Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.5.120.0

First Published: 2018-01-31

Last Modified: 2021-02-12

About the Release Notes

This release notes document describes what is new or changed in this release, instructions to upgrade to this release, and provides information about the open and resolved caveats for this release. Unless otherwise noted, in this document, Cisco Wireless Controllers are referred to as *controllers*, and Cisco lightweight access points are referred to as *access points* or *APs*.

Revision History

Table 1: Revision History for 8.5.120.0

Modification Date	Modification Details
August 23, 2018	Open Caveat—Added CSCvk44249
March 13, 2018	Supported Cisco Access Point Platforms section—Added information about support for Integrated Access Point on Cisco 1100 Integrated Services Router.
March 09, 2018	Open Caveats section—Added CSCvi32951, CSCvi11287, CSCvi07609, CSCvi01675, and CSCvi09424.
Febuary 07, 2018	• Open Caveats section—Removed CSCvf16869, CSCvh70614, CSCvg60452, and CSCvh58599. • Resolved Caveats section—Added CSCvg60452 and CSCvg13374.

Supported Cisco Wireless Controller Platforms

The following Cisco Wireless Controller platforms are supported in this release:

- Cisco 2500 Series Wireless Controllers (Cisco 2504 Wireless Controller)
- Cisco 3500 Series Wireless Controllers (Cisco 3504 Wireless Controller)
- Cisco 5500 Series Wireless Controllers (Cisco 5508 and 5520 Wireless Controllers)

- Cisco Flex 7500 Series Wireless Controllers (Cisco Flex 7510 Wireless Controller)
- Cisco 8500 Series Wireless Controllers (Cisco 8510 and 8540 Wireless Controllers)
- Cisco Virtual Wireless Controller (vWLC) on the following platforms:
    - VMware vSphere Hypervisor (ESXi) Version 5.x and 6.x
    - Hyper-V on Microsoft Servers 2012 and later versions

      Note Support introduced in Release 8.4.

    - Kernel-based virtual machine (KVM)

      Note Support introduced in Release 8.1. 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 3504 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.
- Cisco WiSM2 for Cisco Catalyst 6500 Series Switches
- Cisco Mobility Express Solution

Supported Cisco Access Point Platforms

The following Cisco AP platforms are supported in this release:

- Cisco Aironet 1600 Series Access Points
- Cisco Aironet 1700 Series Access Points
- Cisco Aironet 1800 Series Access Points
- Cisco Aironet 1810 Series OfficeExtend Access Points
- Cisco Aironet 1810W Series Access Points
- Cisco Aironet 1815 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 700 Series Access Points
- Cisco Aironet 700W Series Access Points
- Cisco AP802 Integrated Access Point
- Cisco AP803 Integrated Access Point
- Integrated Access Point on Cisco 1100 Integrated Services Router
- Cisco ASA 5506W-AP702
- Cisco Aironet 1530 Series Access Points
- Cisco Aironet 1540 Series Access Points
- Cisco Aironet 1550 Series Access Points with 128-MB memory

  Note From Release 8.4, Cisco 1550 APs with 64-MB memory are not supported.

- Cisco Aironet 1560 Series Access Points
- Cisco Aironet 1570 Series Access Points
- Cisco Industrial Wireless 3700 Series Access Points

Note

- Cisco AP802 and AP803 are integrated access point modules on the Cisco 800 Series Integrated Services Routers (ISRs). For more information about the stock-keeping units (SKUs) for the AP802s and AP803s Cisco ISRs, see

  https://www.cisco.com/c/en/us/products/routers/800-series-routers/brochure-listing.html.

  Before you use a Cisco AP802 series lightweight access point module with Cisco Wireless Release 8.5, you must upgrade the software in the Cisco 800 Series ISRs to Cisco IOS 15.1(4)M or later releases.

- For more information about Integrated Access Point on Cisco 1100 ISR, see the product data sheet at https://www.cisco.com/c/en/us/products/collateral/routers/1000-series-integrated-services-routers-isr/datasheet-c78-739512.html.

For information about Cisco Wireless software releases that support specific Cisco access point modules, see the "Software Release Support for Specific Access Point Modules" section in the Cisco Wireless Solutions Software Compatibility Matrix document.

What's New in Release 8.5.120.0

There are no new features introduced in this release. For more information about updates in this release, see the Caveats section in this document.

Note For complete listing of all the documentation published for Cisco Wireless Release 8.5, see the Documentation Roadmap:

https://www.cisco.com/c/en/us/td/docs/wireless/doc-roadmap/doc-roadmap-release-85.html

Software Release Types and Recommendations

Table 2: Release Types

Release Type	Description	Benefit
Maintenance Deployment (MD)	Software releases that provide bug-fix support and ongoing software maintenance. These releases are categorized as Maintenance Deployment (MD) These are long-living releases with ongoing software maintenance.	Provides you with a software release that offers stability and long support duration with periodic maintenance releases (MRs).
Early Deployment (ED)	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.

For detailed release recommendations, see the *Guidelines for Cisco Wireless Software Release Migration Bulletin* at:

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

Table 3: Upgrade Path to Cisco WLC Software Release 8.5.120.0

Current Software Release	Upgrade Path to 8.5.120.0 Software
8.3.x.0	You can upgrade directly to Release 8.5.120.0
8.4.100.0	You can upgrade directly to Release 8.5.120.0

Note If you are using Release 8.2.x, we recommend that you upgrade to Release 8.3.x and then upgrade to Release 8.5.x.

