Release Notes for Cisco Wireless Controllers and Lightweight Access Points for Cisco Wireless Release 8.1.102.0

First Published: May 8, 2015

This release notes document describes what is new in Cisco Wireless Release 8.1.102.0, instructions to upgrade to this release, and open and resolved caveats for this release. Unless otherwise noted, in this document, all Cisco Wireless Controllers are referred to as *Cisco WLCs*, and all Cisco lightweight access points are referred to as *access points* or *Cisco APs*.

Revision History

Table 1 Revision History

Modification Date	Modification Details
October 10, 2017	• Features Not Supported on Cisco Virtual WLCs, page 26 – Added Wired Guest.
September 14, 2016	• What's New in This Release, page 4 – Added: Cisco Flex 7510 WLC support for TrustSec (Security Group Tag Exchange Protocol (SXP) feature. • Features Not Supported on Cisco Flex 7510 WLCs, page 25 – Removed: TrustSec SXP from features not supported on Cisco Flex 7510 WLCs section.
August 17, 2016	• Guidelines and Limitations, page 12 – Added this statement: If you downgrade from Release 8.3 to Release 8.1, the Cisco Aironet 1850 Series AP, whose mode prior to the downgrade was Sensor is shown to be in unknown mode after the downgrade. This is because the Sensor mode is not supported in Release 8.1.

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

Cisco Wireless Controller and Cisco Lightweight Access Point Platforms

Supported Cisco Wireless Controller Platforms

The following Cisco WLC platforms are supported in this release:

- Cisco 2500 Series Wireless Controllers (Cisco 2504 Wireless Controller)
- Cisco 5500 Series Wireless Controllers (Cisco 5508 and 5520 Wireless Controllers)
- Cisco Flex 7500 Series Wireless Controllers (Cisco Flex 7510 Wireless Controller)
- Cisco 8500 Series Wireless Controllers (Cisco 8510 and 8540 Wireless Controllers)
- Cisco Virtual Wireless Controllers on the Cisco Services-Ready Engine (Cisco SRE) or the Cisco Wireless LAN Controller Module for Cisco Integrated Services Routers G2 (UCS-E)

  Kernel-based virtual machine (KVM) is supported in Cisco Wireless Release 8.1.102.0 and later releases.

Note After KVM is deployed, we recommend that you do not downgrade to a Cisco Wireless release that is older than Release 8.1.102.0.

- Cisco Wireless Controllers for high availability for Cisco 2500 Series (no AP SSO support), Cisco 5500 Series (5508 and 5520 Wireless Controllers), Cisco Wireless Services Module 2 (Cisco WiSM2), Cisco Flex 7500 Series, and Cisco 8500 Series WLCs (8510 and 8540 Wireless Controllers)

Note AP Stateful switchover (SSO) is not supported on Cisco 2500 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 24.

Supported Access Point Platforms

The following access point platforms are supported in this release:

- Cisco Aironet 1040 Series Access Points
- Cisco Aironet 1140 Series Access Points
- Cisco Aironet 1260 Series Access Points
- Cisco Aironet 1600 Series Access Points
- Cisco Aironet 1700 Series Access Points
- Cisco Aironet 2600 Series Access Points
- Cisco Aironet 2700 Series Access Points
- Cisco Aironet 3500 Series Access Points

- Cisco Aironet 3600 Series Access Points
- Cisco Aironet 3700 Series Access Points
- Cisco Aironet 600 Series OfficeExtend Access Points
- Cisco Aironet 700 Series Access Points
- Cisco Aironet 700W Series Access Points
- Cisco AP802 Integrated Access Point
- Cisco Aironet 1530 Series Access Points
- Cisco Aironet 1550 Series Access Points
- Cisco Aironet 1570 Series Access Points

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

For information about features that are not supported on some access point platforms, see Features Not Supported on Access Point Platforms, page 27.

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

- AP860:

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

- AP880:

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

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

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

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

- AP890:

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

  Before you use a Cisco AP802 series lightweight access point with Cisco Wireless Release 8.1.102.0, you must upgrade the software in the Cisco 880 Series ISRs to Cisco IOS 15.1(4)M or later releases.

Unsupported Cisco Wireless Controller Platforms

The following Cisco Wireless Controller platforms are not supported:

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

What's New in This Release

- This release supports two new Cisco Wireless Controller models:
  - Cisco 5520 Wireless Controller
  - Cisco 8540 Wireless Controller
- The Cisco Aironet 1040 Series, 1140 Series, and 1260 Series access points have feature parity with Cisco Wireless Release 8.0. Features introduced in Cisco Wireless Release 8.1 and later are not supported on these access points.
- We recommend that you install Cisco Wireless Controller Field Upgrade Software, Release 1.10.0.0 for the following platforms:
  - Cisco Flex 7500 Series Wireless Controllers
  - Cisco 8500 Series Wireless Controllers
  - Cisco Virtual Wireless Controller

  For more information, see *Release Notes for Cisco Wireless Controller Field Upgrade Software, Release 1.10.0.0*.
- Enhanced HD experience:
  - Dynamic Bandwidth Selection (DBS)—Automatic and intelligent configuration of 5-GHz channel bandwidth (20, 40, 80 MHz) for good channel width. This can be achieved by the learning of both client mix and the presence of neighboring APs and wireless networks.
  - Flexible Dynamic Frequency Selection (DFS)—Automatic adjustment of channel selection and channel width for 5 GHz spectral regions requiring radar detection and avoidance.
  - Enhanced Interference Mitigation—Event-driven RRM (ED-RRM) is additionally triggered by Wi-Fi interference (faster channel change than the typical dynamic channel assignment cycle in RRM).
  - Optimized Roaming Extensions—802.11v Basic Service Set (BSS) Transition Management (the infrastructure provides explicit advice to clients for reassociation and roaming).
- Cisco WLAN Express and Best Practices on Wireless Controllers—The following enhancements are made to the Cisco WLAN Express feature in this release:
  - Simplified initial (day 0) setup for Cisco WLCs is now extended to all Cisco WLCs and also comes with over-the-air setup. The best practices defaults now also enable RF parameter optimization and network profiles.
  - Improved user-interface is modern, responsive, flexible, and mobile friendly.

- New dashboard enables easy monitoring of AP and Client performance parameters. Search capability along with AP and Client detail pages allows for easy wireless troubleshooting.
- Best Practices monitoring page reports status of Best Practices and provides a one-click Fix It option to enable them (or roll back).

For more information about the new dashboard and Best Practices, see the *Online Help*.

- Application Visibility and Control (AVC) for FlexConnect local switched access points—This release extends the AVC functionality from Cisco WLC to the AP. The AVC on FlexConnect AP provides application visibility and control for locally switched client traffic. The AVC on FlexConnect uses Protocol Pack 8.0 and NBAR engine version 16.
- Monitoring the High Availability (HA) standby WLC—The HA-MIB that enables the administrator to monitor the status and health of the active and standby WLC is enhanced. Standby WLC information is available via CLI, WLC GUI, and SNMP. Management platforms can use the SNMP information to monitor the HA pair instance using a single interface.
- Cisco WLC integration with Lync SDN API—This feature enables a Cisco WLC to integrate with a Microsoft Lync Server. Using Microsoft Lync SDN API, the Lync Server sends a notification when a Lync event, such as a voice call, video call, file transfer, or Desktop sharing, occurs on the network. The Cisco WLC interprets the API message, to take the appropriate QoS actions, and provides more visibility (mean opinion score [MOS] or Lync Client Heath) into the Lync events on the wireless network using the Lync SDN dashboard.

Note This feature is supported only with 1.2 or other 1.2 version compatible Microsoft Lync Server SDN API.

The Cisco WLC integration with Lync SDN API feature is not supported on Cisco 2504 Wireless Controller.

