Release Notes for Cisco Wireless Controllers and Lightweight Access Points for Cisco Wireless Release 8.1.131.0

First Published: November 06, 2015

This release notes document describes what is new in Cisco Wireless Release 8.1.131.0, instructions to upgrade to this release, and open and resolved caveats for this release. Unless otherwise noted, in this document, all Cisco Wireless Controllers are referred to as *Cisco WLCs*, and all Cisco lightweight access points are referred to as *access points* or *Cisco APs*.

Note For information specific to the Cisco Mobility Express solution, see "Cisco Mobility Express Solution Release Notes" section on page 36.

Revision History

Table 1 Revision History

Modification Date	Modification Details
October 10, 2017	• Features Not Supported on Cisco Virtual WLCs, page 25 – Added Wired Guest.
September 14, 2016	• Features Not Supported on Cisco Flex 7510 WLCs, page 24 – Removed: TrustSec SXP from features not supported on Cisco Flex 7510 WLCs section.
August 19, 2016	• Guidelines and Limitations, page 11 – Added information about CSCva84464.
August 17, 2016	• Guidelines and Limitations, page 11 – 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.
May 18, 2016	• Open Caveats, page 29 – Added bug: CSCuw48922 - IW 3702: Poor roaming behavior with 2 6M video streams
May 17, 2016	• Upgrading to Cisco WLC Software Release 8.1.131.0, page 11 – Added this statement: "If you upgrade from Release 8.0.110.0 to a later release, the **config redundancy mobilitymac** *mac-addr* command's setting is removed. You must manually reconfigure the mobility MAC address after the upgrade."
February 18, 2016	• Features Not Supported on Cisco Aironet 1830 and 1850 APs, page 26 – Added Telnet to the list of unsupported features

Cisco Wireless Controller and Cisco Lightweight Access Point Platforms

The section contains the following subsections:

- Supported Cisco Wireless Controller Platforms, page 2
- Supported Access Point Platforms, page 3
- Unsupported Cisco Wireless Controller Platforms, page 4

Supported Cisco Wireless Controller Platforms

The following Cisco WLC platforms are supported in this release:

- Cisco 2500 Series Wireless Controllers (Cisco 2504 Wireless Controller)
- Cisco 5500 Series Wireless Controllers (5508 and 5520 Wireless Controllers)

- Cisco Flex 7500 Series Wireless Controllers (Cisco Flex 7510 Wireless Controller)

- Cisco 8500 Series Wireless Controllers (8510 and 8540 Wireless Controllers)

- Cisco Virtual Wireless Controllers on the Cisco Services-Ready Engine (Cisco SRE) or the Cisco Wireless LAN Controller Module for Cisco Integrated Services Routers G2 (UCS-E)

  Kernel-based virtual machine (KVM) is supported in Cisco Wireless Release 8.1.131.0 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 8.1.131.0.

- Cisco Wireless Controllers for High Availability for Cisco 2504 WLC (no AP SSO support), Cisco 5508 WLC, Cisco 5520 WLC, Cisco Wireless Services Module 2 (Cisco WiSM2), Cisco Flex 7510 WLC, Cisco 8510 WLC, and Cisco 8540 WLC.

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

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

For information about features that are not supported on the Cisco WLC platforms, see Features Not Supported on Cisco WLC Platforms, page 23.

Supported Access Point Platforms

The following access point platforms are supported in this release:

- Cisco Aironet 1040 Series Access Points
- Cisco Aironet 1140 Series Access Points
- Cisco Aironet 1260 Series Access Points
- Cisco Aironet 1600 Series Access Points
- Cisco Aironet 1700 Series Access Points
- Cisco Aironet 1830 Series Access Points
- Cisco Aironet 1850 Series Access Points
- Cisco Aironet 2600 Series Access Points
- Cisco Aironet 2700 Series Access Points
- Cisco Aironet 3500 Series Access Points
- Cisco Aironet 3600 Series Access Points
- Cisco Aironet 3700 Series Access Points
- Cisco Aironet 600 Series OfficeExtend Access Points
- Cisco Aironet 700 Series Access Points
- Cisco Aironet 700W Series Access Points
- Cisco AP802 Integrated Access Point

- Cisco AP803 Integrated Access Point

- Cisco ASA 5506W-AP702

- Cisco Aironet 1530 Series Access Points

- Cisco Aironet 1550 Series Access Points

- Cisco Aironet 1570 Series Access Points

- Cisco Industrial Wireless 3700 Series Access Points

✎

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

For information about features that are not supported on some access point platforms, see Features Not Supported on Access Point Platforms, page 26.

✎

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_4615 43.html

- AP880:

  http://www.cisco.com/c/en/us/products/collateral/routers/887-integrated-services-router-isr/data_s heet_c78_459542.html

  http://www.cisco.com/c/en/us/products/collateral/routers/800-series-routers/data_sheet_c78-61348 1.html

  http://www.cisco.com/c/en/us/products/collateral/routers/880-3g-integrated-services-router-isr/dat a_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_c78-51993 0.html

  Before you use a Cisco AP802 series lightweight access point with Cisco Wireless Release 8.1.131.0, 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

Cisco Hyperlocation

Cisco Hyperlocation is an ultra-precise location solution that attaches to the back of your Cisco Aironet 3700i and 3600i Series wireless access points. It combines Wi-Fi and Bluetooth Low Energy (BLE) technologies to pinpoint beacons, inventory, and personal mobile devices. While some other networks use multiple access points to get location coordinates within 5 to 7 meters of accuracy, Cisco Hyperlocation can track locations to within a single meter.