Upgrading Cisco WLC Software Release

Guidelines and Limitations

- If you are using Release 8.4 and want to upgrade to a later release, it is necessary that you upgrade to Release 8.5.105.0 and then move to a later release.

  Note This restriction is applicable only to Release 8.4 and not any other release.

- The image format of Cisco Aironet 1700, 2700, 3700, and IW3702 APs has been changed from ap3g2 to c3700. Therefore, if you are upgrading to Release 8.5 or a later release from Release 8.3 or an earlier release, these APs will download the image twice and reboot twice.
- Support for Dynamic WEP is reintroduced in Cisco Wave1 APs in this release.
- The AAA database size is increased from 2048 entries to 12000 entries for these Cisco WLCs: Cisco Flex 7510, 8510, 5520, and 8540. Therefore, if you downgrade from Release 8.5 to an earlier release that does not include this enhancement, you might lose most of the AAA database configuration, including management user information. To retain at least 2048 entries, including management user information, we recommend that you follow these downgrade instructions and back up the configuration file before proceeding with the downgrade:

  1. From Release 8.5, downgrade to one of the following releases, which support 2048 database size and include the enhancement.
     - Release 8.4.100.0 or a later 8.4 release
     - Release 8.3.102.0 or a later 8.3 release
     - Release 8.2.130.0 or a later 8.2 release
     - Release 8.0.140.0 or a later 8.0 release
  2. Downgrade to a release of your choice.

- In Release 8.5, the search functionality in the Cisco WLC Online Help for all WLCs is disabled due to memory issues encountered in these WLCs: Cisco 2504, 5508, and WiSM2.
- Release 8.4 and later releases support additional configuration options for 802.11r FT enable and disable. The additional configuration option is not valid for releases earlier than Release 8.4. If you downgrade from Release 8.5 to Release 8.2 or an earlier release, the additional configuration option is invalidated and defaulted to FT disable. When you reboot Cisco WLC with the downgraded image, invalid configurations are printed on the console. We recommend that you ignore this because there is no functional impact, and the configuration defaults to FT disable.

- If you downgrade from Release 8.5 to a 7.x release, the trap configuration is lost and must be reconfigured.
- If you downgrade from Release 8.5 to Release 8.1, the Cisco Aironet 1850 Series AP whose mode was Sensor prior to the downgrade is shown to be in unknown mode after the downgrade. This is because the Sensor mode is not supported in Release 8.1.
- If you have an IPv6-only network and are upgrading to Release 8.4 or a later release, ensure that you perform the following activities:
    - Enable IPv4 and DHCPv4 on the network—Load a new Cisco WLC software image on all the Cisco WLCs along with the supplementary AP bundle images on Cisco 2504 WLC, Cisco 5508 WLC, and Cisco WiSM2, or perform a predownload of AP images on the corresponding Cisco WLCs.
    - Reboot Cisco WLC immediately or at a preset time.
    - Ensure that all Cisco APs are associated with Cisco WLC.
    - Disable IPv4 and DHCPv4 on the network.
- After downloading the new software to the Cisco APs, it is possible that a Cisco AP may get stuck in an upgrading image state. In such a scenario, it might be necessary to forcefully reboot Cisco WLC to download a new image or to reboot Cisco WLC after the download of the new image. You can forcefully reboot Cisco WLC by entering the **reset system forced** command.
- It is not possible to download some of the older configurations from Cisco WLC because of the Multicast and IP address validations. See the "Restrictions on Configuring Multicast Mode" section in the *Cisco Wireless Controller Configuration Guide* for detailed information about platform support for global multicast and multicast mode.
- 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 downgrade to Release 8.0.140.0 or 8.0.15x.0, and later upgrade to a later release and and also have the multiple country code feature configured, then the configuration file could get corrupted. When you try to upgrade to a later release, special characters are added in the country list causing issues when loading the configuation. For more information, see CSCve41740.

  Note Upgrade and downgrade between other releases does not result in this issue.

- If you are upgrading from a 7.4.x or an 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 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 Cisco Wireless 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 or 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 about FUS and the applicable Cisco WLC platforms, see the Field Upgrade Software release notes listing.

Note For Cisco 2504 WLC, we recommend that you upgrade to FUS 1.9.0 release or a later release.

- If FIPS is enabled in Cisco Flex 7510 WLC, the reduced boot options are displayed only after a bootloader upgrade.

  Note Bootloader upgrade is not required if FIPS is disabled.

- When downgrading 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 that are saved in the backup server, or to reconfigure Cisco WLC.
- It is not possible to directly upgrade to this release from a release that is earlier than Release 7.0.98.0.
- When you upgrade Cisco WLC to an intermediate release, wait until all the APs that are associated with 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 AP.
- You can upgrade to a new release of the Cisco WLC software or downgrade to an earlier release even if FIPS is enabled.
- When you upgrade to the latest software release, the software on the APs associated with the Cisco WLC is also automatically upgraded. When an AP is loading software, each of its LEDs blinks in succession.
- We recommend that you access the Cisco WLC GUI using Microsoft Internet Explorer 11 or a later version, or Mozilla Firefox 32 or a later version.
- Cisco WLCs support standard SNMP MIB files. MIBs can be downloaded from the software download page on Cisco.com.
- The Cisco WLC software is factory installed on your Cisco WLC and is automatically downloaded to the APs after a release upgrade and whenever an AP joins a Cisco WLC. We recommend that you install the latest software version available for maximum operational benefit.
- Ensure that you have a TFTP, HTTP, 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 image. Some TFTP servers that support files of this size are tftpd32 and the TFTP server within Cisco Prime Infrastructure. If you attempt to download the Cisco WLC software image 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 5508 WLC differ from the menu options for the other Cisco WLC platforms.