- AVC Updates and enhancements for user role, device, and application-specific policy include:
  - New Protocol Pack 12.0.0
  - New NBAR Engine Version 16
  - Per-Client AAA override for AVC profiles
  - AVC per application, per client-based rate limiting on WLAN
  - Integration of AVC profiles with local policy classification on WLC
  - AVC directional QoS DSCP marking for upstream and downstream traffic
- Seamless roaming with Inter-Release Controller Mobility (IRCM) between Cisco 8510 WLC, Cisco 8540 WLC, and Cisco 5520 WLC with Cisco 5760 WLC—Enables seamless mobility and wireless services across high scale WLCs running Cisco AireOS and Cisco IOS using new mobility for features such as Layer 2 and Layer 3 roaming and guest access or termination.
- With Release 8.1 in a New Mobility environment, Cisco WLCs running Cisco Wireless software cannot function as mobility controllers (MC). However, the Cisco WLCs can function as guest anchors.
- AAA override of VLAN for FlexConnect—Allows a VLAN name to map to different VLAN IDs depending on the local site or FlexConnect group.
- Kernel-based virtual machine (KVM) support is added for Virtual Wireless Controller

- Guest Anchor Priority—Assigns a fixed priority to each anchor WLC or HA pair. The highest priority Cisco WLC is designated as the primary anchor. This feature also allows load distribution in round-robin fashion if the priorities are of the same assigned value.
- Multi-country domain support on WLC—Enables multiple country codes to be configured on a single Cisco WLC with bridge mode APs connected.
- Improved Mesh convergence time—Builds upon improvements made in Release 8.0 by adding channel change notification messaging, further improving network availability times.
- RRM on 5GHz RAP—RRM algorithms can run on the 5-GHz backhaul radio for root access points (RAPs) that do not have a child mesh access point (MAP) associated with them. This allows the RAP to find the optimal 5-GHz channel to operate on. When a MAP associates with this RAP, the RRM functionality is automatically disabled to ensure stable backhaul performance.
- Ethernet over GRE (EoGRE) tunneling from Cisco WLC and AP—Enables tunneling of data traffic from Cisco WLC or AP to a mobile packet core using EoGRE tunnels.

Note The EoGRE feature is not supported on Cisco 700 Series Access Points.

- TrustSec support on Cisco 5520 WLC, Cisco Flex 7510 WLC, and Cisco 8500 Series WLC—Security Group Tag Exchange Protocol (SXP) support on Cisco 5520, Flex 7510, 8510, and 8540 WLCs can be used to advertise Security Group TAG (SGT) information to SGT-capable switches so that appropriate role-based access control lists (RBACLs) can be activated depending on the role information represented by the SGT.
- FlexConnect Client Debugging on AP—FlexConnect client-based debugging allows client specific debugging to be enabled for an AP or groups of APs, and allows the syslog server configuration to log those debug messages.
- Other enhancements:
  - With Release 8.1.102.0, in Cisco vWLC, by default, the WLAN is locally switched.
  - License management for Cisco vWLC is changed from requiring a license file to Right to Use Licensing model. Users are required to accept an End User License Agreement (EULA) to the entitled quantity.

    For more information about using the Right to Use Licensing feature, see the Configuring Right to Use Licensing section in the *Cisco Wireless Controller Configuration Guide*.
  - Log Source IP on failed attempts to log into WLC (CSCul84825)
  - Add metadata to backup config file (CSCuq51498)
  - Rogue AP validation against AAA (CSCuj15410)
  - Framed MTU size (CSCuh33897)
  - Added support for RFC3576 Global DNS config (CSCug92480)
  - DNS RADIUS feature changes (CSCug92480)
  - Create configurable DOT1x exclusion attempts (CSCuo87508)
  - WLC—RADIUS multiple UDP source port support for RADIUS protocol (CSCus51456)

    Enabling multiple source ports allows the number of outstanding RADIUS requests to be increased. With single source port, the number of outstanding requests was limited to 255 for each authentication and accounting request. Added the following command to address this:

    config radius ext-source-ports {**enable** | **disable**}

Note Cisco 5508 WLC and WiSM2 support 8 RADIUS queues; Cisco 5520, Flex 7500 Series, and 8500 Series WLCs support 16 RADIUS queues.

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

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

Table 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	8.0.x
1140 Series	AIR-LAP1141N	5.2.157.0	—
	AIR-LAP1142N	5.2.157.0	—
1220 Series	AIR-AP1220A	3.1.59.24	7.0.x
	AIR-AP1220B	3.1.59.24	7.0.x
1230 Series	AIR-AP1230A	3.1.59.24	7.0.x
	AIR-AP1230B	3.1.59.24	7.0.x
	AIR-LAP1231G	3.1.59.24	7.0.x
	AIR-LAP1232AG	3.1.59.24	7.0.x
1240 Series	AIR-LAP1242G	3.1.59.24	8.0.x
	AIR-LAP1242AG	3.1.59.24	8.0.x

Table 2 Software Support for Access Points (continued)

Access Points		First Support	Last Support
1250 Series	AIR-LAP1250	4.2.61.0	8.0.x
	AIR-LAP1252G	4.2.61.0	8.0.x
	AIR-LAP1252AG	4.2.61.0	8.0.x
1260 Series	AIR-LAP1261N	7.0.116.0	—
	AIR-LAP1262N	7.0.98.0	—
1300 Series	AIR-BR1310G	4.0.155.0	7.0.x
1400 Series	Standalone Only	—	—
1600 Series	AIR-CAP1602I-x-K9	7.4.100.0	—
	AIR-CAP1602I-xK910	7.4.100.0	—
	AIR-SAP1602I-x-K9	7.4.100.0	—
	AIR-SAP1602I-xK9-5	7.4.100.0	—
	AIR-CAP1602E-x-K9	7.4.100.0	—
	AIR-SAP1602E-xK9-5	7.4.100.0	—
1700 Series	AIR-CAP1702I-x-K9	8.0.100.0	—
	AIR-CAP1702I-xK910	8.0.100.0	—
AP801		5.1.151.0	8.0.x
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	—
3500 Series	AIR-CAP3501E	7.0.98.0	—
	AIR-CAP3501I	7.0.98.0	—
	AIR-CAP3502E	7.0.98.0	—
	AIR-CAP3502I	7.0.98.0	—
	AIR-CAP3502P	7.0.116.0	—

Table 2 Software Support for Access Points (continued)

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

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

Table 2 Software Support for Access Points (continued)

Access Points		First Support	Last Support
1552S	AIR-CAP1552SA-x-K9	7.0.220.0	—
	AIR-CAP1552SD-x-K9	7.0.220.0	—
1570	AIR-AP1572EAC-x-K9	8.0.110.0	
	AIR-AP1572ICy[3]-x-K9	8.0.110.0	
	AIR-AP1572ECy-x-K9	8.0.110.0	

[1] The Cisco 3600 AP was introduced in Cisco Wireless Release 7.1.91.0. If your network deployment uses Cisco 3600 APs with Cisco Wireless Release 7.1.91.0, we highly recommend that you upgrade to Cisco Wireless Release 7.2.115.2 or a later release.

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

[3] y—Country DOCSIS Compliance, see ordering guide for details.

Software Release Types and Recommendations

Release Types

Table 3 Release Types

Release Type	Description	Benefit
Maintenance Deployment (MD) releases	Software releases that provide bug-fix support and ongoing software maintenance. These releases are categorized as Maintenance Deployment (MD) and may be part of the AssureWave program.[1] These are releases with long life and ongoing software maintenance.	Provides you with a software release that offers stability and long support duration with periodic maintenance releases (MRs).
Early Deployment (ED) releases	Software releases that provide new features and new hardware platform support in addition to bug fixes. These releases are categorized as Early Deployment (ED). These are short-lived releases.	Allows you to deploy the latest features and new hardware platforms or modules.

