Release Notes for Cisco Wireless Controllers and Lightweight Access Points for Release 8.0.100.0

First Published: February 20, 2015

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

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 10, 2017	• Open Caveats, page 36 – Added CSCvc65568
October 10, 2017	• Features Not Supported on Cisco Virtual WLCs, page 32 – Added Wired Guest and FlexConnect central switching.
February 19, 2016	• Upgrading to Cisco WLC Software Release 8.0.100.0, page 20 – Added the statement—In Cisco Wireless Releases prior to 8.0.100.0, the behavior of the Redirect-URL-ACL (as returned via RADIUS attributes) may have been incorrect. The ACL was applied in only the Ingress direction (traffic destined for the LAN or distribution system) of the radio interface. These ACLs should also be applied in the Egress direction (traffic destined for the wireless client). Therefore, after upgrading to a Cisco Wireless Release 8.0 or a later release, you may need to adjust the ACL to accommodate the correction of this behavior.

Cisco Wireless LAN Controller and Access Point Platforms

The section contains the following subsections:

Supported Cisco Wireless LAN Controller Platforms

The following Cisco WLC platforms are supported in this release:

- Cisco 2500 Series Wireless LAN Controllers
- Cisco 5500 Series Wireless LAN Controllers
- Cisco Flex 7500 Series Wireless LAN Controllers
- Cisco 8500 Series Wireless LAN Controllers
- Cisco Virtual Wireless Controllers on Cisco Services-Ready Engine (SRE) or Cisco Wireless LAN Controller Module for Integrated Services Routers G2 (UCS-E)
- Cisco Wireless Controllers for high availability (HA Cisco WLCs) for the Cisco 2500 Series (no AP SSO support), 5500 Series, Wireless Services Module 2 (WiSM2), Flex 7500 Series, and 8500 Series WLCs
- Cisco WiSM2 for Catalyst 6500 Series Switches

For information about features that are not supported on the Cisco WLC platforms, see Features Not Supported on Cisco WLC Platforms, page 30f.

Supported Access Point Platforms

The following access point platforms are supported in this release:

- Cisco Aironet 1040, 1130, 1140, 1240, 1250, 1260, 1600, 1700, 2600, 2700, 3500, 3500p, 3600, 3700, Cisco 600 Series OfficeExtend, 702, 702W, AP801, and AP802 Series indoor access points
- Cisco Aironet 1520 (1522, 1524), 1530, 1550 (1552) Series outdoor access points

For information about features that are not supported on some access point platforms, see Features Not Supported on Access Point Platforms, page 33.

Note AP801 and AP802 are integrated access points on the Cisco 800 Series Integrated Services Routers (ISRs). For more information about the stock-keeping units (SKUs) for the access points and the 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

  AP802 is an integrated access point on the next generation Cisco 880 Series ISRs.

  Before you use an AP802 series lightweight access point with Cisco WLC software release 8.0.100.0, you must upgrade the software in the Next Generation Cisco 880 Series ISRs to Cisco IOS 15.1(4)M or later releases.

Unsupported Cisco Wireless LAN Controller Platforms

The following Cisco WLC 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 LAN Controller software on Cisco SRE running on ISM 300, SM 700, SM 710, SM 900, and SM 910
- Cisco Catalyst 6500 Series and 7600 Series WiSM
- Cisco Wireless LAN Controller Module (NM/NME)

What's New in This Release?

This section provides a brief description of what is new in Release 8.0.100.0. For instructions about how to configure these features, see *Cisco Wireless LAN Controller Configuration Guide, Release 8.0*.

This section contains the following topics:

Cisco Aironet Access Point and Scale Features

- Keep-alives over CAPWAP data tunnel—Keep-alives are sent over the CAPWAP data tunnel too. Previously, the keep-alives were sent over the CAPWAP control tunnel. By default, this feature is enabled and is run every 30 seconds. No configuration is required.
- Flex + Bridge AP mode—A new AP mode called Flex + Bridge is introduced, which enables FlexConnect functionality across mesh-enabled APs. This feature provides outdoor and indoor mesh AP redundancy links over the wireless network if Ethernet is not operational.

Note The Flex + Bridge AP mode is not supported on Cisco AP1130 and AP1240.

- Mesh fast convergence—Allows mesh convergence parameters such as parent loss detection and keepalive timers to be automatically configured to standard, fast, and very fast convergence methods. This feature enables faster convergence by reducing mesh convergence time per hop to less than 20 seconds.
- VLAN tagging on AP700W—Allows you to define individual VLAN tags for each individual Ethernet port available on Cisco Aironet 700W Series Access Points. This feature allows traffic to be separated not only between wireless and wired networks, but also among the four Ethernet ports.
- PPPoE on FlexConnect APs—The point-to-point protocol over the Ethernet (PPPoE) submode on FlexConnect access points is supported. A FlexConnect AP can act as a PPPoE client. This eliminates the need of an external PPPoE router.

Note This feature was first introduced in Releases 7.3 and 7.4 for market validation. It is reintroduced in Release 8.0.100.0.

Note PPPoE is not supported in Flex/Mesh deployments.

- DCA on RF profiles—Dynamic Channel Assignment (DCA) is supported on RF profiles. This feature enables multi-country support with one AP group per country, each with a defined channel list in RF Profiles. This feature also simplifies managing mixed-channel (802.11n/ac 40 MHz/80 MHz) environments. For more information, see the *Configuring RF Profiles* chapter of the configuration guide.

Note This feature is not supported on APs that are in Bridge mode and mesh APs.

- Rx SOP—Support is introduced for the Receiver Start of Packet Detection Threshold (Rx SOP) feature. Rx SOP determines the Wi-Fi signal level in dBm at which the radio of an access point demodulates and decodes a packet. As the Wi-Fi level increases, the radio sensitivity decreases and the receiver cell size becomes smaller. Reduction of the cell size affects the distribution of clients in the network.

  Rx SOP is used to address clients with weak RF links, sticky clients, and client load balancing across access points. Rx SOP helps to optimize the network performance at high-density deployments such as stadiums and auditoriums where access points need to optimize the nearest and strongest clients.

  For more information, see the *Configuring Receiver Start of Packet Detection Threshold* chapter of the configuration guide.
- Optimized roaming—Support is introduced for optimized roaming. Optimized roaming resolves the problem of sticky clients that remain associated to access points that are far away and outbound clients that attempt to connect to a Wi-Fi network without having a stable connection. This feature disassociates clients based on the RSSI of the client data packets and data rate. The client is disassociated if the RSSI alarm condition is met and the current data rate of the client is lower than the optimized roaming data rate threshold. You can disable the data rate option so that only RSSI is used for dissociating clients. For more information, see the *Configuring Optimized Roaming* chapter of the configuration guide.
- Radio monitoring on 80 MHz—Radio monitoring is supported on all three widths: 20 MHz, 40 MHz, and 80 MHz. The 80-MHz 802.11ac channel can be detected and reported.
- Cisco Aironet 1700 Series Access Points are supported.
- CleanAir Express on AP1600 and AP1700—Support is introduced for CleanAir Express on Cisco Aironet 1600 and 1700 Series Access Points. For more information see Cisco CleanAir Express.
- OEAP Enhancements:
  - Basic Firewall—A basic firewall provides port/application protection that can be controlled by the OEAP end-user using user accessible GUI
  - Split Tunneling— Split tunneling enables OEAP clients to reach Internet directly through the WAN instead of going through the corporate network
  - Voice QoS—Enhanced OEAP offers high priority for voice packets for customers using VOIP in remote offices
  - Link Tests—Link tests allow end-users to test the OEAP link metrics (latency, jitter) on demand or periodically
- Increased scale on vWLC—Increased scale to support up to 6000 clients on Cisco Virtual Wireless LAN Controller (Cisco vWLC).
- Wired guest access on 2500 WLC—Wired guest access is supported on Cisco 2500 Series WLC.
- Cisco Wireless Release 8.0 is required for –S regulatory domain access points to be supported with the Hong Kong country code.

Native IPv6

- IPv6 addressing used by Cisco WLC:
  - ::/128—Unspecified; used as a source address until an address is assigned
  - ::1/128—Loopback address
  - fd09::/8—Unique local; private network 10.0.0.0, 172.16.0.0, 192.168.0.0
  - fe80::/64—Link-local; non-routed, self-generated addresses that do not exist outside the layer 3 link
  - ff00::/8—Multicast; used to identify multicast groups
  - 2000::/3—Global Unicast; assigned using stateful/stateless DHCPv6 or SLAAC
  - ::ffff/96—IPv4-Mapped; used to embed an IPv4 address in IPv6

Caution If a non-default IPv6 address is configured on the management interface of a WLC using Release 8.0.100.0, you can add the WLC only to Cisco Prime Infrastructure Release 2.2, which is yet to be released. To remove the IPv6 address, you must either reset the WLC to factory defaults or downgrade to Release 7.6.

