



Release Notes for Cisco Wireless Controllers and Lightweight Access Points for Cisco Wireless Release 8.1.111.0

First Published: July 25, 2015

This release notes document describes what is new in Cisco Wireless Release 8.1.111.0, 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*.



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

Revision History

Table 1 **Revision History**

Modification Date	Modification Details
October 10, 2017	<ul style="list-style-type: none"> • Features Not Supported on Cisco Virtual WLCs, page 26 <ul style="list-style-type: none"> – Added Wired Guest.
September 14, 2016	<ul style="list-style-type: none"> • Features Not Supported on Cisco Flex 7510 WLCs, page 25 <ul style="list-style-type: none"> – Removed: TrustSec SXP from features not supported on Cisco Flex 7510 WLCs section
August 17, 2016	<ul style="list-style-type: none"> • Guidelines and Limitations, page 12 <ul style="list-style-type: none"> – 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.
February 18, 2016	<ul style="list-style-type: none"> • Features Not Supported on Cisco Aironet 1850 APs, page 27 <ul style="list-style-type: none"> – 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 8.1.111.0 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 8.1.111.0.

- 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 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 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 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 8.1.111.0, 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 Aironet 1850 Series Access Points](#), page 5
- [QoS Mapping](#), page 5
- [Linux Kernel-based Virtual Machine](#), page 5
- [Solution for Certificate Expiration](#), page 6
- [Cisco Universal Small Cell 8x18 Dual-Mode Module](#), page 6

Cisco Aironet 1850 Series Access Points

The [Cisco Aironet 1850 Series Access Points](#) are supported.

The Cisco Aironet 1850 Series, which is ideal for small and medium-sized networks, delivering optimal performance for enterprise and service provider markets via enterprise-class 4x4 MIMO, four-spatial-stream access points (APs) that support the IEEE's new 802.11ac Wave 2 specification. The Cisco Aironet 1850 Series extends support to a new generation of Wi-Fi clients, such as smart phones, tablets, and laptops that have integrated 802.11ac Wave 1 or Wave 2 support.

The following features are supported:

- 802.11ac Wave 2
- MU-MIMO
- Explicit Compressed Beamforming Feedback (ECBF) or Transmit Beamforming (TxBF)
- Link Aggregation, using Link Aggregation Control Protocol (LACP) only



Note Link Aggregation is not supported on Port Aggregation Protocol (PAgP).

For more information about 802.11ac Wave 2, MU-MIMO, and ECBF, see the [802.11ac section](#) in the *Cisco Wireless Controller Configuration Guide*.

For more information about link aggregation for Cisco Aironet 1850 Series APs, see the [Configuring Link Aggregation](#) chapter in the *Cisco Wireless Controller Configuration Guide*.

QoS Mapping

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

For more information about QoS Mapping, see the [QoS Mapping](#) section in the *Cisco Wireless Controller Configuration Guide*.

Linux Kernel-based Virtual Machine

Linux Kernel-based Virtual Machine (KVM) support is added for Cisco Virtual Wireless Controller. For more information, see:

http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-1/KVM/b_CUWN8-1-vWLC-Deployment-Guide-using-LinuxKVM.html.

Solution for Certificate Expiration

Cisco Lightweight Access Points that were manufactured over 10 years ago may fail to create a CAPWAP or LWAPP connection due to certificate expiration. You may allow the Access Points with Manufactured Installed Certificates (MICs) or Self-signed Certificates (SSCs) beyond their expiration date to associate with Cisco WLC.

On Cisco WLCs, the AP lifetime-check parameter is enabled by default. After upgrading, we recommend that you configure the Cisco WLC to ignore the expiration date on the APs' MICs and SSCs by entering this command:

```
(Cisco Controller) >config ap cert-expiry-ignore {mic | ssc} enable
```

When the **config ap cert-expiry-ignore {mic | ssc} enable** command is entered, Cisco WLC ignores the expiration date on the APs' MICs or SSCs, allowing APs or Cisco WLCs with certificates that are more than 10 years old to connect with each other. The AP lifetime-check parameter must remain enabled as long as APs with expired MICs or SSCs are managed by this Cisco WLC.

To view the configuration state, enter this command:

```
(Cisco Controller) >show certificate summary

Web Administration Certificate..... 3rd Party
Web Authentication Certificate..... Locally Generated
Certificate compatibility mode:..... off
Lifetime Check for MIC ..... Enable
Lifetime Check for SSC ..... Enable
```

For more information, see <http://www.cisco.com/c/en/us/support/docs/field-notices/639/fn63942.html>.