[1] AssureWave is a Cisco program that focuses on satisfying customer quality requirements in key industry segments in the mobility space. This program links and expands on product testing conducted within development engineering, regression testing, and system test groups within Cisco. The AssureWave program has established partnerships with major device and application vendors to help ensure broader interoperability with our new release. The AssureWave certification marks the successful completion of extensive wireless 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) releases	7.0 MD release train (latest release: 7.0.252.0)	7.4 MD release train (7.4.140.0 is the MD release)
Early Deployment (ED) releases for pre-802.11ac deployments	7.2 ED releases 7.3 ED releases	7.4 MD release train (7.4.140.0 is the MD release)
Early Deployment (ED) releases for 802.11ac deployments	7.5 ED release 7.6 ED release	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

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 8.1.102.0

Guidelines and Limitations

- When using Mobility Anchor WLANs, after you upgrade from a release that is prior to Release 8.1, guest client may not be exported because after the Cisco WLC boots with the new 8.1 image, the anchor list does not get updated with the correct priority in the new 8.1 feature for anchor priority list. The workaround is to update the anchor list with the correct priority in the priority list.

Note Release 8.1.111.0 and later have a fix for this issue and you do not have to apply this workaround. For more information, see CSCuu97761.

- If you are using Cisco Virtual Wireless Controller and upgrade from Release 8.0.x to Release 8.1.x, the AP counts from the license are not retained. The workaround is to remove the license file and manually add the AP count using the Right to Use Licensing feature.

  For more information about using the Right to Use Licensing feature, see the Configuring Right to Use Licensing section in the *Cisco Wireless Controller Configuration Guide*.

- Cisco WLC Release 7.3.112.0, which is configured for new mobility, might revert to old mobility after upgrading to Release 7.6, even though Release 7.6 supports new mobility. This issue occurs when new mobility, which is compatible with the Cisco 5760 Wireless LAN Controller and the Cisco Catalyst 3850 Series Switch, are in use. However, old mobility is not affected.

  The workaround is as follows:

  a. Enter the following commands:

```
config boot backup
show boot

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

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

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

config boot primary

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

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

- If you downgrade from Release 8.1.102.0 to a 7.x release, the trap configuration is lost and must be reconfigured.
- If you have ACL configurations in a Cisco WLC, and downgrade from a 7.4 or later release to a 7.3 or earlier release, you might experience XML errors on rebooting the Cisco WLC. However, these errors do not have any impact on any of the functionalities or configurations.
- If you are upgrading from Release 8.0.140.0 or 8.0.15x.0 to a later release and also have the multiple country code feature configured, the feature configuration is corrupted after the upgrade. For more information, see CSCve41740.
- If you are upgrading from a 7.4.x or earlier release to a release later than 7.4, the Called Station ID type information is mapped to the RADIUS Accounting Called Station ID type; which, by default, is set to apradio-mac-ssid. You can configure the RADIUS Authentication Called Station ID type information by using the **config radius auth callStationIdType** command.
- When FlexConnect APs (known as H-REAP APs in the 7.0.x releases) that are associated with a Cisco WLC that has all the 7.0.x software releases prior to Release 7.0.240.0, upgrade to Release 8.1.102.0, the APs lose the enabled VLAN support configuration. The VLAN mappings revert to the default values of the VLAN of the associated interface. The workaround is to upgrade from Release 7.0.240.0 and later 7.0.x releases to Release 8.1.102.0.

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

- When a client sends an HTTP request, the Cisco WLC intercepts it for redirection to the login page. If the HTTP GET request that is intercepted by the Cisco WLC is longer than 2000 bytes, the Cisco WLC drops the packet. Track CSCuy81133 for a possible enhancement to address this restriction.
- We recommend that you install Release 1.9.0.0 of Cisco Wireless LAN Controller Field Upgrade Software (FUS), which is a special AES package that contains several system-related component upgrades. These include the bootloader, field recovery image, and FPGA/MCU firmware. Installing

the FUS image requires special attention because it installs some critical firmware. The FUS image is independent of the runtime image. For more information, see http://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/fus_rn_OL-31390-01.html.

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

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

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

Note Bootloader upgrade is not required if FIPS is disabled.

- If you have to downgrade from one release to another, you might lose the configuration from your current release. The workaround is to reload the previous Cisco WLC configuration files saved on the backup server, or to reconfigure the Cisco WLC.
- It is not possible to directly upgrade to Release 8.1.102.0 release from a release that is earlier than Release 7.0.98.0.
- You can upgrade or downgrade the Cisco WLC software only between certain releases. In some instances, you must first install an intermediate release prior to upgrading to Release 8.1.102.0. Table 5 shows the upgrade path that you must follow before downloading Release 8.1.102.0.

Caution If you upgrade directly to Release 7.6.x or a later release from a release that is earlier than Release 7.5 directly to Release 7.6.X or a later release, the predownload process on Cisco Aironet 2600 and 3600 APs 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 Cisco 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.

Table 5 Upgrade Path to Cisco WLC Software Release 8.1.102.0

Current Software Release	Upgrade Path to 8.1.102.0 Software
7.0.x releases	You can upgrade directly to 8.1.102.0. **Note** If you have VLAN support and VLAN mappings defined on H-REAP access points and are currently using a 7.0.x Cisco WLC software release that is earlier than 7.0.240.0, we recommend that you upgrade to the 7.0.240.0 release and then upgrade to 8.1.102.0 to avoid losing those VLAN settings. **Note** In case of FlexConnect VLAN mapping deployment, we recommend that the deployment be done using FlexConnect groups. This allows you to recover VLAN mapping after an AP rejoins the Cisco WLC without having to manually reassign the VLAN mappings.
7.1.91.0	You can upgrade directly to 8.1.102.0.
7.2.x releases	You can upgrade directly to 8.1.102.0. **Note** If you have an 802.11u HotSpot configuration on the WLANs, we recommend that you first upgrade to the 7.3.101.0 Cisco WLC software release and then to the 8.1.102.0 Cisco WLC software release. You must downgrade from the 8.1.102.0 Cisco WLC software release to a 7.2.x Cisco WLC software release if you have an 802.11u HotSpot configuration on the WLANs that are not supported.
7.3.x releases	You can upgrade directly to 8.1.102.0.
7.4.x releases	You can upgrade directly to 8.1.102.0.
7.5.x releases	You can upgrade directly to 8.1.102.0.
7.6.x	You can upgrade directly to 8.1.102.0.
8.0.x	You can upgrade directly to 8.1.102.0.

- When you upgrade the Cisco WLC to an intermediate software release, you must wait until all of the access points that are associated with the Cisco WLC are upgraded to the intermediate release before you install the latest Cisco WLC software. In large networks, it can take some time to download the software on each access point.
- You can upgrade to a new release of the Cisco WLC software or downgrade to an earlier release even if Federal Information Processing Standard (FIPS) is enabled.
- 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.

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

- Cisco WLCs support standard SNMP MIB files. MIBs can be downloaded from the Software Center on Cisco.com.
- The Cisco WLC software is factory installed on your Cisco WLC and is automatically downloaded to the access points after a release upgrade and whenever an access point joins a Cisco WLC. We recommend that you install the latest software version available for maximum operational benefit.
- Ensure that you have a TFTP, FTP, or SFTP server available for the software upgrade. Follow these guidelines when setting up a server:
  - Ensure that your TFTP server supports files that are larger than the size of Cisco WLC software Release 8.1.102.0. Some TFTP servers that support files of this size are tftpd32 and the TFTP server within the Prime Infrastructure. If you attempt to download the 8.1.102.0 Cisco WLC software and your TFTP server does not support files of this size, the following error message appears:

    ```
    TFTP failure while storing in flash.
    ```

  - If you are upgrading through the distribution system network port, the TFTP or FTP server can be on the same subnet or a different subnet because the distribution system port is routable.
- When you plug a Cisco WLC into an AC power source, the bootup script and power-on self test is run to initialize the system. During this time, press **Esc** to display the bootloader Boot Options menu. The menu options for the Cisco 5500 Series WLC differ from the menu options for the other Cisco WLC platforms.

  Bootloader menu for Cisco 5500 Series WLC:

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

  Bootloader menu for other Cisco WLC platforms:

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

Enter **1** to run the current software, enter **2** to run the previous software, enter **4** (on Cisco 5500 Series WLC), or enter **5** (on Cisco WLC platforms other than 5500 series) to run the current software and set the Cisco WLC configuration to factory defaults. Do not choose the other options unless directed to do so.

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

- The Cisco WLC bootloader stores a copy of the active primary image and the backup image. If the primary image becomes corrupted, you can use the bootloader to boot with the backup image.

  With the backup image stored before rebooting, choose **Option 2: Run Backup Image** from the boot menu to boot from the backup image. Then, upgrade with a known working image and reboot the Cisco WLC.

- You can control the addresses that are sent in the Control and Provisioning of Wireless Access Points (CAPWAP) discovery responses when NAT is enabled on the Management Interface using the following command:

  config network ap-discovery nat-ip-only {**enable** | **disable**}

  Here:

  - **enable**—Enables use of NAT IP only in a discovery response. This is the default. Use this command if all the APs are outside the NAT gateway.
  - **disable**—Enables use of both NAT IP and non-NAT IP in a discovery response. Use this command if APs are on the inside and outside the NAT gateway, for example, Local Mode and OfficeExtend APs are on the same Cisco WLC.

Note To avoid stranding of APs, you must disable AP link latency (if enabled) before you use the disable option for the **config network ap-discovery nat-ip-only** command. To disable AP link latency, use the **config ap link-latency disable all** command.

