Release Notes for Cisco Wireless Controllers and Lightweight Access Points for Cisco Wireless Release 8.2.110.0 and 8.2.111.0

First Published: June 01, 2016

This release notes document describes what is new in Cisco Wireless Release 8.2.x, 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 38.

Revision History

Table 1 Revision History

Modification Date	Modification Details
January 29, 2018	• Features Not Supported on Cisco Virtual WLCs, page 30 – Modified information about FlexConnect central switching.
October 16, 2017	• Features Not Supported on Cisco Aironet 1810 OEAP, 1810W, 1830, 1850, 2800, and 3800 Series APs, page 32 – Added SIP snooping with FlexConnect in local switching mode
October 10, 2017	• Features Not Supported on Cisco Virtual WLCs, page 30 – Added Wired Guest and FlexConnect central switching.

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

Table 1 Revision History

Modification Date	Modification Details
November 22, 2016	• Features Not Supported on Cisco 2504 WLC, page 28 – Added: EoGRE • Features Not Supported on Cisco Virtual WLCs, page 30 – Added: EoGRE (Supported in only local switching mode)
October 13, 2016	• Features Not Supported on Cisco Aironet 1810 OEAP, 1810W, 1830, 1850, 2800, and 3800 Series APs, page 32 – Added: Telnet
September 22, 2016	• Features Not Supported on Cisco Aironet 1810 OEAP, 1810W, 1830, 1850, 2800, and 3800 Series APs, page 32 – Removed: Enhanced Local Mode (ELM)
September 13, 2016	• Features Not Supported on Cisco Access Point Platforms, page 31 – Added: Features Not Supported on Cisco Aironet 1810 OEAP, 1810W, 1830, 1850, 2800, and 3800 Series APs – Added: Features Not Supported on Cisco Aironet 1810 OEAP and 1810W Series APs – Added: Features Not Supported on Cisco Aironet 1830 and 1850 Series APs
June 24, 2016	• Added What's New in Release 8.2.111.0, page 5

Cisco Wireless Controller and Cisco Lightweight Access Point Platforms

The section contains the following subsections:

Supported Cisco Wireless Controller Platforms

The following Cisco WLC platforms are supported in this release:

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

Note Kernel-based virtual machine (KVM) is supported in Cisco Wireless Release 8.1 and later releases.

After KVM is deployed, we recommend that you do not downgrade to a Cisco Wireless release that is earlier than Release 8.1.

- Cisco Wireless Controllers for High Availability for Cisco 2504 WLC, Cisco 5508 WLC, Cisco 5520 WLC, Cisco Wireless Services Module 2 (Cisco WiSM2), Cisco Flex 7510 WLC, Cisco 8510 WLC, and Cisco 8540 WLC.

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

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

For information about features that are not supported on the Cisco WLC platforms, see "Features Not Supported on Cisco WLC Platforms" section on page 28.

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 1810 Series OfficeExtend Access Points
- Cisco Aironet 1810W 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 2800 Series Access Points
- Cisco Aironet 3500 Series Access Points
- Cisco Aironet 3600 Series Access Points
- Cisco Aironet 3700 Series Access Points
- Cisco Aironet 3800 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 Cisco Access Point Platforms, page 31.

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

- AP860:

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

- AP880:

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

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

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

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

- AP890:

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

  Before you use a Cisco AP802 series lightweight access point with Cisco Wireless Release 8.2.110.0, 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 Release 8.2.111.0

Release 8.2.111.0 is a repost of Release 8.2.110.0 to incorporate the fix for CSCuz15475 listed in Table 2. There are no other updates in this release.

Table 2 Resolved Caveats in Release 8.2.111.0

Bug ID	Headline
CSCuz15475	Cisco 1800, 2800, or 3800 APs: CAPWAP DNS discovery not picking domain-name string

Note If you are using Cisco 1800, 2800, or 3800 Series APs, and want to enable the DNS Discovery for CAPWAP Join feature, we recommend that you upgrade to Release 8.2.111.0. If you do not want to enable this feature, you do not have to upgrade, and can continue to use Release 8.2.110.0.

What's New in Release 8.2.110.0

Note For information specific to the Cisco Mobility Express solution, see "Cisco Mobility Express Solution Release Notes" section on page 38.

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

Cisco Aironet 2800 and 3800 Series Access Points

The Cisco Aironet 2800 Series and 3800 Series Wi-Fi access points (AP) are 802.11ac Wave2 APs that include Multi-User MIMO (MU MIMO), 160-MHz channel support, Cisco High Density Experience (HDX) and High Performance wireless to name a few features included in the APs. The APs have Flexible Radio feature assigns radio roles and bands (2.4 GHz or 5 GHz) based on a FRA algorithm, and has Dual 5 GHz Radio with bandwidth supporting up to 2.6 Gbps per radio.The APs support full interoperability with leading 802.11ac clients, and support a mixed deployment with other access points and controllers.

Note Cisco Aironet 2800 and 3800 Series APs supports Cisco CleanAir only on 20MHz, 40MHz, and 80MHz.