Cisco Universal Small Cell 8x18 Dual-Mode Module

Cisco Universal Small Cell (USC) 8x18 Dual-Mode Module is an external module (4G/LTE) that can be plugged into the Cisco Aironet 3600I APs or Cisco Aironet 3700I APs. You can configure VLAN tagging for the external module's traffic.

For more information about the Cisco USC 8x18 Dual-Mode Module, see:

<http://www.cisco.com/c/en/us/support/wireless/universal-small-cell-8000-series/tsd-products-support-series-home.html>.

For more information about configuring the Cisco USC 8x18 Dual-Mode Module, see the [Cisco Universal Small Cell 8x18 Dual-Mode Module](#) 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	—
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	—	—

Table 2 Software Support for Access Points (continued)

Access Points		First Support	Last Support
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	—
1850 Series	AIR-AP1852I-UXXK9	8.1.111.0	—
	AIR-AP1852I-UXXK910	8.1.111.0	—
	AIR-AP1852I-UXXK9C	8.1.111.0	—
	AIRAP1852I-UXXK910C	8.1.111.0	—
	AIR-AP1852E-UXXK9	8.1.111.0	—
	AIR-AP1852E-UXXK910	8.1.111.0	—
	AIR-AP1852E-UXXK9C	8.1.111.0	—
	AIRAP1852E-UXXK910C	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
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-UXXK9	8.0.110.0	—

Table 2 **Software Support for Access Points (continued)**

Access Points		First Support	Last Support
3500 Series	AIR-CAP3501E	7.0.98.0	—
	AIR-CAP3501I	7.0.98.0	—
	AIR-CAP3502E	7.0.98.0	—
	AIR-CAP3502I	7.0.98.0	—
	AIR-CAP3502P	7.0.116.0	—
3600 Series 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-UXX9	8.0.120.0	—
	IW3702-4E-UXX9	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 11](#)
- [Software Release Recommendations, page 12](#)

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 8.1.111.0

Guidelines and Limitations

- 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 8.1.111.0 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 8.1.111.0, 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 8.1.111.0.



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 8.1.111.0 release from a release that is earlier than Release 7.0.98.0.
- The Cisco Air Time Fairness feature is not supported.
- 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 8.1.111.0. [Table 5](#) shows the upgrade path that you must follow before downloading Release 8.1.111.0.

**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 8.1.111.0

Current Software Release	Upgrade Path to 8.1.111.0 Software
7.0.x releases	<p>You can upgrade directly to 8.1.111.0.</p> <p>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 8.1.111.0 to avoid losing those VLAN settings.</p> <p>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.</p>
7.1.91.0	You can upgrade directly to 8.1.111.0.
7.2.x releases	<p>You can upgrade directly to 8.1.111.0.</p> <p>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 8.1.111.0 Cisco WLC software release.</p> <p>You must downgrade from the 8.1.111.0 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.</p>
7.3.x releases	You can upgrade directly to 8.1.111.0.
7.4.x releases	You can upgrade directly to 8.1.111.0.
7.5.x releases	You can upgrade directly to 8.1.111.0.
7.6.x	You can upgrade directly to 8.1.111.0.
8.0.x	You can upgrade directly to 8.1.111.0.
8.1.102.0	You can upgrade directly to 8.1.111.0.

- 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 8.1.111.0. 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 8.1.111.0 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 8.1.111.0 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 8.1.111.0 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 8.1.111.0 (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 8.1.111.0 software:

- a. Click this URL to go to the Software Center:
<https://software.cisco.com/download/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 8.1.111.0 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 8.1.111.0](#)” section on page 12.

Interoperability with Other Clients

This section describes the interoperability of Cisco WLC Software, Release 8.1.111.0 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	8.1.111.0
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 4322HMS	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 ? GT-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:

- [Features Not Supported on Cisco 2504 WLC, page 24](#)
- [Features Not Supported on Cisco WiSM2 and Cisco 5508 WLC, page 25](#)
- [Features Not Supported on Cisco Flex 7510 WLCs, page 25](#)
- [Features Not Supported on Cisco 5520, 8510, and 8540 WLCs, page 26](#)
- [Features Not Supported on Cisco Virtual WLCs, page 26](#)
- [Features Not Supported on Mesh Networks, page 27](#)