- Stateless Address Auto-configuration (SLAAC) uses EUI-64 to select an IPv6 address. This is applicable only for service port.
- Stateless DHCPv6 is supported
- IPv6 Neighbor binding—Eight IPv6 addresses are supported per client. Upon the ninth, the Cisco WLC removes the oldest stale entry.
- Management access—Cisco WLC can be accessed from wired or wireless through its IPv4 or IPv6 management using Telnet, SSH, HTTP, or HTTPS.
- Service port—Service port can be statically assigned an address or select an address through SLAAC. This is the only SLAAC interface on the WLC.
- IPv6 CLI configuration—Use the **config ipv6** commands.
- CAPWAP Preferred mode—This mode is to allow you to configure CAPWAP L3 transport (IPv4 and IPv6) through which APs associate with the WLC. There are two levels of preferred mode: AP group specific and Global. The default value of Global preferred mode is set to IPv4.
- DTLS—Similar to CAPWAP, DTLS also uses the IPv6 address of the AP.
- AP Discovery mechanisms:
  - DHCPv6 Option 52—OPTION_CAPWAP_AC_V6 (52) RFC 5417. As part of the DHCPv6 Reply, the server provides the IPv6 WLC management IPv6 address. AP begins unicast CAPWAP discovery.
  - Multicast discovery—Broadcast does not exist in IPv6; Send CAPWAP discovery messages to "All ACs multicast address" (FF01::18C)
  - Using DNS—Configure DNS server to resolve cisco-capwap-controller.domain-name; domain-name and DNS server should be returned from DHCPv6 server
  - AP Priming—Preconfiguring the AP with a primary, secondary, and tertiary IPv6 managed WLC.

- AP Failover—Management IP address must be reachable. One entry allowed per WLC. The AP associates with either the IPv4 or IPv6 address of the WLC, regardless of the management IP listed. All other AP failover behavior is the same as previous releases.
- AP High Availability—Backup WLCs are supported.
- Upload/Download with FTP/TFTP/SFTP—Upload or download can be initiated through the Cisco WLC. We recommend Tftpd64 server. Either IPv4 or IPv6 address can be used.
- RADIUSv6 support—RADIUSv6 servers can be added using their IPv6 address. When using IPv6, for simplicity and efficiency, bind to one IPv6 address (one IPv6 address bound to the WLC IPv6 management address). At present, there is no Cisco Enterprise IPv6 RADIUS support.
- TACACS+v6 Support—TACACS+v6 servers can be added using their IPv6 address.
- LDAP is supported.
- NTPv3—NTP server can be configured with IPv4 or IPv6 address. We recommend Cisco IOS router/switch as the NTP server.
- Syslog over IPv6—Syslog can be over IPv4 or IPv6.
- SNMP Trap Receiver—SNMP MIBs are sent to the IPv6 destination.
- Ping—Ping supports both IPv4 and IPv6. Link-local and Globally unique addresses can be pinged. Both WLC GUI and CLI are supported.
- UDP Lite—UDP Lite computes checksum on the pseudo-header of datagram. Enabling UDP Lite speeds up packet processing time. The IP protocol ID is 136, uses the same CAPWAP ports as UDP. To enable UDP Lite, you must ensure that the network firewall allows protocol 136. Switching between UDP and UDP Lite causes all APs to rejoin the WLC. UDP Lite is enabled by default. You can configure UDP Lite for an AP or all APs.

  To configure UDP Lite, use the **config ipv6 capwap udplite** {**enable** | **disable**} {**all** | **ap-name**} command.
- CDPv6—CDP detects both IPv4 and IPv6 neighbors at both WLC and AP.
- Guest Access—Virtual IP address is only IPv4. Uses IPv4-mapped address for IPv6 web-authentication clients. Virtual IP should be the same for all WLCs in the same mobility group. For example the IPv6 address will display as [::ffff:192.0.2.1].
- AP Multicast Mode—Enable IPv6 multicast routing on IOS router or switch. IPv6 AP multicast works the same way as IPv4.

  IPv6 multicast messaging for mobility/roaming for IPv6 is not supported. Mobility group members can still have IPv6 address.
- Mobility Groups/Auto-Anchor—In mixed environments of 8.0 and 7.x releases, both the ends must be IPv4 and the guest anchor should be on Release 8.0. This allows WLCs using Release 8.0.100.0 that share the mobility group to connect using EOIP tunnels with WLCs that are using older releases.
- IPv6 TCP MSS (global/per AP) is supported
- AP crash or core dump using TFTP method is supported for both IPv4 and IPv6 addresses
- Config Wizard for IPv6 is supported on both WLC GUI and CLI
- CPU and interface ACLs are supported
- Static RRM is supported
- IPv6 network routes are supported to access WLC over service port
- Features not supported:

  - Deployment modes—FlexConnect-local switched, mesh/outdoor, teleworker/OEAP, converged access
  - Services—Multicast DNS, AVC, and TrustSec
  - APs—Bridge-mode APs or APs with 64-MB RAM: 600 OEAP, ISR 800/802, 1130, 1240, 1250, 1310, 1410, 1520.
  - Miscellaneous configuration options—Internal DHCPv6 server, DHCPv6 proxy, auto-configuration, dynamic interfaces, RA interfaces, OSCP and CA server URL, VLAN pooling
  - Protocols—NTPv4, MLDv2, IPSec v3 and IKEv2, RLDP and CIDS, PMIPv6, mDNS IPv6 clients, and New Mobility
  - IPv6 is not supported for HA Redundancy Interface configuration
  - Auto-RRM, Dynamic Anchoring, DNS RADIUS/TACACS+, core dump.
- Important Notes on Native IPv6:
  - The initial deployment of native IPv6 might not have management IPv6 address. This does not stop the configuration of stateless address autoconfiguration (SLAAC) on the service port. Suppose a scenario where Cisco WLC does not have native IPv6 address except the service port and syslog IPv6 address is configured. The traffic generated on Cisco WLC can leak into service subnet.
  - Anycast addresses are not supported on Cisco WLCs.

Note Anycast addresses are allocated from the unicast address space, using any of the defined unicast address formats. Anycast addresses are syntactically indistinguishable from unicast addresses. When a unicast address is assigned to more than one interface, thus turning it into an anycast address, the nodes to which the address is assigned must be explicitly configured to know that it is an anycast address.

  - The WLC has a configured default IPv6 route on management interface. If you assign an IPv6 address on service port on subnet A (for example 2001::/64), and you have a host in subnet B (for example 2002::/64) that tries to communicate with WLC on service port for subnet B, the WLC sends an NDP (NS) on the management interface.
  - Data DTLS for CAPWAP APs joining over IPv6 tunnels is not supported on Cisco vWLC.
  - FlexConnect APs join IPv4 or IPv6 multicast group if AP multicast mode is configured as "multicast." You might experience data throughput degradation of up to 13 percent in FlexConnect centrally switched scenarios compared to when AP multicast mode is configured as "unicast."

Security and RADIUS-related Features

- Vendor-specific Attribute Value Pairs (AVPs)—Service providers can configure the Cisco WLC to learn new vendor-specific AVPs (VSAs). This is done by importing a text file that is similar to an XML file that provides the VSAs and their values to the Cisco WLC and also tells the Cisco WLC what to do with the VSAs.
- You can configure Cisco WLC to use the realm value of a service provider as a tag to choose the RADIUS servers on which Authentication and/or Accounting has to be performed for a client. Configure this feature by following these steps:

a. Enable the feature on a WLAN.

b. Tag the RADIUS servers with the realm values as needed (up to 30 per RADIUS)

- If a client requests a web page through HTTPS, the client is redirected to the WebAuth login page.
- For RADIUS authentication, Cisco WLCs can send WLAN IDs and RADIUS can be configured to allow users to connect only from a specific WLAN and reject authentication from other WLANs. Previously, this rejection worked on web authentication WLANs, but not on other 802.1X or EAP WLANs. In Release 8.0.100.0, 802.1X or MAC filtering is also rejected if the WLAN ID does not match with the value returned from the AAA server. In addition, an SSID Cisco Attribute Value Pair (AVP) is supported that allows web authentication, 802.1X, or MAC filtering to be rejected based on values returned from the AAA server.
- In the earlier releases, for rogue rules, you were required to set a minimum RSSI value for the rogue APs to be classified. In this release, for friendly rogue rules, you are now required to set a maximum RSSI value. The RSSI value of the rogue AP must be less than the maximum RSSI value set for the rogue AP to be classified as a friendly rogue.

  For malicious and custom rogue rules, there is no change in functionality.

  For example, for a friendly rogue rule, the RSSI value is set at –80 dBm. All the rogue APs that are detected and have RSSI value that is less than –80 dBm are classified as friendly rogues. For malicious and custom rogue rules, the RSSI value is set at –80 dBm. All the rogue APs that are detected and have RSSI value that is more than –80 dBm are classified as malicious or custom rogue APs.

Ease of Management Features

- In previous releases, to change SSID and WLAN profile names, you were required to delete the WLAN and create it again. In Release 8.0.100.0, you can make these changes without having to delete the WLAN. For WLANs that are configured with PSK, you must reenter the PSK value.
- Ping can be sourced from a dynamic interface with repeat count and packet size as extended options. This enhancement is available only on the CLI. On the GUI, basic ping is available from the management interface.

  ```
  (Cisco Controller) >ping 209.165.200.225 ?
  [<interface-name>] [<repeat count[1-100]>] [<packet size[10-2000]>]
  Enter interface name and/or repeat count(1-100) and/or packet size(10-2000).
  ```

  Example:

  ```
  (Cisco Controller) > ping 209.165.200.225 MyDynamicInt 10 1000
  Send count=10, Receive count=10 from 10.1.1.254, Packet size = 1000
  ```

- The **show ap summary** command displays the IP address of the AP.

