CSCux22286	snmpset clMeshNodeRAPDownlinkBackhaul get-response is the old value
CSCux00803	New Mobility clients stuck in DHCP_REQD state with NAT IP on Foreign WLC
CSCuw14938	New Mobility system does not respond on Task Name mmMaListen
CSCuw95402	SNMP does not return correct information for roaming client
CSCuw93917	NetFlow configuration cannot be modified after downgrading from Release 8.2 to Release 8.1
CSCux05901	Cisco 5508 WLC does not honor AAA override for upload bandwidth for web authentication
CSCux28768	Cisco 1142 AP radios appear to be operational on CLI but down on Cisco WLC (clients cannot connect)
CSCux17026	Frequent channel changes on 40-MHz DCA
CSCuw36069	Threshold MIBs incorrectly set for WSSI modules
CSCux14487	Cisco WLC becomes unresponsive during 802.11b advanced config is loading through CLI
CSCux22620	Cisco 8510 WLC stops responding in radiusTransportThread system task
CSCuw94949	ME: Invalid FTIE MIC on ME WLC when client tries FT roam between IOS APs
CSCux20608	Cisco WLC becomes unresponsive when entering long PSK for IPsec via WebUI
CSCux20592	Cisco WLC needs X.509v3 certificate revocation checking for IPsec
CSCux28814	AP priming information is lost on power outage
CSCuw70505	System unresponsive while accessing FlexConnect AVC statistics
CSCuw98120	Master AP not shown in GUI when added via CLI
CSCux24989	ME: Schedule later time stamp should have been preserved on screen
CSCux25466	Monitor/Clients display does not show subsequent pages on GUI
CSCux30086	Sanity: Unable to click Start button in ME Day-0 admin/login account page
CSCux22140	Security policy is shown as disabled for wpapsk rogue AP's in GUI
CSCux27149	Wired and Wireless Day 0 is not working simultaneously
CSCus69131	Client is stuck on DHCP_REQ when switching from802.1x SSID to CWA SSID
CSCuw50867	show invalid-config, ap mgmtuser invalid config

Table 11 Open Caveats (continued)

Identifier	Description
CSCuu09701	Clients with static IP stuck in DHCP required state in ME WLC
CSCuw98460	ImageSchedule later, ME does not reboot if set reboot time is less than upgrade time
CSCux12392	ME: Configs are not pushed in a particular instance
CSCux23944	ME: DNS lookup failed for NTP server after ME WLC (1850) reboot
CSCux23710	IW3702: LED status observed behavior inconsistent with user guide

Resolved Caveats

Table 12 Resolved Caveats

Identifier	Description
CSCuv99415	Access Point should boot up even if CAPWAP IOS download is corrupted
CSCuv41888	Cisco AP 1570 RCV153-3-JA3/JA4 image sends Bridge Protocol Data Units to the network
CSCuv03380	During Mesh Roam security error, Gateway is not reachable leading to CAPWAP Restart
CSCuu17338	Cisco AP 1142 Configuration loss occurs after cold reboot
CSCur76547	Access Point with static Internet Protocol configured behavior is seen in Dynamic Host Configuration Protocol (DHCP) client after reload
CSCuv40330	Deb CAPWAP shows IPv6 addresses incorrectly
CSCut86489	RADIUIS on Cisco WLC shows DOWN but is UP on the Access Points with Queue already full
CSCuv93051	Access Point unexpected reload seen due to ‘Signature Validation Failed’
CSCuv36306	Cisco AP 2702 In Monitor Mode sensord_crash File No CleanAir mSMTS
CSCuv33747	Cisco AP 3600 ‘Tx jammed’ error is seen and radio is reset due to sensord stuck
CSCuu01474	“dot11 ant-band-mode” CLI is not present in 1570 AP
CSCus78002	Cisco AP1262 unexpected reload is seen right after STACKLOW for Dot11 DB Audit
CSCut82091	Cisco AP-3702/3602/1602 unexpected reload is seen with this Process: “CAPWAP CLIENT”
CSCuw36636	Cisco Access Point shows no RST code when DFS triggers
CSCuv61271	Window DHCP BAD_ADDRESS displays for Access Points
CSCuv81004	Autonomous Access Point fails to create MCST key with single SSID multi VLAN AAA
CSCuv02592	Gig1 configuration is not restored when Access Point is reloaded on 2700/1700 APs
CSCus91214	Cisco AP802 15.3(3)JAB unexpectedly reloads always on issuing “dir all-filesystems” ISR C881W
CSCuw88703	Unable to start host pad after enable/disable Access Point
CSCuo95728	Cisco Access Point not validating UDP-Lite checksum

Table 12 Resolved Caveats (continued)