  The following is the Bootloader menu for Cisco 5508 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:
  ```

  The following is the 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 5508 WLC),
  or enter 5 (on Cisco WLC platforms other than 5508 WLC) 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 of the respective Cisco WLC platform for more details on running the bootup script and the 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 Options** menu to boot from the backup image. Then, upgrade with a known working image and reboot 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**}

  The following are the details of the command:

  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 in the **config network ap-discovery nat-ip-only** command. To disable AP link latency, use the **config ap link-latency disable all** command.

- Do not power down Cisco WLC or any AP during the upgrade process. If you do this, the software image might get corrupted. Upgrading Cisco WLC with a large number of APs can take as long as 30 minutes, depending on the size of your network. However, with the increased number of concurrent AP upgrades supported, the upgrade time should be significantly reduced. The APs must remain powered, and Cisco WLC must not be reset during this time.
- To downgrade from this release 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 Cisco WLC, reboot it for the changes to take effect:
  - Enable or disable LAG
  - Enable a feature that is dependent on certificates (such as HTTPS and web authentication)
  - Add a new license or modify an existing license

    Note Reboot is not required if you are using Right-to-Use licenses.

  - 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

Changes in Images and Installation Procedure for Cisco 2504 WLC, Cisco 5508 WLC, and Cisco WiSM2

Due to an increase in the size of the Cisco WLC software image, the Cisco 2504 WLC, Cisco 5508 WLC, and Cisco WiSM2 software images are split into the following two images:

- Base Install image, which includes the Cisco WLC image and a subset of AP images (excluding some mesh AP images and AP80x images) that are packaged in the Supplementary AP Bundle image
- Supplementary AP Bundle image, which includes AP images that are excluded from the Base Install image. The APs that feature in the Supplementary AP Bundle image are:
    - Cisco AP802
    - Cisco AP803
    - Cisco Aironet 1530 Series AP
    - Cisco Aironet 1550 Series AP (with 128-MB memory)
    - Cisco Aironet 1570 Series APs
    - Cisco Aironet 1600 Series APs

Note There is no change with respect to the rest of the Cisco WLC platforms.

Image Details

The following table lists the Cisco WLC images that you have to download to upgrade to this release for the applicable Cisco WLC platforms:

Table 4: Image Details of Cisco 2504 WLC, 5508 WLC, and WiSM2

Cisco WLC	Base Install Image	Supplementary AP Bundle Image [1]
Cisco 2504 WLC	AIR-CT2500-K9-8-5-120-0.aes	AIR-CT2500-AP_BUNDLE-K9-8-5-120-0.aes
Cisco 5508 WLC	AIR-CT5500-K9-8-5-120-0.aes AIR-CT5500-LDPE-K9-8-5-120-0.aes	AIR-CT5500-AP_BUNDLE-K9-8-5-120-0.aes AIR-CT5500-LDPE-AP_BUNDLE-K9-8-5-120-0.aes
Cisco WiSM2	AIR-WISM2-K9-8-5-120-0.aes	AIR-WISM2-AP_BUNDLE-K9-8-5-120-0.aes

[1] AP_BUNDLE or FUS installation files from Release 8.5 for the incumbent platforms should not be renamed because the filenames are used as indicators to not delete the backup image before starting the download.

If renamed and if they do not contain “AP_BUNDLE” or “FUS” strings in their filenames, the backup image will be cleaned up before starting the file download, anticipating a bigger sized regular base image.

Upgrading Cisco WLC Software (GUI)

Procedure

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 software:

a) Browse to Cisco Software Central at: https://software.cisco.com/download/navigator.html.

b) Click **Software Download**.

c) On the **Download Software** page, choose **Wireless** > **Wireless LAN Controller**.

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

- **Integrated Controllers and Controller Modules**
- **Mobility Express**
- **Standalone Controllers**

d) Select the Cisco WLC model number or name.

e) Click **Wireless LAN Controller Software**.

f) The software releases are labeled as described here 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.

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

Note For Cisco 2504 WLC, Cisco 5508 WLC, and Cisco WiSM2, the Cisco WLC software image is split into two images, the Base Install image and the Supplementary AP Bundle image. Therefore, in order to upgrade, repeat Step 2 through Step 14 to complete the installation of both the Base Install image and the Supplementary AP Bundle image.

Download the Supplementary AP Bundle image only if you are using any of these APs: AP802, AP803, Cisco Aironet 1530 Series AP, Cisco Aironet 1550 Series AP (with 128-MB memory), Cisco Aironet 1570 Series APs, Cisco Aironet 1600 Series APs, or all of these APs.