- For more information about Cisco Aironet 2800 Series APs, see

http://www.cisco.com/c/en/us/support/wireless/aironet-2800-series-access-points/tsd-products-support-series-home.html

- For more information about Cisco Aironet 3800 Series APs, see

http://www.cisco.com/c/en/us/support/wireless/aironet-3800-series-access-points/tsd-products-support-series-home.html

Restrictions on Cisco Aironet 2800 and 3800 Series Access Points

- The 160-MHz channel related information is not displayed on the Main Dashboard of the Cisco WLC GUI.
- The Cisco Flexible Radio information is displayed on the Network Summary and AP Detail pages of the Cisco WLC GUI.

Cisco Aironet 1810 Series OfficeExtend Access Points

The Cisco Aironet 1810 Series OfficeExtend Access Point (OEAP) offers a highly secure enterprise wireless and wired connection to the home, micro-branch, or other types of remote sites. The APs connect to the home or site broadband Internet access and establish a highly secure tunnel to the corporate network. This tunnel enables remote employees to access data, voice, video and cloud services for a mobility experience consistent with that at the corporate office.

The Cisco Aironet 1810 Series OEAPs allow wired access via Power over Ethernet (PoE). This feature provides wired access with PoE out for other devices such as IP phones, security cameras, and many other devices; this is in addition to the AC power adapter to power the device.

For more information about Cisco Aironet 1810 Series OEAPs, see

http://www.cisco.com/c/en/us/support/wireless/aironet-1810-series-officeextend-access-points/tsd-products-support-series-home.html

Cisco Aironet 1810W Series Access Points

The Cisco Aironet 1810W Series Access Points offer a compact AP with multiple mountable options. This AP can be wall plate–vertically mountable or placed on the desk using the optional sleek desk cradle, making it ideal for hospitality, cruise ships, residential halls or other multi-dwelling-unit deployments.

The Aironet 1810W Series combines simultaneous dual radios, and dual band with 802.11ac Wave 2 MU-MIMO Wi-Fi providing a data rate of up to 867 Mbps on the 5-GHz radio, and Gigabit Ethernet port wired connectivity built to take advantage of existing cabling infrastructure.

For more information about Cisco Aironet 1810W Series APs, see

http://www.cisco.com/c/en/us/support/wireless/aironet-1810w-series-access-points/tsd-products-support-series-home.html

Restrictions on Cisco Aironet 1810 and 1810W Series Access Points

The Remote LAN clients and slots are displayed as 2.4-GHz clients and slots, and the respective data counters remain at zero in the Cisco WLC Main Dashboard.

Support for –B Domain

The FCC (USA) rule-making on 5-GHz released on April 1, 2014, (FCC 14-30 Report and Order) goes into effect for products that are sold or shipped on or after June 2, 2016. Cisco APs and Cisco WLCs will comply with the new rules by supporting the new regulatory domain (–B) for the US and will create new AP SKUs that are certified under the new rules. Examples of new rules include new 5-GHz band channels permitted for outdoor use, and transmission (Tx) power level increased to 1W for indoor, outdoor, and point-to-point transmissions.

Note Cisco APs and Cisco WLCs that are in the –A domain category can continue to operate and even coexist with –B domain devices without any issues.

We recommend that you upgrade Cisco APs and Cisco WLCs to the appropriate software release that supports –B domain.

–B Domain Compliant Cisco APs in this Release

- AP803
- AP700i/w
- AP1532i/e
- AP1552
  - H
  - SA
  - SD
  - WU

- AP1600i/e
- AP1700i
- AP1810 (OEAP)
- AP1810W
- AP2600i/e
- AP2700i/e
- AP2800
- AP3600i/e
- AP3700i/e
- AP3700p
- AP3800
- IW3702
- AP702i

–B Domain Compliant Cisco APs Prior to this Release

- AP1570
- AP1830
- AP1850i/e

Multi-Gigabit Ethernet

Cisco's Multi-Gigabit Ethernet (mGig) technology allows you to leverage 802.11ac Wave 2 speeds on your device. This enables speeds of 100 Mbps, 1 Gbps, 2.5 Gbps, and 5 Gbps on Category 5e and 10GBASE-T cables. This feature is currently available on the Cisco Aironet 3800 Series APs.

Flexible Radio Assignment

The Flexible Radio Assignment feature allows for either manual configuration of capable APs or for these APs to intelligently determine the operating role of the integrated radios based on the available RF environment. APs with flexible radio can automatically detect when a high number of devices are connected to a network and changes the dual radios in the access point from 2.4 GHz/5 GHz to 5 GHz/5 GHz to serve more clients. The AP performs this task while still monitoring the network for security threats and RF Interference that may affect performance. Flexible Radio Assignment improves mobile user experience for high-density networks. This feature also reduces 2.4-GHz cell congestion by marking some of the 2.4GHz radios as redundant and switching them to 5GHz (client-serving role) or monitor role (2.4GHz and 5GHz). Use the CLI or GUI to configure the radio role.

An AP with flexible radio can operate in the following modes:

- Default operating mode—One radio serves clients in 2.4 GHz mode, while the other serves clients in 5 GHz mode.
- Dual 5 GHz Mode—Both radios operate in the 5 GHz band, actively serving clients to maximize the benefits of 802.11ac Wave 2 and to increase client device capacity.

- Wireless Security Monitoring—One radio serves 5 GHz clients and the other radio scans both 2.4 GHz and 5 GHz bands for wIPS attackers, CleanAir interferers, and rogue devices.