Identifier	Description
CSCut23325	Cisco 1700 AP not encrypting Internet Control Message Protocol (ICMP) and Address Resolution Protocol (ARP) sent from the client over the air
CSCuv54033	Egress Access Control List (ACL) not working when it is switched from Ingress to Egress
CSCuv86360	Error code mismatch on the Access Point during the debugs for Access Control List (ACL) is not found
CSCur58057	Flex Access Point loses some Wireless Local Area Networks (WLAN)s after radio resets
CSCuw61901	Local Auth Extensible Authentication (EAP)-Flexible Authentication via Secure Tunneling (FAST) not working for Flex AP Auth user with any connect
CSCuw28531	Network Address Translation (NAT) is not working with two different Wireless Local Area Networks (WLANs) in PPPoE submode
CSCut40485	Spurious messages seen on Access Point console
CSCuv08570	Cisco 1532 AP loses all configuration at times after power cycle
CSCuw02551	UX Access Point cannot use 80mhz bandwidth
CSCut40592	AC Rates are missing when speed set through GUI
CSCut85027	Cisco Access Point is generating corrupted core dump
CSCuw27198	Clarify debug dfs simulate command on Lightweight Access Point Protocol (LWAP)
CSCut68661	Cisco Access Point crash AP702 - ar9300_set_desc_link is seen
CSCur85640	8.1.10.72 - Access Points reboot with background scanning enabled after show ver command
CSCuu22083	Access Point unexpected reload is seen in MESH ASTools PROCESS during mesh initialization
CSCuu31357	Access Point unexpected reload is seen in [Adj Process] for VW-ap1530.cc6c.map2
CSCut81253	Ethernet Bridging does not work on Returned Accounts Procedure (RAP) with 5ghz backhaul
CSCuw18306	Mesh AP 5GHz channel on non-configured channel in Dynamic Channel Assignment (DCA) list on Cisco WLC
CSCuu77304	Clients are deauthenticated from OEAP 600 Local Area Network (LAN) ports
CSCuv69967	OEAP600 wired 802.1x remote Local Area Network (LAN) forward traffic is seen in 802.1x Required State
CSCut15726	“AP MAC address” changes to “AP MAC address (Ethernet to CM)”
CSCux12850	Connection monitor is active on 1850 AP
CSCuv53770	Version reported as Cisco Cheetah AP in Cisco Discovery protocol (CDP) neighbor information
CSCut99150	Cisco 2702 AP is requesting as a Type 1 power device instead of Type 2
CSCuv59274	1142 CPU spike and utilization is 100% all the time
CSCuw91227	Air Time Fairness (ATF) is not supported on Cisco 1700 AP model
CSCuv10692	AckFailureCount is getting huge value in short period

Table 12 Resolved Caveats (continued)

Identifier	Description
CSCuw57578	Access Point send retry packets are more than configured “packet retries”
CSCut56741	Cisco AP1600: Radio reset with “STOPPING CPQ FWD TRACE ON Bad CPQ removal”
CSCut57453	Cisco AP2700 in mesh bridge mode disconnects from Returned Accounts Procedure (RAP) frequently
CSCuv39290	Cisco AP2700/3700 PAK Stuck is seen on Returned Accounts Procedure (RAP) Radio d1 reset: fp cl
CSCuw27385	Cisco Access Point: 3702 radio reset 'transmitter seems to have stopped' error is seen.
CSCuu02281	Access Points on Cisco WLC with wireless networks gets disabled while detecting rogues
CSCuu06047	Packet drops on Cisco 2702 Access Point in Flex Local Auth/Local Switch mode
CSCut95812	QN - Access Point Radio Reset with Beacons Stuck
CSCut95835	QN - Access Point Radio Reset with PAK Stuck
CSCut66360	Cisco AP1570 does not display operating temperature for some Access Points
CSCuu46746	Radio resets with off channel request stuck
CSCuu64553	Reduce RAM disk usage to allow DFS Debugging
CSCuv34176	SF3:Transmitter Stop Radio is reset due Delivery Traffic Indication Message Multicast PAK stuck[BZ 976]
CSCuo33980	Workgroup Bridge roaming delay up to 10 seconds is seen
CSCuv48278	Unable to connect clients in 802.11ac Mode for -D domain
CSCuw87468	Rogue containment not working on 8.0.120.0 for Cisco AP3700 with Wireless Security Module (WSM) module
CSCuv35186	Txpower change is not working as expected for Radio Resource Management (RRM) Interop.
CSCuw23023	Cisco 3700 Access Point Sniffer Mode not capturing on 5ghz radio with Rx-SOP set
CSCut30549	Inconsistent Access Point inventory information is seen between Cisco WLC and Access Point.
CSCuv27320	Wired clients in 702w Access Point leaking traffic across Ports/VLANS
CSCuw57048	Workgroup Bridge (WGB) roams with “Had to lower data rate”; minimum-rate is not configured
CSCut94260	Access Point Wireless Intrusion Prevention System (WIPS) module sending random characters in the alarm message
CSCuw57588	Cisco C3600 AP unexpected reload is seen on am_xml_GetChildCount
CSCuv40794	Access Point Impersonator alarm is seen for Cisco AP 3602i
CSCuv26697	Cisco 1532 Access Points not passing VLAN Trunking Protocol (VTP) info over the bridge link
CSCur62558	Add Link Layer Discovery Protocol (LLDP) support for autonomous Access Points
CSCuu45186	dot11 ARP-cache does not works well
CSCuq03928	IPV6 MIB support to show dual stack

Table 12 Resolved Caveats (continued)