You can integrate Cisco Hyperlocation with other Cisco wireless solutions for additional uses. Combining it with Cisco Connected Mobile Experiences (CMX), for instance, can result in more precise location analytics that help you deliver more targeted content to users. When you use CMX with Cisco CleanAir® frequency scanning, it's simple to locate failed, lost, and even rogue beacons.

For more information about Cisco Hyperlocation, see the following documents:

- Cisco CMX Release Notes
- The Hyperlocation section in the *Cisco Wireless Controller Configuration Guide*

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	—

Table 2   Software Support for Access Points (continued)

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

Table 2   Software Support for Access Points (continued)

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

Table 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	—
IW3700	IW3702-2E-UXK9	8.0.120.0	—
	IW3702-4E-UXK9	8.0.120.0	—

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

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

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

Software Release Types and Recommendations

This section contains the following topics:

- Release Types, page 10
- Software Release Recommendations, page 11

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	8.0 ED release (8.0.120.0 is 8.0MR2 on the 8.0 release train)

For detailed release recommendations, see the software release bulletin:

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

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

Upgrading to Cisco WLC Software Release 8.1.131.0

Guidelines and Limitations

- When you change the WLAN profile name, then FlexConnect APs (using AP-specific VLAN mapping) will become WLAN-specific. If FlexConnect Groups are properly configured, the VLAN mapping will become Group-specific.

- 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 8.1.131.0 to a 7.x release, the trap configuration is lost and must be reconfigured.

- If you upgrade from Release 8.0.110.0 to a later release, the **config redundancy mobilitymac** *mac-addr* command's setting is removed. You must manually reconfigure the mobility MAC address after the upgrade.

- If you are upgrading from Release 8.0.140.0 or 8.0.15x.0 to a later release and also have the multiple country code feature configured, the feature configuration is corrupted after the upgrade. For more information, see CSCve41740.

- If you have ACL configurations in a Cisco WLC, and downgrade from a 7.4 or later release to a 7.3 or earlier release, you might experience XML errors on rebooting the Cisco WLC. However, these errors do not have any impact on any of the functionalities or configurations.

- If you are upgrading from a 7.4.x or 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 8.1.131.0, 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 8.1.131.0.

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 8.1.131.0 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 8.1.131.0. Table 5 shows the upgrade path that you must follow before downloading Release 8.1.131.0.

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

Table 5   Upgrade Path to Cisco WLC Software Release 8.1.131.0

Current Software Release	Upgrade Path to 8.1.131.0 Software
7.0.x releases	You can upgrade directly to 8.1.131.0. **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 8.1.131.0 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 8.1.131.0.
7.2.x releases	You can upgrade directly to 8.1.131.0. **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 8.1.131.0 Cisco WLC software release. You must downgrade from the 8.1.131.0 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 8.1.131.0.
7.4.x releases	You can upgrade directly to 8.1.131.0.
7.5.x releases	You can upgrade directly to 8.1.131.0.
7.6.x	You can upgrade directly to 8.1.131.0.
8.0.x	You can upgrade directly to 8.1.131.0.
8.1.x	You can upgrade directly to 8.1.131.0.

- When you upgrade the Cisco WLC to an intermediate software release, you must wait until all of the access points that are associated with the Cisco WLC are upgraded to the intermediate release before you install the latest Cisco WLC software. In large networks, it can take some time to download the software on each access point.

- You can upgrade to a new release of the Cisco WLC software or downgrade to an earlier release even if Federal Information Processing Standard (FIPS) is enabled.

- When you upgrade to the latest software release, the software on the access points associated with the Cisco WLC is also automatically upgraded. When an access point is loading software, each of its LEDs blinks in succession.

- We recommend that you access the Cisco WLC GUI using Microsoft Internet Explorer 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 8.1.131.0. 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 8.1.131.0 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 8.1.131.0 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 8.1.131.0 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 8.1.131.0 (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 8.1.131.0 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 8.1.131.0 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 8.1.131.0" section on page 11.

Interoperability with Other Clients

This section describes the interoperability of Cisco WLC Software, Release 8.1.131.0 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	8.1.131.0
Cisco WLC	Cisco 55xx Controller

Table 6   Test Bed Configuration for Interoperability (continued)

Access points	1142, 3502, 3602, 1602, 2602, 1702, 2702, 3702, 702, 702W, 1852
Radio	802.11ac, 802.11a, 802.11g, 802.11n2, 802.11n5
Security	Open, WEP, PSK (WPA and WPA2), 802.1X (WPA-TKIP and WPA2-AES) (LEAP, PEAP, EAP-FAST, EAP-TLS)
RADIUS	ACS 4.2, ACS 5.2
Types of tests	Connectivity, traffic, and roaming between two access points

