Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.3.111.0, 8.3.112.0

First Published: 2017-02-27

Last Modified: 2018-08-30

About the Release Notes

This release notes document describes what is new or changed in this release, instructions to upgrade to this release, and 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*.

Content Hub

Explore the Content Hub, the all-new product documentation portal in which you can use faceted search to locate content that is most relevant to you, create customized PDFs for ready reference, benefit from context-based recommendations, and much more.

Get started with the Content Hub at https://content.cisco.com/ to craft a personalized documentation experience.

Do provide feedback about your experience with the Content Hub.

Revision History

Table 1: Revision History

Modification Date	Modification Details
August 23, 2018	Open Caveat—Added CSCvk44249
January 29, 2018	Key Features Not Supported on Cisco Virtual WLCs section—Modified information about FlexConnect central switching.
October 16, 2017	Key Features Not Supported on Cisco Aironet 1810 OEAP, 1810W, 1815, 1830, 1850, 2800, and 3800 Series APs section—Added SIP snooping with FlexConnect in local switching mode.
October 10, 2017	Key Features Not Supported on Cisco Virtual WLCs section—Added Wired Guest and FlexConnect central switching.
May 16, 2017	Key Features Not Supported on Cisco Aironet 1810 OEAP, 1810W, 1815, 1830, 1850, 2800, and 3800 Series APs section—Removed Proxy ARP from the list of unsupported FlexConnect features.

Modification Date	Modification Details
March 21, 2017	Resolved Caveats section—Added CSCvd23510 and CSCvd48226.

Cisco Wireless Controller and Access Point Platforms

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 5500 Series Wireless Controllers (Cisco 5508 and 5520 Wireless Controllers)
- Cisco Flex 7500 Series Wireless Controllers (Cisco Flex 7510 Wireless Controller)
- Cisco 8500 Series Wireless Controllers (Cisco 8510 and 8540 Wireless Controllers)
- Cisco Virtual Wireless Controllers on VMware ESXi and Kernel-based virtual machine (KVM) systems.

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

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 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 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 1560 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.

Note Before you associate Cisco Aironet 1830 Series and 1850 Series APs with Cisco vWLC running Cisco 8.3.112.0 release software, you must upgrade the APs to Cisco 8.3.112.0 release.

Note Cisco AP802 and AP803 are integrated access points 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 http://www.cisco.com/c/en/us/products/routers/800-series-routers/brochure-listing.html. Before you use a Cisco AP802 series lightweight access point with Cisco Wireless Release 8.4, you must upgrade the software in the Cisco 800 Series ISRs to Cisco IOS 15.1(4)M or later releases.

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

What's New in Release 8.3.112.0

Release 8.3.112.0 is a repost of the now deferred Release 8.3.111.0 to address the caveats listed in the table below. There are no other updates in this release.

Note Cisco 1562 APs and 1800 Series APs must be manually upgraded to Cisco 8.3.112.0 release before associating them with Cisco vWLC running 8.3.112.0 release. The upgrade can be done using the TFTP server.

See the deferral notice for Release 8.3.111.0 at https://www.cisco.com/c/en/us/td/docs/wireless/deferral/Deferral_Notice_8_3_111_0.html.

Table 2: Resolved Caveats in Release 8.3.112.0

Caveat ID Number	Description
CSCvd23510	Cisco 2800, 3800 APs, and 1800 ME: SSH affected by CVE-2016-7406 – 7409
CSCvd48226	Cisco 1800, 2800, and 3800 APs: unable to see SSID configuration after upgrade

Temporal Key Integrity Protocol (TKIP) Support

The TKIP security protocol coverage which extended its support in 8.3.111.0 release for the Cisco Wave 2 APs, remains supported in Release 8.3.112.0.

The TKIP security protocol combination table is applicable to the Cisco Wave2 APs only. The legacy APs continue to support the protocols without any change in this release.