Identifier	Description
CSCup82047	Syslog trap level for Access Point is inconsistent in controller
CSCuw44480	802dot11r client fails Authorization if self reset is done before user idle timeout expires
CSCuv69535	Graphical User Interface (GUI) access to IR829 AP is broken
CSCut54776	Invalid value returned for walk, cLIpv6AclCounterClear
CSCuw99278	Air Time Fairness (ATF) Policy id range mis-match is seen in Cisco WLC CLI and GUI
CSCun52472	“show dtls connection” shows blank in Access Point Name column for Capwap_Data
CSCus50404	Access Point Name is mismatched between Controller and Access Point
CSCut97161	Static IPv6 Config on Access Point does not take effect, need to reboot Access Point
CSCur98573	Memory increase on Datagram Transport Layer Security (DTLS) connections is seen when >500 APs join 5508 WLC
CSCuv97132	Show Access Point image all output will not fetch spamPreDownLoadInProgress
CSCuu48845	Simple Network Management Protocol (SNMP) Error thrown when IPv4 static IP is set for AP
CSCuw59579	Simple Network Management Protocol (SNMP): returns reversed DNS IP address when configured from Prime
CSCuu51641	WiSM2: 'config ap tcp-mss-adjust enable all 1363' is missing in High Availability (HA) configuration.
CSCuu88193	Wrong info shown on controller with no crash file in Access Point core
CSCut78949	XML validation error is seen while downloading configuration
CSCuw06127	Silent crash in 8.0.120 is seen due to memory leak in Cisco Discovery Protocol (CDP) Main
CSCuw09545	Incorrect DHCP “Pool Usage” on the Cisco WLC when queried via Simple Network Management Protocol (SNMP)
CSCut24658	Option 82 remote-id attribute “apname-vlan_id” information is not shown
CSCuu99344	Cisco WLC unexpectedly reloads- Dynamic Host Configuration Protocol (DHCP) packet content while on new mobility
CSCus86831	Cisco WLC uses old Access Point-Group name in Ethernet over GRE (EoGRE) DHCP option 82
CSCut37572	“show ap eogre” displays status for LOCAL mode Access Point
CSCut76523	Access Point should drop client data traffic when Access Point sends Internet Control Message Protocol (ICMP) error message to client
CSCux07616	Client cannot get Dynamic Host Configuration Protocol (DHCP) over Ethernet over GRE (EoGRE) when Dynamic Host Configuration Protocol (DHCP) required is enabled on Wireless Local Area Network (W LAN).
CSCut47494	Client is unable to join in Local switching Open Wireless Local Area Network (W LAN) with Local mode Access Point.
CSCut44073	Ethernet over GRE (EoGRE) static Profile Name is not displayed in Cisco WLC traplog it displays empty

Table 12 Resolved Caveats (continued)

Identifier	Description
CSCut47036	Ethernet over GRE (EoGRE): Access Point current active gateway/gateway status is not synced to standby
CSCuu07760	Ethernet over GRE (EoGRE): Need warning message when * is configured.
CSCuv34973	Fast SSID switching causes SIMPLE IP to be treated as a Ethernet over GRE (EoGRE) client
CSCut78696	Show run-config commands shows the Ethernet over GRE (EoGRE) Show commands
CSCuu17340	Cisco WLC unexpected reload on Tunnel Process Task is seen while adding gateway name 129 max character from UI
CSCus68335	Cisco WLC: Deletes the command config Access Point Ethernet duplex in full speed
CSCuw63311	Increased Ping latency & Reduced traffic is seen on 8510
CSCuw24476	Increased Ping latency & Reduced traffic is seen on 8510 with Quality of service (QoS) rate limiting
CSCuw12544	Rate-limiting is causing 500ms gap of traffic when roaming
CSCuv30948	Local Net Users is not saved in config backup
CSCuu12045	Mobility media access control (MAC) configuration should not be uploaded in the configuration file
CSCuu71471	Maximum Transmission Unit (MTU) value stacks in High Availability (HA)
CSCuu83548	Traceback observed in export-foreign standby Cisco WLC while disassociating client
CSCuu13860	'autoconvert flexconnect' is stored as 'disable' on startup-commands
CSCut61668	Application Identifiers (AID) errors is seen on the controller for Flexconnect Access Points
CSCuu07274	BGL-Alpha: “FP0.00:failed to find scb” error prints at 5500 standby console
CSCut57138	BGL-Alpha: The system has failed decoding vendor specific payload
CSCuu11959	Cisco 7925 phone using Cisco Centralized Key Management (CCKM) does not roam gracefully in FlexConnect environment.
CSCus30338	Clients with Static IP gets authenticated for Dynamic Host Configuration Protocol (DHCP) Required wireless local area network (WLAN)
CSCut60058	CTLR does not deauthenticate clients when AAA Flex-ACL is not present on Access Point
CSCuu93296	Extensible Authentication Protocol Transport Layer Security (EAP-TLS) loosing device certificate in standalone mode after reboot
CSCuu43770	Flex connect Central-DHCP Values is not getting applied to Flex Connect Access Points
CSCuw31813	Flex Local Auth, client roaming in-out-in during dot1x
CSCuu80153	Flex Analog Voice Channel (AVC) unable to update rate limit value
CSCut55043	FlexConnect Group with space in name renders terminal session unusable
CSCut68635	FT- Username is not getting updated in standby.Access VLAN is not updated in active

Table 12 Resolved Caveats (continued)