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



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

- Mobility controller functionality in converged access mode

Features Not Supported on Cisco Virtual WLCs

- Cisco Aironet 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 1850 APs, page 27](#)
- [Features Not Supported on Cisco Aironet 1550 APs \(with 64-MB Memory\), page 28](#)

Features Not Supported on Cisco Aironet 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, page 28](#)
- [Open Caveats, page 29](#)
- [Resolved Caveats, page 32](#)

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 28](#)

Table 8 **Open Caveats**

Bug ID	Headline
CSCti97556	Cannot configure IP address x.x.x.255 or x.x.x.0 as gateway from CLI
CSCuI07738	DPAA Tx/Rx stuck; reload due to Ethernet interface receive failure [FSL]
CSCuI92993	RFC 2139—WLCs fail to send FRAMED-IP attribute to AAA server
CSCun52472	The show dtls connection shows blank in AP Name column for Capwap_Data
CSCuq73590	WLC adds incorrect class attribute in accounting stop
CSCuq86263	False DFS detection on 1600
CSCuq86274	Cisco 1530 AP Dynamic Frequency Selection (DFS) detection across all channels
CSCur22862	802.11r reauthentication fails during 4-way handshake after Cisco WLC HA failover
CSCur23631	FlexConnect config issue in AP specific WLAN ACL mapping
CSCur66626	DHCP Proxy behavior on 7.6 release is inconsistent Anchored versus Non Anchored
CSCur68316	FlexConnect mode in Cisco 802AP and ISR 891 is losing VLAN mapping after power cycle
CSCur71315	Cisco Aironet Mesh 1552 bridge transmit voice queue is stuck leading to out of Tx buffers
CSCur90555	Cisco WLC in 8.0 release keeps ghost client entry
CSCus02070	FlexConnect APs losing VLAN mapping and falling on native VLAN
CSCus20991	RADIUS NAC Client authentication issues for 7.6.130.0 release
CSCus61445	DNS ACL on Cisco WLC does not work; AP does not send DTLS to Cisco WLC
CSCus62890	Cisco WLC unexpectedly reloads due to RADIUS client profiler task taking 100 percent cpu usage
CSCus64550	Mobility client IP Address as 0.0.0.0 in foreign controller
CSCus68595	HA Error msg: RF failure notification ErrorType: 31 Reason
CSCus80478	Cisco 1530AP does not forward packets to wired side after bootup
CSCus80685	AP sends few frames with previous security association's packet number
CSCus92667	Group Encrypted Transport (GET) on AP groups table response missing
CSCut23325	Cisco 1700AP not encrypting ICMP and ARP sent over the air from the client
CSCut33114	Link status in Cisco 5520/8540 APs display UP when just SFPs are connected
CSCut41100	802.11a radio reset due to channel change on RRM cycle
CSCut42406	Cisco 5508AP unexpectedly reloads while disabling Mobility oracle.

Table 8 **Open Caveats**

CSCut42926	Cisco WLC unexpectedly reloads on SNMPtask after doing config audit from PI
CSCut45010	Issue with installing certificates in UTC
CSCut48743	FlexConnect AVC—policy-map not getting deleted/add when AP is in apgroup
CSCut48750	In Cisco 1850 AP the BAR storm causes delay in client reassociation
CSCut57957	FlexConnect 1602 APs do not maintain VLAN 1 configuration after reload
CSCut63331	FlexConnect AVC—not able to change value of marking once configured
CSCut65485	FlexConnect AVC profile not blocking Gmail traffic in flex-group
CSCut66994	Anchor/Foreign WLC accounting packets has nas-update=true
CSCut70112	FlexConnect AVC policy is getting applied even though there is no FlexConnect AVC
CSCut85185	FlexConnect AVC wlan_specific mapping is not pushing to AP
CSCut91348	WLC unexpectedly reloads with fatal condition at broffu_fp_dapi_cmd.c:4081
CSCut96598	Cisco 2504 WLC sends access request with same RADIUS id to two different ACS servers
CSCut98006	DFS detections due to high energy profile signature
CSCut98217	VSRE while upgrade from 8.0 to 8.1 release license EULA changed to not accepted
CSCut99150	Cisco 2702AP requesting as a Type 1 power device instead of Type 2
CSCuu00893	Cisco 8500AP Data Plane (DP) exception unexpectedly reloads after resetting controller
CSCuu05565	NDP packets not transmitted to secondary 20 channels
CSCuu06047	Packet drops on Cisco 2702 AP in FlexConnect local authentication/local switch mode
CSCuu06144	Controller Statistics do not match Veriwave or AP statistics
CSCuu07274	“FP0.00:failed to find scb” prints in Cisco 5500AP standby console”
CSCuu08012	Cisco 2700AP CleanAir sensors stopped functioning due to (src/dspm_main.c:389) - slot 0
CSCuu08592	Override interface interf-group not been applied on reauthentication for IPv6 clients
CSCuu10781	Multicast configuration mismatch on Web/CLI
CSCuu20224	Splash page web redirect not redirecting or inconsistent
CSCuu20336	TCP throughput very low for Cisco 1850 AP
CSCuu24920	Guest clients roam from MC to MA failing
CSCuu30805	VWLC licenses deactivated after upgrade to 8.1
CSCuu35352	Cisco 1850 AP Getting lower TCP throughput with Mu-MIMO
CSCuu37437	WLC8510 unexpectedly reloads while NMSP polling in progress.
CSCuu40156	ATF: After Controller reboots, AP's Policies go to default state.
CSCuu40393	Monitor AP using RLDP will send DHCP request even on Association failure
CSCuu45186	Cisco AP702 802.11 arp-cache cannot work
CSCuu47016	Cisco 3602AP unexpectedly reloads when configured in FlexConnect mode