  Also, on the GUI, you can use the IP address of an AP as a filter to search for APs.

- The following set of new show system commands are added:

  ```
  (Cisco Controller) >show system ?
  dmesg          Displays dmesg logs
  interfaces     Displays information about the configured network interfaces
  interrupts     Displays the number of interrupts
  iostat         Displays CPU and input/output statistics for devices
  meminfo        Displays system memory information
  neighbours     Displays the IPv6 Neighbor Cache
  netstat        Display system network stats
  process        Displays process related information
  route          Displays system routing table
  ```

```
slabs           Displays memory usage on slab level
timers          Display system timer info
top             Displays the cpu usage
vmstat          Displays system virtual memory statistics
```

- The **show run-config startup-commands** is introduced. Use this command to:
  - see the list of startup configuration
  - perform recovery configuration by using its output
- You can globally enable Telnet and/or SSH for all APs that are associated or the APs that will associate with the Cisco WLC. In previous releases, this was possible only at the level of an individual AP. When you enable this feature, Telnet or SSH is allowed on APs that are yet to associate with the Cisco WLC regardless of their mode.
- An alternate color theme is available for the Cisco WLC GUI. This is useful when you have multiple GUI open at the same time, for example a production Cisco WLC GUI and a lab Cisco WLC GUI, and the two GUI can have separate themes so that they can be easily distinguished. Two options are available: Default and Red.

  To configure the color theme of Cisco WLC GUI, go to **Controller > General**; from the **Web Color Theme** drop-down list, choose between **Default** and **Red**.

  For more information, see the Enabling Web and Secure Modes section in the configuration guide.
- Cisco WLC software enables you to flash the LEDs on a Cisco AP to locate the AP. All Cisco IOS lightweight access points support this feature. In Release 8.0.100.0, you can also configure the flashing LEDs on the Cisco WLC GUI. In previous releases, you could configure this feature only the Cisco WLC CLI. For more information, see the *Configuring Flashing LEDs* section in the configuration guide.
- The **show client detail** command now shows the WLAN name and its profile.
- The **show ap join stats** command now shows the modified name of a Cisco AP, if the name of the AP was changed after the AP associated with the Cisco WLC. In previous releases, the command showed the old name of the AP that was present at the time of its association with the Cisco WLC and not the modified name.

  In a High Availability scenario, the modified name of the AP is synchronized.
- The debug client command now also shows the name of the Cisco AP that the client is associated with and the RSSI.
- You can now update the Organizationally Unique Identifier (OUI) list without having to wait for a future Cisco WLC software release.
  1. Copy the latest OUI list available at http://standards.ieee.org/develop/regauth/oui/oui.txt to the default directory of your server.
  2. On the Cisco WLC GUI, choose **Commands > Download File**. From the **File Type** drop-down list select the relevant options (**OUI Update** for OUI list).
  3. Click **Download**.
  4. After the download is complete, reboot the system.
- The IEEE 802.11v standard is supported. For more information, see the *Configuring 802.11v* section in the configuration guide.
- Support is added for the 802.11r mixed mode.

Note Legacy clients may not connect to 802.11r because of the added IE/OUI.

- Support is added for Cisco WLC to include Option 82, Sub-Option 5 when relaying the DHCPDiscover message from the client. The Sub-Option 5 defines the subnet, thereby allowing the GIADDR to only have one job, being just the relay source, the address that the relay agent can be reached at. The relay source can be any IP on the Cisco WLC that can easily be reachable from the DHCP server, for example the management interface IP.

  You can also use Sub-Option 151 to tell the DHCP the VPN-id or the VRF name of the subnet. Cisco Network Registrar (CNR) supports multiple IP pools based on VPN-ids or VRF names. The Cisco WLC can send the VPN-id or VRF name of the pool from which address has to be assigned.

  You can use Sub-Option 152 to know if the DHCP understood Sub-Option 151.

High Availability Enhancements

Infrastructure Enhancements

- 802.11ac configuration is supported in a High Availability scenario.
- You can see the status of bulk synchronization of access points and clients after the active and standby Cisco WLCs pair up.
- Enhanced debug options included where new categories of statistics can be viewed:
  - All
  - Infra
  - Transport
  - Keep-Alive
  - GW-Reachability
  - Config-Sync
- You can configure the keep-alive and peer search parameters.
- ICMP ping on redundancy management interface (RMI) is replaced with UDP message. This is useful when ICMP pings might be discarded under heavy loads.
- Default gateway reachability is enhanced—upon six consecutive ping drops, address resolution protocol request is sent to the gateway.
- If the peer redundancy port (RP) and/or default gateway reachability is lost, the standby Cisco WLC enters into maintenance mode 'on-the-fly' without requiring a reboot.
- Faster HA pair-up—Comparison of XMLs and reboot of the standby Cisco WLC are not performed during pair-up.

Client SSO Enhancements

- Internal DHCP server—To serve wireless clients of the Cisco WLC, the internal DHCP server data is synchronized from the active WLC to the standby WLC. All the assigned IP addresses remain valid, and IP address assignation continues when the role changes from active WLC to standby WLC occurs.
- Sleeping client database synchronization is supported between active WLC and standby WLC.

  Sleeping clients avoid web reauthentication if they wake up within the sleeping client timeout interval post switchover.

- Cisco 600 Series OfficeExtend Access Points (OEAPs) do not require the CAPWAP tunnel to be reset. Clients continue their connection with the new active WLC in a seamless manner.

For more information about configuring High Availability, see the *High Availability* section in the configuration guide.

Multicast DNS Enhancements

- Multicast DNS (mDNS) policies—mDNS policies allow creation of mDNS service groups and service instances within the group. Service instance mandates how the service instance is shared by configuring MAC address and name of the service instance; location of type of the service instance by AP group, AP name, or AP location. Service instance
- Policy Enhancements—You can create multiple mDNS profiles on the WLC and override them, configure what services should be available for the profiles, attach a profile to your SSID, and, if required, attach the profile to a local policy.

For more information about configuring mDNS, see the *Configuring Multicast Domain Name System* section in the configuration guide.

Application Visibility and Control Enhancements

- NBAR2 Protocol Pack 11.0.0 for Wireless LAN Controllers is available. For more information, see http://www.cisco.com/c/en/us/td/docs/wireless/controller/nbar2_prot_pack/11-0-0/b-nbar2-prot-pack-1100.html.
- AVC AAA override—AAA AVC profiles override per clients to get different AVC profiles when they are connected to the same WLAN. In previous releases, you could configure AVC profiles on a WLAN and all clients connected to the WLAN inherited the same AVC profile.

  AAA attribute for client or for a user profile can be configured on AAA servers, for example open RADIUS, Cisco ACS, or ISE.
- AVC per application, per client rate limiting on WLAN—In the previous release, only bidirectional per client bandwidth control was available. The downstream rate limiting per client was performed at the Cisco WLC, and the upstream rate limiting per client is performed at the AP. In Release 8.0.100.0, per client and per application based bidirectional rate limiting is available. In this feature, you can have per application bandwidth control per client
- AVC Integration with Local Profiling—You can apply AVC profiles to the local policy classification per user and per device.
- AVC Directional QoS—In the previous release, QoS marking could be configured as an application rule on the AVC profile. The marking configured is a DSCP marking and is applied bidirectionally for both upstream and downstream. In Release 8.0.100.0, you can configure an additional parameter where the marking can be specified with respect to the direction.

For more information about configuring AVC, see the *Configuring Application Visibility and Control* chapter in the configuration guide.

Miscellaneous Features

- Assigning a unique range of VLAN IDs to each client can exceed the limit of 4096 VLANs. The 802.1Q-in-Q VLAN tag feature encapsulates the 802.1Q VLAN tag within another 802.1Q VLAN tag. The outer tag is assigned according to the AP group, and the inner VLAN ID is assigned dynamically by the AAA server.