Identifier	Description
CSCur40277	High traffic loss is seen for Flex Access Point clients once CAPWAP tunnel is re-established
CSCuu07744	Interface not created when we have both Access Control List (ACL) and WLAN-VLAN mapping
CSCuu89294	Master Access Point in Flex Group is not saved in Cisco WLC cfg nor commands backup
CSCuu87832	Mobility Express: Client not moving to exclude state after association failure
CSCut81484	TB observed on Access Point when we have more number of rules on 8500
CSCuu72585	When Access Point in flexconnect mode, Cisco WLC AAA override occurs causing traffic Blackholing
CSCut10131	Cisco WLC fails to resend ciscoLwappDot11ClientMovedToRunState traps
CSCuv20940	Client fails to ping IPv6 gateway, clients with High Availability (HA) switchover
CSCut40919	Configuration download fails via service port using IPv6 addressing.
CSCuu08592	Override Interface-Interface group not applied on reauthentication for IPv6 clients
CSCuu07107	Simple Network Management Protocol (SNMP) walk on clsNetworkRouteConfigTable fails
CSCut72081	Cisco WLC: IPV6-3-CREATE_BINDING_FAILED error gets flooded
CSCuw13264	702w missing interface information on controller is seen after High Availability (HA) failover
CSCuv27120	Cannot configure IP address x.x.x.255 or x.x.x.0 as gateway is seen.
CSCuw35349	Dynamic Host Configuration Protocol (DHCP) registration keeps failing when mask from Cisco WLC interface does not match client received mask
CSCuu51747	Dynamic Interface accepts name as empty string in Cisco WLC CLI
CSCuu04464	License command causes Cisco WLC unexpected reload (possible buffer size overwrite)
CSCut98217	VSRE While upgrade from 8.0 to 8.1 Lic End User License Agreement (EULA) is changed to not accepted
CSCus90165	Calibration debugs not available
CSCuu58800	S60 Payload mismatch (PLM) Path Loss Measurement should be disabled by default
CSCuw34311	Cisco WLC drops Received Signal Strength Indicator (RSSI) reporting with Fast locate feature
CSCuv99533	Lync: Old history calls are not getting deleted once we reach max.
CSCuu03329	Simple Network Management Protocol (SNMP) Get is not fetching latest value for port, protocol & status
CSCut37414	CI: Jian High Availability (HA) has Trivial File Transfer Protocol (TFTP) failure while storing on flash error
CSCuv87458	“show mesh config” doesn't show mesh CA status when Carrier Access Codes (CAC) is enabled.
CSCut65562	8.1.14.13 - Subset channel isn't removed after channel change
CSCus97385	Access Point name chopped for “show mesh cac access (long AP name)”

Table 12 Resolved Caveats (continued)

Identifier	Description
CSCut91086	Client associated to Mobile Application Part (MAP) doesn't get AAA override in Flex+Bridge mode
CSCuv76883	Error inconsistent to Ethernet state when change mode “bridge” -> “local”
CSCuu77412	High memory usage from mesh-msg_task due to weird Bridge Group Name present
CSCut05488	Inconsistent/incorrect backhaul info/missing a channel for Radio frequency (RF) used
CSCut37465	Incorrect “AP MAC” in the response of “show mesh stats <AP Name>”
CSCuu96201	Invalid characters shown on the Bridge Group Name
CSCut48172	Locally Significant Certificate (LSC) Access Point provisioning happening after Mobile Application Part (MAP) is disconnected for long time
CSCuv16895	Mobile Application Part (MAP) count is shown wrongly in “show mesh ap summary” command in Cisco WLC CLI
CSCut38592	Mesh Backhaul shows up as “auto” instead of actual data rate
CSCuu72171	No response “config mesh link data <AP name>” non-mesh or mesh Access Point
CSCut04864	No response of “show mesh as tools stats” or with Cisco Access Point name
CSCut55891	Non-mesh Access Points not detected for “show mesh queue-stats AP name” and “all”
CSCuu59340	Signal-to-Noise Ratio (SNR) alarms for mesh APs have invalid content, is not working as expected
CSCut60912	Virtual LAN (VLAN) Support check or uncheck no updated in “Mesh” bar after Apply
CSCut85294	Cisco WLC CLI “show mesh neigh detail” command showing unreasonable years
CSCuw31820	Cisco WLC Consolidation Point unexpected reload is seen due to System unexpected reload for apfMsConnTask_6
CSCut92776	Configuration mobility group does not accept 24th member in case of IPv6
CSCuv43484	Device is switching to Multiple Access (MA) mode after mobility new-architecture enable
CSCut42569	GA: Client is not anchored after changing export anchor config on wireless local area network (WLAN)
CSCuu26369	Message “Handoff 802.1x PEM state “is not filtered by debug client
CSCuv85747	Mobility Member entries going stale
CSCuu83941	8510: Error enabling global multicast with CAPWAP mode unicast
CSCuw50324	Unexpected reload seen on high CPU usage
CSCut88319	FF08:/16 range of organization-local IPv6 multicast addresses
CSCuv22052	Link local multicast control traffic sent by Access Points, Internet Group Management Protocol (IGMP) Snooping Enabled
CSCuv43125	mdnsQueryDelayHandler tracebacks in 8.0 WLC flooding syslog server
CSCuu10781	Multicast configuration mismatch on Web / CLI
CSCut36686	FlexAVC: 8.1.10.201 WLAN ID displayed incorrect on Access Point