Table 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	v13.4
Intel 5100/5300	v14.3.2.1
Intel 6200	15.15.0.1
Intel 6300	15.16.0.2
Intel 6205	15.16.0.2
Intel 1000/1030	v14.3.0.6
Intel 7260	17.16.0.4
Intel 7265	17.16.0.4
Intel 3160	17.16.0.4
Broadcom 4360	6.30.163.2005
Linksys AE6000 (USB)	5.1.2.0
Netgear A6200 (USB)	6.30.145.30
Netgear A6210(USB)	5.1.18.0
D-Link DWA-182 (USB)	6.30.145.30
Engenius EUB 1200AC(USB)	1026.5.1118.2013
Asus AC56(USB)	
Dell 1395/1397/Broadcom 4312HMG(L)	5.30.21.0
Dell 1501 (Broadcom BCM4313)	v5.60.48.35/v5.60.350.11
Dell 1505/1510/Broadcom 4321MCAG/4322HM	5.60.18.8
Dell 1515(Atheros)	8.0.0.239
Dell 1520/Broadcom 43224HMS	5.60.48.18
Dell 1530 (Broadcom BCM4359)	5.100.235.12
Dell 1540	6.30.223.215
Cisco CB21	1.3.0.532
Atheros HB92/HB97	8.0.0.320

Table 7   Client Types (continued)

Client Type and Name	Version
Atheros HB95	7.7.0.358
MacBook Pro	OSX 10.10.4
MacBook Air old	OSX 10.10.4
MacBook Air new	OSX 10.10.4
Macbook Pro with Retina Display	OSX 10.10.4
Macbook New 2015	OSX 10.10.4
Tablets	
Apple iPad2	iOS 8.4(12H143)
Apple iPad3	iOS 8.4(12H143)
Apple iPad mini with Retina display	iOS 8.4(12H143)
Apple iPad Air	iOS 8.4(12H143)
Apple iPad Air 2	iOS 8.4(12H143)
Samsung Galaxy Tab Pro SM-T320	Android 4.4.2
Samsung Galaxy Tab 10.1- 2014 SM-P600	Android 4.4.2
Samsung Galaxy Note 3 - SM-N900	Android 5.0
Microsoft Surface Pro 3	Windows 8.1
Microsoft Surface Pro 2	Windows 8.1
Google Nexus 9	Android 5.0.2
Google Nexus 7 2nd Gen	Android 5.0
Intermec CK70	Windows Mobile 6.5 / 2.01.06.0355
Intermec CN50	Windows Mobile 6.1 / 2.01.06.0333
Symbol MC5590	Windows Mobile 6.5 / 3.00.0.0.051R
Symbol MC75	Windows Mobile 6.5 / 3.00.2.0.006R
Phones and Printers	
Cisco 7921G	1.4.5.3.LOADS
Cisco 7925G	1.4.5.3.LOADS
Cisco 8861	Sip88xx.10-2-1-16
Ascom i75	1.8.0
Spectralink 8030	119.081/131.030/132.030
Apple iPhone 4S	iOS 8.4(12H143)))
Apple iPhone 5	iOS 8.4(12H143)
Apple iPhone 5s	iOS 8.4(12H143)
Apple iPhone 5c	iOS 8.4(12H143)
Apple iPhone 6	iOS 8.4(12H143)
Apple iPhone 6 Plus	iOS 8.4(12H143)
HTC One	Android 5.0

Table 7   Client Types (continued)

Client Type and Name	Version
OnePlusOne	Android 4.3
Samsung Galaxy S4 T-I9500	Android 5.0.1
Sony Xperia Z Ultra	Android 4.4.2
Nokia Lumia 1520	Windows Phone 8.1
Google Nexus 5	Android 5.1
Nexus 6	Android 5.1.1
Samsung Galaxy S5-SM-G900A	Android 4.4.2
Huawei Ascend P7	Android 4.4.2
Samsung Galaxy S III	Android 4.3
SpectraLink 8450	3.0.2.6098/5.0.0.8774
Samsung Galaxy Nexus GTI9200	Android 4.4.2
Samsung Galaxy Mega SM900	Android 4.4.2
Samsung Galaxy S6	Android 5.0.2

Features Not Supported on Cisco WLC Platforms

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

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

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
- Cisco 5508 WLC cannot function as mobility controller (MC). However, Cisco 5508 WLC can function as guest anchor in a New Mobility environment.
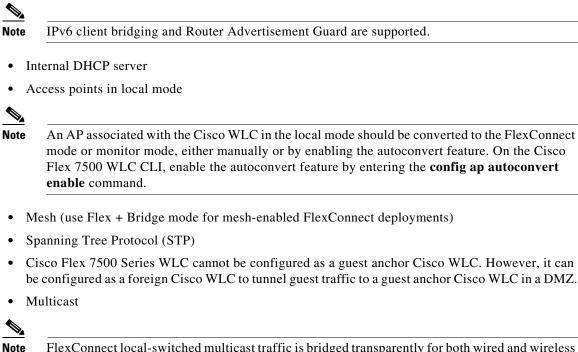
Features Not Supported on Cisco Flex 7510 WLCs

- 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

Note   We recommend that you do not use the multicast-unicast mode in these Cisco WLCs.