Table 3: Supported TKIP Security Protocol Combination for Cisco Wave2 APs in Release 8.3.112.0

AP Mode	Authentication Owner	State	Policy	Supported
Local	NA	NA	WPA TKIP/802.1x	Yes
Local	NA	NA	WPA TKIP/PSK	Yes
FlexConnect	Central Authentication	Connected	WPA TKIP/802.1x	Yes
FlexConnect	Central Authentication	Connected	WPA TKIP/PSK	Yes
FlexConnect	Local Authentication	Connected	WPA TKIP/802.1x	No
FlexConnect	Local Authentication	Connected	WPA TKIP/PSK	Yes
FlexConnect	Local Authentication	Standalone	WPA TKIP/802.1x	No
FlexConnect	Local Authentication	Standalone	WPA TKIP/PSK	Yes
Any	Any	Any	WPA2 TKIP/Any	No

What's New in Release 8.3.111.0

Adaptive 802.11r

802.11r is the IEEE standard for fast roaming also known as Fast Transition (FT). The Adaptive feature allows you to set up a network without explicitly enabling Fast Transition. Cisco APs and Apple devices (iOS 10 clients) mutually signal that adaptive 802.11r is supported on the network and perform an FT association on the WLAN, doing fast roaming when required. Legacy wireless clients that do not support 802.11r can still join the same network, however they do not benefit from faster FT roaming, joining as normal 802.11i/WPA2 devices. This mode hides FT support to the legacy clients preventing possible interoperability issues.

802.11r (FT) clients that do not support Adaptive feature, would join as regular clients, and would not be able to do fast roaming on WLANs that have Adaptive enabled.

See the following table for a summary of the support matrix:

Client support	WLAN PSK/dot1x	WLAN PSK/dot1x + Adaptive	WLAN PSK/dot1x + FT
Legacy (RSN only)	RNS roaming (PKC, full auth, etc)	RNS roaming (PKC, full auth, etc)	RNS roaming (PKC, full auth, etc)
802.11ft	RNS roaming (PKC, full auth, etc)	RNS roaming (PKC, full auth, etc)	FT fast roaming

Client support	WLAN PSK/dot1x	WLAN PSK/dot1x + Adaptive	WLAN PSK/dot1x + FT
802.11ft + Adaptive	RNS roaming (PKC, full auth, etc)	FT fast roaming	FT fast roaming

This feature is supported on the following Wave2 APs:

- Cisco Aironet 1560 Series APs
- Cisco Aironet 1800 Series APs
- Cisco Aironet 2800 Series APs
- Cisco Aironet 3800 Series APs

QoS Fastlane

QoS Fastlane simplifies the application traffic prioritization process so that network congestion is minimized and time sensitive traffic (like voice or video) is delivered on time.

To choose which iOS apps have their traffic prioritized by QoS Fastlane, configure the network with a configuration profile.

This feature support now extends to the following Cisco APs:

- Cisco Aironet 1560 Series APs
- Cisco Aironet 1800 Series APs
- Cisco Aironet 2800 Series APs
- Cisco Aironet 3800 Series APs

Cisco Aironet 1560 Series Outdoor Access Points

The Cisco Aironet 1560 Series Access Points are ideal for applications requiring rugged outdoor Wi-Fi coverage. These APs offer the latest IEEE 802.11ac Wave 2 radio standard in a compact, aesthetically pleasing, easy-to-deploy package. The flexibility of using internal and external antennas helps service providers, enterprise networks, and public safety networks to deploy the fastest links possible for mobile, outdoor clients (smartphones, tablets, and laptops) and wireless backhaul.

The 5-GHz radios have 802.11ac Wave 2 capability. The clients can access the network using 2.4-GHz or 5-GHz radio. Depending on the model, the access point can support up to 1.3-Gbps data rates.

The Cisco Aironet 1560 Series include Cisco wireless innovations such as:

- Cisco CleanAir Technology to view, characterize, and avoid wireless interference
- Cisco ClientLink technology for beamforming
- Radio Resource Management (RRM) for dynamic transmitter channel and power control

Note In this release, Cisco 1560 Series APs support local, flex, and Mobility Express modes, however, mesh functionality is not supported in this release.

For more information, see https://www.cisco.com/c/en/us/products/wireless/aironet-1560-series/index.html.

Cisco Aironet 1815i Access Points

The Cisco Aironet 1815i access point is an 802.11 a/b/g/n/ac (Wave 2) access point, with internal antennas only. The access point can be mounted on a wall or a ceiling, and supports 2x2:2 SS MU-MIMO applications.