EDCA and QoS Enhancements

Enhanced distributed channel access (EDCA) parameters provide preferential wireless channel access for voice, video, and other quality of service (QoS) traffic. From this release, EDCA customized option is supported for both the 802.11a and the 802.1b network. The **config advanced** {**802.11a** | **802.11b**} **edca-parameter custom-set** *profile name* command is added to configure a customized QoS profile for 802.11a and 802.11b.

FlexConnect Mode support

FlexConnect mode support is added for Cisco Aironet 1800, 2800, and 3800 Series APs.

Key FlexConnect Features supported on these access points are:

- Local switching
- Standalone mode
- WLAN-VLAN mapping
- Layer2 ACL
- AAA Override ACL
- VLAN ACL Web Authentication
- Pre-authentication web authentication policy
- Local authentication
- Smart Upgrade
- 802.11r
- AAA VLAN override

Software Release Support for Access Points

Table 3 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 3 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	—

Table 3 Software Support for Access Points (continued)

Access Points		First Support	Last Support
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	—	—
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	—
1810 Series	AIR-OEAP1810-x-K9	8.2.111.0	—

Table 3 Software Support for Access Points (continued)

Access Points		First Support	Last Support
1810W Series	AIR-AP1810W-x-K9	8.2.111.0	—
1830 Series	AIR-AP1832I-UXK9	8.1.120.0	—
	AIR-AP1832I-x-K9	8.1.120.0	—
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	—
2800 Series	AIR-AP2802E-x-K9	8.2.111.0	—
	AIR-AP2802I-x-K9	8.2.111.0	—

Table 3 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	—
3800 Series	AIR-AP3802E-x-K9	8.2.111.0	—
	AIR-AP3802I-x-K9	8.2.111.0	—
	AIR-AP3802P-x-K9	8.2.111.0	—
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 3 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	—

Table 3 Software Support for Access Points (continued)

Access Points		First Support	Last Support
1550	AIR-CAP1552C-x-K9	7.0.116.0	—
	AIR-CAP1552E-x-K9	7.0.116.0	—
	AIR-CAP1552H-x-K9	7.0.116.0	—
	AIR-CAP1552I-x-K9	7.0.116.0	—
	AIR-CAP1552EU-x-K9	7.3.101.0	—
	AIR-CAP1552CU-x-K9	7.3.101.0	—
	AIR-CAP1552WU-x-K9	8.0.100.0	—
	AIR-CAP1552H-B-K9	8.2.110.0	—
	AIR-CAP1552WU-B-K9	8.2.110.0	—
1552S	AIR-CAP1552SA-x-K9	7.0.220.0	—
	AIR-CAP1552SD-x-K9	7.0.220.0	—
	AIR-CAP1552SA-B-K9	8.2.110.0	—
	AIR-CAP1552SD-B-K9	8.2.110.0	—
1570 version ID 01 (V01)	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	—
1570 version ID 02 (V02)[4]	AIR-AP1572EAC-B-K9	8.0.135.0	—
	AIR-AP1572EC1-B-K9	8.0.135.0	—
	AIR-AP1572EC2-B-K9	8.0.135.0	—
	AIR-AP1572IC1-B-K9	8.0.135.0	—
	AIR-AP1572IC2-B-K9	8.0.135.0	—
IW3700	IW3702-2E-UXK9	8.0.120.0	—
	IW3702-4E-UXK9	8.0.120.0	—
	IW3702-4E-B-K9	8.2.110.0	—
	IW3702-2E-B-K9	8.2.110.0	—

1. The Cisco 3600 AP was introduced in Cisco Wireless Release 7.1.91.0. If your network deployment uses Cisco 3600 APs with Cisco Wireless Release 7.1.91.0, we highly recommend that you upgrade to Cisco Wireless Release 7.2.115.2 or a later release.
2. These access points are supported in a separate 4.1.19x.x mesh software release and in Release 5.2 or later releases. These access points are not supported in the 4.2, 5.0, and 5.1 releases.
3. y—Country DOCSIS Compliance, see ordering guide for details.
4. Cisco 1570 V02 APs are supported on only specific Cisco Wireless Controller software releases. For more information, see Cisco Wireless Solutions Software Compatibility Matrix.

Software Release Types and Recommendations

This section contains the following topics:

Release Types

Table 4 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 5 Software Release Recommendations

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

For detailed release recommendations, see the software release bulletin:

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

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

Upgrading to Cisco WLC Software Release 8.2.110.0

Guidelines and Limitations

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

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

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

  This occurs in the following conditions:

  a. LAG is not configured.

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

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

  The workaround is to configure all interfaces with VLANs.

  You can track this issue via CSCux75436.

- Effective with Release 8.2.100.0, you cannot download some of the older configurations from the Cisco WLC because of the Multicast and IP address validations introduced in this release. The platform support for global multicast and multicast mode are listed in the following table.

Table 6 Platform Support for Global Multicast and Multicast Mode

Platform	Global Multicast	Multicast Mode	Support
Cisco 5520, 8510, and 8540 WLCs	Enabled	Unicast	No
	Enabled	Multicast	Yes
	Disabled	Unicast	Yes
	Disabled	Multicast	No
Cisco Flex 7510 WLC	Multicast is not supported.		
Cisco 5508 WLC	Enabled	Unicast	Yes
	Enabled	Multicast	Yes
	Disabled	Unicast	Yes
	Disabled	Multicast	No
Cisco 2504 WLC	Only multicast mode is supported.		
Cisco vWLC	Multicast is not supported.		