- You can configure 802.1p tagging by using the **config qos dot1p-tag** {**bronze** | **silver** | **gold** | **platinum**} command. For Release 7.2.103.0 and later releases, if you tag 802.1p packets, the tagging has an impact on only wired packets. Wireless packets are impacted only by the maximum priority level set for QoS.
- You can reduce the network downtime using the following options:
  - You can predownload the AP image.
  - For FlexConnect access points, use the FlexConnect AP upgrade feature to reduce traffic between the Cisco WLC and the AP (main site and the branch). For more information about the FlexConnect AP upgrade feature, see the *Cisco Wireless Controller Configuration Guide*.

Note Predownloading Release 8.1.102.0 on a Cisco Aironet 1240 access point is not supported when upgrading from a previous Cisco WLC release. If predownloading is attempted on a Cisco Aironet 1240 access point, an AP disconnect will occur momentarily.

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

- To downgrade from Release 8.1.102.0 to Release 6.0 or an earlier release, perform either of these tasks:
  - Delete all the WLANs that are mapped to interface groups, and create new ones.
  - Ensure that all the WLANs are mapped to interfaces rather than interface groups.
- After you perform the following functions on the Cisco WLC, reboot the Cisco WLC for the changes to take effect:
  - Enable or disable link aggregation (LAG)
  - Enable a feature that is dependent on certificates (such as HTTPS and web authentication)
  - Add a new license or modify an existing license
  - Increase the priority of a license
  - Enable HA
  - Install the SSL certificate
  - Configure the database size
  - Install the vendor-device certificate
  - Download the CA certificate
  - Upload the configuration file
  - Install the Web Authentication certificate
  - Make changes to the management interface or the virtual interface
  - Make changes to TCP MSS settings
- If you downgrade from Release 8.3 to Release 8.1, the Cisco Aironet 1850 Series AP, whose mode prior to the downgrade was Sensor is shown to be in unknown mode after the downgrade. This is because the Sensor mode is not supported in Release 8.1.

Upgrading to Cisco WLC Software Release 8.1.102.0 (GUI)

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

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

Step 2 Follow these steps to obtain Cisco Wireless Release 8.1.102.0 software:

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

http://www.cisco.com/cisco/software/navigator.html

b. Choose **Wireless** from the center selection window.

c. Click **Wireless LAN Controllers**.

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

- Integrated Controllers and Controller Modules
- Standalone Controllers

d. Select the Cisco WLC model number or name.

   The **Download Software** page is displayed.

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

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

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

g. Click **Download**.

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

i. Save the file to your hard drive.

j. Repeat steps a. through i. to download the remaining file.

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

Step 4 (Optional) Disable the Cisco WLC 802.11a/n and 802.11b/g/n networks.

Note For busy networks, Cisco WLCs on high utilization, and small Cisco WLC platforms, we recommend that you disable the 802.11a/n and 802.11b/g/n networks as a precautionary measure.

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

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

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

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

Step 9 If you are using a TFTP server, the default value of 10 retries for the **Maximum Retries** text field, and 6 seconds for the Timeout text field should work correctly without any adjustment. However, you can change these values, if desired. To do so, enter the maximum number of times that the TFTP server attempts to download the software in the Maximum Retries text box and the amount of time (in seconds) for which the TFTP server attempts to download the software, in the **Timeout** text box.

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

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

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

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

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

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

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

A message appears indicating the status of the download.

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 8.1.102.0 Cisco WLC software is installed on your Cisco WLC, click **Monitor** on the Cisco WLC GUI and view the Software Version field under Controller Summary.

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

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

Important Note for Customers in Russia

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

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

Downloading and Installing a DTLS License for an LDPE Cisco WLC

Step 1 To download the Cisco DTLS license:

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

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

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

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

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

Step 2 Copy the license file to your TFTP server.

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

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

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

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

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

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

Upgrading from an LDPE to a Non-LDPE Cisco WLC

Step 1 Download the non-LDPE software release:

a. Go to the Cisco Software Center at:

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

b. Choose the Cisco WLC model.

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

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

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

f. Click **Download**.

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

h. Save the file to your hard drive.

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

Step 3 Upgrade the Cisco WLC with this version by performing Step 3 through Step 19 detailed in the "Upgrading to Cisco WLC Software Release 8.1.102.0" section on page 12.

Interoperability with Other Clients

This section describes the interoperability of Cisco WLC Software, Release 8.1.102.0 with other client devices.

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

Table 6 Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	8.1.102.0
Cisco WLC	Cisco 5508 Wireless Controller

Table 6 Test Bed Configuration for Interoperability (continued)

Access points	1142, 3502, 3602, 1602, 2602, 1702, 2702, 3702, 702, 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 7 lists the client types on which the tests were conducted, including laptops, handheld devices, phones, and printers.

Table 7 Client Types

Client Type and Name	Version
Laptop	
Intel 4965	13.4
Intel 5100/5300	14.3.2.1
Intel 6200	15.15.0.1
Intel 6300	15.15.0.1
Intel 6205	15.15.0.1
Intel 1000/1030	14.3.0.6
Intel 7260	17.14
Intel 7265	17.14
Intel 3160	17.14
Broadcom 4360	6.30.163.2005
Linksys AE6000 (USB)	5.1.2.0
Netgear A6200 (USB)	6.30.145.30
Netgear A6210(USB)	5.1.18.0
D-Link DWA-182 (USB)	6.30.145.30
Engenius EUB 1200AC(USB)	1026.5.1118.2013
Dell 1395/1397/Broadcom 4312HMG(L)	5.30.21.0
Dell 1501 (Broadcom BCM4313)	5.60.48.35/5.60.350.11
Dell 1505/1510/Broadcom 4321MCAG/4322HM	5.60.18.8
Dell 1515(Atheros)	8.0.0.239
Dell 1520/Broadcom 43224HMS	5.60.48.18
Dell 1530 (Broadcom BCM4359)	5.100.235.12
Dell 1540	6.30.223.215
Cisco CB21	1.3.0.532
Atheros HB92/HB97	8.0.0.320
Atheros HB95	7.7.0.358

Table 7 Client Types (continued)

Client Type and Name	Version
MacBook Pro	OSX 10.10.2
MacBook Air old	OSX 10.10.2
MacBook Air new	OSX 10.10.2
Macbook Pro with Retina Display	OSX 10.10.2
Tablets	
Apple iPad2	iOS 8.2(12D508)
Apple iPad3	iOS 8.2(12D508)
Apple iPad mini with Retina display	iOS 8.2(12D508)
Apple iPad Air	iOS 8.2(12D508)
Apple iPad Air 2	iOS 8.2(12D508)
Samsung Galaxy Tab Pro SM-T320	Android 4.4.2
Samsung Galaxy Tab 10.1- 2014 SM-P600	Android 4.4.2
Samsung Galaxy Note 3 - SM-N900	Android 4.4.2
Microsoft Surface Pro 3	Windows 8.1 Driver: 15.68.3073.151
Microsoft Surface Pro 2	Windows 8.1 Driver: 14.69.24039.134
Google Nexus 9	Android 5.0
Google Nexus 7 2nd Gen	Android 5.0
Intermec CK70	Windows Mobile 6.5 / 2.01.06.0355
Intermec CN50	Windows Mobile 6.1 / 2.01.06.0333
Symbol MC5590	Windows Mobile 6.5 / 3.00.0.0.051R
Symbol MC75	Windows Mobile 6.5 / 3.00.2.0.006R
Phones and Printers	
Cisco 7921G	1.4.5.3.LOADS
Cisco 7925G	1.4.5.3.LOADS
Ascom i75	1.8.0
Spectralink 8030	119.081/131.030/132.030
Apple iPhone 4S	iOS 8.2(12D508)
Apple iPhone 5	iOS 8.2(12D508)
Apple iPhone 5s	iOS 8.2(12D508)
Apple iPhone 5c	iOS 8.2(12D508)
Apple iPhone 6	iOS 8.2(12D508)
Apple iPhone 6 Plus	iOS 8.2(12D508)
HTC One	Android 5.0
OnePlusOne	Android 4.3

Table 7 Client Types (continued)

Client Type and Name	Version