RFID and Wi-Fi Tag Support

802.11 (Wi-Fi) active RFID tags are designed to operate in the unlicensed ISM bands of 2.4 to 2.4835 GHz or 5.8 to 5.825 GHz. These tags exhibit the characteristics of active RFID tags, but also comply with applicable IEEE 802.11 standards and protocols. Wi-Fi RFID tags can readily communicate directly with standard Wi-Fi infrastructure without any special hardware or firmware modifications. They can co-exist alongside Wi-Fi clients such as laptops, VoWLAN phones, and so on. When powered on, assets equipped with 802.11 Wi-Fi client radios can be tracked natively without the need to have an asset tag attached.

For more information on this feature, see the RFID Tag Technology section in the *Wi-Fi Location-Based Services 4.1 Design Guide*.

This feature support now extends to the following Cisco APs:

- Cisco Aironet 1560 Series APs
- Cisco Aironet 1800 Series APs
- Cisco Aironet 2800 Series APs
- Cisco Aironet 3800 Series APs

Federal Information Processing Standard (FIPS) Support

The main feature is “NSA Suite B Cryptography”, support to serve as a cryptographic base for both unclassified information and most classified information.

The new security protocols supported in this release are:

- Support DTLS 1.2 for AP-WLC CAPWAP connection

  Note Only AP1852 and AP3802 supports DTLSv1.2

- Support new GCM CIPHER Suites for DTLS

  Note ECC cipher suites are supported when LSC is used and CA server is capable of signing certificates with ECDS. If LSC is not used RSA_AES128_GCM_SHA256 or RSA_AES256_GCM_SHA384 ciphers can be used.

    - ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
    - ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

- The new 802.11 Encryption Modes supported in this release are:
    - CCMP-256
    - GCMP-128
    - GCMP-256
- SCEP over HTTPS is supported for getting LSC, download the CA certificate manually to authenticate the CA server during the TLS handshake.
    - WLC requires the device certificate when LSC is enabled, admin has to initiate the request
- IPsec configuration is profile-based
    - Create the IPsec profile and apply it to the desired interface
    - IPsec profiles applied to an interface cannot be modified
    - IPsec profile configuration via SNMP is not supported
- Syslog over IPsec is supported
- Driven by configuration, either IKEv1/IKEv2 is supported

  Note SHA-256 hash function is not supported with IKEv1.

- CSR can be generated on WLC for WebAuth, WebAdmin, and IPsec certificates, CSR could be RSA/ECC based, driven by configuration
- WebAdmin and WebAuth now support TLSv1.2 with ECC ciphers suites, both are independently configurable
- Download option is provided to have different CMX server CA certificate, and you can use TLSv1.2 for connectivity with CMX server

Note After you enable or disable FIPS, we recommend that you manually change the DTLS support to "**DTLS all**" from "**DTLS v1.2**." This allows the Cisco APs to associate with the Cisco WLC. Configure the DTLS version by entering the following command: **config ap dtls-version** *dtls_all*

Temporal Key Integrity Protocol (TKIP) Support

TKIP security protocol option is supported on the following Cisco APs:

Note In this release, the WPA+TKIP and WPA+AES protocols are supported, however WPA2+TKIP protocol is not supported.

- Cisco Aironet 1560 Series APs
- Cisco Aironet 1810 Series APs
- Cisco Aironet 1815 Series APs
- Cisco Aironet 1830 Series APs
- Cisco Aironet 1850 Series APs
- Cisco Aironet 2800 Series APs
- Cisco Aironet 3800 Series APs

For more information about this feature, see WPA1 and WPA2 section in the *Cisco Wireless Controller Configuration Guide*.

AAA Database Enhancement

The AAA Database is used for authenticating local user accounts which includes guest users, MAC-based authentication for APs for association with the controller, and allowing guests to associate with a particular WLAN, among other functions.