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

  The workaround is as follows:

  a. Enter the following commands:

  ```
  config boot backup
  show boot

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

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

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

  config boot primary

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

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

- If you downgrade from Release 8.2.110.0 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 8.2.110.0, the APs lose the enabled VLAN support configuration. The VLAN mappings revert to the default values of the VLAN of the associated interface. The workaround is to upgrade from Release 7.0.240.0 and later 7.0.x releases to Release 8.2.110.0.

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 8.2.110.0 release from a release that is earlier than Release 7.0.98.0.
- You can upgrade or downgrade the Cisco WLC software only between certain releases. In some instances, you must first install an intermediate release prior to upgrading to Release 8.2.110.0. Table 7 shows the upgrade path that you must follow before downloading Release 8.2.110.0.

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 7 Upgrade Path to Cisco WLC Software Release 8.2.110.0

Current Software Release	Upgrade Path to 8.2.110.0 Software
7.6.x	You can upgrade directly to 8.2.110.0.
8.0.x	You can upgrade directly to 8.2.110.0.
8.2.x	You can upgrade directly to 8.2.110.0.

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

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

- Cisco WLCs support standard SNMP MIB files. MIBs can be downloaded from the Software Center on Cisco.com.
- The Cisco WLC software is factory installed on your Cisco WLC and is automatically downloaded to the access points after a release upgrade and whenever an access point joins a Cisco WLC. We recommend that you install the latest software version available for maximum operational benefit.
- Ensure that you have a TFTP, FTP, or SFTP server available for the software upgrade. Follow these guidelines when setting up a server:
  - Ensure that your TFTP server supports files that are larger than the size of Cisco WLC software Release 8.2.110.0. Some TFTP servers that support files of this size are tftpd32 and the TFTP server within the Prime Infrastructure. If you attempt to download the 8.2.110.0 Cisco WLC software and your TFTP server does not support files of this size, the following error message appears:

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

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

  Bootloader menu for Cisco 5500 Series WLC:

  ```
     Boot Options
  Please choose an option from below:
  ```

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

Bootloader menu for other Cisco WLC platforms:

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

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

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

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

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

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

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

  Here:

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

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

- You can configure 802.1p tagging by using the **config qos dot1p-tag** {**bronze** | **silver** | **gold** | **platinum**} command. For Release 7.2.103.0 and later releases, if you tag 802.1p packets, the tagging has an impact on only wired packets. Wireless packets are impacted only by the maximum priority level set for QoS.

- You can reduce the network downtime using the following options:
  - You can predownload the AP image.
  - For FlexConnect access points, use the FlexConnect AP upgrade feature to reduce traffic between the Cisco WLC and the AP (main site and the branch). For more information about the FlexConnect AP upgrade feature, see the *Cisco Wireless Controller Configuration Guide*.

Note Predownloading Release 8.2.110.0 on a Cisco Aironet 1240 access point is not supported when upgrading from a previous Cisco WLC release. If predownloading is attempted on a Cisco Aironet 1240 access point, an AP disconnect will occur momentarily.

- Do not power down the Cisco WLC or any access point during the upgrade process; otherwise, you might corrupt the software image. Upgrading a Cisco WLC with a large number of access points can take as long as 30 minutes, depending on the size of your network. However, with the increased number of concurrent access point upgrades supported, the upgrade time should be significantly reduced. The access points must remain powered, and the Cisco WLC must not be reset during this time.
- To downgrade from Release 8.2.110.0 to Release 6.0 or an earlier release, perform either of these tasks:
  - Delete all the WLANs that are mapped to interface groups, and create new ones.
  - Ensure that all the WLANs are mapped to interfaces rather than interface groups.
- After you perform the following functions on the Cisco WLC, reboot the Cisco WLC for the changes to take effect:
  - Enable or disable link aggregation (LAG)
  - Enable a feature that is dependent on certificates (such as HTTPS and web authentication)
  - Add a new license or modify an existing license
  - Increase the priority of a license
  - Enable HA
  - Install the SSL certificate
  - Configure the database size
  - Install the vendor-device certificate
  - Download the CA certificate
  - Upload the configuration file
  - Install the Web Authentication certificate
  - Make changes to the management interface or the virtual interface
  - Make changes to TCP MSS settings

Upgrading to Cisco WLC Software Release 8.2.110.0 (GUI)

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

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

Step 2 Follow these steps to obtain Cisco Wireless Release 8.2.110.0 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 8.2.110.0 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 8.2.110.0" section on page 16.

Interoperability with Other Clients

This section describes the interoperability of Cisco WLC Software, Release 8.2.110.0 with other client devices.

Table 8 describes the configuration used for testing the client devices.

Table 8 Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	8.2.110.0
Cisco WLC	Cisco 55xx Series Controller
Access points	3802, 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 5.2, ISE 1.4
Types of tests	Connectivity, traffic, and roaming between two access points

The following tables list the client types on which the tests were conducted. The clients included laptops, hand-held devices, phones, and printers.

- Laptop: Table 9 lists the laptop client types on which the tests were conducted.

Table 9 Laptop Client Type List

Client Type and Name	Version
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 3160	18.40.0.9
Intel 7260	18.40.0.9
Intel 7265	18.40.0.9
Intel 8260	18.40.0.9
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)	1027.515.2015
Dell 1395/1397/Broadcom 4312HMG(L)	5.30.21.0
Dell 1501 (Broadcom BCM4313)	v5.60.48.35/v5.60.350.11

Table 9 Laptop Client Type List

Client Type and Name	Version
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
Dell 1560	6.30.223.262
Cisco CB21	1.3.0.532
Atheros HB92/HB97	8.0.0.320
Atheros HB95	7.7.0.358
MacBook Pro	OSX 10.11.4
MacBook Air old	OSX 10.11.4
MacBook Air new	OSX 10.11.4
Macbook Pro with Retina Display	OSX 10.11.4
Macbook New 2015	OSX 10.11.4

- Tablet: Table 10 lists the tablet client types on which the tests were conducted.

Table 10 Tablet Client Type List

Client Type and Name	Version
Apple iPad2	iOS 9.3.1(13E238)
Apple iPad3	iOS 9.3.1(13E238)
Apple iPad mini with Retina display	iOS 9.3.1(13E238)
Apple iPad Air	iOS 9.3.1(13E238)
Apple iPad Air 2	iOS 9.3.1(13E238)
Apple iPad Pro	iOS 9.3.1(13E238)
Samsung Galaxy Tab Pro SM-T320	Android 4.4.2
Samsung Galaxy Tab 10.1- 2014 SM-P600	Android 4.4.2
Samsung Galaxy Note 3 – SM-N900	Android 5.0
Microsoft Surface Pro 3	Windows 8.1 Driver: 15.68.3093.197
Microsoft Surface Pro 2	Windows 8.1 Driver: 14.69.24039.134
Google Nexus 9	Android 6.0.1
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

Table 10 Tablet Client Type List

Client Type and Name	Version
Symbol MC5590	Windows Mobile 6.5 / 3.00.0.0.051R
Symbol MC75	Windows Mobile 6.5 / 3.00.2.0.006R

- Phones: Table 11 lists the phone client types on which the tests were conducted.

Table 11 Phone Client Type List

Client Type and Name	Version
Cisco 7921G	1.4.5.3.LOADS
Cisco 7925G	1.4.5.3.LOADS
Cisco 8861	Sip88xx.10-2-1-16
Apple iPhone 4S	iOS 9.3.1(13E238)
Apple iPhone 5	iOS 9.3.1(13E238)
Apple iPhone 5s	iOS 9.3.1(13E238)
Apple iPhone 5c	iOS 9.3.1(13E238)
Apple iPhone 6	iOS 9.3.1(13E238)
Apple iPhone 6 Plus	iOS 9.3.1(13E238)
HTC One	Android 5.0
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
Google Nexus 5X	Android 6.0.1
Google 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
Samsung Galaxy Nexus GTI9200	Android 4.4.2
Samsung Galaxy Mega SM900	Android 4.4.2
Samsung Galaxy S6	Android 6.0.1
Samsung Galaxy S7	Android 6.0.1
Xiaomi Mi 4c	Android 5.1.1
Xiaomi Mi 4i	Android 5.1.1

Features Not Supported on Cisco WLC Platforms

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

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

Features Not Supported on Cisco 2504 WLC

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

Note However, AVC for local mode APs is supported.

- Bandwidth Contract
- Service Port
- AppleTalk Bridging
- Right-to-Use Licensing
- Smart Licensing
- PMIPv6
- EoGRE
- AP Stateful Switchover (SSO) and client SSO
- Multicast-to-Unicast
- Cisco Smart Software Licensing

Note The features that are not supported on Cisco WiSM2 and Cisco 5508 WLC are not supported on Cisco 2504 WLCs too.

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

Features Not Supported on Cisco WiSM2 and Cisco 5508 WLC

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

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

- Configuration of 802.3 bridging, AppleTalk, and Point-to-Point Protocol over Ethernet (PPPoE)
- Fragmented pings on any interface
- Right-to-Use Licensing
- Cisco 5508 WLC cannot function as mobility controller (MC). However, Cisco 5508 WLC can function as guest anchor in a New Mobility environment.
- Smart Licensing

Features Not Supported on Cisco Flex 7510 WLCs

- Static AP-manager interface

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

- TrustSec SXP
- IPv6 and Dual Stack client visibility

Note IPv6 client bridging and Router Advertisement Guard are supported.

- Internal DHCP server
- Access points in local mode

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

- Mesh (use Flex + Bridge mode for mesh-enabled FlexConnect deployments)
- Spanning Tree Protocol (STP)
- Cisco Flex 7500 Series WLC cannot be configured as a guest anchor Cisco WLC. However, it can be configured as a foreign Cisco WLC to tunnel guest traffic to a guest anchor Cisco WLC in a DMZ.

- Multicast

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

- PMIPv6
- Smart Licensing

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

- Internal DHCP Server
- Mobility controller functionality in converged access mode

Note Smart Licensing is not supported on Cisco 8510 WLC.

Features Not Supported on Cisco Virtual WLCs

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

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

- FlexConnect central switching in large-scale deployments

Note FlexConnect central switching is supported in only small-scale deployments, wherein the total traffic on Cisco WLC ports is not more than 500 Mbps.

FlexConnect local switching is supported.

- AP and Client SSO in High Availability
- PMIPv6
- EoGRE (Supported in only local switching mode)
- 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 Cisco Access Point Platforms

- Features Not Supported on Cisco Aironet 1550 APs (with 64-MB Memory), page 31

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
```