  Using the 802.1Q-in-Q feature you can use a single VLAN to support multiple VLANs. With the 802.1Q-in-Q feature you can preserve VLAN IDs and segregate traffic of different VLANs. The figure below shows the untagged, 802.1Q-tagged, and 802.1Q-in-Q tagged Ethernet frames. For more information, see the *Configuring 802.1Q-in-Q VLAN Tagging* chapter.
- Mobility Access Gateway (MAG) on AP is supported on FlexConnect mode APs in a locally switched WLAN. For PMIPv6 clients, all the data traffic from the clients is tunneled to the LMA in the Generic Routing Encapsulation (GRE) tunnel established between the MAG and the LMA. Similarly, all packets received from the LMA in the GRE tunnel. For more information, see the *Configuring Proxy Mobile IPv6* chapter.
- VideoStream for FlexConnect local switched deployments—VideoStream enables conversion of multicast to unicast streams at the AP with appropriate Quality of Service (QoS) for high priority video traffic. VideoStream on FlexConnect provides smooth, reliable multicast video delivery over the WAN to multiple clients at remote sites.
- This release targets to have the following federal certifications:
  - FIPS (Federal Information Processing Standard) for all non-military government agencies and government contractors
  - Common Criteria: Federal Government and Organizations with Critical Infrastructure across the globe
  - UcAPL: Single consolidated list of products that have completed Interoperability (IO) and Information Assurance (IA) certification
  - USGv6: The National Institute of Standards and Technology to develop infrastructure standards and testing to support wide-scale adoption of IPv6 in the US Government.
- Based on guidance from the Wi-Fi alliance (WFA), WPA/TKIP can only be configured on a secondary interface (CLI). Any previously saved TKIP configurations are retained upon upgrade and can be viewed on the CLI. This allows customers with Wi-Fi clients that only support WPA/TKIP to have a planned migration to devices that support AES. For additional guidance, see the Technical Note for Removal of TKIP from Wi-Fi® Devices.
- Wired guest access is supported on Cisco 2500 Series WLCs.
- Changes in country code:
  - The country code KR is changed to KE (for Korea)
  - The country code JP (for Japan) is removed

  For a full list of Wireless LAN products and the specific countries each product is currently certified in for order and shipment, see http://www.cisco.com/c/en/us/products/collateral/wireless/access-points/product_data_sheet0900aecd80537b6a.html

Software Release Support for Access Points

Table 2 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 access point. For access points that are not supported in ongoing releases, the Last Support column lists the last release that supports the access point.

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

Table 2 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	—
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	—
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	—
	AIR-LAP1242AG	3.1.59.24	—
1250 Series	AIR-LAP1250	4.2.61.0	—
	AIR-LAP1252G	4.2.61.0	—
	AIR-LAP1252AG	4.2.61.0	—
1260 Series	AIR-LAP1261N	7.0.116.0	—
	AIR-LAP1262N	7.0.98.0	—

Table 2 Software Support for Access Points (continued)

Access Points		First Support	Last Support
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	—
AP801		5.1.151.0	—
AP802		7.0.98.0	—
AP802H		7.3.101.0	—
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	—

Table 2 Software Support for Access Points (continued)

Access Points		First Support	Last Support
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	—
3600 Series	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	—
Note The Cisco 3600 Access Point was introduced in Release 7.1.91.0. If your network deployment uses Cisco 3600 Access Points with Release 7.1.91.0, we highly recommend that you upgrade to Release 7.2.115.2 or a later release.			
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 2 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[1]	—
		All other reg. domains: 4.1.191.24M or 5.2 or later[1]	—
	AIR-LAP1522HZ	-A and N: 4.1.190.1 or 5.2 or later[1]	—
		All other reg. domains: 4.1.191.24M or 5.2 or later[1]	—
	AIR-LAP1522PC	-A and N: 4.1.190.1 or 5.2 or later[1]	—
		All other reg. domains: 4.1.191.24M or 5.2 or later[1]	—
	AIR-LAP1522CM	7.0.116.0 or later.	—
	AIR-LAP1524SB	-A, C and N: 6.0 or later	—
		All other reg. domains: 7.0.116.0 or later.	—
	AIR-LAP1524PS	-A: 4.1.192.22M or 5.2 or later[1]	—
1530	AIR-CAP1532I-x-K9	7.6	—
	AIR-CAP1532E-x-K9	7.6	—

Table 2 Software Support for Access Points (continued)

Access Points		First Support	Last Support
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-CAP1552-CU-x-K9	7.3.101.0	—
	AIR-CAP1552WU-x-K9	8.0.100.0	—
1552S	AIR-CAP1552-SA-x-K9	7.0.220.0	—
	AIR-CAP1552SD-x-K9	7.0.220.0	—

1. These access points are supported in a separate 4.1.19x.x mesh software release or in Release 5.2 or later releases. These access points are not supported in the 4.2, 5.0, or 5.1 releases.

An access point must always be connected to the POE-IN port to associate with the Cisco WLCs. The POE-OUT port is for connecting external devices only.

Software Release Types and Recommendations

This section contains the following topics:

Types of Releases

Table 3 Types of Releases

Type of Release	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 long-lived releases with ongoing software maintenance.	Provides you with a software release that offers stability and long support duration with periodic maintenance releases (MRs).
Early Deployment (ED) 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 4 Software Release Recommendations

Type of Release	Deployed Release	Recommended Release
Maintenance Deployment (MD) release	7.0 MD release train (latest release: 7.0.250.0)	7.4 MD release train (7.4.121.0 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 (7.4.121.0 is the MD release)
Early Deployment (ED) releases for 802.11ac deployments	7.5 ED release 7.6 ED release	7.6 ED release (7.6.130.0 is MR3 on 7.6 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

Solution Compatibility Matrix

Table 5 Solution Compatibility Matrix

Software Release	ISE	Cisco Prime Infrastructure	Cisco MSE
7.0 (MD train)	1.2	2.0	7.6
7.4 (MD train)	1.2	2.0	7.6
7.6 (ED)	1.2	Update 1 for 1.4.0.45	7.6
8.0 (MD train)	1.3	2.1.1	8.0

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 8.0.100.0

Guidelines and Limitations

- In Cisco Wireless Releases prior to 8.0.100.0, the behavior of the Redirect-URL-ACL (as returned via RADIUS attributes) may have been incorrect. The ACL was applied in only the Ingress direction (traffic destined for the LAN or distribution system) of the radio interface. These ACLs should also be applied in the Egress direction (traffic destined for the wireless client). Therefore, after upgrading to a Cisco Wireless Release 8.0 or a later release, you may need to adjust the ACL to accommodate the correction of this behavior.
- Cisco WLCs validate client IP address at the time of learning, using the dynamic interface IP address as per the VLAN assigned to the client. Ensure that the clients and the dynamic interface VLAN of the clients are on the same subnet, even if DHCP proxy is disabled at the Cisco WLC.
- 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 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, 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 8.0.100.0 to a 7.x release, the trap configuration is lost and must be reconfigured.
- If you have ACL configurations in the Cisco WLC and downgrade from a 7.4 or a later release to a 7.3 or an earlier release, you might experience XML errors on rebooting the Cisco WLC. However, these errors do not have any impact on any functionality or configurations.
- If you are upgrading from a 7.4.X or an earlier release to a later release, the Called Station ID type information is mapped to the RADIUS Accounting Called Station ID type; the RADIUS Authentication Called Station ID type, 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 access points (known as H-REAP access points 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 8.0.100.0, the access points 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 or a later 7.0.x release to Release 8.0.100.0.
- When a client sends an HTTP request, the Cisco WLC intercepts it for redirection to the login page. If the HTTP request 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 Field Upgrade Software (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 ACLs 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 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 8.0.100.0 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 8.0.100.0. Table 6 shows the upgrade path that you must follow before downloading Release 8.0.100.0.

Caution If you upgrade from a release that is prior to Release 7.5 directly to Release 7.6.X or a later release, the predownload process on Cisco AP2600 and AP3600 fails. After the Cisco WLC is upgraded to Release 7.6.X or a later release, the new image is loaded on Cisco AP2600 and AP3600. After the upgrade to a Release 7.6.X image, the predownload functionality works as expected. The predownload failure is only a one-time failure, which is limited to the predownload process.

Table 6 Upgrade Path to Cisco WLC Software Release 8.0.100.0

Current Software Release	Upgrade Path to 8.0.100.0 Software
7.4.x releases	You can upgrade directly to 8.0.100.0.
7.6.100.0	You can upgrade directly to 8.0.100.0.

- 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.
- Cisco Prime Infrastructure 2.1.1 is needed to manage Cisco WLC software Release 8.0.100.0.
- 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.
- We recommend that you insert Interoperability test for RADIUS to show Cisco ISE.
- 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 9 or a later version or Mozilla Firefox 17 or a later version.
- Cisco WLCs support standard SNMP Management Information Base (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 8.0.100.0. 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 8.0.100.0 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 a 5500 series Cisco WLC), or enter **5** (on another Cisco WLC platform) 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 address(es) are sent in the 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 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**} tag. For Release 7.2.103.0 and later releases, if you tag 802.1p packets, the tagging has impact only on 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 LAN Controller FlexConnect Configuration Guide*.

Note Predownloading Release 8.0.100.0 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.
- If you want to downgrade from Release 8.0.100.0 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 these functions on the Cisco WLC, you must 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 for a license

- Enable the 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
- For TCP MSS to take effect

Upgrading to Cisco WLC Software Release 8.0.100.0 (GUI)

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

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 the 8.0.100.0 Cisco WLC 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 available:

- Integrated Controllers and Controller Modules
- Standalone Controllers

d. Depending on your Cisco WLC platform, select one of these options.

e. Click the Cisco WLC model number or name.

The **Download Software** page is displayed.

f. Click a Cisco WLC software release number. The software releases are labeled as follows to help you determine which release to download:

- **Early Deployment (ED)**—These software releases provide new features and new hardware platform support as well as bug fixes.
- **Maintenance Deployment (MD)**—These software releases provide bug fixes and ongoing software maintenance.
- **Deferred (DF)**—These software releases have been deferred. We recommend that you migrate to an upgraded release.

g. Click a software release number.

h. Click the filename (*filename*.aes).

i. Click **Download**.