h) Click **Download**.

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

j) Save the file to your hard drive.

k) Repeat steps *a* through *j* 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 802.11 networks.

Note For busy networks, Cisco WLCs on high utilization, and small Cisco WLC platforms, we recommend that you disable the 802.11 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** field, 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** field, and 6 seconds for the **Timeout** field should work correctly without any adjustment. However, you can change these values, if required. To do so, enter the maximum number of times the TFTP server attempts to download the software in the **Maximum Retries** field and the amount of time (in seconds) for which the TFTP server attempts to download the software, in the **Timeout** field.

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

Step 11 In the **File Name** field, 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** field, enter the username with which to log on to the FTP server.
b) In the **Server Login Password** field, enter the password with which to log on to the FTP server.
c) In the **Server Port Number** field, 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 indicating the status of the download is displayed.

Note For Cisco 2504 WLC, Cisco 5508 WLC, and Cisco WiSM2, the Cisco WLC software image is split into two images: the Base Install image and the Supplementary AP Bundle image. Therefore, in order to upgrade, repeat Step 2 through Step 14 to complete the installation of both the Base Install image and the Supplementary AP Bundle image.

Download the Supplementary AP Bundle image only if you are using any of these APs: AP802, AP803, Cisco Aironet 1530 Series AP, Cisco Aironet 1550 Series AP (with 128-MB memory), Cisco Aironet 1570 Series APs, Cisco Aironet 1600 Series APs, or all of these APs.

Note Ensure that you choose the **File Type** as **Code** for both the images.

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, check the port channel and re-enable the port channel, if necessary.

Step 18 If you have disabled the 802.11 networks, re-enable them.

Step 19 To verify that the Cisco WLC software is installed on your Cisco WLC, on the Cisco WLC GUI, click **Monitor** and view the **Software Version** field under **Controller Summary**.

Interoperability with Other Clients

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

The following table describes the configuration used for testing the client devices.

Table 5: Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	8.5.120.0
Cisco WLC	Cisco 5508 and 5520 Wireless Controllers
Access Points	AIR-CAP3802E-B-K9, AIR-AP1852E-B-K9, AIR-CAP3602E-A-K9
Radio	802.11ac, 802.11a, 802.11g, 802.11n (2.4 GHz / 5.0 GHz)
Security	Open, PSK (WPA-TKIP-WPA2-AES), 802.1X (WPA-TKIP-WPA2-AES) (EAP-FAST, EAP-TLS)
RADIUS	ISE 2.2, ISE 2.3
Types of tests	Connectivity, traffic (ICMP), and roaming between two APs

The following table lists the client types on which the tests were conducted. Client types included laptops, handheld devices, phones, and printers.

Table 6: Client Types

Client Type and Name	Version
Laptop	
Intel 6300	15.16.0.2
Intel 6205	15.16.0.2
Intel 7260	18.33.3.2
Intel 7265	19.10.1.2
Intel 3160	18.40.0.9
Intel 8260	19.10.1.2
Broadcom 4360	6.30.163.2005
Dell 1520/Broadcom 43224HMS	5.60.48.18
Dell 1530 (Broadcom BCM4359)	5.100.235.12
Dell 1560	6.30.223.262

Client Type and Name	Version
Dell 1540	6.30.223.215
Samsung Chromebook	55.0.2883.103
HP Chromebook	55.0.2883.103
MacBook Pro	OSX 10.11.6
MacBook Air old	OSX 10.11.5
MacBook Air new	OSX 10.12.2
Macbook Pro with Retina Display	OSX 10.12
Macbook New 2015	OSX 10.12.4
Printers	
HP Color LaserJet Pro M452nw	2.4.0.125
Tablets	
Apple iPad2	iOS 10
Apple iPad3	iOS 10
Apple iPad mini with Retina display	iOS 10
Apple iPad Air	iOS 10
Apple iPad Air 2	iOS 11
Apple iPad Pro	iOS 11.0.3
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
Microsoft Surface Pro 4	Windows 10
	Driver: 15.68.9040.67
Google Nexus 9	Android 6.0.1
Google 10.2" Pixel C	Andriod 7.1.1
Toshiba Thrive AT105	Android 4.0.4
Mobile Phones	
Cisco 7926G	CP7925G-1.4.5.3.LOADS
Cisco 7925G-EX	CP7925G-1.4.8.4.LOADS

Client Type and Name	Version
Cisco 8861	Sip88xx.10-2-1-16
Cisco-9971	Sip9971.9-4-1-9
Cisco-8821	Sip8821.11-0-3ES2-1
Apple iPhone 4S	iOS 10.2.1
Apple iPhone 5	iOS 10.2.1
Apple iPhone 5s	iOS 10.2.1
Apple iPhone 5c	iOS 10.3.1
Apple iPhone 6	iOS 10.3.1
Apple iPhone 6 Plus	iOS 10.3.1
Apple iPhone 6s	iOS 10.2.1
Apple iPhone 7	iOS 11.2.5
Apple iPhone X	iOS 11.1.2
HTC One	Android 5.0
OnePlusOne	Android 4.3
OnePlus3	Android 6.0.1
Samsung Galaxy S4 T-I9500	Android 5.0.1
Sony Xperia Z Ultra	Android 4.4.2
Nokia Lumia 1520	Windows Phone 8.10.14219.341
Google Nexus 5	Android 6.0.1
Google Nexus 5X	Android 8.0.0
Google Pixcel	Android 7.1.1
Samsung Galaxy S5-SM-G900A	Android 4.4.2