Features Not Supported on Cisco Aironet 1810 OEAP, 1810W, 1830, 1850, 2800, and 3800 Series APs

Table 12 Features Not Supported on Cisco Aironet 1810 OEAP, 1810W, 1830, 1850, 2800 and 3800 Series APs

Operational Modes	• Spectrum Expert Connect • Workgroup Bridge (WGB) mode as a part of Cisco Mobility Express • Mesh mode • Flex plus Mesh • 802.1x supplicant for AP authentication on the wired port
Protocols	• 802.11u • Full Cisco Compatible Extensions (CCX) support • Rogue Location Discovery Protocol (RLDP) • Native IPv6 • Telnet
Security	• Encryption – Temporal Key Integrity Protocol (TKIP) • Locally Significant Certificate (LSC) • TrustSec SXP • CKIP, CMIC, and LEAP with Dynamic WEP • Static WEP key for TKIP or CKIP [1]
Quality of Service	• Cisco Air Time Fairness (ATF)
Spectrum Utilization	• Wi-Fi Tag • Aggressive Load Balancing
Packet Forwarding	• Split tunnels • PPPoE • NAT

Table 12 Features Not Supported on Cisco Aironet 1810 OEAP, 1810W, 1830, 1850, 2800 and 3800 Series APs (continued)

Location Services	• Data RSSI (Fast Locate)
FlexConnect Features	• Per Client AAA (QoS Override) • Bidirectional rate-limiting • Link aggregation (LAG) • Split Tunneling • EoGRE • Multicast to Unicast (MC2UC) • Traffic Specification (TSpec) – Cisco Compatible Extensions (CCX) – Call Admission Control (CAC) • DHCP Option 60 • NAT/PAT support • VSA/Realm Match Authentication • Proxy ARP • SIP snooping with FlexConnect in local switching mode

1. For more details, see the Wi-Fi Alliance Technical Note TKIP document in the Wi-Fi Organization's website.

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 1810 OEAP and 1810W Series APs

Table 13 Features Not Supported on Cisco Aironet 1810 OEAP and 1810W Series APs

Operational Modes	• Monitor Mode • Multiple client on wired ports

Features Not Supported on Cisco Aironet 1830 and 1850 Series APs

Table 14 Features Not Supported on Cisco Aironet 1830 OEAP and 1850 Series APs

Operational Modes	• Monitor Mode

Caveats

Caveats describe unexpected behavior in a product. The Open Caveats section lists open caveats that apply to the current release and may apply to previous releases. A caveat that is open for a prior release and is still unresolved applies to all future releases until it is resolved.

To view the details of the software bugs pertaining to your product, perform the following task:

Click the Caveat ID/Bug ID number in the table.

The corresponding Bug Search Tool page is displayed with details of the Caveat ID/Bug ID.

The Bug Search Tool (BST), which is the online successor to the Bug Toolkit, is designed to improve the effectiveness in network risk management and device troubleshooting. The BST allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data, such as bug details, product, and version. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of a caveat whose ID you do not have, perform the following procedure:

1. Access the BST using your Cisco user ID and password:

   https://tools.cisco.com/bugsearch/

2. In the Bug Search window that is displayed, enter the necessary information in the corresponding fields.

For more information about how to use the Cisco Bug Search Tool effectively, including how to set email alerts for bugs and to save bugs and searches, see the Bug Search Tool Help & FAQ page.

Open Caveats

Table 15 Open Caveats for Release 8.2.110.0

Bug ID	Headline
CSCuw48922	IW 3702: Poor roaming behavior with 2 6M video streams
CSCux76622	Cisco 1810 and 1810W APs–2X2 detecting 802.3af power type with power injector
CSCux78581	Multiple client support on LAN port on Cisco 1810 AP wall plate
CSCux84505	IW 3702: Downlink TCP traffic is dropped by AP
CSCux94399	Sequence number of frames not resetting when wrap around
CSCuy05898	Cisco wIPs: AP1850 is not showing some of the alarms
CSCuy39487	Cisco 1810 and 1810W APs–When in standalone mode, unable to match PMKID for 4way handshake
CSCuy53942	Cisco 3800 AP not including Channel Switch Announce IEs after radar
CSCuy79069	Access Point OS (AP-OS) APs–Always joins Backup Secondary although Primary is present
CSCuz15637	Aggregation not working with Cisco 1850
CSCuz27637	Cisco 1810W AP–802.11r results in MIC errors from Cisco Cius devices
CSCuz38954	Cisco 3800 AP Flex mode–U-APSD-More and EOSP data bits not set correctly
CSCuz42168	Cisco Unified IP Phones 7921 and 7926 get disconnected at random times
CSCuz48887	Cisco 2800 and 3800 APs–False radar detection with dual 5GHz 160MHz channel
CSCuz56926	Radio reset due to “No CleanAir msmts 0”
CSCuz57169	Radio reset due to “No DFS Msmts”
CSCuz58908	Cisco 3800 AP–FRA configurations not retained in HA setup
CSCuz59350	Cisco 2800 APs–Kernel panic - PC is at deactivate_slab+0x104/0x3c8
CSCuz61598	A-MSDU cannot be disabled on BE
CSCuz61726	A-MSDU cannot be enabled on VO
CSCuz65175	Cisco Mobility Express 1852–HTTP profiling causes CPU spikes and degraded performance
CSCuz65327	Cisco 3800 AP Flex mode- WGB client cannot join
CSCuz66026	Client disconnecting on standalone mode after WLAN session timeout
CSCuz68479	Cisco 3800 AP not reassembling wireless fragmented frames