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

k. Save the file to your hard drive.

l. Repeat steps a. through k. 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, or small Cisco WLC platforms, we recommend that you disable the 802.11a/n and 802.11b/g/n networks as a precautionary measure.

Step 5 Choose **Commands > Download File** to open the Download File to Controller page.

Step 6 From the **File Type** drop-down list, choose **Code**.

Step 7 From the **Transfer Mode** drop-down list, choose **TFTP**, **FTP**, or **SFTP**.

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

Step 9 If you are using a TFTP server, the default values 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) that the TFTP server attempts to download the software, in the **Timeout** text box.

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

Step 11 In the **File Name** text box, enter the name of the software file (*filename*.aes).

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

a. In the **Server Login Username** text box, enter the username to log on to the FTP server.

b. In the **Server Login Password** text box, enter the password to log on to the FTP server.

c. In the **Server Port Number** text box, enter the port number on the FTP server through which the download occurs. The default value is 21.

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

A message appears indicating the status of the download.

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

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

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

Step 17 For Cisco WiSM2 on the Catalyst switch, check the port channel and re-enable the port channel if necessary.

Step 18 If you have disabled the 802.11a/n and 802.11b/g/n networks in Step 4, re-enable them.

Step 19 To verify that the 8.0.100.0 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 Download the Cisco DTLS license.

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

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

b. On the Product License Registration page, choose **Get New > IPS, Crypto, Other Licenses**.

c. Under **Wireless**, choose **Cisco Wireless Controllers (2500/5500/7500/8500/WiSM2) DTLS License**.

d. Complete the remaining steps 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. You can install the license either by using the Cisco WLC web GUI interface or the CLI:

- To install the license using the 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 this URL:

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 19 detailed in the "Upgrading to Cisco WLC Software Release 8.0.100.0" section on page 20.

Interoperability With Other Clients in Release 8.0.100.0

This section describes the interoperability of Release 8.0.100.0 of the Cisco WLC software with other client devices.

Table 7 describes the configuration used for testing the clients.

Table 7 Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	8.0.100.0
Cisco WLC	Cisco 5500 Series Controller
Access points	1142, 3500e, 3500i, 3600, 2602, 3702, 2702, 702W
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 8 lists the client types on which the tests were conducted. The clients included laptops, handheld devices, phones, and printers.

Table 8 Client Types

Client Type and Name	Version
Laptop	
Intel 4965	v13.4
Intel 5100/5300/6200	v14.3.2.1
Intel 6300	v15.11.0.7
Intel 1000/1030/6205	v14.3.0.6
Intel 7260 (11AC)	17.0.5.8
Intel 3160 (11AC)	17.0.5.8
Broadcom 4360 (11AC)	6.30.163.2005
Linksys AE6000 (USB 11AC)	5.0.7.0
Netgear A6200 (USB 11AC)	6.30.145.30
D-Link DWA-182 (USB 11AC)	6.30.145.30
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)	v5.100.235.12
Cisco CB21	v1.3.0.532
Atheros HB92/HB97	8.0.0.320
Atheros HB95	7.7.0.358
MacBook Pro (Broadcom)	OSX 10.9.4
MacBook Air	OSX 10.9.4, BCM43xx 1.0(6.30.223.154.45)
Macbook Pro with Retina Display 2013	OSX 10.9.4
Tablets	
Apple iPad2	iOS 8.1.2(12B440)
Apple iPad3	iOS 8.1.2(12B440)
Apple iPad mini with Retina display	iOS 8.1.2(12B440)
Apple iPad Air	iOS 8.1.2(12B440)
Asus Transformer	Android 4.0.3
Sony Tablet S	Android 3.2.1
Toshiba Thrive	Android 3.2.1
Samsung Galaxy Tab	Android 3.2
Samsung Galaxy Tab 10.1- 2014 SM-P600 (11AC)	Android 4.4.2
Samsung Galaxy Note 3 SM-N900(11AC)	Android 4.4.2
Microsoft Surface Pro 3 Tablet (11AC)	Windows 8.1 Driver: 15.68.3044.85

Table 8 Client Types (continued)

Client Type and Name	Version
Microsoft Surface Pro 2	Windows 8.1 Driver: 14.69.24039.134
Motorola Xoom	Android 3.1
Nexus 7 2nd Gen	Android 4.4.2
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
Ascom i75	1.8.0
Spectralink 8030	119.081/131.030/132.030
Apple iPhone 4S	iOS 8.1.2(12B440)
Apple iPhone 5	iOS 8.1.2(12B440)
Apple iPhone 5s	iOS 8.1.2(12B440)
Apple iPhone 5c	iOS 8.1.2(12B440)
HTC One(11AC)	Android 4.2.2
Samsung Galaxy S4 GT-I9500 (11AC)	Android 4.3
Sony Xperia Z Ultra(11AC)	Android 4.3
Nokia Lumia 1520 (11AC)	Windows Phone 8.1
Google Nexus 5 (11AC)	Android 4.4.3
Samsung Galaxy S5-SM-G900A (11AC)	Android 4.4.2
HTC Sensation	Android 2.3.3
Samsung Galaxy S III	Android 4.3
SpectraLink 8450	3.0.2.6098/5.0.0.8774
Samsung Galaxy Nexus GTI9200	Android 4.2.2
Sony Xperia Z Ultra (11AC)	Android 4.4.2
Samsung Galaxy Mega SM900 (11AC)	Android 4.4.2

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 2500 Series WLCs
- Features Not Supported on WiSM2 and Cisco 5500 Series WLCs
- Features Not Supported on Cisco Flex 7500 WLCs

Features Not Supported on Cisco 2500 Series WLCs

- Bandwidth Contract
- Service Port
- AppleTalk Bridging
- Right-to-Use licensing
- PMIPv6
- AP stateful switchover (SSO) and client SSO
- Multicast-to-Unicast

Note The features that are not supported on Cisco WiSM2 and Cisco 5500 Series WLCs are not supported on Cisco 2500 Series WLCs too.

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

Features Not Supported on WiSM2 and Cisco 5500 Series WLCs

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

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

- Configuration of 802.3 bridging, AppleTalk, and Point-to-Point Protocol over Ethernet (PPPoE)
- Fragmented Pings on any interface
- Right-to-Use licensing

Features Not Supported on Cisco Flex 7500 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 like an AP-manager interface by default, and the access points can join on this interface.

- TrustSec SXP
- IPv6/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 IGMP or MLD snooping.

- PMIPv6

Features Not Supported on Cisco 8500 WLCs

- TrustSec SXP
- Internal DHCP Server

Features Not Supported on Cisco Virtual WLCs

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

- Multicast

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

- FlexConnect central switching

Note FlexConnect local switching is supported.

- AP and Client SSO in High Availability
- PMIPv6
- WGB
- Mesh (use Flex + Bridge mode for mesh enabled FlexConnect deployments)

Note Outdoor APs in the FlexConnect mode are supported.

- Application Visibility and Control (AVC)
- Client downstream rate limiting for central switching
- SHA2 certificates

Features Not Supported on Mesh Networks

- Multicountry support
- Load-based 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 1130 and 1240 APs

All the features introduced in Release 7.2 and later releases are not supported on 1130 and 1240 APs. In addition to these, the following features are not supported on 1130 and 1240 APs:

- Central-DHCP functionality

- Split tunneling
- Configuration of Network Address Translation (NAT) and Port Address Translation (PAT) on FlexConnect locally switched WLANs
- Point to Point Protocol (PPP) and Point to Point Protocol over Ethernet (PPPoE) for APs in FlexConnect mode
- 802.11u
- 802.11r Fast Transition
- LLDP
- Rate Limiting per AP
- mDNS AP
- EAP-TLS and PEAP for Local Authentication support as EAP method
- WLAN-to-VLAN mapping when AP part of FlexConnect Group
- Per user AAA AireSpace ACL name override
- Local MFP
- DNS-based (fully qualified domain name) access control lists (ACLs)
- Flex + Bridge mode (introduced in Release 8.0.100.0)

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

- PPPoE
- PMIPv6

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

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

Cisco Wireless LAN Controller Release 8.0 Features Not Configurable in Prime Infrastructure, Release 2.1.1

The following Release 8.0.100.0 features cannot be configured via pre-packaged templates in Cisco Prime Infrastructure, Release 2.1.1; you can use Cisco Prime Infrastructure CLI templates or Cisco Wireless LAN Controller GUI to configure these features:

- Cisco Aironet 1700 Series Access Points
- Native IPv6 Infrastructure
- DHCP relay Option 82, Sub-Options 5, 151
- CMX FastLocate
- Advanced Rogue Reporting

- Client Deauthentication/Blocked List (Geo Fencing)
- Adaptive wIPS enhancements
- EAP-AKA support
- HTTPS support for web authentication
- PMIPv6 on AP
- Q-in-Q
- mDNS per user and per device policies
- Cisco 2500 Series WLC wired guest access
- DCA RF profiles
- Data packet RSSI
- FlexConnect + Bridge mode for mesh-enabled FlexConnect APs
- Receiver Start of Packet Detection Threshold (Rx-SOP)
- HDX—optimized roaming
- VideoStream support for FlexConnect local switched deployments
- Support for a new –F domain (Indonesia) on Cisco AP702I and AP3700
- Cisco AP701E (India only) with External Antenna support
- Cisco 600 Series OEAP enhancements—Basic Firewall, End-user GUI enhancements, Split-tunnel for Internet traffic, Voice QoS enhancements, HA support for OEAP
- PPPoE on Cisco FlexConnect APs
- VLAN tagging on Cisco Aironet 700W Series Access Points

Note For a comprehensive list, including features in previous WLC releases that cannot be configured via pre-packaged templates in Cisco Prime Infrastructure 2.1.1, see *Cisco Prime Infrastructure 2.1.1 Release Notes*.