Samsung Galaxy S III	Android 4.3
Samsung Galaxy S4	Android 5.0.1
Samsung Galaxy S5	Android 4.4.2
Samsung Galaxy S6	Android 7.0
Samsung Galaxy S7	Android 7.0
Samsung Galaxy Nexus GTI9200	Android 4.4.2
Samsung Galaxy Mega SM900	Android 4.4.2
LG G4	Android 5.1
Xiaomi Mi 4c	Android 5.1
Xiaomi Mi 4i	Android 6.0.1

Key Features Not Supported in Controller Platforms

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

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

Key Features Not Supported in Cisco 2504 WLC

- Domain-based ACLs
- Autoinstall
- Controller integration with Lync SDN API
- Application Visibility and Control (AVC) for FlexConnect locally switched APs
- Application Visibility and Control (AVC) for FlexConnect centrally switched APs

  Note AVC for local mode APs is supported.

- URL ACL
- Bandwidth Contract
- Service Port
- AppleTalk Bridging
- Right-to-Use 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.
- Directly connected APs are supported only in local mode.

Key Features Not Supported in Cisco 3504 WLC

- Cisco WLAN Express Setup Over-the-Air Provisioning
- Mobility controller functionality in converged access mode
- VPN Termination (such as IPsec and L2TP)

Key Features Not Supported in Cisco WiSM2 and Cisco 5508 WLC

- Domain-based ACLs
- VPN Termination (such as IPSec and L2TP) —IPSec for RADIUS/SNMP is supported; general termination is not supported.
- Fragmented pings on any interface
- Right-to-Use Licensing
- Cisco 5508 WLC and Cisco WiSM2 cannot function as mobility controller (MC). However, it can function as guest anchor in a New Mobility environment.
- Cisco Smart Software Licensing

Key Features Not Supported on Cisco Flex 7510 WLC

- Domain-based ACL
- Cisco Umbrella—Not supported in FlexConnect locally switched WLANs; however, it is supported in centrally switched WLANs.
- Static AP-manager interface

Note For Cisco Flex 7510 WLCs, it is not necessary to configure an AP-manager interface. The management interface acts as an AP-manager interface by default, and the APs can associate with the controller on this interface.

- IPv6 and dual-stack client visibility

Note IPv6 client bridging and Router Advertisement Guard are supported.

- Internal DHCP server
- APs in local mode

Note A Cisco AP associated with a controller in local mode should be converted to FlexConnect mode or monitor mode, either manually or by enabling the autoconvert feature. From the Cisco Flex 7510 WLC CLI, enable the autoconvert feature by entering the **config ap autoconvert enable** command.

- Mesh (Use Flex + Bridge mode for mesh-enabled FlexConnect deployments)
- Cisco Flex 7510 WLC cannot be configured as a guest anchor controller. However, it can be configured as a foreign controller to tunnel the guest traffic to a guest anchor controller in a DMZ.
- Multicast

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

- PMIPv6
- Cisco Smart Software Licensing

Key Features Not Supported in Cisco 5520, 8510, and 8540 WLCs

- Internal DHCP Server
- Mobility controller functionality in converged access mode
- VPN termination (such as IPsec and L2TP)
- Fragmented pings on any interface

Note Cisco Smart Software Licensing is not supported on Cisco 8510 WLC.

Key Features Not Supported in Cisco Virtual WLC

- Cisco Umbrella
- Domain-based ACLs
- Internal DHCP server
- Cisco TrustSec
- Access points in local mode
- Mobility/Guest Anchor
- Wired Guest

- Multicast

Note FlexConnect locally switched multicast traffic is bridged transparently for both wired and wireless on the same VLAN. FlexConnect APs 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 controller ports is not more than 500 Mbps.
- FlexConnect local switching is supported.

- Central switching on Microsoft Hyper-V deployments
- AP and Client SSO in High Availability
- PMIPv6
- Datagram Transport Layer Security (DTLS)
- EoGRE (Supported in only local switching mode)
- Workgroup bridges
- Client downstream rate limiting for central switching
- SHA2 certificates
- Controller integration with Lync SDN API
- Cisco OfficeExtend Access Points

Key Features Not Supported in Access Point Platforms

Key Features Not Supported in Cisco Aironet 1540, 1560, 1800i, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800, and 3800 Series APs

Table 7: Key Features Not Supported in Cisco Aironet 1540, 1560, 1800i, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800 and 3800 Series APs

Operational Modes	• Autonomous Bridge and Workgroup Bridge (WGB) mode • Mesh mode **Note** Supported on 1540 and 1560 APs. • Flex + Mesh • 802.1x supplicant for AP authentication on the wired port • LAG behind NAT or PAT environment
Protocols	• Full Cisco Compatible Extensions (CCX) support • Rogue Location Discovery Protocol (RLDP) • Telnet • Internet Group Management Protocol (IGMP)v3
Security	• CKIP, CMIC, and LEAP with Dynamic WEP • Static WEP for CKIP • WPA2 + TKIP **Note** WPA +TKIP and TKIP + AES protocols are supported.