In this release, the AAA database supports up to 12000 entries, an increase from the earlier 2048 entry limit for the following Cisco WLCs:

- Cisco 5520 WLCs
- Cisco Flex 7510 WLCs
- Cisco 8510 WLCs
- Cisco 8540 WLCs

Local Policy Enhancement

You can now create up to 512 local policies, an increase from the earlier 64 policy limit on the following Cisco WLCs:

- Cisco 5520 WLCs
- Cisco Flex 7510 WLCs
- Cisco 8510 WLCs
- Cisco 8540 WLCs

For more information on this enhancement, see Local Policies section in the *Cisco Wireless Controller Configuration Guide*.

Support for Multiple Clients on Wired Ports

Support is introduced for multiple clients on wired ports of Cisco Aironet AP 1810W and OEAP 1810 Series APs. Each port on the AP supports up to four MAC addresses.

Software Release Types and Recommendations

Table 4: 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: https://www.cisco.com/c/en/us/products/collateral/wireless/8500-series-wireless-controllers/bulletin-c25-738147.html.

Upgrading the Cisco WLC Software Release

Guidelines and Limitations

- Release 8.3 supports additional configuration options for 802.11r FT enable and disable. The additional configuration option is not valid for older releases. If you downgrade from Release 8.3.112.0 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 8.3.112.0 to a 7.x release, the trap configuration is lost and must be reconfigured.
- If you downgrade from Release 8.3.112.0 to Release 8.1, the Cisco Aironet 1850 Series AP, whose mode prior to the downgrade was Sensor is shown to be in unknown mode after the downgrade. This is because the Sensor mode is not supported in Release 8.1.

- If you have an IPv6-only network and are upgrading to Release 8.3.112.0 or a later release, ensure that the following is done:
    - Enable IPv4 and DHCPv4 on the network—Load a new Cisco WLC software image on all Cisco WLCs plus Supplementary AP Bundle images on the Cisco 2504 WLC, 5508 WLC, and WiSM2 or perform a predownload of AP images on the required Cisco WLCs.
    - Reboot Cisco WLC immediately or at the preset time.
    - Ensure that all Cisco APs are associated with Cisco WLC.
    - Disable IPv4 and DHCPv4 on the network.
- After downloading new software to the Cisco APs, it is possible that a Cisco AP may get stuck in an "upgrading image" state. In such a case of a stranded Cisco AP, it may be necessary to forcefully reboot the Cisco WLC to download a new image or to reboot the Cisco WLC after the download of the new image. You can forcefully reboot the Cisco WLC by entering the **reset system forced** command.
- It is not possible to download some of the older configurations from the Cisco WLC because of the Multicast and IP address validations. See the *Restrictions on Configuring Multicast Mode* section in the 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 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 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 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 8.3.112.0, 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 8.3.112.0.

    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 https://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 8.3.112.0 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 8.3.112.0. The following table shows the upgrade path that you must follow before downloading Release 8.3.112.0.

Note 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.

For detailed release recommendations, see the *Guidelines for Cisco Wireless Software Release Migration Bulletin* at: https://www.cisco.com/c/en/us/products/collateral/wireless/8500-series-wireless-controllers/bulletin-c25-738147.html

Table 5: Upgrade Path to Cisco WLC Software Release 8.3.112.0

Current Software Release	Upgrade Path to 8.3.112.0 Software
8.0.x	You can upgrade directly to 8.3.112.0.
8.2.x	You can upgrade directly to 8.3.112.0. See the "Changes in Images and Installation Procedure for Cisco 2504 WLC, Cisco 5508 WLC, and Cisco WiSM2" section about special upgrade instructions for Cisco 2504 WLC, 5508 WLC, and WiSM2.
8.3.x	You can upgrade directly to 8.3.112.0.

- 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 8.3.112.0. 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 8.3.112.0 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 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 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.
- 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 8.3.112.0 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

- From Release 8.3 or a later release, ensure that the configuration file that you back up does not contain the < or > special characters. If either of the special characters is present, the download of the backed up configuration file fails.