Table 12 Resolved Caveats (continued)

Identifier	Description
CSCut63331	FlexAVC - not able to change value of marking once configured
CSCut48743	FlexAVC - policy-map not getting deleted/added when Access Point is in AP group
CSCut39707	FlexAVC profile should not show about not supported WLANs
CSCut85185	FlexAVC-WLAN_specific mapping is not pushing to Access Point
CSCuu91001	NetFlow record sent without client IP address
CSCut70083	show run-config command is not showing FlexAVC rules
CSCuw39667	WiSM2 unexpected reload/rebooting on task emWeb
CSCut45024	Cisco WLC showing 0 as application in FlexAVC stats
CSCuv86494	Cisco WLC clears Access Point MAC before deleting client, sends NetFlow with Zero AP MAC
CSCuu28666	BGl-Alpha: SNTP-3-SOCK_OPT_FAILED: Failed to set the socket option
CSCus97953	8510 Silent unexpected reload seen- Uhhuh. NMI received for unknown reason 2d
CSCuw28246	CT8540 / CT5520 dose not detect power supply cable failure
CSCuu16052	Does not set DF bit for non-CAPWAP traffic from Cisco WLC such as RADIUS
CSCut26363	GUI and telnet very slow, almost unresponsive
CSCuw03414	WiSM2 8.0.102.0 unexpected reload on apfMsConnTask_2 reason “System Crash”
CSCuv79793	Cisco WLC is leaking packets from virtual IP onto Local Area Network (LAN)
CSCuv01337	“config pmipv6 add profile” error not clear when profile length>32
CSCut74263	Mobile Access Gateway (MAG) on Access Point: Access Point does not clear bindings after session/user timeout & deauth
CSCut64180	Access Point holds BW after call when Cisco WLC High Availability SO happens during call setup
CSCuw21213	Downstream: QoS Bronze Profile not marking traffic to AF11 on Flex
CSCut96390	Inconsistent counter behavior of Signalling Connection Control Part (SCCP) call when Address complete message (ACM) is not enabled
CSCuu96349	QosMap shows pre-configured values after upgrade from 8.1 CCO
CSCuu20097	Token Bucket leak is seen when QoS Roles is setup and when working with WebAuth
CSCuv88984	“show ap universal summary” CLI dos not exist
CSCuu07817	Access Point is not detecting Rogues when joined to controller in IPv6 pref. mode
CSCuv34472	Longevity: Ambassador in longevity unexpectedly reloads with Task:Emweb in 8.1.104.38
CSCuw38795	5508 Cisco WLC unexpected reloads upon pushing RF calibration template from PI
CSCuw38022	8510 Simple Network Management Protocol (SNMP) Agent reverses octet order of clrRrmPakRssiNtp object
CSCut32955	a-mpdu tx priority command missing from backup config
CSCut59663	Add channels 100-140 as default in 11a
CSCuu43603	Channel assignment leader IPv4 address not showing.
CSCus79791	Client connected to 11n Access Point shows as 11ac client on Cisco WLC

Table 12 Resolved Caveats (continued)

Identifier	Description
CSCuu80383	Clients is denied association by neighbor Access Point during optimized roaming
CSCut23857	Issues of a Access Point in Radios 802.11a/n/ac from Global mode to Custom mode
CSCuu71487	Minimum users is sometimes selected incorrectly
CSCut59679	Modify output of sh run-config, to reduce duplicate info on Access Points
CSCuw56127	Need to re-evaluate Tunisia for –I radio types
CSCuv67144	Need to re-evaluate Algeria if in –E or –I
CSCuw27160	RF Grouping Algorithm > update interval NOT synchronized on controllers
CSCuu14124	RF-profile losing the channel and coverage values after downloading configuration file
CSCuv96996	Radio Resource Management (RRM) setting 24 channel width to 40, leading to CleanAir crash
CSCuu42378	RX-SOP threshold not working correctly
CSCut27056	Traplog message for radar Clear event needs correction
CSCuw79951	Unable to disable Assisted Roaming or Load Balancing through CLI
CSCuw62850	WiSM2 8.0.120.5 unexpected reload. mwar_ms_deadlock.crash
CSCuw33715	Cisco WLC unexpected reload on 11k processing is seen
CSCuw66299	Cisco WLC msglog showing NMSP Transmit Failure even when there is no MSE
CSCur40006	Cisco WLC: Group size exceeded with static RF Group member add
CSCuv08631	“Failed to add new AP Group: test” misleading when max Access Point Group hit
CSCut10882	11r clients not moving L2authentication to Run state on Cisco WLC
CSCuw48488	4-way handshake fails on 11r+11w (FT+PMF) Wireless Local Area Network (WLAN)
CSCuv36505	8.0 Cisco WLC messages flooding CLI after debug client
CSCut90276	AireOS Traceback: APF-4-PROC_ACTION_FAILED
CSCut86986	Audit-session-id not learned correctly during L3 roam-Radius Network Access Control (NAC0 disable
CSCut71612	OUI string should be synced across High Availability (HA)
CSCuv40033	Cisco WLC IPv6 IAPP WIPS Report Vulnerability
CSCuw62172	Unexpected reload seen on High Availability (HA) standby while setting Auth-priority order from Prime Infrastructure in 7.6
CSCut02524	Default NAS-ID value at the AP-Groups should be empty or “none”
CSCus61445	Domain Name System (DNS) Access Control List (ACL) on WLC is not working - Access Point not Send DTLS to Cisco WLC
CSCuu07700	Extensible Authentication Protocol (EAP) Packet does not get encrypted in Re-Auth request from client
CSCuw91763	Feature “AES Key Wrap” does not work
CSCus92667	GET on Access Point groups Table after set - response missing
CSCuw35341	IP address lost on AAA override+muiltiple subnetworks per vlan+DHCP req