Resolved Caveats

Table 16 Resolved Caveats for 8.2.110.0

Bug ID	Headline
CSCuf71713	Cisco WLC SP port not usable in SSO mode
CSCuq21626	IP address reversed in duplicate IP trap in Cisco 8500 WLC
CSCus07279	OEAP WLC GUI shows AP IP as private instead of public IP
CSCut76824	Anchor WLC will not forward DHCP request to the DHCP server
CSCuu65672	DTLS Capwap_Ctrl connections not cleared for APs connecting through WAN
CSCuv62410	Ping failed from Cisco WLC to direct AP
CSCuv68892	Cisco WLC loses default kernel route when dynamic int is created on the 2nd port
CSCuv74719	Apple Clients EAP-FAST Authentication Failure
CSCuw12472	Cisco 5520 and Cisco 8540 WLCs Port Link Status and Activity LED unexpected behavior
CSCuw34289	AP values have high variance for Cisco FastLocate environment
CSCuw50867	Show invalid-config, ap mgmtuser invalid configure
CSCuw57850	Filtering for client calibration pulses with frequency offset
CSCuw82858	Cisco Air Time Fairness takes around 10-15secs to delete an Air Time Fairness policy
CSCuw83312	The command show rules output mess up when use telnet or ssh
CSCuw86539	RADIUS pending requests counter not clearing
CSCuw89375	Able to map 3G enable interface on ap-group
CSCuw93917	Netflow config not able to modify, Cisco WLC downgraded from 8.2 to 8.1 release
CSCuw94949	Invalid FTIE MIC on ME WLC when client tries FT roam between IOS APs
CSCux00531	Cisco 2500 and Cisco 5508 WLCs have partial collection failure file transfer configuration
CSCux00803	New Mobility clients stuck in DHCP_REQD state with NAT IP on Foreign
CSCux05901	Cisco 5508 WLC is not honoring AAA override for upload bandwidth for webauthentication
CSCux08557	Reaper reset because of SNMPTASK : VALIDATE_GUEST_SESSION_FAILED
CSCux11666	Cisco 8500 WLC returns differing cLMobilityGroupMembersTable values
CSCux13032	Anchor not appending client MAC in external webauthentication redirect with HTTPS
CSCux13299	SSID not brodcasting when AP mode changed from local to Cisco Flex mode in Cisco vWLC
CSCux15311	Cisco WLC does not send all accounting messages to TACACS+ server

Table 16 Resolved Caveats for 8.2.110.0 (continued)

Bug ID	Headline
CSCux18259	Prime Infrastructure 3.0 - Sync Issue on Flexconnect Native VLAN Configuration
CSCux21537	Long delays & intermittent disconnect after 802.11r roaming (FT PSK)
CSCux38853	Grep command unavailable for Cisco WLC local ReadOnly management user
CSCux41354	Evaluation of Cisco WLC for OpenSSL December 2015 vulnerabilities
CSCux50941	Cisco Hyperlocation: incorrect (+) RSSI values on channels other than U-NII-3
CSCux52043	Cisco WLC: Memory leak in k_mib_cisco_lwapp_wlan
CSCux53607	Cisco WLC SNMP for cLAPGroups802dot11bgRFProfileName returns wrong value
CSCux57925	Cisco Controller entering yellow zone at 1.6 GB with Teredo traffic
CSCux58427	Clients cannot connect, drops and high latency pings to Cisco WLC management interface
CSCux61747	Cisco WLC hangs when configuring DNS-based ACL
CSCux75544	Cisco WLC reloads unexpectedly on emweb multiple times in Cisco 8.2.x build
CSCux82955	Anchor WLC does not forward DHCP request to server as VLAN is set to 0
CSCuy07338	Evaluation of Cisco WLC for OpenSSL January 2016
CSCuy12650	Tracebacks On Autonomous WGB Cisco IW3702s
CSCuy27190	Cisco 1850 and 1830 APs draw 24.8Watts
CSCuy28318	Cannot delete stale Angle of Arrival (AoA) configuration from Cisco WLC
CSCuy36572	Evaluation of Cisco WLC for glibc_feb_2016
CSCuy40264	Client association and disassociation traps returning a SNR/RSSI value of 0
CSCuy55634	Cisco 1530 AP in Mesh Flex-bridge mode does not Tx traffic if connected at 100M
CSCuy58091	Evaluation of Cisco WLC for OpenSSL March 2016
CSCuy59925	Issues in cLApDot11XorRadioBand and cLApDot11RadioSubType
CSCuy71595	Cisco 1552S AP on Cisco 8.2.x release, the 5GHz radio does not join Cisco WLC for -M reg domain code QA
CSCuy82556	Cisco Discovery Protocol (CDP) limitiing per AP
CSCuy98783	AP reloads unexpectedly due to invalid platform type detection
CSCuz02510	Cisco Hyperlocation not working on AP MAC address starting from 00
CSCuz48589	Local SSID allowed to be same as Corporate SSID on Cisco Aironet 1810 OEAP

Cisco Mobility Express Solution Release Notes

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

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

In the Cisco Mobility Express wireless network solution, one AP, which runs the Cisco Mobility Express wireless LAN controller, is designated as the 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. It also operates as an AP to serve clients. The subordinate APs behave as normal lightweight APs to serve clients.