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 Release 8.3.112.0 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:

  - AP802
  - Cisco Aironet 1530 Series AP
  - Cisco Aironet 1550 Series AP (with 64-MB memory)
  - Cisco Aironet 1550 Series AP (with 128-MB memory)
  - Cisco Aironet 1570 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 Release 8.3.112.0 for the applicable Cisco WLC platforms:

Table 6: 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-K9-8-3-112-0.aes	AIR-CT2500-AP_BUNDLE-K9-8-3-112-0.aes
Cisco 5508 WLC	AIR-CT5500-K9-8-3-112-0.aes AIR-CT5500-LDPE-K9-8-3-112-0.aes	AIR-CT5500-AP_BUNDLE-K9-8-3-112-0.aes AIR-CT5500-LDPE-AP_BUNDLE-K9-8-3-112-0.aes
Cisco WiSM2	AIR-WISM2-K9-8-3-112-0.aes	AIR-WISM2-AP_BUNDLE-K9-8-3-112-0.aes

[1] AP_BUNDLE or FUS installation files from Release 8.3 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 to Cisco WLC Software Release 8.3.112.0 (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 Release 8.3.112.0 software:

a) Browse to https://software.cisco.com/download/home.

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
- Mobility Express
- 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).

Note In Release 8.3.102.0, 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, to upgrade to Release8.3.112.0, 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, Cisco Aironet 1530 Series AP, Cisco Aironet 1550 Series AP (with 64-MB memory), Cisco Aironet 1550 Series AP (with 128-MB memory), and/or Cisco Aironet 1570 Series APs. For more information, see the "Changes in Images and Installation Procedure for Cisco 2504 WLC, Cisco 5508 WLC, and Cisco WiSM2" section.

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.

Note In Release 8.3.102.0, 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, to upgrade to Release8.3.112.0, 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, Cisco Aironet 1530 Series AP, Cisco Aironet 1550 Series AP (with 64-MB memory), Cisco Aironet 1550 Series AP (with 128-MB memory), and/or Cisco Aironet 1570 Series APs. For more information, see the "Changes in Images and Installation Procedure for Cisco 2504 WLC, Cisco 5508 WLC, and Cisco WiSM2" section.

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 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, re-enable them.

Step 19 To verify that the 8.3.112.0 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.

Interoperability With Other Clients in Release 8.3.112.0

This section describes the interoperability of Cisco WLC Software, Release 8.3.112.0 with other client devices.

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

Table 7: Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	8.3.112.0
Cisco WLC	Cisco 55xx Series Wireless Controller
Access points	AIR-CAP3802E-B-K9, AIR-AP1852E-B-K9
Radio	802.11ac, 802.11a, 802.11g, 802.11n (2.4 GHz / 5.0 GHz)
Security	Open, PSK (WPA-TKIP and WPA-TKIP-WPA2-AES), 802.1X (WPA-TKIP and WPA-TKIP-WPA2-AES) (LEAP, EAP-FAST)
RADIUS	ACS 5.3
Types of tests	Connectivity, traffic (ICMP), and roaming between two access points

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

Table 8: Laptops

Client Name	Version Details
Asus AC56(USB)	1027.515.2015
Broadcom 4360	6.30.163.2005
D-Link DWA-182 (USB)	6.30.145.30
Dell 1520/Broadcom 43224HMS	5.60.48.18
Dell 1530 (Broadcom BCM4359)	5.100.235.12
Dell 1540	6.30.223.215
6.30.223.215	6.30.223.262
Engenius EUB 1200AC(USB)	1026.5.1118.2013

Client Name	Version Details
HP Chromebook	55.0.2883.103
Intel 3160	18.40.0.9
Intel 6205	15.16.0.2
Intel 6300	15.16.0.2
Intel 7260	18.33.3.2
Intel 7265	19.10.1.2
Intel 8260	19.10.1.2
Linksys AE6000 (USB)	5.1.2.0
MacBook Air new	OSX 10.11.5
MacBook Air old	OSX 10.11.5
Macbook New 2015	OSX 10.12
MacBook Pro	OSX 10.11.6
Macbook Pro with Retina Display	OSX 10.12
Netgear A6200 (USB)	6.30.145.30
Netgear A6210(USB)	5.1.18.0
Samsung Chromebook	55.0.2883.103