Table 12 Resolved Caveats (continued)

Identifier	Description
CSCut45010	Issue with installing certs in Universal Time (UTC)
CSCuu66675	Lock unexpected reload is seen on RADIUS Transport Thread during CMCC External Auth
CSCut29535	Not able to remove domain name system, configured radius server.
CSCuv90333	afpmsConntask floods when running client console debug
CSCuu51713	RADIUS and Accounting Fall back does not work properly
CSCuu62544	RFC 3576 - Disconnect MSG not handled with WLC
CSCuu08752	Service Exchange Platform (SXP) unexpectedly reloads when running Trust Sec clients is seen
CSCuu15866	Unexpected Local Extensible Authentication Protocol (EAP) authentication abort.
CSCuu36172	Venue Name max takes 253 vs. CLI 200 characters for AP
CSCut92934	Cisco VWLC - Access Point with expire Mic not able to join with Ignore Mic settings
CSCuv97793	WiSM2 unexpected reload AP_DB_CREATE_ERR Message queue MFP-Q is nearing full
CSCuv82711	Cisco WLC 5508 8.1.111.0. RFC-3576 Disconnect-Request not heard from port 3799
CSCuq73590	Cisco WLC adds incorrect class attribute in accounting stop
CSCut08222	Cisco WLC local policy behavior is abnormal
CSCuw16295	Cisco WLC show boot shows backup image as Error failing to read linux.bak.img
CSCuw89581	Cisco WLC System unexpected reload on apfReceiveTask
CSCuv04058	Error is seen while trying to change the default trap receiver port.
CSCuw26629	Management Information Base (MIB) message of Power supply Status on 7500 is wrong
CSCut57471	Simple Network Management Protocol (SNMP) Interface Management Information Base (MIB)on 5520 is wrong
CSCuu64447	CleanAir device commands become disabled after restoring backup config
CSCuv43466	Garbage character are shown in CLI “show run-config startup-command”
CSCuu24064	Simple Network Management Protocol (SNMP): cLApUniversalPrimeStatus not returning for all APs
CSCuv55994	“Error in adding VLAN Map” popped up when VLAN ID is out of range
CSCuu97320	“Flex+Bridge&SE-Connect” filtering back to uncheck after “Change Filter”
CSCuv65301	“WLAN SSID” popped up when invalid or unsupported IPv6 in server address
CSCuw34565	7500 Cisco WLC unexpected after deleting Access Point crash logs from GUI
CSCuv47252	Access point RF Troubleshoot legend issue is seen for channel
CSCuw97240	Access Control list (ACL) Rule: Adding Destination. port as HTTPS is not working
CSCuu08387	AQ graph shown twice in drop down of interference devices in Cisco WLC GUI
CSCuu67169	Bridge data rates are not shown for 1572 Access Points in controller GUI

Table 12 Resolved Caveats (continued)

Identifier	Description
CSCuv79354	Cannot configure IP address x.x.x.255 or x.x.x.0 as gateway in GUI
CSCut81543	Click “Back” does not go back to filtered Access Points after going to an AP page for RADIUS
CSCut58777	Cisco WLC GUI does not have options to configure 2.4GHz HT Rates
CSCuw26377	Unexpected reload seen due to invalid form field validation on switch_cfg_rw.html
CSCur39649	Unexpected reload seen on /screens/base/tunnel_gtpv2_cfg.html
CSCuv18734	Dialogue message missing when Client “Removed” from Cisco WLC5500
CSCut15677	DS/US Channels are empty for CM Statistic on Cisco WLC GUI for AP/CM
CSCuw78528	Flex group name is missing when refresh flex Access Point's wlan-avc mapping page
CSCus80870	GUI: Observed popup error message when disabling the Protected Management Frames (PMF) in WLAN
CSCut60950	Inconsistent errors seen during setup unsupported channel procedure on 40MHz/80MHz
CSCuu19563	Incorrect pop message seen in GUI 802.11 coverage
CSCuv44023	Local policy name with UTF-8 character is showing as junk in edit page
CSCuw51155	Mobility Express UI: Overwrites some Wireless Local Area Network (WLAN) config when edited from UI
CSCuv79155	Mismatch in config for Address Resolution Protocol (ARP) Timeout value in Cisco WLC CLI and GUI
CSCuv29025	Mobility domain name is displayed as Junk if created in UTF-8 character
CSCuu95889	Mobility Group without MAC “Error in creating Member” improperly popped
CSCuv07657	Monitor page does not support Session timeout in VWLC
CSCut62786	Native VLAN id textbox missing in webUI
CSCuu61286	No error displayed but silently quit for “Power Injector State” is seen.
CSCuu50538	No pop-up shown when affected channels field is selected without any i/p
CSCuu42415	Non-realistic 102% or 120% displayed for Interference Impact
CSCux03140	Not able to add valid Phase-Shift Keying (PSK) key from GUI
CSCuu23237	Parameters got expanded when clicking back button in Best Practices page
CSCuv96333	Read only user able to change “Telnet Capability” setting
CSCuw73215	RF profile> coverage, exception clients range differs in Cisco WLC GUI and CLI
CSCuu14734	RFDB: Client Performance: client connections: size and position of donuts vary
CSCuw02258	Severity Filter for Monitoring CleanAir Interferer's does not work
CSCut95326	Showing access-VLAN when client is in Quarantine state in GUI-flexmodeAP
CSCuu11129	Switching from 2.4 G to 5G, the proposed high-chart disappeared on Safar
CSCuu88339	Unable to configure Central DHCP Flex+Mesh/Flexconnect WLAN from WLC GUI
CSCut63507	Cisco VWLC showing application ID instead of application name
CSCuv79867	WLAN GUI: WLAN edit can't accept 20 characters password for Phase-Shift Keying (PSK)