Features Not Supported on Cisco Virtual WLCs

- Cisco Aironet 1830 and 1850 Series APs
- 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 1830 and 1850 APs

- Cisco Virtual Wireless Controller
- Mesh mode
- Flex mode
- Monitor mode
- Sniffer mode
- Workgroup Bridge (WGB) mode
- OfficeExtend mode
- Enhanced Local Mode (ELM)
- Integrated BLE
- Basic spectrum analysis
- USB-based Bluetooth Low Energy (BLE) device support
- Cisco CleanAir
- Cisco Wireless ClientLink 3.0

- Rogue Location Discovery Protocol (RLDP)
- Cisco Compatible eXtensions (CCX) Specification
- 802.1x supplicant for AP authentication on the wired port
- Static WEP key for TKIP or CKIP
- Dynamic Transmit Power Control (DTPC)
- Federal Information Processing Standard (FIPS) and Common Criteria
- 40-MHz Rogue detection
- Native IPv6
- Telnet

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

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

- PPPoE
- PMIPv6

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

(Cisco Controller) >show mesh ap summary

Caveats

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 Cisco Bug Search Tool (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
CSCul07738	DPAA Tx/Rx stuck; reload due to Ethernet interface receive failure [FSL]
CSCun52472	Show dtls connection shows blank in AP Name column for Capwap_Data
CSCuq73590	WLC adds incorrect class attribute in accounting stop
CSCuq76115	Cisco Work Group Bridge (WGB) clients with DSCP marking to QoS queue mapping does not work on Cisco 819 router
CSCuq86263	False DFS detection on Cisco 1600AP
CSCur58057	Cisco Flex AP loses some WLANs after radio resets
CSCus02070	FlexConnect AP losing vLAN Mapping and falling on Native vLAN
CSCus61445	DNS ACL on WLC is not working - AP not Send DTLS to WLC
CSCus64550	Mobility client IP Address as 0.0.0.0 in foreign controller
CSCus77368	WLC: Unexpectedly reloads on ewaFormSubmit_cell_edit
CSCus79056	Cisco 5508 controller management frames are not marked with CS6
CSCus80685	AP sends few frames with previous security association's packet number
CSCus91214	Cisco AP802 running 15.3(3)JAB always reloads unexpectedly on entering the dir all-filesystems on Cisco ISR C881W router
CSCus92667	GET on AP groups Table after set - response missing
CSCus97021	Cisco 2500 and Cisco 5508 WLC possible bricking on kernel unexpected reload
CSCus97953	Cisco 8510 WLC reloads unexpectedly on Uhhuh. NMI received for unknown reason 2d
CSCut23325	Cisco 1700AP not encrypting ICMP and ARP sent from the client over the air
CSCut42406	Cisco 5508WLC reloaded unexpectedly while disabling Mobility oracle.
CSCut42926	WLC unexpectedly reloads on SNMPtask after doing configuration audit from PI
CSCut45010	Issue with installing certificates in UTC
CSCut52223	FlexConnect AP loses local EAP certificate when it looses registration with the WLC
CSCut63507	vWLC showing application ID instead of application name
CSCut66994	Anchor / Foreign WLC accounting packets has nas-update=true
CSCut68661	Cisco 702AP unexpectedly reloads on ar9300_set_desc_link
CSCut74263	Mobile Access Gateway on AP does not clear bindings after session/user timeout & de-authentication
CSCut80440	WLC not sending Flex AVC configuration to Mesh AP
CSCut82091	Cisco 3702/3602/1602 AP unexpectedly reloads on CAPWAP CLIENT process
CSCut88319	WLC does NOT support FF08::/16 range of organization-local IPv6 multicast addresses

Table 8   *Open Caveats*

Bug ID	Headline (continued)
CSCut92934	vWLC - AP with expire Manufacturing Installed Certificates (MIC) not able to join with Ignore MIC settings
CSCut95812	AP radio reset with beacons stuck
CSCut95835	AP radio reset with PAK stuck
CSCut98540	Cisco Mobility Express Port statistics are not correct and are not cleared completely
CSCut99150	Cisco 2702AP requesting as a Type 1 power device instead of Type 2
CSCuu02281	APs on WLC with wireless networks disabled detecting rogues
CSCuu04464	License command causes WLC to reload unexpectedly (possible buffer size overwrite)
CSCuu06047	Packet drops on Cisco 2702 AP in Cisco FlexConnect local authentication /local switch mode
CSCuu07107	SNMP walk on clsNetworkRouteConfigTable fails
CSCuu07274	FP0.00: failed to find scb prints at Cisco 5500 WLC standby console
CSCuu08012	Cisco 2700AP CleanAir sensor died (src/dspm_main.c:389) - slot 0
CSCuu08592	Override interf interf-group not been applied on re-authentication for IPv6 clients
CSCuu10781	Multicast configuration mismatch on Web / CLI
CSCuu11959	Cisco 7925 phone using CCKM does not roam gracefully in FlexConnect environment
CSCuu12944	Increase WPA handshake timeout for flex local Authentication
CSCuu13860	'autoconvert flexconnect' is stored as 'disable' on startup-commands
CSCuu14124	RF-profile losing the channel and coverage values after downloading configuration file
CSCuu15866	Local EAP authentication terminates unexpectedly.
CSCuu22083	AP unexpectedly reloads on MESH ASTools PROCESS during mesh initialization
CSCuu24920	Guest clients roam from MC to MA failing
CSCuu31357	AP unexpectedly reloads on VW-ap1530.cc6c.map2
CSCuu33740	WLC unexpectedly reloads while editing SNMP community - waFormSubmit_snmp_comm_list
CSCuu42378	Rx-SOP threshold not working correctly
CSCuu45186	802.11 arp-cache does not work as expected
CSCuu54431	In WLC CLI, copying new tunnel profile with same name unexpectedly reloads the WLC
CSCuu59340	SNR alarms for mesh APs have invalid content and are not working as expected
CSCuu60475	Cisco 3702AP in continuous integration reloads unexpectedly in Process: Net Background
CSCuu63964	Apple clients cannot reconnect Cisco 1850i on forceful de-authentication
CSCuu64295	Domain mismatched on Cisco 1832I,1852I APs
CSCuu64447	CleanAir device commands are disabled after restoring backup configuration file