Samsung Galaxy S4 GT-I9500 (11AC)	Android 4.4.2
Sony Xperia Z Ultra	Android 4.4.2
Nokia Lumia 1520	Windows Phone 8.1
Google Nexus 5	Android 5.0
Google Nexus 6	Android 5.0
Samsung Galaxy S5-SM-G900A	Android 4.4.2
Huawei Ascend P7	Android 4.4.2
Samsung Galaxy S III	Android 4.3
SpectraLink 8450	3.0.2.6098/5.0.0.8774
Samsung Galaxy Nexus GTI9200	Android 4.4.2
Samsung Galaxy Mega SM900	Android 4.4.2

Features Not Supported on Cisco WLC Platforms

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

Features Not Supported on Cisco 2504 WLC

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

Note However, AVC for local mode APs is supported.

- 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 Cisco WiSM2 and Cisco 5508 WLC

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

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

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

Features Not Supported on Cisco Flex 7510 WLCs

- Static AP-manager interface

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

- IPv6 and Dual Stack client visibility

Note IPv6 client bridging and Router Advertisement Guard are supported.

- Internal DHCP server
- Access points in local mode

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

- Mesh (use Flex + Bridge mode for mesh-enabled FlexConnect deployments)

- Spanning Tree Protocol (STP)
- Cisco Flex 7500 Series WLC cannot be configured as a guest anchor Cisco WLC. However, it can be configured as a foreign Cisco WLC to tunnel guest traffic to a guest anchor Cisco WLC in a DMZ.
- Multicast

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

- PMIPv6

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

- Internal DHCP Server
- Local authentication
- Wired Guest
- Mobility controller functionality in converged access mode

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.

- High Availability
- PMIPv6
- Workgroup Bridges
- Client downstream rate limiting for central switching
- SHA2 certificates

Features Not Supported on Mesh Networks

- Load-based call admission control (CAC). Mesh networks support only bandwidth-based CAC or static CAC
- High availability (fast heartbeat and primary discovery join timer)

- AP acting as supplicant with EAP-FASTv1 and 802.1X authentication
- Access point join priority (mesh access points have a fixed priority)
- Location-based services

Features Not Supported on Access Point Platforms

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

- PPPoE
- PMIPv6

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

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

Caveats

Cisco Bug Search Tool

The Bug Search Tool (BST), which is the online successor to the Bug Toolkit, is designed to improve the effectiveness in network risk management and device troubleshooting. The BST allows Cisco partners and customers to search for software bugs based on product, release, 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 27.

Table 8 Open Caveats

Bug ID	Headline
CSCue19327	Local switching AP intermittently sends broadcasts with bad group key
CSCui74495	AP2600I low througput for 2 spatial stream Linksys AE 2500 USB adaptor
CSCui77831	AP3700 can see CleanAir failure hals0buf 276
CSCul07738	DPAA Tx/Rx stuck; reload due to Ethernet interface receive failure [FSL]
CSCul92993	RFC 2139 - WLCs fail to send FRAMED-IP attribute to AAA server
CSCun46053	AP3700 repeated radio command timeouts and dropping from WLC
CSCuq03928	IPv6 MIB support to show dual stack
CSCuq79645	Cisco IOS XE Release 3.7E: Catalyst 3650 to Cisco 5508 Wireless Controller mobility tunnel takes more than 1h to come up
CSCuq79884	1702/2700/3700 LWAPP PI reports incorrect Critical Alarm on Low Power
CSCuq86263	False DFS detection on AP1600
CSCur22862	802.11r reauth fails during 4-way handshake after WLC HA failover
CSCur23631	FlexConnect config issue in AP specific WLAN ACL mapping
CSCur64130	WiSM wireless client intermittently connects through wrong interface
CSCur66626	DHCP Proxy behavior on Release 7.6 is inconsistent Anchored versus Non
CSCur68316	802AP-891 in FlexConnect mode are losing VLAN mapping after power cycle
CSCur71315	AP1552 bridge Transmit voice queue stuck leading to out of TX buffers
CSCur75776	AP1600: Radio reset with generating event.rX
CSCur76547	AP with static IP configured behave DHCP client after reload
CSCur91936	mDNS discovery issue with WLC 8.0.100
CSCur96317	PMIPv6 Webauth traffic to client is not dropped in WEB_auth reqd state
CSCus02070	FlexConnect AP losing VLAN mapping and falling on Native VLAN
CSCus39552	Foreign WLC fails to send url-redirect-acl if ACL ID is 0
CSCus53495	DFS detection due to Broadcom spurious emissions AP2700/3700
CSCus61445	DNS ACL on Cisco WLC does not work; AP does not send DTLS to Cisco WLC
CSCus61679	Problem in Client Stats Reports - Follow up CDETS
CSCus62890	WLC crash due to radius client profiler task taking 100 percent cpu
CSCus68595	HA Error msg: RF failure notification ErrorType: 31 Reason
CSCus69131	Client is stuck on DHCP_REQ when switching from Dot1x ssid to CWA ssid
CSCus79791	Client connected to 11n AP shows as 11ac client on WLC
CSCus91214	AP802 15.3(3)JAB always crash on issuing “dir all-filesystems” ISR C881W
CSCus92667	GET on Ap groups Table after set - response missing
CSCus93490	Vocera badges experience initial delay for multicast audio
CSCus96449	Client connectivity loss on AP802 802.1x/EAP-SIM SSID 7.6 and 8.0
CSCus97021	2500/5508 possible bricking on kernel crash
CSCut04924	Long delay between frame retransmissions on 1532; packet drops

Table 8 Open Caveats

Bug ID	Headline
CSCut07170	AP1532 WGB intermittently does not see incoming probe responses
CSCut11100	Client not getting anchored properly
CSCut15074	Radio resets on both radios of 3700 and 1142 APs on 5508 WLC
CSCut23325	AP1700 not encrypting ICMP and ARP sent from the client over the air
CSCut27598	Client unable to get IP when switching wlan on New mobility.
CSCut30152	FlexConnect LWAP loses 5 GHz static power setting after reboot
CSCut32955	a-mpdu tx priority command missing from backup config
CSCut33114	Link status in 5520/8540 WLC is displaying UP when only SFPs are connected
CSCut39526	WLC cannot send device type value to MSE
CSCut41100	802.11a radio reset due to channel change on RRM cycle
CSCut41680	Cisco 5520 WLC: Kernel Panic followed by DP crash observed on active wlc
CSCut42406	WLC5508 crashed while disabling Mobility oracle.
CSCut42694	The **show client details** *mac-addr* command does not include Client Statistics value
CSCut42926	WLC crash on SNMPtask after doing config audit from PI
CSCut44986	WLC throwing error when accounting is disabled on WLAN
CSCut48172	LSC AP provisioning happening after MAP is disconnected for long time
CSCut48743	FlexConnect AVC: Policy-map not getting deleted/add when AP is in apgroup
CSCut50245	vWLC: No command to enable FlexConnect AVC visibility on WLAN
CSCut52223	FlexConnect AP losing local EAP certificate
CSCut52235	AP3502 crashes on Unexpected exception to CPU: vector 1400
CSCut54640	Cannot monitor channel utilization counter after radio interface reset
CSCut56031	AP2702: IAPP packets sent in aggregated mode.
CSCut56166	5500 crash: Task Name: emWeb Reason: System Crash
CSCut56741	AP1600: Radio reset with “STOPPING CPQ FWD TRACE ON Bad CPQ removal”
CSCut59663	Add channels 100-140 as default in 11a
CSCut61103	WLC seen #SOCKET_TASK-7-DATA_PROCESSING_FAILED due to DHCPv6
CSCut63331	FlexConnect AVC: Not able to change value of marking once configured
CSCut63787	Username with spanish character Ñ ASCII164 created by lobbyadmin garbled
CSCut63818	WiSM2 mbuff leak
CSCut64180	AP holds BW after call when WLC HA SO happens during call setup
CSCut65096	AP1142 5-GHz radio reset with reason code 51 71
CSCut65231	Calibration not working for specific floor
CSCut65290	UX 2702i access points using AirProvision tool incompatible with note-4
CSCut65485	AVC profile not blocking Gmail traffic in flex-group
CSCut65537	Potential malformed beacon on AP2600/3600[BZ 1093]

Table 8 Open Caveats

Bug ID	Headline
CSCut65784	Changing from anchored local web auth to CWA anchored SSID allows access
CSCut66994	Anchor / Foreign wlc accounting packets has nas-update=true
CSCut69432	Gemini Module getting disabled on 3700 with 3rd party switch
CSCut70112	flexavc policy is getting applied eventhough there is no flexavc
CSCut71612	OUI string should be synched across HA
CSCut72536	AP crash with AVC
CSCut73027	8500 HA Observed DP crash when download AVC protocol pack
CSCut74093	WLC is reporting a number of stale client entries
CSCut74263	MAG on AP:AP does not clear bindings after session/user timeout &amp; deauth
CSCut75779	apf_profiler.c taking too much memory.
CSCut76481	WLC sends 1499 bytes MTU switchover
CSCut76824	Anchor WLC will not forward DHCP request to the DHCP server
CSCut78601	WebAuth session-timeout on AAA override expires before the real value
CSCut81252	1532 WGB attempts to transmit stale data while scanning roaming
CSCut81339	WLC: Linksys 11ac USB card - M1 retry exceeded - client cannot connect
CSCut82340	WLAN-VLAN mapping addition fails for newly created FlexConnect group from PI
CSCut83422	vWLC SN changed after mgmt interface ip change
CSCut84949	Beacon Loss on AP1142
CSCut85185	FlexConnect AVC-WLAN specific mapping is not pushing to AP
CSCut85224	AP1600 2.4-GHz radio resets with reason code 71 on event.r0
CSCut85500	AP not forwarding EAP response received on radio