Caveats

Cisco Bug Search Tool

The Bug Search Tool (BST), which is the online successor to 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 listed in this document:

1. Access the BST (use your Cisco user ID and password) at https://tools.cisco.com/bugsearch/.

2. Enter the bug ID in the **Search For:** field.

Note Using the BST, you can also find information about the bugs that are not listed in this section.

Open Caveats

Use the BST to view the details of a caveat listed in this section. For more information about the BST, see the "Cisco Bug Search Tool" section on page 35.

Table 9 Open Caveats

ID	Headline
CSCuq14231	7500 WLC: Efficient upgrade IPv6—subordinates cannot download new image
CSCuo19677	Cisco WLC does not update AP with new bandwidth setting
CSCup80403	Low iMac throughput; supported rate IE in association response has zero length
CSCup26155	The **show profiling policy summary** and **show profiling oui-string summary** command output is empty after download
CSCup46302	Virtual WLC: RSSI missing from Monitor mode AP
CSCup54560	2600 AP in mesh mode dissociates from Cisco WLC
CSCup72151	AP3602: 802.11ac module is not negotiating power with third-party switch
CSCup72502	Cisco 5500 Series WLC using Release 7.6 does not deauthenticate the client when FlexConnect ACL is not present on the Cisco AP
CSCup77631	IPv6 queue full and continuous IPv6 message logs
CSCup47579	AP Core Dump check box disabled (GUI), AP mode change from FlexConnect to Local
CSCun20584	AP replicates broadcast packets to the default gateway
CSCuo95494	Client cleanup does not occur on WLC
CSCun83393	Cannot compile CISCO-LWAPP-DOT11-CLIENT-MIB by MG-Soft
CSCup21962	Client data not passed to anchor WLC with fast SSID change enabled
CSCuc78713	dWEP client cannot receive broadcast after broadcast key rotation
CSCup81511	Incorrect WMM UP to DSCP markings on AP1131 and AP1242
CSCup00196	Local auth EAP-FAST not working for Flex AP Auth users on AP1240
CSCuj93777	Mesh AP should block data packets before BPDU packets are handled
CSCup29095	Mesh: PI not showing the neighbor details in mesh links page of Parent
CSCup60282	Ping generated from WLC seen as incorrect ICMP type
CSCuo27106	Radio Reset: (SC2) with FW stuck in macenb() in AP3500
CSCup49763	RRM: All channel scan option does not work in AP702 and AP702w
CSCuo48442	Stale old DTLS data_encryption session histories are left on WLC
CSCun34295	WiSM2 crash on task radiusTransportThread
CSCuj60872	WLC crash due to reaper reset for apfMsConnTask_6
CSCup64468	WLC device sends invalid format "#" in front of syslog message

Table 9 Open Caveats (continued)

ID	Headline
CSCud76513	WLC Issue: Neighbor information missing
CSCup78183	WLC: MSGQ running high. Traceback and numerous messages
CSCup57457	WS-SVC-WISM2-K9 unable to change Rogue state
CSCuj27382	AP local authentication, PEAP authentication fails, with EAP-TLS enabled and no/expired cert
CSCum94488	DHCP Packets are not forwarded when LAG enabled
CSCuo05142	EAP-AKA Client Unable to Reauth Using Fast Re-Auth Id & Mult Auth Server
CSCuo48496	9971 phones frequently getting disconnected
CSCuo70310	Flex+bridge with PPPoE mode AP not associating with Cisco WLC
CSCup23562	WLC crash when uploading a big file (add user section under FlexConnect group)
CSCup46986	The first DHCP client needs to be kicked off after detected duplicate IP
CSCup98461	Cisco WiSM2: BCAST-DATA-Q queue full and dropped message
CSCsv54436	SSH to WLC is sometimes denied “Sorry, telnet is not allowed on..”
CSCum25947	PPPoE configurations are still retained after write erase on AP
CSCun59052	Page error occurs after applying the configuration on the VLAN mapping page
CSCun96815	OEAP ACLs and network lists are deleted after upload/download of the configuration
CSCuo43002	Enabling IP Protocol 119 from GUI does not display on show-run
CSCup02792	CLI configuration issues regarding enabling or disabling of rogue traps
CSCup24106	Cisco 600 Series OEAP has DHCP when infrastructure running QoS on switchport
CSCup31640	Changing channel to Auto does not set maximum bandwidth for FlexConnect APs
CSCup71136	Mac filter: MAC delimiter does not change in accounting message
CSCup82618	The **show ap coredump** command treats IPv4 TFTP server address as IPv6
CSCup82681	8500 GUI AP core dump TFTP server IPv6 address is in reverse format
CSCup86941	GUI: Policy type for “Static WEP” clients is showing as N/A
CSCup96492	IPv6 route with /128 prefix removes after reboot
CSCup97263	Flex 7500 WLC: System Crash, Dot1x_NW_MsgTask_2
CSCup98731	https-redirect command is missing in the uploaded config file
CSCup99871	AP1602i radio reset; reason is fp cl pak stuck
CSCuq05410	vWLC/SRE: Boot option 3 to change active boot image is not working
CSCuq21626	IP address reversed in duplicate IP trap in 8500 WLC
CSCuq26793	PPPoE: Beacons stuck RLDP_STOP payload not received AP after RLDP_START
CSCuq27344	Client cannot get IPv6 stateless autoconfig address from direct-connected AP
CSCuq35830	802.11v-MC2UC conversion not happening for 802.11v client after a Layer3 roam
CSCui57047	Cisco WLC stopped working with taskname SXP SOCK
CSCul40203	Interface is not marked as dirty because of dual stack clients
CSCum63522	Cisco 2504 WLC stopped working on a boot-up using Release 7.6

Table 9 Open Caveats (continued)

ID	Headline
CSCum89244	Check heap crash due to random 4-byte corruption
CSCun26702	WLC stopped with MSE on Release 8.0
CSCuo96366	RADIUS authentication stops
CSCup15669	mDNS CSV: WLC stops working when downloading a big file
CSCup16770	WLC crash Reaper Reset: Task “emWeb” missed software watchdog
CSCuq11792	WLC stopped working, pmalloc memory corruption all zeros
CSCuq13913	mwar_reaper_watcher.crash
CSCuq14453	Memory leak on WLC when using PMIPv6 clients
CSCuq21999	CAPWAPv6 DTLS sessions tear down when data DTLS is enabled
CSCuq26869	Cisco 5508 WLC stopped working on loading newer AVC protocol-pack
CSCuq28913	WLC login fails form GUI for Local/Mgmt User
CSCuq28973	Cisco 8500 WLC stopped working on “IPv6_Msg_Task”
CSCuq32731	WLC stopped working on mmRemoveHbMbr while peering with new mobility
CSCuq33496	Inaccurate accounting information in interim packets
CSCuq33765	Cisco AP1600 in FlexConnect mode with local switching does not forward DHCP broadcast
CSCuq36863	Adding member to mobility domain is not working
CSCvc65568	Cisco Wireless IP Phone 8821 fails 802.11r FT roam with 'Invalid FTIE MIC'

Resolved Caveats

Use the BST to view the details of a caveat listed in this section. For more information about the BST, see the “Cisco Bug Search Tool” section on page 35

Table 10 Resolved Caveats

ID	Headline
CSCuq16408	WiSM2: Multiple crashes on Release 7.6.130.0
CSCsz82878	4.2 Mesh controller unresponsive with Task Name: reaperWatcher
CSCtc16222	FFT: %OSAPI-0-INVALID_TIMER_HANDLE: timerlib_mempool.c:240
CSCtd34834	MFP traps cannot be disabled, filling logs on LWAPP/CAPWAP platforms
CSCtj06944	Kernel panic, not syncing; failed to allocate SKB for hardware pool 0
CSCtq32444	Cisco 5500 Series WLC:SNMP message port UP trap went missing in LAG mode
CSCtx69300	CAPWAP-3-SEM_RELEASE_ERR errors in syslog
CSCuc68995	Webauth client was not authenticated to the network and HTTP GET from the client arrived at the controller in multiple TCP segments.
CSCud57046	Client entry seen on multiple Cisco WLCs
CSCud69426	AAA overridden ACL is not applied in WLAN change

Table 10 Resolved Caveats (continued)