Table 8 **Open Caveats**

Bug ID	Headline (continued)
CSCuu65672	DTLS Capwap_Ctrl connections not cleared for APs connecting through WAN
CSCuu66484	WLC: GUI 'downloaded AVP' page just keeps reloading
CSCuu66675	During CMCC external authentication, lock unexpectedly reloads on radiusTransportThread
CSCuu71017	Invalid neighbors with bogus IP/RSSI/channel are seen with NDP protected mode
CSCuu72585	When AP is in FlexConnect mode, WLC AAA override cause traffic Black holing
CSCuu75181	Cisco 3702AP under 80MHz is showing "0" as channel or stuck on 40MHz
CSCuu77738	Prime Infrastructure 3.0 Auto Provisioning is not working
CSCuu78888	Web GUI unresponsive after HTTPS-redirect enabled
CSCuu80383	Clients are denied association by neighboring AP during optimized roaming
CSCuu83748	WLC sends bsnRogueAPRemoved Trap when notify configured value is none
CSCuu83941	Cisco 8510WLC: Error enabling global multicast with CAPWAP mode on unicast
CSCuu86781	Cisco 8.1.x release running Cisco 2702AP unexpectedly reloads on LWAPP REAP PROCESS
CSCuu89294	Primary AP in Flex Group not saved in WLC CFG nor in commands backup
CSCuu90899	Cisco 1850AP: Setting telnet to AP specific, enable, changes the AP to WIPS
CSCuu91001	Netflow record sent without client IP address
CSCuu93296	EAP-TLS loosing device certificate in standalone mode after reboot
CSCuu97757	Turning off 2.4GHz & 5 GHz band not reflecting on SPARTAN
CSCuu98988	CAPWAPv6 not doing DNSv6 query for CISCO-CAPWAP-CONTROLLER
CSCuu99344	WLC unexpectedly reloads when DHCP packet content sent is not properly handled while on new mobility
CSCuv03380	During Mesh Roam, security error, Gateway not reachable leading to CAPWAP Restart
CSCuv03963	Multiple Cisco 8510WLC running 8.0.110.18 release unexpectedly reloads Data Plane
CSCuv04255	Cisco 8510 WLC not getting portal page while doing central web authentication
CSCuv08570	Cisco 1532AP loses all configuration at times after power cycle
CSCuv10692	AckFailureCount getting huge value in short period.
CSCuv18403	WLC not lifting mobility tunnel (Data Path Down) running 8.1 release
CSCuv20940	Client fail to ping IPv6 gateway, clients with HA switchover
CSCuv22052	Link local multicast control traffic sent by APs, with IGMP Snooping Enabled
CSCuv22951	Radio reset with reset code of 37
CSCuv27120	Cannot configure IP address x.x.x.255 or x.x.x.0 as gateway
CSCuv27320	Wired clients in Cisco 702W AP leaking traffic across ports/vLANs
CSCuv30948	Local Net Users not saved in configuration backup file
CSCuv33255	Cisco Mobility Express UI: CDP/LLDP showing blank for IOS AP -should display Cisco Discovery Protocol (CDP) info