CSCut85555	APF_HA-3-SYNC_RETRANSMIT_FAIL Messages in show msglog
CSCut86489	Radios on WLC show DOWN but are UP on the AP with Queue already full
CSCut86825	HREAP-7-ACL_ENTRY_DONOT_EXIST: Unable to find an ACL by name
CSCut87326	WLC generates SNMP traps to PI 2.2 for AIR-3702 PoE+ getting low power
CSCut88060	“Err: User DB Full” followed by a crash during day0 config
CSCut89108	DHCP fails or hanging with local APs 802.11a only and MAC on Failure
CSCut90276	AireOS Traceback: APF-4-PROC_ACTION_FAILED
CSCut90452	WLC HTTPS access not working after Web Auth cert install on Release 7.6.130.0
CSCut91036	FlexConnect split tunnel broken in Release 8.0
CSCut91086	Client associated to MAP does not get AAA override in Flex+Bridge mode
CSCut91348	WLC Crashing with “fatal condition at broffu_fp_dapi_cmd.c:4081”
CSCut92026	WLC stops responding after failed accounting attempt
CSCut92208	FlexConnect VLAN mode changed to Disabled on power cycle (1142/3502/3702)
CSCut92800	Client info remains on AP unexpectedly after radio reset happened

Table 8 Open Caveats

Bug ID	Headline
CSCut93712	AP not send RM IE for 11k in association response; no 11k for iOS > 8.1
CSCut94192	VLAN Select Feature Not Marking Interfaces As Dirty Properly
CSCut94260	AP wIPS module sending random characters in the alarm message
CSCut95262	FlexConnect group Primary/Subordinate predownload fails on 3502 subordinate AP
CSCut96026	SGT remains for client when moving between WLANs with Fast SSID change
CSCut96598	2504 WLC sends access-request with same Radius-id to 2 diff. ACS servers
CSCut96691	TFTP address for AP core dump is goofed up after HA switchover
CSCut98006	DFS detections due to high energy profile signature
CSCut98913	WiSM2 crash due to Web auth redirect on Release 7.6.130.x
CSCut99032	There have 2 channels 00 on 5-GHz DCA list and cannot remove it
CSCut99150	2702 AP requesting as a Type 1 power device instead of Type 2
CSCut99894	Power level limitation of 15 dBm for AP802H
CSCuu00826	AP sends disassociation to clients on new channel when switching channel
CSCuu00893	8500 DP Exception Crash After Resetting Controller
CSCuu02281	APs on WLC with wireless networks disabled detecting rogues
CSCuu02970	CSCuq19142 workaround does not work on very old 4400s with Airespace MIC
CSCuu02991	Assert in hals0_sb.c Clean air failure
CSCuu17340	WLC crash Tunnel Process Task when add gw name 129 max character from UI
CSCuu19497	Length of the PMIP and EoGRE Parameters length is reduced by 1 byte/char
CSCuu20683	RAP might lose the Native VLAN configuration on downgrade from Release 8.1
CSCuu23521	WLC 5520 crash with task name radiusTransportThread
CSCuu32602	1550 mesh mode, BVI down when using G3 as uplink

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 27.

Table 9 Resolved Caveats

Bug ID	Headline
CSCun96815	OEAP ACLs and Network lists gets deleted after upload/download the config
CSCup68372	Stats are carried over when session timeout occurs
CSCuq00494	Prevent a radio reset when WGB roams between two UNI1/UNI2 channel
CSCtl96208	The **capwap ap hostname** command CLI returns "ERROR!!! Command is disabled."
CSCui19253	WLC reports: AP reported timeout communicating to controller

Table 9 Resolved Caveats

Bug ID	Headline
CSCuj93777	Mesh AP should block data packets before BPDU packets are handled
CSCul11348	AP3700 fails Wi-Fi 4.2.55 Operational Mode Notification test
CSCum17260	DATACORRUPTION-1-DATAINCONSISTENCY on vstack mgmt vlan bringup on nbr sw
CSCun20584	AP replicates broadcast packets to the default gateway
CSCuo69314	AP does not stop pkt-dump after HA switchover
CSCup85228	AP IO memory leak in DPAA module
CSCup88910	630937505 - AP impersonation flood of events on WLC 8510-SR14-00512
CSCup96204	AP1142 disconnects a client by Association Response having Failure code
CSCuq09859	APs sending GARP and ARP requests aprox every 2 seconds.
CSCuq14231	7500: Efficient upgrade IPv6 subordinates cant download new image
CSCuq19142	LAP/WLC MIC or SSC lifetime expiration causes DTLS failure
CSCuq36265	802.11ac: Surface client not associating on 11ac if ssid is not broadcast
CSCuq48800	Low throughput due to UAPSD for Intel 7260 Wi-Fi chipset
CSCuq56829	Flex+Bridge Maps drop after association; failed to receive data keep-alive
CSCuq71068	AP traffic issue causing client to lose Layer 3 connectivity
CSCuq90632	AP3702 crashed with a traceback
CSCuq99230	AP syslog fails due to default setting ‘logging server-arp’
CSCur11060	False positive on honeypot alert with multiple SSIDs
CSCur18669	Client ingress QoS policy not installing with table-map
CSCur20846	AP power mode output in CLI does not reflect real power state
CSCur22714	AP3602 trying to contain its own RM3000AC module
CSCur24512	3602i AP crash at dot11_driver_ie_find
CSCur38682	AP FlexConnect - local switch/local auth sends deauth 802.1x on PSK wlan
CSCuo40061	Web Authentication bypass after IP address change
CSCup31640	Changing Channel to Auto does not set max bandwidth for FlexConnect APs
CSCup46302	Virtual WLC: RSSI missing from Monitor mode AP
CSCup57457	WS-SVC-WISM2-K9 unable to change Rogue state
CSCup59183	Temperature is showing as 5000c for a device.
CSCup60282	Ping generated from WLC seen as incorrect ICMP type
CSCup64468	WLC device sends invalid format “#” in front of syslog message
CSCup66047	bsnPingTestIPAddress not supported for IPv6
CSCup71136	Mac-filter: MAC Delimiter will not change in Accounting message
CSCup72205	Unable to add SNMP community in WLC GUI
CSCup72502	5500 on 7.6 does not deauth client when Flex ACL is not present on AP
CSCup81574	Foreign client IP unknown in access-session detail- 5508 anchor-dhcpreq

Table 9 Resolved Caveats

Bug ID	Headline
CSCup85611	WLC disallows configuration of rogue rule SSID with space as first char
CSCup85896	Interference profile failure for secondary40 channel
CSCup94618	SNMP Traps being sent from WLC when SNMP trap controls has them disabled
CSCup96492	IPv6 route with /128 prefix removes after reboot
CSCup98731	https-redirect command is missing in the uploaded config file
CSCuq05475	Controller GUI shows AP's NAT IP instead of private
CSCuq32731	Controller crash on mmRemoveHbMbr while peering with new mobility 76MR3
CSCuq60042	Memory leak on WLC when using PMIPv6 clients pem_api.c
CSCuq72285	Unable to insert line break in Internal Web-Auth message window
CSCul94524	WLAN with WebAuth + Flex Local Switch + Anchor function broken on 7.4
CSCum86031	Roaming 5508 to 5760 applies wrong QOS policy on configuring aaa-override
CSCup29095	Mesh: PI not showing the neighbor details in mesh links page of Parent
CSCup75446	Default interface takes precedence over foreign VLAN mapping with CWA
CSCup80403	Low iMac Tput -supported rate IE in association response has ZERO length
CSCup91420	GUI: (PR-179) Multi Country Configuration - Invalid warning message
CSCup97263	Flex 7500 WLC: System Crash Dot1x_NW_MsgTask_2
CSCuq05007	extended -show client summary- not showing output next page
CSCuq48218	WLC cannot process multiple sub-attributes in single RADIUS VSA
CSCuq49410	GUI:TKIP only wlan shows up as wpa2-aes enabled after upgrade to 8.0cco
CSCuq50069	SHA1 key cipher not working between WLC Release 8.0 and MSE Release 8.0.
CSCuq54269	AP clear config does not remove the IPv6 static configuration
CSCuq54548	Anchor Memory Leak when Sleeping Client Feature is enabled
CSCuq59501	show tech not showing show run-config commands output
CSCuq63642	Internal web page appears after successful redirect to external webauth
CSCuq68753	5500 anchor running 7.6.122.21 crashed on osapiBsnTimer
CSCuq71056	CMCC portal protocol cannot work on VWLC/8500/7500
CSCuq72354	Unable to configure Cyprus/Antigua AP to country HongKong (RegDom -E-S)
CSCuq73072	Mesh Convergence list includes incorrect channel.
CSCuq74491	WLC 8.0.100.0 crashes due to Task Name: apfRogueTask_0
CSCuq75748	multicast config SET failing to commit
CSCuq77109	wlc_main build break
CSCuq82079	iBeacon clustering not happening with APs in monitor mode
CSCuq84698	Cannot enable syslog logging format rfc-5424
CSCuq84708	Cannot enable logging exception value
CSCuq88748	Rogue APs wrong classification from malicious to unclassified
CSCuq89123	WLC: No debugs enabled but debug invalid module messages in log

Table 9 Resolved Caveats

Bug ID	Headline
CSCuq91181	Client does not regain IP connectivity after roaming
CSCuq94587	EAP profile name display as Junk character if created in UTF-8 character
CSCuq97276	Disabling AVC profile via CLI disables AVC completely
CSCuq97914	PI 1.4 cannot finish auditing WLC
CSCur00288	8.0.100.0 client is shown with “ip address unknown” and “dhcp required”
CSCur02514	8.0.100.0: SNMP trap is not sent out on HA switch-over
CSCur06605	SNMP table is not able to retrieve all entry from cLReapApCentralDhcp
CSCur13400	DHCP Option 82 and Sub Option 5 issue in WLC 8.0
CSCur17406	AP impersonation appearing for 1530 AP(s)
CSCur19519	MAP stuck on 802.1x after error condition + roaming
CSCur20154	HA SSO pair memory leak
CSCur23783	Ap core dump output showing ipv6
CSCur24785	Snmp walk failed for CISCO-LWAPP-MOBILITY-MIB.cLMobilityMulticastMessagi
CSCur25239	Controller crash on mping command over telnet/ssh
CSCur25742	mDNS service not-learnt displays mac address with space instead of zero
CSCur30618	SNMP WALK fails for all APS if Country code is not presnet for single AP
CSCur32475	NewMobility Web-Auth on MacFilter Failure always send client to web-auth