For more information about the solution, including setup and configuration, see the *Cisco Mobility Express User Guide for Release 8.2*, at:

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

Supported Cisco Aironet Access Points

APs Supported as Primary (Support Integrated Wireless Controller Capability)	APs Supported as Subordinate
Cisco Aironet 1850 Series Cisco Aironet 1830 Series	In addition to the following, all the APs that are supported as 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

Mobility Express Features

The following features and functionalities are present in this release:

- CLI-based Initial configuration wizard
- Up to three Network Time Protocol (NTP) servers, with support for FQDN names.
- Simple Network Management Protocol (SNMP) version 3 polling, supported via CLI only.
- IEEE 802.11r with support for Over-the-Air Fast BSS transition method, Over-the-DS Fast BSS transition method, and Fast Transition PSK authentication. Fast BSS transition methods are supported via CLI only.
- CCKM, supported via CLI only.
- Client ping test
- Changing the country code on the controller and APs on the network, via the controller GUI.
- Syslog messaging towards external server
- Software image download using HTTP for networks containing only AP 1850, AP 1830, or both kinds of access points.

The following are existing features, with continued support in the current release:

Note Even if the Cisco AP is 802.3ad (LACP)-compliant, link aggregation groups (LAG) are not supported on the AP while it has a Cisco Mobility Express software image.

- Scalability:
  - Up to 25 APs
  - Up to 500 clients
  - Up to 16 WLANs
  - Up to 100 rogue APs
  - Up to 1000 rogue clients
- License—Does not require any licenses (Cisco Right-To-Use License or Swift) for APs.
- Operation— The 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. Available for initial provisioning only.
- Management—Through a web interface Monitoring Dashboard.
- Cisco Wireless Controller Best Practices.
- Quality of Service (QoS).
- Multicast with default settings.
- Application Visibility and Control (AVC)—Limited HTTP, with only Application Visibility and not Control. Deep Packet inspection with 1,500+ signatures.
- WLAN access control lists (ACLs).

- Roaming—Layer 2 roaming without mobility groups.
- IPv6—For client bridging only.
- High Density Experience (HDX)—Supported when managing APs that support HDX.
- Radio Resource Management (RRM)—Supported within AP group only.

Note Cisco 2800 and 3800 APs may experience issues forming RF neighborhood when NDP encryption is turned on in a mix deployment environment.

- WPA2 Security.
- WLAN-VLAN mapping.
- Guest WLAN login with Web Authorization.
- Local EAP Authentication (local RADIUS server).
- Local profile.
- Network Time Protocol (NTP) Server.
- Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP).
- Clean Air.
- Simple Network Management Protocol (SNMP).
- Management—SSH, Telnet, Admin users.
- Reset to factory defaults.
- Serviceability—Core file and core options, Logging and syslog.
- Cisco Prime Infrastructure.
- Cisco CMX 10.x—Only CMX Presence is supported. CMX Connect, Location and Analytics are not supported.
- BYOD—Onboarding only.
- UX regulatory domain.
- Authentication, Authorization, Accounting (AAA) Override.
- IEEE 802.11k
- IEEE 802.11r
  - Supported—Over-the-Air Fast BSS transition method
  - Not Supported—Over-the-DS Fast BSS transition and Fast Transition PSK authentication
- Passive Client
- Voice with Call Admission Control (CAC), with Traffic Specification (TSpec)
- Fast SSID
- Terminal Access Controller Access Control System (TACACS)
- Management over wireless
- High Availability and Redundancy—Built-in redundancy mechanism to self-select a primary AP and to select a new AP as primary in case of a failure. Supported using VRRP.
- Software upgrade with preimage download
- Migration to controller-based deployment.

New Features and Functionalities

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

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

Compatibility with Other Cisco Wireless Solutions

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

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

Software Release Information

Cisco Mobility Express software for Cisco Wireless Release 8.2.110.0, is as follows:

Software Pype and purpose	For AP 1850	For AP 1830
Software to be used only for conversion from Unified Wireless Network Lightweight APs software to Cisco Mobility Express software.	AIR-AP1850-K9-8.2.110.0.tar	AIR-AP1830-K9-8.2.110.0.tar
AP software image bundle, to be used for software update, or supported access points images, or both.	AIR-AP1850-K9-ME-8-2-100-0.zip	AIR-AP1830-K9-ME-8-2-100-0.zip

Installing Mobility Express Software

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

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

Caveats

The open caveats applicable to the Cisco Mobility Express solution are listed under the "Caveats" section on page 34. All caveats associated with the Cisco Mobility Express solution have *Cisco Mobility Express* specified in the headline.

Related Documentation

- Cisco Mobility Express User Guide

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

- Cisco Aironet Universal AP Priming and Cisco AirProvision User Guide

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

Installation Notes

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

Warnings

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

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

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

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

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

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

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

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

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

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

Safety Information

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

FCC Safety Compliance Statement

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

Safety Precautions

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

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

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

Installation Instructions

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

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

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

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

Service and Support

Troubleshooting

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

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

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

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

Related Documentation

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

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

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

Obtaining Documentation and Submitting a Service Request

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

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