Table 8   *Open Caveats*

Bug ID	Headline (continued)
CSCuv36096	Some clients are not getting classified even though they are online for flex local switching
CSCuv36306	Cisco 2702AP in Monitor Mode sensord_crashFile with no CleanAir measurements
CSCuv40033	Cisco WLC IPv6 IAPP WIPS reports vulnerability
CSCuv41888	Cisco 1570AP receive 153-3-JA3/JA4 image, sends BPDU to the network
CSCuv48278	Unable to connect clients in 802.11ac Mode for -D domain
CSCuv57038	Cisco 1850 AP - One or more clients ARP not reachable in 200 clients test
CSCuv59060	Cisco Mobility Express: RADIUS authentication will not work if you have multiple servers and delete one of them
CSCuv59274	CPU spike in Cisco 1142AP and utilization is at 100% all the time
CSCuv60759	WLAN: Reading from controller for multiple scenarios (listed) is not working
CSCuv61271	Window DHCP BAD_ADDRESS for Access Points
CSCuv69967	OEAP600 wired 802.1x remote LAN forward traffic in 802.1x Required State
CSCuv78137	Internal AP of Mobility Express unexpectedly reloads in CAPWAP during pre-image download
CSCuv78490	Cisco Mobility Express: No provision to delete the ACL name created in UI
CSCuv80382	Cisco Mobility Express: Kernel panic due possible reuse of buffer
CSCuv80668	Multicast traffic not forwarded when WLAN ID is an even number
CSCuv82711	WLC 5508 8.1.111.0. RFC-3576 Disconnect-Request not heard from port 3799
CSCuw02258	Severity Filter for Monitoring CleanAir Interferes does not work
CSCuw12472	Cisco 5520/8540 controllers show unexpected behavior on Port Link Status/LED activity
CSCuw12544	Rate-limiting is causing 500ms gap of traffic when roaming
CSCuw13264	Cisco 702W AP missing interface information on controller after HA failover
CSCuw19713	Increased Ping latency & Reduced traffic on Cisco 8510WLC with AVC enabled
CSCuw21701	Cisco 1600AP running on 8.2.x release unexpectedly reloads on CFT timer process
CSCuw24958	AP fails to transmit ADDBA response if a data packet is retried previously
CSCuw26377	Cisco WLC reloads unexpectedly because of invalid for field validation on switch_cfg_rw.html
CSCuw26629	MIB message on power supply status on Cisco Flex 7500 WLC is wrong
CSCuw27420	Cisco 3702AP unexpectedly reloads on 8.1MR2 cco image - CFT Timer Process
CSCuw28141	Reaper Reset: Task SNMPTask missed software watchdog
CSCuw28246	Cisco 5520/8540 controllers does not detect power supply cable failure
CSCuw31813	FlexConnect local authentication, client roaming in-out-in during 802.1x
CSCuw31820	WLC CP reloads unexpectedly due to System for apfMsConnTask_6
CSCuw33715	WLC unexpectedly reloads on 802.11k processing
CSCuw48922	IW 3702: Poor roaming behavior with 2 6M video streams

Table 8 Open Caveats

Bug ID	Headline (continued)
CSCuw50324	System unexpectedly reloads on high CPU for bonjour
CSCuw51155	Cisco Mobility Express: Overwrites some WLAN configurations when edited using the UI
CSCuw52341	WLC unexpectedly reloads with RRM task RRM-CLNT-5_0
CSCuw60505	WLC system reloads unexpectedly at apfFreeMobileStationEntry during 802.11x scale test
CSCuw60983	Cisco 3602 AP unexpectedly reloads due to DHCP Client Process
CSCuw61235	Cisco Mobility Express: Multiple 1850APs may become primary controllers at the same time
CSCuw74421	Cisco Mobility Express: Apple iOS devices not connecting to Fast Transition enabled WLAN on IOS APs
CSCuw89581	WLC System unexpectedly reloads on apfReceive Task

Resolved Caveats

Use the Cisco BST to view the details of a caveat listed in this section. For more information about the Cisco BST, see the .

Table 9 Resolved Caveats

Bug ID	Headline
CSCtu45614	Spectrum Management Bit Should be set to 1 all the time
CSCuq79283	Cisco 1142n 1042n 1140 APs traceback dot11_set_frame_templates
CSCur71315	Cisco 1552 MESH AP bridge Transmit voice queue stuck, leading to out of Tx buffers
CSCus53495	DFS detection due to Broadcom spurious emissions in Cisco 2700 and 3700 APs
CSCus61679	Issue in client statistics reports
CSCut07170	Cisco 1532AP: WGB intermittently doesn't see incoming probe responses
CSCut33114	LAG with 1G does not work in Cisco 5520 and Cisco 8540 WLCs
CSCut62319	Broadcast Key Rotation does not occur after MAC Filtering is enabled
CSCut83422	Cisco vWLC serial number changed after management interface ip change
CSCut98006	DFS detections due to high energy profile signature on Cisco 2600AP and 3600AP
CSCuu05565	NDP packets not transmitted on secondary 20 channels
CSCuu32049	WGB attempts to send IAPP change channel event during scanning, roaming
CSCuu34220	Observed traceback in Cisco WLC doing rogue test.
CSCuu37437	Cisco 8510 WLC restarts unexpectedly while NMSP polling in progress
CSCuu47016	Cisco Application Visibility and Control UDP Vulnerability
CSCuu54100	Switching between SSIDs fails with FAST SSID enabled on PMIPv6 WLANs
CSCuu59589	False positive AP sourced AP impersonation on corrupted beacon