Quality of Service	Cisco Air Time Fairness (ATF)
Location Services	Data RSSI (Fast Locate)

FlexConnect Features	• Bidirectional rate-limiting • Split Tunneling • PPPoE • Multicast to Unicast (MC2UC) • Traffic Specification (TSpec) • Cisco Compatible Extensions (CCX) • Call Admission Control (CAC) • VSA/Realm Match Authentication • Link aggregation (LAG) • SIP snooping with FlexConnect in local switching mode

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

Key Features Not Supported in Cisco Aironet 1800i, 1810 OEAP, and 1810W Series APs

Table 8: Key Features Not Supported in Cisco Aironet 1800i, 1810 OEAP and 1810W Series APs

Operational Modes	Mobility Express
FlexConnect Features	Local AP authentication

Key Features Not Supported in Cisco Aironet 1830, 1850, and 1815 Series APs

Table 9: Key Features Not Supported in Cisco Aironet 1830, 1850, and 1815 Series APs

Operational Modes	Mobility Express is not supported in Cisco 1815t APs.
FlexConnect Features	Local AP Authentication

Key Features Not Supported in 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.
- AP join priority (Mesh APs have a fixed priority)

- Location-based services

Key Features Not Supported in Cisco Aironet 1540 Mesh APs

- Dynamic Mesh backhaul data rate.

Note We recommend that you keep the Bridge data rate of the AP as auto.

- Background scanning
- Noise Tolerant Fast Convergence
- Flex+Mesh

Key Features Not Supported on Cisco Aironet 1560 Mesh APs

- Noise Tolerant Fast Convergence
- Flex+Mesh

Caveats

Open Caveats

Table 10: Open Caveats for 8.5.120.0

Caveat ID Number	Description
CSCvb26809	WLC should use port MAC for non LAG and box mac for LAG
CSCvc62540	Smart Licensing "Next Communication Attempt" pre-dates the Controller time after Reboot
CSCvc78347	Cisco 1832 AP stops working in WLAN when voice traffic transmitted through
CSCvd91152	Cisco 3700 APs in FlexConnect reloads unexpectedly on 8.3.111.0 release
CSCve14291	AP1830: "show version" shows old software version as "AP running image" and longer uptime
CSCve18359	Observed traceback on Cisco 1570 AP when changing AP mode to FlexConnect from Flex+Bridge
CSCve79470	Cisco Wave 2 APs sends RADIUS message directly even if Local Authentication is disabled
CSCvf10786	CAP 2800, 3800 sniffer mode logs wrong PHY and data rates for 802.11ac

Caveat ID Number	Description
CSCvf11072	ME: SUBNET_MISMATCH_IP_ADD_ON_MSCB mismatches while registering IP address x.x.x.x
CSCvf31881	Cisco 2800 AP detects Intel Dual Band Wireless-AC 8260 as rogue client/AP
CSCvf65133	Dynamic interface template fails to apply on Cisco WLC with DHCP Option 82 setting
CSCvf83391	Cisco 8.3 Release: AP reloads unexpectedly at TAMD ap-tam process
CSCvf84806	FIQ/NMI Reset AP2800 PC __pci_bus_size_bridges+0x274/0x768 LR warn_slowpath_common+0x58/0x94
CSCvf91228	WLC unable to timeout clients; stale client entries
CSCvf96532	WLC anchor commands are missing from the backup
CSCvg00507	Cisco 3700 AP reloads unexpectedly- PID 104: Process "LWAPP Rogue Monitoring process"
CSCvg06111	WLC " in sync" with NTP while authentication is ignored with invalid keys
CSCvg18543	8.5MR: AP 3700 Tx jammed and radio reloads unexpectedly
CSCvg19242	Cisco 1700/2700/3700 log wrong PHY in sniffer mode for 802.11ac
CSCvg21910	Deleting one SSID will affect another SSID created on the same radio interface
CSCvg24833	Cisco 1530 AP in WGB mode reloads unexpectedly on associating with root
CSCvg27613	DHCP Proxy enabled and removing DHCP Server Info from Dynamic interface disables WLAN
CSCvg28378	AP: cmd timeout AP radio reloads unexpectedly in 8.6 due to Rx hang
CSCvg32087	Cisco 5520 WLC reloads unexpectedly on Task Name: nmspTxServerTask
CSCvg35115	Cisco 3802 running 8.3.130 shows radio core without the crash file
CSCvg40792	Client global IPv6 not correctly mapped to mac address under certain conditions
CSCvg43654	Cisco Wave 2 APs in FlexConect mode do not forward DHCP NAK to wireless client
CSCvg44078	WLC unable to timeout clients; stale client entries
CSCvg46125	Cisco WLC reloads unexpectedly multiple times
CSCvg46708	Cisco 5508 WLC reloading due to memory leak in Anon Pages emweb
CSCvg48395	8.6: TrustSec not working - Environment Data download failing on Cisco 3504 WLC platform
CSCvg56184	IOS APs in sniffer mode shows incorrect TID in captured traffic
CSCvg59338	NMSP drops observed in high density deployments

Caveat ID Number	Description
CSCvg60758	Cisco Wave 2 APs drops TCP retransmit from server
CSCvg62359	Cisco 2800, 3800 APs: Click scheduler 0 stuck at Sched/FSys:1/0 Epoch
CSCvg64750	8.5MR1:HA osapi_file.c:1030 Failed to open the file, %OSAPI-3-SOCK_SEND_FAILED: [SA]osapi_support
CSCvg64993	WLC mDns secure printer service response missing TXT record with mDNS snooping enabled
CSCvg67509	Cisco 1810W AP reloads unexpectedly over a kernel panic
CSCvg70903	WLAN session timeout does not default to dot1x reauth timeout when Webauth is enabled via the GUI