Table 8 **Open Caveats**

CSCuu51625	Cisco WiSM2 unexpectedly reloads
CSCuu53161	WLC occasionally doesn't respond to CoA requests from ISE
CSCuu55010	High cpu usage with CAPWAP client process on AP and join is unstable
CSCuu59340	SNR alarms for Mesh APs have invalid content and not working as expected
CSCuu59697	NGWC Cisco 2702AP does not send EAPoL-Key Message 1 while WLC sends it
CSCuu61905	WLAN A only broadcasting on B/G running 7.6.130.0 release
CSCuu64295	Domain mismatched in Cisco 1832I AP and 1852I AP
CSCuu64447	CleanAir device commands are disabled after restoring backup config
CSCuu65672	DTLS Capwap_Ctrl connections not cleared for APs connecting through WAN
CSCuu68490	Duplicate radius-acct update message sent while roaming
CSCuu71559	Validate if CVE-2015-4000 affects OpenSSL in Cisco WLC
CSCuu72366	Cisco 5508 WLC with 8.0.110.x unexpectedly reloads on mmListen process
CSCuu75181	Cisco 3702AP under 80MHz is showing ""0"" as channel or stuck on 40MHz
CSCuu78888	Web GUI unresponsive after HTTPS-redirect is enabled
CSCuu80383	Clients are denied association by neighbor AP during optimized roaming
CSCuu80441	Anchor controller is not deleting the client entry
CSCuu80484	Cisco 5520 WLC unexpectedly reloads with Release 8.1.102.0
CSCuu83267	Unable to add Cisco 5520 WLC to PI
CSCuu83941	Cisco 8510AP: Error enabling global multicast with capwap mode unicast
CSCuu84797	Local policies are not working with FlexConnect local switching
CSCuu86265	FlexConnect AP Local switching WLAN losing VLAN Mapping Configuration
CSCuu86366	Release 8.1 does not allow zero value for RADIUS ACCT interim update
CSCuu86911	Switching between anchored SSID Leads to stale IP on client
CSCuu87272	Cisco 2700AP can not increase its PMTU after joining Cisco WLC
CSCuu87366	FlexConnect local authentication AP not sending RADIUS request with 802.11r enabled
CSCuu88193	Wrong info shown on controller with no crash file in AP core
CSCuu88579	On MAC Filter failure + Fast SSID bypass captive portal
CSCuu89294	Primary AP in Flex Group not saved in WLC CFG nor commands backup
CSCuu89533	MIC mismatch after session timeout on 802.1x-FT
CSCuu91001	Netflow record sent without client IP address
CSCuu91433	AES-CCMP TSC replays on Root/WGB setup
CSCuu93296	EAP-TLS loosing device certificate in standalone mode after reboot
CSCuu95413	CoA is not acknowledged and send NAK if AAA Server is NATed at FW
CSCuu98792	Cisco 1570AP: antenna enable config is lost on reboot
CSCuu98988	AP not using DNSv6 to discover the Cisco WLC
CSCuu99106	Cisco 3602i APs does not send acknowledgments intermittently to Legacy Clients