CSCur33829	WLC not sending NAS-IP-Address or NAS-Identifier
CSCur36403	Cannot apply VLAN for local policy which is not present on controller
CSCur40308	‘show ap env’ do not show cable modem info for 1570IC/EC
CSCuo48442	Stale old DTLS data_encryption session histories are left on WLC
CSCup92480	802.11ac crash due to PCI reset
CSCuq96986	WLC 2504 crash on upgrade to Release 8.0
CSCur37475	WiSM2 system crash - at client stats AVL corruption
CSCur42476	8510/7510 SNMP IP Address configs reversed on downgrade from 7.6 to 7.4
CSCur43124	WSSI module stops working after upgrade from 7.4.121.0 to 7.6.130.0
CSCur45862	APs cannot discover WLC through option 43 on build 8.0.100.0
CSCur47745	Client not able to join WLAN with FlexConnect Central DHCP processing
CSCur48944	Problem in Client Stats Reports and Optimized Roaming
CSCur49165	WiSM2 system crash radiusTransportThread aaaRadiusAuth
CSCur50378	FlexConnect Local switch+Central DHCP+WebAuth webpage not display
CSCur50819	BEAST Vulnerability not properly resolved in Cisco WLCs
CSCur52246	PMIPv6 GRE key database gets full during scale testing
CSCur54409	OEAP 602 ap retransmit led state &amp; link latency config should be greyed
CSCur54681	GUI: Flex+Bridge Parent inherited Flex VLAN mappings not reflected on Map

Table 9 Resolved Caveats

Bug ID	Headline
CSCur56576	WLC does not support 802.11a for Qatar
CSCur57909	Client misses to override VLAN after shifting wlan.
CSCur60218	New mobility web auth on MAC filter failure Export Anchor request fails
CSCur66836	FlexConnect AP occasionally sends a radius request with no username
CSCur67701	Image download errors for CAPWAP 7500/8500
CSCur68791	Using 3502 monitor as RLDP Linksys, 802.11g AP not found as rogue on wire
CSCur69406	SNMP get on cLApVlanListTable in bridge mode doesn't return all values
CSCur71427	Flex: Client roaming fails "not processing DOT1X_4WAY_COMPLETED_AT_AP"
CSCur72287	EAPOL Security error seen when 1st HOP MAP Roams from RAP1 to RAP2
CSCur74208	Name/OID: cLMobilityExtMgrAddress.0; Returning in IP in Reverse Order
CSCur78697	1st Hop MAP CAPWAP Restart Due to race condition when seeking RAP2
CSCur78836	AP forwards frame to STP Blocked interface
CSCur80827	AP is rebooting if we change mode to same mode it is in
CSCur80841	Apple remote app not working with MDNS snooping enabled.
CSCur85117	FlexConnect Local switch+Central DHCP+WebAuth webpage not displayed
CSCur88307	AP name unknown in dissoc messages (Intermittent)
CSCur88408	LAP does not send discovery request to WLC IP discovered by DNS resolution
CSCur88864	3600 APs with AC module shows 100 per cent Rx utilization on slot-2.
CSCur89433	Message errors from flex AID must include the AP MAC address
CSCur89551	LWAPP-3-INVALID_AID: message observed for Flex 1240 APs
CSCur95365	Controller crashes when issuing command show ap config general
CSCur96221	Standby WLC crash at haSSOServiceTask6
CSCur98240	8500 System crash with 8.0 CCO
CSCur98520	8500 - SNMP Error while setting Multicast IP
CSCus02961	Weak HMAC options on SSH for WLC SHA2 support
CSCus03487	AP 3700 sends wrong TLV during power level negotiation
CSCus03535	AP 1140: Radio d1 reset - Beacon stuck in H/w
CSCus04169	AID leak on 8.0.100.0 FlexConnect local switching scenario
CSCus04711	AP1570: Traceback Crash Dump During EDVT
CSCus06589	AP2700 flooding AP sourced packets out of Aux Gig 1
CSCus06920	Preauth bit set in RSN IE when wlan is wpa2AES
CSCus07013	Adding MAC filter check when client is changing SSID for webauth
CSCus13134	Day0: ping and DHCP issues
CSCus17191	AP1142 DHCP renew delay after EAP-Fast authentication
CSCus20868	WLC ignoring SNMP requests on ports 12225 5246 or 5247
CSCus20968	PI is getting multiple traps from WLC for same LRAD per rogue

Table 9 Resolved Caveats

Bug ID	Headline
CSCus21276	Kernel Panic on WiSM2/5508/2504 in 8.0 when using Webauth
CSCus26067	HA failing after upgrade to 8.0 due to gateway ARP source mac
CSCus30429	OEAP600 not giving ip on remote LAN port in 8.0
CSCus30769	BSSID containing itself and also adding itself to client exclusion list.
CSCus31292	Oct 2014 OpenSSL Vulnerabilities
CSCus33751	Manually classified Rogue APs revert to unclassified
CSCus33759	Local Policies not working after OUI Update
CSCus38268	Memory Leak on WiSM2 due to SNMPTask on 7.4.121.0
CSCus39358	Apple and Android not connecting to WPA2-AES on OEAP600 8.0.110
CSCus39396	8.0.100.0 QoS Bronze Profile not marking traffic to AF11 on Flex
CSCus39461	RADIUS DNS adds both Network and Management Auth + Acct = Enabled
CSCus42727	JANUARY 2015 OpenSSL Vulnerabilities
CSCus44802	WLAN NAS-id is not applied when AP Group NAS-id is changed
CSCus44831	AP1702 reports power error with 802.3af power source
CSCus45806	Enable CDP Spare pair TLV for 1570 and 1530 series access points
CSCus46848	WLC Hangs on rf-profile page if too many rf-profiles are created
CSCus46861	LIZRD attack: Denial of Service
CSCus48452	MAPs do not return to configured channel along with RAP 30 after DFS
CSCus49126	AP3702 floods RTS frames at 8000pps to departed client
CSCus50199	Default route to BVI is present on Central DHCP NAT flex scenario
CSCus52828	snmpv3 rw user creds not working if key length > 32
CSCus53635	Add 802.11a Philippines country support for 1532I APs joined to 5760.
CSCus53822	test dsdump show MSCB outputs to console and not the SSH session
CSCus55004	Kernel Panic with pre-auth ACL and external web-redirect
CSCus55192	WLC8500 crashed during removing SNMP Communities
CSCus58120	Traplog is wrong about Temperature status
CSCus58468	Multicast Address set issue using SNMP
CSCus63569	Sleeping client timer computation is not correct
CSCus64073	1700/2700 APs native VLAN field missing in FlexConnect tab
CSCus66289	WLC crashes after packet-dump
CSCus67081	8.0.110.0: AP does not prime automatically via NDP in Flex+Bridge mode
CSCus68363	Rogue Policies are not applied correctly
CSCus71140	Bonjour service learned via mDNS AP is being forwarded to wired
CSCus72994	"WLC Crash on Task Name: DHCP Socket Task"
CSCus73932	Multicast configuration issue on 8510 WLC OS 8.0.110.4
CSCus79056	WLC5508: Management frames are not marked with CS6

Table 9 Resolved Caveats

Bug ID	Headline
CSCus80059	WLC always send authentication packet to AAA server even though there is no client in WLC
CSCus85337	CAPWAP Restart and Gateway not reachable when MAP roams From RAP1 to RAP2
CSCus85455	First client association does not create NVI int on central DHCP flex
CSCus85767	Flex local switch clients local dhcp are trying to do central DHCP
CSCus89468	Need to add AP802 to list of APs that support Flex+Bridge mode
CSCus90178	AIR-OEAP602I has TCP port 5162 open
CSCus94968	osapiMalloc accepting negative size buffers
CSCut06502	WLC crash due to task name RRM-CLNT-5_0
CSCut07617	Signal 11 crash at PMIPV6_Thread_1
CSCut11821	WLC: ad-hoc containment does not stop
CSCut14210	FlexConnect arp-cache enabled - AP is not responding on behalf of client
CSCut14459	Session ID changes for an intercontroller client roam using EAPFAST
CSCut24611	certificate summary not included can't audit for certificate expiration
CSCut26137	3702 - Voice Queue stuck with no new clients able to associate.
CSCut39118	WLC 8510 Failure to collect feature MobilityExtGroupMember on PI 2.2
CSCut45950	MARCH 2015 OpenSSL Vulnerabilities
CSCut46769	Device Action Info mesg. - Infinite blocked list timeout does not work
CSCut57603	cLNbarAVCFlexProfileApply should have 0 also as an option
CSCut75159	Controller Crash for FlexConnect AP Groups while mapping FlexAVC profile
CSCut75441	Fix illogical **config ap lifetime-check** syntax from CSCuq19142

Installation Notes

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

Warnings

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

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

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

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

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

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

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

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

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

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

Safety Information

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

FCC Safety Compliance Statement

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

Safety Precautions

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

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

Installation Instructions

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

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

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

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

Service and Support

Troubleshooting

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

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

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

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

Related Documentation

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

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

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

Obtaining Documentation and Submitting a Service Request

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

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

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