Table 9   *Resolved Caveats*

Bug ID	Headline (continued)
CSCuu68490	Duplicate radius-acct update message sent while roaming
CSCuu72366	Cisco 5508 WLC reloads unexpectedly on 8.0.110.x mmListen process
CSCuu82416	Evaluation of WLC for OpenSSL June 2015
CSCuu85603	FlexConnect + MeshAP shows Incorrect channel info in **sh mesh convergence list** output
CSCuu86265	FlexConnect AP Local switching WLAN specific losing VLAN Mapping configuration
CSCuu86587	DN1/DN2: Need closed loop on Cisco 5520 and 8540 WLC cavium fan control
CSCuu98667	vWLC: Low Scale VM auto reboots while downloading image -2GB default memory
CSCuu99823	8.0.x: Cisco 7510 WLC and Cisco 8510 WLC reloads unexpectedly with Taskname: Spamreceivetask
CSCuv00107	PMIPv6 client MAC address shows up on the MAC address table of the switch
CSCuv00598	Optimized Roaming per WLAN feature
CSCuv00856	CleanAir process fails to start for 1572 AP when using 169,173 Channel
CSCuv09655	On 8.0.110.x the anchor reloads unexpectedly on new mobility apf_msDeleteTblEntry
CSCuv28555	Cisco 3702 AP - Voice Queue stuck, with no new clients able to associate
CSCuv34946	EOGRE and PMIPv6 client fails to move to Run state
CSCuv37613	Apple devices failing 802.11r Fast Transition roaming
CSCuv43057	Cisco Mobility Express: System reloads unexpectedly on ConfigSynctoAp
CSCuv44568	Downloading RADIUS AVP via GUI does not load Vendor IDs correctly.
CSCuv47241	Cisco 5500 WLC reloads unexpectedly with SNMP walk on 8.2.1.43
CSCuv47679	EoGRE client traffic packet with DF bit set is getting fragmented
CSCuv48219	Cisco Universal Small Cell module does not turn operational after AP reboot in centralized mode
CSCuv51521	Active WLC should send GARPs when HA Re-Paring after Active-Active state
CSCuv57159	Cisco Mobility Express: MC2UC conversion not happening
CSCuv61883	Error message to be corrected for error popped up (a generic issue)
CSCuv63073	Cisco Mobility Express: Confusing message when next-preferred-primary is the current primary AP
CSCuv72545	Mobility Express Controller takes a long time to come up in Day 0 mode
CSCuv74068	Cisco 3700AP low throughput with Cisco 3700 WGB 40mhz
CSCuv74590	Please delay reboot if image upgrade is in progress
CSCuv79694	Cisco Aironet 1850 Access Point Privileged Escalation Vulnerability
CSCuv80866	WLAN Security 'WPA2 Personal' has WPA AES policy enabled
CSCuv81907	Cisco Mobility Express: Show time has garbage on NTP authentication status
CSCuv83856	Read/Write user is unable to edit settings from GUI

Table 9   *Resolved Caveats*

Bug ID	Headline (continued)
CSCuv86624	Cisco Mobility Express: HTTPS Day-1 GUI connection presents WebAuth cert instead of WebAdmin
CSCuv88543	Cisco Mobility Express -UI: Uploads with special characters under Admin acc GUI Kicks off
CSCuv90042	Cisco FastLocate distant clients have strong RSSI value from AP intermittently
CSCuv90508	WLAN Count: Deleting last WLAN does not update WLAN count
CSCuv90567	Cisco Mobility Express: Changing controller country code does not update Internal AP
CSCuv90769	Unable to schedule pre-image download for 12 - 12.30PM
CSCuv92645	SNMP walk on clsDownloadFileType returns invalid enum for Cisco Mobility Express controller
CSCuv92719	vWLC unexpectedly reloads on 8.1.111.x serving the RF dashboard web page
CSCuv93732	Cisco Hyperlocation not working after adding WLC to CMX
CSCuv95254	Failed to associate Cisco 7925 phones
CSCuv97538	Mu-beamformee field in VHT Cap IE is enabled in association response
CSCuw02126	Cisco Hyperlocation last digit of NTP server is dropped when address has 12 digits
CSCuw02922	Show rules is empty for Cisco Mobility Express controller
CSCuw06153	Unauthorized configuration change for web management
CSCuw19551	Cisco Mobility Express: show time not shown as "AUTH SUCCESS" when NTP Sync happens
CSCuw29419	Cisco WLC: Radius Packet of Disconnect Vulnerability
CSCuw30799	Kernel panic at IPReassembler on internal AP, while pre-image download
CSCuw38455	Cisco 1832AP unable to detect rogue ap
CSCuw40623	NBAR timer running for 7 weeks may trigger an unexpected reload
CSCuw47234	Cisco Mobility Express: Transfer upload datatype coredump broken
CSCuw48570	Cisco Mobility Express UI: Apply button in creating WLAN is not working

Cisco Mobility Express Solution Release Notes

✎

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

The Cisco Mobility Express wireless network solution provides a wireless LAN controller functionality bundled into, currently, the Cisco Aironet 1850 and 1830 series access points. This functionality provides a simplified Wi-Fi architecture with limited enterprise-level WLAN capability to small and medium deployments.

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

The primary AP operates as a wireless LAN controller, to manage and control the subordinate APs, and also operates as an access point to serve clients. The subordinate APs behave as normal lightweight access points to serve clients.

For more information on the solution, including set up and configuration, see the *Cisco Mobility Express User Guide for Release 8.1*, at this URL:

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/mob_exp/1/user_guide/b_ME_User_Guide.html

Supported Cisco Aironet Access Points

APs supported as Primary (support integrated wireless controller capability)	APs supported as Subordinates
Cisco Aironet 1850 Series Cisco Aironet 1830 Series	In addition to the following, all APs that are supported as primary APs are also supported as subordinate APs. Cisco Aironet 700i Series Cisco Aironet 700w Series Cisco Aironet 1600 Series Cisco Aironet 1700 Series Cisco Aironet 2600 Series Cisco Aironet 2700 Series Cisco Aironet 3500 Series Cisco Aironet 3600 Series Cisco Aironet 3700 Series