Table 12 Resolved Caveats (continued)

Identifier	Description
CSCuu33740	Cisco WLC unexpectedly reloads while editing SNMP community - waFormSubmit_snmp_comm_list
CSCut79304	Cisco WLC GUI is throwing error for DSCP marking
CSCuv12875	Cisco WLC Spartan: 802.11ac Max Capability issue for all Access Point
CSCut44986	Cisco WLC is throwing error when accounting is disabled on WLAN
CSCus77368	Cisco WLC: Unexpected reload ewaFormSubmit_cell_edit
CSCuu66484	Cisco WLC: GUI 'downloaded AVP' page just keeps reloading
CSCut81459	Cisco WLC: Noise of OFF Access Points shows as blank or as ()
CSCux03108	8510 Unexpected reload on Task Name:portalMsgTask.
CSCur94843	External web Auth URL goes through loop and never gets to the Login page
CSCuv25826	Disabling, mDNS profile on all wireless local area networks (WLAN) throws wrong error msg
CSCuu51728	Enabled UniversalAPAdminMode in wireless local area network (WLAN) gets disabled after config transfer
CSCur88123	Invalid Phase-Shift Keying (PSK) for layer 2 security after controller reboot
CSCuu39294	mDNS snooping is not disabling when flex local switching is enabled
CSCut62944	Mismatch between show run-config commands and device configurations for Cisco WLC
CSCuu16348	Oeap600 RLAN 'quiet' wired clients timing out
CSCuw90458	Prime Infrastructure 3.0 does not properly push template for wireless local area network (WLAN) i
CSCuw31595	Bogus line in show run-config commands output is seen
CSCuu77738	Prime 3.0 Auto Provisioning is not working
CSCuw29532	CAPWAP to Mobility Express conversion: shows incomplete cmd when image download not required
CSCuw12525	Simple Network Management Protocol (SNMP) get on system Temperature attribute returns 5000 on Mobility Express Cisco WLC
CSCut40305	Console logs are creating during AP-GUI login session and PSE status
CSCuw03323	Cisco AP702w draws additional power (22.1 watts) when LAN port 4 is disabled

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 LAN controller functionality bundled into, the Cisco Aironet 1850 and 1830 Series APs currently. 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 LAN controller, is designated as the Master AP. Other access points, referred to as Subordinate APs, associate to this Master AP.

The Master AP operates as a wireless LAN 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 setup and configuration, see the *Cisco Mobility Express User Guide for Release 8.2*, at:

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/mob_exp/82/user_guide/b_ME_User_Guide_82.html

Supported Cisco Aironet Access Points

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

Mobility Express Features

The following features and functionalities are present in this release:

- CLI-based Initial configuration wizard
- Up to three Network Time Protocol (NTP) servers, with support for FQDN names.
- Simple Network Management Protocol (SNMP) version 3 polling, supported via CLI only.
- 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 HTTP for networks containing only AP 1850, AP 1830, or both kinds of access points.

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 Master AP can concurrently function as controller (to manage APs) and as an AP (to serve clients).
- Initial configuration wizard.
- Priming at distribution site.
- Default Service Set Identifier (SSID), set from factory. Available for initial provisioning only.
- Management—Through a 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 (SNMP).
- Management—SSH, Telnet, Admin users.
- Reset to factory defaults.
- Serviceability—Core file and core options, Logging and syslog.
- Cisco Prime Infrastructure.
- Cisco CMX 10.x—Only CMX Presence is supported. CMX Connect, Location and Analytics are not supported.
- 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
- Terminal Access Controller Access Control System (TACACS)
- Management over wireless
- High Availability and Redundancy—Built-in redundancy mechanism to self-select a Master AP and to select a new AP as Master in case of a failure. Supported using VRRP.
- Software upgrade with preimage download
- Migration to controller-based deployment.

New Features and Functionalities

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

- Updates to the Client View page in the Monitoring Dashboard.
- Client ping test and packet capture.
- Changing the country code on the controller and APs on the network.
- NTP servers for automatically setting the date and time.
- Software update using HTTP.
- CCKM support.