ID	Headline
CSCuf77488	wIPS alarm detection time stamp is ahead of AP clock
CSCuf77821	Cisco WLC cross-frame scripting vulnerability
CSCuf79553	SSH to WLC is working when management via dynamic interface is disabled
CSCug04801	After a few failovers, none of the clients gets authenticated
CSCug19563	Cisco WiSM2 secondary stops responding during bootup due to deadlock
CSCug25043	Multicast overridden command not working for group name with quotes
CSCug34802	Rogue detector AP fails to correlate and contain wired rogues on 5 GHz
CSCug38140	Unexpected message on Cisco WLC: `*SNMPTask: Central Switch = TRUE`
CSCug38888	APs broadcast disabled SSIDs
CSCug57545	SNMP NAC should not be allowed without NAC alert enabled
CSCug73845	WLC NAS ID override is taking system name
CSCug74517	WLC shows incorrect interface name when it has hundreds of interfaces
CSCug82058	WLAN policy-mapping configuration is lost after XML download
CSCug82223	AP CLI to configure mode (mesh, local)
CSCug82805	RRM group leader not getting formed for 2.4 GHz
CSCug91684	Layer 2 ACL not working in Virtual WLC central switching
CSCuh08009	WPA2-PSK MAC filter assign interface incorrect after client roaming is back
CSCuh09591	Msglog: Service specific query: Sending series specific query failed
CSCuh11730	FlexConnect local switching: delete mn 0d0d.0d0d.0d0d
CSCuh12796	Consecutive SNMP 'set' commands for same MIB variable on WLC fails
CSCuh14286	Mobility multicast should be independent of global multicast
CSCuh16842	Override of assigned interface on interface group due to static IP breaks IPv6
CSCuh16870	Override of assigned interface on interface group due to static IP removed on reauthentication
CSCuh19576	IPv6 issues with Guest Wired client after HA switchover
CSCuh26716	The **show redundancy summary** command shows “HA SKU” even if it is not an HA-SKU machine.
CSCuh42398	#NIM-3-CANT_DISABLE_MCAST: nim.c:4542 Cannot disable multicast state
CSCuh42665	Release 7.4: Invalid trap notifications are sent
CSCuh44430	SE-Connect mode APs CleanAir status is “NA” after fallback
CSCuh46442	Cisco Lightweight AP (LAP) displays %CAPWAP-3-ERRORLOG messages when AP joins
CSCuh65866	CDP should not be advertised both over physical & LAG ports
CSCuh69558	Default interface takes precedence over foreign VLAN mapping with AAA override
CSCuh81923	WLC sends incorrect RADIUS accounting attributes
CSCuh94259	mDNS on interface group fails: Active WLAN using interface group

Table 10 Resolved Caveats (continued)

ID	Headline
CSCuh97457	WLC incompatibility behavior on CoA for RFC 3576 implementation
CSCui01948	PI: SNMP operation to device failed, table too large; possible agent loop
CSCui02779	LDPE and non-LDPE should not be allowed to form an HA pair
CSCui09037	H-REAP (FlexConnect) client IP address did not get updated on WLC sometimes
CSCui14583	mDNS: configuration knob to control sharing of wireless services to DS
CSCui16915	IRCM: Guest tunneling broken with Cisco 5700 Series WLC as guest controller and Cisco 5500 Series WLC as mobility controller
CSCui22330	Define default QoS DSCP and CoS (802.1p) value to meet IEEE/IETF standards
CSCui26077	FT roams do not work with FlexConnect APs
CSCui37300	mDNS: WLC uses 0.0.0.0 as source IP for query/response when using native VLAN
CSCui38822	OC: GUI does not allow change of HA secondary WLC to primary WLC
CSCui48331	Virtual WLC stops responding when brought up if management interface is not connected
CSCui56456	RNG in Web Management Cookie is not cryptographically secure
CSCui65855	WLC sends traffic from the virtual interface IP address on the wire
CSCui75794	Foreign WLC does not respond to ARP which is from foreign client -> local
CSCui90116	AP sends FT-auth original and retry packet to WLC causing MIC mismatch
CSCui94634	FlexConnect AP dissociates after ACL push; CAPWAP processing hangs DTLS timeout
CSCui95938	Fast switching SSID and iPad issue
CSCui99062	Console is unavailable after Ctrl+Shift+6 is pressed
CSCuj04921	802.11ac module: S4 LinkSys 3x3 and Macbook Air clients do not reach m8/m9 data rates
CSCuj05274	WLC Crash Reaper Reset: Task “loggerMainTask” missed software watchdog
CSCuj11877	Configuration backup adds duplicate entries for 802.11a only WLAN
CSCuj12969	Remove **show syslog** command
CSCuj15593	Configuration with RF-profile commands cannot be uploaded
CSCuj15647	RRM normalization when Cisco AP2600 and AP3600 are on UNII-1 and UNII-3 channels
CSCuj17683	802.11r roaming: AP might sometimes send deauthentication with reason code 7
CSCuj28495	clmgmtLicenseUsageCountRemaining does not return the remaining AP count
CSCuj29192	WLC: Traceback error seen with multiple instances
CSCuj32157	iPad/iPhone are unable to discover print services
CSCuj32257	AP secures CAC bandwidth for SIP phone during inter-WLC roaming without call
CSCuj33908	Wired Guest Anchoring fails due to bad proxy ARP behavior on Foreign WLC
CSCuj35236	Changing H-REAP (FlexConnect) SSID settings leads to error if two profiles have the same SSID
CSCuj36599	On the same FlexConnect AP, P2P blocking for 802.1X WLAN does not work

Table 10 Resolved Caveats (continued)

ID	Headline
CSCuj48021	Client stays in web authentication required state roam from a 7.4 maintenance release to Release 7.6
CSCuj53861	The **config advanced statistics** ports configuration command is not applicable
CSCuj58625	Local EAP FAST crashes WLC
CSCuj60088	MM-3-MEMORY_READ_ERROR: msg logs on Cisco 5508 WLC
CSCuj61455	FlexConnect clients are being deauthenticated for an unknown reason
CSCuj64462	AP radio flapping with CleanAir not operational; could not connect to spectrum FW
CSCuj66912	Cisco WiSM2 SNMP get for secondary power supply is incorrect
CSCuj73249	Unable to enable Telnet for AP after configuring AP global credentials
CSCuj74920	Intermittent RADIUS assigned VLAN fails during inter-WLC roam
CSCuj75643	Sanity: Cisco AP1600 radio FW DL error; timed out waiting for FW ready
CSCuj77222	FlexConnect AP should not be renewing DHCP address in standalone mode
CSCuj78942	Cisco AP1240 does not save trunk VLAN tag set under the Advanced tab
CSCuj83637	WLC HA: Service port with DHCP address loses connectivity after failover
CSCuj84256	Cisco 602 OEAP: If WMM is disabled on WLAN, DHCP fails for some 802.1X clients
CSCuj85183	Incorrect fan status is reported after one power supply goes down
CSCuj85557	MAP is not able to join RAP after reboot
CSCuj95892	Syslog Msg not generated when a port in a LAG comes back up
CSCuj96172	bsnDot11StationAssociate varbinds order is different than what is defined
CSCuj97293	Cisco WLC stops working at PKI_GetCertIssuerInfo with **show local-auth certificates** command
CSCuj97899	Cisco MSE interprets Cisco WLC time in UTC time zone
CSCul03672	Commands of backup WLC are lost after restoration on Release 7.5.102.0
CSCul04029	Cisco 5508 WLC using Release 7.3.112.0 stopped working on task “emWeb”
CSCul04090	Reaper Reset: Task “SNMPTask” missed software watchdog
CSCul10779	Cisco WLC Release 7.5 stopped working on task “emweb”
CSCul15555	FlexConnect AP decrypt errors after CCKM roam phone stuck in DHCP required state
CSCul16709	Unable to associate the AP with the WLC
CSCul16911	CAPWAP causing APs to dissociate due to DTLS errors
CSCul25617	Enabling AP Manager on Cisco 2500 Series WLC shows irrelevant mDNS profile popup
CSCul27458	Need to alert management VLAN tagging requirement when enabling HA
CSCul28720	Incorrect MIB values with configuration encryption
CSCul31732	FlexConnect VLAN mode was changed to Disabled after power cycle
CSCul34417	WLCs stay in Active-Active without auto-recovery while network converges
CSCul35067	Mobility CAPWAP data path down after an HA failover

Table 10 Resolved Caveats (continued)