Table 8 **Open Caveats**

CSCuu99222	Cisco AP1530 in MAP mode—radio restarts while Tx is in progress
CSCuu99344	Cisco WLC unexpectedly reloads because of DHCP packet content while on new mobility
CSCuv00856	In Cisco 1572AP the CleanAir process fails to start when using 169
CSCuv01918	FlexConnect AP Fails to Associate Clients in AP Group with multiple WLANs
CSCuv03963	Cisco 7510 WLC unexpectedly reloads corrupting the configuration. Leading to reconfiguring the device
CSCuv04058	Error occurred while trying to change the default trap receiver port.
CSCuv04255	Cisco 8510 WLC not getting portal page while doing Central Web Authentication (CWA)
CSCuv06017	802.11w(PMF) WLAN rejects association from Microsoft Surface tablet
CSCuv07136	Cisco WiSM2 AP SSO Memory leak caused Cisco WLC to unexpectedly reload //mwar_ms_deadlock.crash
CSCuv08570	Cisco 1532AP loses all configuration at random after power cycle
CSCuv09655	Anchor WLC unexpectedly reloads on Release 8.0.110.x on New Mobility apf_msDeleteTblEntry
CSCuv09747	Cisco APs drops FlexConnect DHCP replies in unicast
CSCuv09794	”Cisco 1600AP radio PCI reset
CSCuv10692	AckFailureCount getting huge value in short period.
CSCuv10902	Cisco 7925, 7921 VoWiFi phones are trying to roam on Cisco 1850 AP continuously
CSCuv12050	Cisco 5520 WLC unexpectedly reloads with 8.1.102.0 release
CSCuv17204	CAPWAP continuously restarts in Cisco 1850 AP with 8.1.x build
CSCuv22611	In Cisco 1850 AP the LED is stuck in blinking amber after pre-download image
CSCuv24339	Cisco 1850 AP: CDP neighbors on the switch show same for both port IDs
CSCuv46483	AP1850 does not accept DHCP offer unless default gateway is included

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 [“Cisco Bug Search Tool”](#) section on page 28.

Table 9 **Resolved Caveats**

Bud ID	Headline
CSCuu97761	Foreign WLC upgraded to 8.1 fails to export clients to Anchor WLC
CSCut72230	Cisco 3700AP transmits 20 MHz rates when set to 80 MHz
CSCuu20683	RAP might lose the Native VLAN configuration on downgrade from 8.1 release
CSCuu37077	Cisco 3600AP limited channels/power similar to CSCus35411
CSCut46811	Cisco 3702AP not accepting clients on 5GHz when WIPs submode is enabled
CSCuu44155	RAP takes 15 minutes to use wired connection if there are wireless peers available

Table 9 **Resolved Caveats (continued)**

CSCuu32602	Cisco 1550AP-BVI stops functioning when using G3 as uplink in mesh mode
CSCut87326	Cisco WLC generates SNMP traps to PI 2.2 for Cisco AIR-3702 PoE+ getting low power
CSCuu23521	Cisco 5520 WLC unexpectedly reloads with task name radiusTransportThread
CSCut39118	Cisco 8510 WLC—Failure to collect feature MobilityExtGroupMember on PI 2.2
CSCuu86366	Release 8.1 does not allow zero value for RADIUS ACCT Interim update
CSCuu20256	Traffic drop on Cisco WLCs with Release 7.6.130.206 and PMIPv6
CSCut16170	Mobility tunnel down after switchover on 7.6 release
CSCut27598	Client unable to get IP when switching WLAN on New mobility.
CSCur53041	DTLS connection failure
CSCut96026	SGT remains for client when moving between WLANs with Fast SSID change
CSCut76481	Cisco WLC sends 1499 bytes MTU switchover
CSCut97683	Cisco WLC unexpectedly reloads on spamApTask2 in 8.0.110.0 release
CSCut31679	Kernel panic—Unhandled kernel unaligned access
CSCuu52140	Cisco WLC crashing on RRM data read
CSCuu37409	Cisco 8540 WLC unexpectedly reloads on “mmListen” task
CSCuu56538	Cisco 5508 WLC unexpectedly reloads when software fails while accessing the data located at:0x20bdef20
CSCuu22705	BIP should be advertised in RSN IE when PMF=Optional
CSCuu78033	SNMP error while setting new mobility on Cisco 8500AP/Cisco 5520AP devices

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.

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

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

© 2015 Cisco Systems, Inc. All rights reserved.