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

Cisco Mobility Express software for Cisco Wireless Release 8.2.100.0, is as follows:

Software Pype and purpose	For AP 1850	For AP 1830
Software to be used only for conversion from Unified Wireless Network Lightweight APs software to Cisco Mobility Express software.	AIR-AP1850-K9-8.2.100.0.tar	AIR-AP1830-K9-8.2.100.0.tar
AP software image bundle, to be used for software update, or supported access points images, or both.	AIR-AP1850-K9-ME-8-2-100-0.zip	AIR-AP1830-K9-ME-8-2-100-0.zip

Installing Mobility Express Software

See the "Getting Started" section in the *Mobility Express User Guide* at the following URL:

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/mob_exp/82/user_guide/b_ME_User_Guide_82.html

Caveats

The open caveats applicable to the Cisco Mobility Express solution are listed under the "Caveats" section on page 38. All caveats associated with the Cisco Mobility Express solution have *Cisco Mobility Express* specified in the headline.

Related Documentation

- Cisco Mobility Express User Guide

  http://www.cisco.com/c/en/us/td/docs/wireless/access_point/mob_exp/82/user_guide/b_ME_User_Guide_82.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

Installation Notes

This section contains important information to keep in mind when installing Cisco WLCs and access points.

Warnings

Warning **This warning means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.** Statement 1071

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Warning **Do not locate the antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, as they may cause serious injury or death. For proper installation and grounding of the antenna, please refer to national and local codes (e.g. U.S.: NFPA 70, National Electrical Code, Article 810, Canada: Canadian Electrical Code, Section 54).** Statement 280

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductors (all current-carrying conductors).** Statement 13

Warning **This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground connector. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 1024

Warning **Read the installation instructions before you connect the system to its power source.** Statement 10

Warning **Do not work on the system or connect or disconnect any cables (Ethernet, cable, or power) during periods of lightning activity. The possibility of serious physical injury exists if lightning should strike and travel through those cables. In addition, the equipment could be damaged by the higher levels of static electricity present in the atmosphere.** Statement 276

Warning **Do not operate the unit near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.** Statement 364

Warning **In order to comply with radio frequency (RF) exposure limits, the antennas for this product should be positioned no less than 6.56 ft. (2 m) from your body or nearby persons.** Statement 339

Warning **This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.** Statement 1017

Safety Information

Follow the guidelines in this section to ensure proper operation and safe use of the Cisco WLCs and access points.

FCC Safety Compliance Statement

FCC Compliance with its action in ET Docket 96-8, has adopted a safety standard for human exposure to RF electromagnetic energy emitted by FCC-certified equipment. When used with approved Cisco Aironet antennas, Cisco Aironet products meet the uncontrolled environmental limits found in OET-65 and ANSI C95.1, 1991. Proper operation of this radio device according to the instructions in this publication results in user exposure substantially below the FCC recommended limits.

Safety Precautions

For your safety, and to help you achieve a good installation, read and follow these safety precautions. They might save your life.

- If you are installing an antenna for the first time, for your own safety as well as others', seek professional assistance. Your Cisco sales representative can explain which mounting method to use for the size and type of antenna you are about to install.
- Select your installation site with safety as well as performance in mind. Electric power lines and phone lines look alike. For your safety, assume that any overhead line can kill you.
- Call your electric power company. Tell them your plans and ask them to come look at your proposed installation. This is a small inconvenience considering your life is at stake.
- Plan your installation carefully and completely before you begin. Successfully raising a mast or tower is largely a matter of coordination. Each person should be assigned to a specific task and should know what to do and when to do it. One person should be in charge of the operation to issue instructions and watch for signs of trouble.
- When installing an antenna, remember:
  - Do not use a metal ladder.
  - Do not work on a wet or windy day.
  - Do dress properly—shoes with rubber soles and heels, rubber gloves, long-sleeved shirt or jacket.
- If the assembly starts to drop, get away from it and let it fall. Remember that the antenna, mast, cable, and metal guy wires are all excellent conductors of electrical current. Even the slightest touch of any of these parts to a power line completes an electrical path through the antenna and the installer: **you!**

- If any part of an antenna system should come in contact with a power line, do not touch it or try to remove it yourself. Call your local power company. They will remove it safely.
- If an accident should occur with the power lines, call for qualified emergency help immediately.

Installation Instructions

See the appropriate quick start guide or hardware installation guide for instructions on installing Cisco Wireless Controllers and APs.

Note To meet regulatory restrictions, all external antenna configurations must be installed by experts.

Personnel installing the Cisco WLCs and APs must understand wireless techniques and grounding methods. APs with internal antennas can be installed by an experienced IT professional.

The Cisco WLC must be installed by a network administrator or qualified IT professional, and the proper country code must be selected. After the installation, access to the Cisco WLC should be password protected by the installer to maintain compliance with regulatory requirements and ensure proper unit functionality.

Service and Support

Troubleshooting

Step 1 For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at:

http://www.cisco.com/c/en/us/support/index.html

Step 2 Choose **Product Support > Wireless**.

Step 3 Choose your product and click **Troubleshooting** to find information about the problem you are experiencing.

Related Documentation

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 Controller Configuration Guide*
- *Cisco Wireless Controller Command Reference*
- *Cisco Wireless Controller System Message Guide*

You can access these documents at http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/tsd-products-support-series-home.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.