ID	Headline
CSCul35507	Frequent message displayed: `#DEBUG-4-INVALID_MODULE: debug.c:2636 Unhandled debug`
CSCul38572	CCKM roaming fails between a WLC using Release 7.0 and a WLC using Release 7.4.
CSCul40660	The **grep** command does not work on the **show run-config** commands
CSCul42704	wIPS-Rogue APs are mistaken as infrastructure devices
CSCul43921	Valid wireless APs in network are recognized as rogue APs
CSCul44588	Channel N/A was shown in wIPS alarms
CSCul57266	The **show client detail** command on WLC is inaccurate compared to the FlexConnect AP
CSCul57988	Cisco WLC stopped working on Task Name: EAP Framework
CSCul72669	Deauthentication frame is not sent out before interface reset by RLDP
CSCul72696	Clean-up LWAPP-3-INVALID_AID2 message on standby in scale set-up
CSCul75283	Cisco 2500 WLC end user warning correction for anchored WLAN to 1-16
CSCul78198	RAID Volume Status should show proper error codes instead of unknown
CSCul82557	FlexConnect group PMK cache causes SpamReceieveTask 100 percent making AP not join
CSCul87119	Cisco WLC log: ICMP destination unreachable; reported as invalid ping response
CSCul89084	APF-RG-Q task to gracefully handle messages under Q full condition
CSCul98577	Wired guest can leak traffic out WLC Management Interface
CSCum00101	Cisco AP2600, AP3600: Data tunnel stuck with DTLS encryption enabled
CSCum13073	Security Rogue Error messages
CSCum15629	Cisco AP1140 in FlexConnect mode stops working on Release 7.4.110.0 due to authentication timer in loop
CSCum42581	Standby XML corrupted and go into configuration wizard in some scenario
CSCum53429	AP1130 FlexConnect VLAN mapping corrupted after VLAN mapping change
CSCum61068	“SNMP connection failure” error for Cisco WLCs on PI 2.0
CSCum63497	Cisco vWLC: Release 7.6 service port on distributed switch breaks communication
CSCum66202	FlexConnect: Per-user ACL + WebAuth success/logout page not displayed
CSCum73288	Friendly rogue AP disappears after 2 minutes
CSCum77921	OC: Cisco 5508 WLC stopped working @sshpmLscScepTask when enabling AP LSC provisioning
CSCum80614	WLC: Tracebacks seen with ‘cannot create ACL’ messages
CSCum86401	LAP in UNKNOWN_STATE on WLC
CSCum87244	Client becomes Associated status without receiving M4
CSCum87504	MFP Anomaly Detected messages continuously displayed
CSCum93435	WLC Tracebacks seen with mfpKeyRefreshTask - #SSHPM-3-NOT_INIT
CSCum93447	AP detected wIPS alarm not getting uploaded to MSE for some alarm

Table 10 Resolved Caveats (continued)

ID	Headline
CSCun03228	#DTL-3-NPUARP_ADD_FAILED: dtl_arp.c:2550
CSCun11124	Cisco vWLC serial number changes when using DRS or Vmotion
CSCun12864	AP group NAS ID not applied on client in AAA override enabled WLAN
CSCun15820	WLC reports its own MAC address in Duplicate IP message
CSCun18315	RADIUS server anomalies with WLC
CSCun19827	DHCP IPv6 address detected as duplicate on Mac/Linux
CSCun22507	The **transfer run-config** command lacks WLAN and L2ACL configuration information
CSCun25987	AP stays in RLDP process for a long time resulting in beacon outage
CSCun29362	#SNTP-3-FATAL_ERROR_OCCURED: sntp_main.c:233
CSCun34605	RADIUS profiling fails on Windows XP and Windows 7
CSCun38541	Conditional web redirect not working
CSCun40401	Cisco AP1552C blocks Ethernet port to CM
CSCun45503	FlexConnect: Wired client's MAC address table not updated on WGB roaming
CSCun47705	Multicast direct (MC2UC) does not work on Cisco 8500 Series WLC
CSCun62368	RADIUS NAC client authentication issues in Release 7.6
CSCun66868	WLC stops working on snmpApCurrChanChangedTrapSend task
CSCun67484	Synchronization failed on standby for the usmdb:HA_send_usmDbMsAddToBlackList task
CSCun69089	Vocera Badges Broadcast stops working randomly
CSCun85954	Release 7.6: Cisco 5508 HA WLC stops working on rsyncmgrXferMain task
CSCun88824	SNTP_FATAL_ERR: Unable to flush socket errno:Socket operatn on non-socket
CSCun93966	TTL expiry refresh is not working _universal._sub._ipp._tcp.local
CSCun99205	Rogue Containment issues in Cisco AP3600 with NOS module in Release 7.6
CSCuo04630	Cisco AP700 does not allow clients to connect when WPA1-PSK-TKIP is used
CSCuo12679	Cisco WLC does not delete client after dissociation by SmartRoam
CSCuo18203	Remove Mgmt via Wireless per SSID feature from 8.0
CSCuo18300	WLC: DNS-based ACL feature is case sensitive and should not be
CSCuo18573	Safeway: AP Queue full when WLAN-VLAN configuration is pushed
CSCuo20386	WLC Release 7.6.110.0: Incorrect AP detail for 802.11ac module
CSCuo20684	The value timestamp-tolerance is changed from 1000 to 0 after restoring
CSCuo20803	ACL rule direction is changed from any to out during backup
CSCuo21355	AP shows logs with 'Bad refcount in datagram_done' traceback
CSCuo35247	LAP unable to set up DTLS with WLC if packets arrive out of order
CSCuo36531	WLC crashing with Task Name: mmListen
CSCuo39416	AP1131/1242 not forwarding CWA redirects in Release 7.6
CSCuo44310	AP3600 loses country code on reboot, joins Disabled

Table 10 Resolved Caveats (continued)

ID	Headline
CSCuo59440	WLC Release 7.6: (GA) Guest account suspension on ISE does not disconnect client
CSCuo62930	Unable to map ACL to WLAN through GUI
CSCuo63046	WLC stops working on spamApTask6 task
CSCuo63103	Client local switching to central mode load, AAA override, RADIUS NAC
CSCuo69228	AP802 FlexConnect resets radios on connecting back to WLC from standalone mode
CSCuo69578	AP1532E/I bridge throughput is very low on 802.11n
CSCuo71252	Express Setup Wizard Country and Timezone set to US regardless of configuration
CSCuo71809	CleanAir: Stale Bluetooth device entries in down state in AP with WSSI
CSCuo73572	Unable to add Cisco 8510 and 7510 WLCs to Prime Infrastructure Release 2.1
CSCuo74061	AP1600: Intermittent low throughput (less than 1 Mbps to 2 Mbps)
CSCuo74117	20/40/80 MHz off-channel scan on serving channel
CSCuo82443	WLC resets cumulative user connection period on roaming
CSCuo83747	DHCP RADIUS profiling not working over FlexConnect APs
CSCuo84219	Wi-Fi: AP1600 drops packets when a burst of A-MSDU data is received
CSCuo85511	WiSM2 entity MIB does not specify WLC type
CSCuo86478	WLC set incorrect DHCP relay agent for Layer-2 roaming
CSCuo86819	WLC stops working when using Release 7.6.120.0; memory corruption caused by web authentication
CSCuo87769	Unable to apply more than 7 RF Profiles to AP group
CSCuo97883	Cisco AP3700 5-GHz clients stop forwarding traffic under load with TKIP
CSCup03098	New Mobility configuration missing from Cisco 2504 WLC GUI.
CSCup03264	Anchor WLC does not append client parameters for external web authentication redirect
CSCup13788	Cisco 8510 WLC sends trap for unsuccessful login attempts with reversed IP
CSCup17073	WLC drops all PMIPv6 packets after it gets an unknown packet with port 5436
CSCup18354	Japanese DBCS characters are garbled in internal web authentication login.html page
CSCup22587	Multiple Vulnerabilities in OpenSSL
CSCup32781	Bundle CSCuh20155 bootloader fix into Cisco AP2600 and AP3600 IOS
CSCup37463	AP1552C Cable Modem AP's Gig Ethernet Link marked down
CSCup40557	HIGH CPU (98 percent) on webauthRedirect
CSCup42789	AP3602 with RM3000AC module unable to pass traffic
CSCup44648	PMIPv6: Add SSHPM Rules for PMIPv6 Control only when MAG enabled
CSCup47474	Unable to contain rogue multicast bit set in BSSID printed log
CSCup50131	Release 7.4.121.0: WLC stops working at RRM-MGR-2_4 task
CSCup55226	Apple client cannot authenticate on AP1130 and AP1240 using WLC software Release 7.6 with FT
CSCup62958	WLC no audit session ID for authentication for LWA external webauth

Table 10 Resolved Caveats (continued)

ID	Headline
CSCup60494	Gradual memory leak in 2048 byte chunks
CSCuo73696	RLDP config mismatch after RLDP STOP PAYLOAD resulted in radio reset
CSCup80133	AP802 crashed due to high memory with data encryption enabled
CSCuq04762	AP1532: Low power when using PWR-INJ4 in daisy chain configuration
CSCuq02173	PR 3600 Crash: capwap_ap_send_dot11_mgmt_msg
CSCup90929	802.11v: AP3700 radio reset while running MC traffic to DMS client
CSCuq08015	WLC crash: spamGetRadGroupName
CSCuq18025	High CPU 99% on webauth Redirect Task
CSCup24331	Wireless controller LDAP server in connected state instead of IDLE state

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!

1. 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.

2. 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.
3. 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.
4. 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.
5. When installing an antenna, remember:
   a. Do not use a metal ladder.
   b. Do not work on a wet or windy day.
   c. Do dress properly—shoes with rubber soles and heels, rubber gloves, long-sleeved shirt or jacket.
6. 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!**
7. 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.
8. 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 WLCs and access points.

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

Personnel installing the Cisco WLCs and access points must understand wireless techniques and grounding methods. Access points 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. Following 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

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

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

Click **Product Support > Wireless**. Then choose your product and **Troubleshooting** to find information on 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 LAN Controller Configuration Guide*
- *Cisco Wireless LAN Controller Command Reference*
- *Cisco Wireless LAN Controller System Message Guide*
- *Cisco Wireless Mesh Access Points, Design and Deployment Guide*

You can access these documents at this URL: http://www.cisco.com/c/en/us/support/index.html.

Obtaining Documentation and Submitting a Service Request

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

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.