Supported Features

- Scalability:
  - Up to 25 APs
  - Up to 500 clients
  - Up to 16 WLANs
  - Up to 100 rogue APs
  - Up to 1000 rogue clients
- License—Does not require any licenses (Cisco Right-To-Use License or Swift) for access points.
- Operation— The primary AP can concurrently function as controller (to manage APs) and as an AP (to serve clients).
- Initial configuration wizard.
- Priming at distribution site.
- Default Service Set Identifier (SSID), set from factory—Yes, for initial provisioning only.
- Management—Through a web interface monitoring dashboard.
- Cisco Wireless Controller Best Practices.
- Quality of Service (QoS).
- Multicast with default settings.
- Application Visibility and Control (AVC)—Limited HTTP, with only Application Visibility and not Control. Deep packet inspection with 1,500+ signatures.
- WLAN access control lists (ACLs).
- Roaming—Layer 2 roaming without mobility groups.
- IPv6—For client bridging only.
- High Density Experience (HDX)—Supported when managing access points that support HDX.
- Radio Resource Management (RRM)—Supported within AP group only.
- WPA2 Security.
- WLAN-VLAN Mapping.
- Guest WLAN login (Web Authorization).
- Local EAP Authentication (Local Radius Server) .
- Local Profile.
- Network Time Protocol (NTP) Server.
- Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP).
- Clean Air.
- Simple Network Management Protocol (SNMP).
- Management - SSH / Telnet / Admin users.
- Reset to factory defaults.
- Serviceability - Core file and core options, Logging and syslog.
- Cisco Prime Infrastructure.

- CMX 10.x - Only Location Presence.
- BYOD - On boarding only.
- UX Regulatory Domain.
- Allow Authentication, Authorization, Accounting (AAA) Override.
- IEEE 802.11k
- IEEE 802.11r.
  - Supported: Over-the-Air Fast BSS transition method
  - Not Supported: Over-the-DS Fast BSS transition and Fast Transition PSK authentication
- Passive Client
- Voice with Call admission control (CAC), with Traffic Specification (TSpec)
- Fast SSID
- TACACS (Terminal Access Controller Access Control System)
- Management over wireless
- High Availability and Redundancy—Built-in redundancy mechanism to self-select a primary AP and to select a new AP as primary in case of a failure. Supported using VRRP.
- Software upgrade with pre image download
- Migration to controller-based deployment.

Compatibility with Other Cisco Wireless Solutions

See the *Cisco Wireless Solutions Software Compatibility Matrix*, at the following URL:

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

New Features and Functionalities

This release focuses on bug fixes. No new features or functionalities have been introduced in this release in comparison to the previous release.

Software Release Information

Cisco Mobility Express software for Cisco Wireless Release 8.1.131.0, is as follows:

Software type and purpose	For AP 1850	For AP 1830
Software to be used only for conversion from Unified Wireless Network Lightweight Access Points software to Cisco Mobility Express software.	AIR-AP1850-K9-8.1.131.0.tar	AIR-AP1830-K9-8.1.131.0.tar
Access Point software image bundle, to be used for software update and/or supported access points images.	AIR-AP1850-K9-ME-8-1-131-0.zip	AIR-AP1830-K9-ME-8-1-131-0.zip

Installing Mobility Express Software

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

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/mob_exp/1/user_guide/b_ME_User_Guide.html

Caveats

The open caveats applicable to the Cisco Mobility Express solution are listed under the "Caveats" section on page 27. All caveats associated with the Cisco Mobility Express solution have *Cisco Mobility Express* mentioned in the headline.

Related Documentation

- Cisco Mobility Express User Guide

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/mob_exp/1/user_guide/b_ME_User_Guide.html

- Cisco Aironet Universal AP Priming and Cisco AirProvision User Guide

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

Installation Notes

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

Warnings

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

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

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

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

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

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

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

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

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

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

Safety Information

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

FCC Safety Compliance Statement

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

Safety Precautions

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

- If you are installing an antenna for the first time, for your own safety as well as others', seek professional assistance. Your Cisco sales representative can explain which mounting method to use for the size and type of antenna you are about to install.

- Select your installation site with safety as well as performance in mind. Electric power lines and phone lines look alike. For your safety, assume that any overhead line can kill you.

- Call your electric power company. Tell them your plans and ask them to come look at your proposed installation. This is a small inconvenience considering your life is at stake.

- Plan your installation carefully and completely before you begin. Successfully raising a mast or tower is largely a matter of coordination. Each person should be assigned to a specific task and should know what to do and when to do it. One person should be in charge of the operation to issue instructions and watch for signs of trouble.

- When installing an antenna, remember:
    - Do not use a metal ladder.
    - Do not work on a wet or windy day.
    - Do dress properly—shoes with rubber soles and heels, rubber gloves, long-sleeved shirt or jacket.

- If the assembly starts to drop, get away from it and let it fall. Remember that the antenna, mast, cable, and metal guy wires are all excellent conductors of electrical current. Even the slightest touch of any of these parts to a power line completes an electrical path through the antenna and the installer: **you!**

- If any part of an antenna system should come in contact with a power line, do not touch it or try to remove it yourself. Call your local power company. They will remove it safely.

- If an accident should occur with the power lines, call for qualified emergency help immediately.

Installation Instructions

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

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

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

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

Service and Support

Troubleshooting

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

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

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

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

Related Documentation

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

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

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

Obtaining Documentation and Submitting a Service Request

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

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