CSCvg74107	WiSM2 reloads unexpectedly on Dot1x_NW_MsgTask due to Dynamic VLAN feature handling for CAP 702
CSCvg76168	5GHz radio interface on 1532 APs remains down due to DFS even when not all channels are on the blocked list.
CSCvg77711	System reloads at random on running mesh commands
CSCvg78101	Local EAP profiles changed not retained after it is applied
CSCvg80249	AP 3700: cannot get complete core file in flash due to memory too low
CSCvg86324	WLC reloads unexpectedly with SNMP operation with Flex ACL
CSCvg94522	TxFSM stuck on Radio 0 with new signature
CSCvg94718	Standby WLC reloads unexpectedly on spamApTask
CSCvg96183	Proxy ARP always enabled in Beacon IE for Flex mode AP irrespective of ARP cache config
CSCvg96852	Cisco 1815W SnifferMode AP beacons allows clients to join and blackhole traffic
CSCvg97013	Cisco 8540 WLC reloads unexpectedly on Task Name: emWeb on 8.5.110.0
CSCvg98078	AP does not forward packets from wire to the air when Flex AVC profile is applied
CSCvg98098	AP1852 5G radio FW crash @0x00981CED and @0x0099010D
CSCvg99652	Cisco WLC reloads unexpectedly with task name RRM-MGR-5_0 and spamApTask7
CSCvh07545	AP2800/3800 Kernel Panic due to processing of RX frames before driver is initialized
CSCvh10530	Flexconnect AP dropped SYN+ACK packet when redirected the web authentication page
CSCvh14989	Client in RUN state on anchor with 0.0.0.0 IP address
CSCvh16970	WLC does not apply correctly ACL Template from PI

Caveat ID Number	Description
CSCvh19127	AP1815I no response from wired side -
CSCvh20238	Cisco 2800, 3800 APs joining the WLC in flex-mode fail to update FlexACL in group policies
CSCvh21486	WLC reloads unexpectedly due to Task "apfMsConnectionTask" when MBUF debug is enabled
CSCvh23473	AP1572 shows incorrect regulatory power level for Qatar domain
CSCvh23785	AireOS WLC: Multiple wireless clients failing the broadcast Key refresh (M5).
CSCvh25039	SNMP causes unexpected reloads
CSCvh25368	WLC memory leak on CDP
CSCvh27557	Cisco 1562 AP limited to 54 Mbps in 2.4-GHz backhaul
CSCvh27570	cLSiIdrClusterAffectedChannels OID returning unexpected values
CSCvh28229	Incorrect count for cLApWlanStatsOnlineUserNum when SSID is changed
CSCvh30872	Decrypt errors on Cisco 1532 AP
CSCvh33064	Config logging traceinfo setting not restored correctly
CSCvh47521	AP decrypt failed
CSCvh49820	WLAN disabled after any change due to PSK lost
CSCvh51489	AIR-AP1572EC running 8.2mr5 and 8.2mr6 becomes non responsive with no console access
CSCvh54235	Cisco 3800 AP FW crash on Radio 0
CSCvh55157	WLC reuses Acct-Session-Id when Client changes WLANs
CSCvh58148	AP COS uses invalid CAPWAP-Data keep-alive source port
CSCvh59002	AP702w Continuous Pak ownership errors /w Freeing pak:xx in the radio TX or RX ring, owner:FACD1010
CSCvh59834	ME : Cannot change the role of XOR radio from Auto to Manual on AP2802E
CSCvh61939	1562 MAP is not forwarding BPDUs sent by the RAP when using Ethernet bridging
CSCvh63417	d0: *** sensord died (src/dspm_main.c:1662/0) - slot 0 ***
CSCvh67549	Cisco 8540 Data Plane reloads unexpectedly on __udp_input
CSCvh72867	Radio reset with transmitter seems to have stopped, FST06
CSCvh73674	Cisco 1562 MAP not sending Air Quality reports to WLC

Caveat ID Number	Description
CSCvh75213	Cisco AP reloads unexpectedly on config file copy
CSCvi01675	New Mobility with 3650MA and 5520 Achor - Guest users cannot reach DG on 8.3.x
CSCvi07609	Cisco 5520 WLC experiences fatal dataplane crash at broffu_fp_dapi_cmd.c:4588
CSCvi09424	Layer 3 Roam fails back to L2 Anchor with MAC Filtering MAB
CSCvi11287	Cisco 2800 AP consistently reboots around 1 second after joining to the WLC
CSCvi32951	Cisco Wave 2 APs ignore scanning defer and goes offchannel
CSCvk44249	WLC 5508 - foreign mapping is missing on a WLAN when restoring a backup

Resolved Caveats

Table 11: Resolved Caveats for 8.5.120.0

Caveat ID Number	Description
CSCve09179	CAP 3800 sending deauth to connected clients when CAPWAP flaps
CSCve70752	SNMP issue: Tx power level returns null causing Cisco PI, WLC sync to not update AP information
CSCvf08272	Blocked list timer is showing as "blacklist due to be cleared" but still blocked list timer remaining
CSCvf23079	CAPWAP_HA-3-AP_TEMP_DB_ADD_ERR in standby WLC when changing CAPWAP mode continuously
CSCvf51131	DHCPv6 stateless not working
CSCvf88312	User is not able to add any source to any destination acl from ME GUI (0.0.0.0 to 0.0.0.0)
CSCvg07617	AP1810W:Kernel Panic reloads unexpectedly PC is at _ZN17ContentHashFilter11clear_staleEv+0x1ac/0x1d0
CSCvg08001	Cisco WiSM2 reloads unexpectedly on task name spamApTask3 8.2.151.0
CSCvg13374	CCO download DNS breaks after poll and and manually configuring to invalid DNS server
CSCvg24476	AP2802/3802 E-SKU: XOR Operational State UP on 5GHz when DART connector not plugged in
CSCvg25773	Cisco 7510 WLC on 8.2.151.0 reloads unexpectedly with TaskName:spamApTask7
CSCvg25902	AIR-CT3504 WLC: AP Cannot Join Controller When Direct Connected to GigE Port 1

Caveat ID Number	Description
CSCvg27361	Adding "switchport voice vlan x" causes wired phone not to pull an IP address.
CSCvg27599	Cisco WLC reloads unexpectedly sometime when client switches between FT enabled SSID and CCKM SSIDs
CSCvg34444	IW3702 WGB one way broadcast traffic on 5 GHz (but good in 2.4 GHz) in a MESH network 1572 AP
CSCvg38669	ERROR-MeshSecurity: Processing EAPOL from CAWAWP, Mesh mode is not started
CSCvg38681	FlexConnect AP's WLAN-VLAN mappings inheritance is lost when a WLAN is deleted from AP group
CSCvg39960	Cisco WLC reloads unexpectedly on task - sntpReceiveTask
CSCvg42928	CDP-4-DUPLEX_MISMATCH is observed when Cisco 1852 and 3802 APs are connected to CAT 3650 switch
CSCvg45301	8.6: Cisco 1800 AP watchdog reloads unexpectedly due to OOM
CSCvg49532	HA : "config service statistics" not synced
CSCvg50635	[8.6] Cisco 3504 WLC UI filter on SSID does not work
CSCvg57548	Beacon stuck observed on radio 0
CSCvg60452	aIOS and flex standalone failure on FT-dot1x authentication or M3 RSN IE
CSCvg62039	False radar detection on AP 1832 with 40MHz CW
CSCvg63216	WLC RFID queue Breached with more than 4000 tags.
CSCvg67318	TPC version is not included in the run-config commands
CSCvg67755	Traceback during WLC upgrade
CSCvg70352	AP 1832/1852 Kernel Panic crash at __kmalloc_poolid+0xb8/0x16c
CSCvg70384	AP 1832/1852 radio crash at 0x009A497D
CSCvg73522	Cisco 5508 WLC reloads unexpectedly due to memory leak in snmpApPowerTrap()
CSCvg82215	Cisco 3504 WLC undergoes unexpected silent reloads when using mGig port
CSCvg82784	Cisco Wave 2 APs start the Channel Availability Check (CAC) timer after rolling to a lower bandwidth
CSCvg85175	Cisco WLC reloads unexpectedly with task name spamApTask0
CSCvg89807	Silver QoS profile is assigned to RLAN when configuration is imported
CSCvg91108	WQE size constantly increasing, error messages
CSCvg91708	WLC emweb reloads unexpectedly at commandConfigSpamApAntennaMonitor

Caveat ID Number	Description
CSCvg93191	8.3.134.40: AP3800 beacon stuck when radio reloads unexpectedly with signature "B0B0"
CSCvg97208	AP1852: Apple clients connection fails in 802.11r adaptive mode in WLAN
CSCvg97712	sm4: 1850 console flooded with "Total NR report Length exceeds Max Buffer Size -1067447752"
CSCvh00398	WSA: Flex RADIUS Stats data parsing fails
CSCvh01089	Cisco Wave 2 APs: false beacon stuck issue due to no beacon updates in WCP message Host Triggered a radio crash
CSCvh04894	Cisco 3800, 2800 APs: not writing core files when the storage space is not enough but is less than 95%
CSCvh08020	AP stuck in ap: after upgrade - flashfs[0]: writing to flash handle Illegal Operation
CSCvh28506	Cisco 3504 WLC cannot use USB for transfer file
CSCvh32031	ME: Update Root CA Cert for Mobility Express Cisco.com Software Download Method
CSCvh58917	Cisco WLC MAC authentication web redirected URL is broken

Related Documentation

Wireless Products Comparison

- Use this tool to compare the specifications of Cisco wireless access points and controllers:

  https://www.cisco.com/c/en/us/products/wireless/wireless-lan-controller/product-comparison.html

- Product Approval Status:

  https://prdapp.cloudapps.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL_SEARCH

- Wireless LAN Compliance Lookup:

  https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html

Cisco Wireless Controller

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

- The quick start guide or installation guide for your particular Cisco WLC or access point
- Cisco Wireless Solutions Software Compatibility Matrix
- *Cisco Wireless Controller Configuration Guide*
- *Cisco Wireless Controller Command Reference*

- *Cisco Wireless Controller System Message Guide*

For all Cisco WLC software related documentation, see:

http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/tsd-products-support-series-home.html

Cisco Mobility Express

- *Cisco Mobility Express Release Notes*
- *Cisco Mobility Express User Guide*
- *Cisco Aironet Universal AP Priming and Cisco AirProvision User Guide*

Cisco Aironet Access Points for Cisco IOS Releases

- *Release Notes for Cisco Aironet Access Points for Cisco IOS Releases*
- *Cisco IOS Configuration Guides for Autonomous Aironet Access Points*
- *Cisco IOS Command References for Autonomous Aironet Access Points*

Open Source Used in Controller and Access Point Software

Click this link to access the documents that describe the open source used in controller and access point software:

https://www.cisco.com/c/en/us/about/legal/open-source-documentation-responsive.html

Cisco Prime Infrastructure

Cisco Prime Infrastructure Documentation

Cisco Mobility Services Engine

Cisco Mobility Services Engine Documentation

Cisco Connected Mobile Experiences

Cisco Connected Mobile Experiences Documentation

Cisco Digital Network Architecture

https://www.cisco.com/c/en/us/support/wireless/dna-spaces/series.html

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.

- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.