Table 9: Tablets

Client Name	Version Details
Apple iPad Air	iOS 10
Apple iPad Air 2	iOS 10
Apple iPad mini with Retina display	iOS 10
Apple iPad Pro	iOS 10
Apple iPad2	iOS 10
Apple iPad3	iOS 10
Google 10.2" Pixel C	Andriod 7.1.1
Google Nexus 9	Android 6.0.1
Microsoft Surface Pro 2	Windows 8.1 - Driver: 14.69.24039.134

Client Name	Version Details
Microsoft Surface Pro 3	Windows 8.1 - Driver: 15.68.3093.197
Microsoft Surface Pro 4	Windows10 - Driver: 15.68.9040.67
Samsung Galaxy Note 3 - SM-N900	Android 5.0
Samsung Galaxy Tab 10.1- 2014 SM-P600	Android 4.4.2
Samsung Galaxy Tab Pro SM-T320	Android 4.4.2
Toshiba Thrive AT105	Android 4.0.4

Table 10: Mobile Devices and Printers

Client Name	Version Details
Apple iPhone 4S	iOS 10.2
Apple iPhone 5	iOS 10.2
Apple iPhone 5c	iOS 10
Apple iPhone 5s	iOS 10.2
Apple iPhone 6	iOS 10.2
Apple iPhone 6 Plus	iOS 10.2
Apple iPhone 6s	iOS 10.2
Apple iPhone 7	iOS 10.2
Cisco 7921G	1.4.5.3.LOADS
Cisco 7925G	1.4.5.3.LOADS
Cisco-8821	SIP8821.11-0-3ES2-1
Cisco 8861	Sip88xx.10-2-1-16
Cisco-9971	Sip88xx.10-2-1-16
Google Nexus 5	Android 6.0.1
Google Nexus 5X	Android 6.0.1
Google Pixel	Android 7.1.1
HP Color LaserJet Pro M452nw Printer	2.4.0.125
HTC One	Android 5.0
LG G4	Android 5.1

Client Name	Version Details
Nokia Lumia 1520	Windows Phone 8.10.14219.341
OnePlusOne	Android 4.3
OnePlus3	Android 6.0.1
Samsung Galaxy Mega SM900	Android 4.4.2
Samsung Galaxy Nexus GTI9200	Android 4.4.2
Samsung Galaxy S III	Android 4.3
Samsung Galaxy S4	Android 5.0.1
Samsung Galaxy S4 T-I9500	Android 5.0.1
Samsung Galaxy S5	Android 4.4.2
Samsung Galaxy S5-SM-G900A	Android 4.4.2
Samsung Galaxy S6	Android 6.0.1
Samsung Galaxy S7	Android 6.0.1
Sony Xperia Z Ultra	Android 4.4.2
Xiaomi Mi 4c	Android 5.1
Xiaomi Mi 4i	Android 6.0.1

Key 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.

Key Features Not Supported on Cisco 2504 WLCs

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

Note However, AVC for local mode APs is supported. 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.

- 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.

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

Key Features Not Supported on WiSM2 and Cisco 5508 WLCs

- 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.
- Cisco Smart Software Licensing

Key Features Not Supported on Cisco Flex 7510 WLCs

- Static AP-manager interface

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

- IPv6 and Dual Stack client visibility

  Note IPv6 client bridging and Router Advertisement Guard are supported.

- Internal DHCP server
- Access points in local mode

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

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

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

- PMIPv6
- Cisco Smart Software Licensing

- EoGRE

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

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

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

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

Note You can replicate this functionality 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
- Cisco 5520, 8510, and 8540 WLCs cannot function as mobility controller (MC). However, they can function as guest anchor in a New Mobility environment.

Key Features Not Supported on Cisco Virtual WLCs

- Internal DHCP server
- TrustSec SXP
- Access points in local mode
- Mobility/Guest Anchor
- Wired Guest
- Multicast

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

- 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
- Datagram Transport Layer Security (DTLS)
- EoGRE (Supported in only local switching mode)
- Workgroup Bridges
- Client downstream rate limiting for central switching
- SHA2 certificates
- Cisco WLC integration with Lync SDN API
- Cisco OfficeExtend Access Points

Key Features Not Supported on Access Point Platforms

Key Features Not Supported on Cisco Aironet 1520 and 1550 APs (with 64 MB memory)

- PPPoE
- PMIPv6

See the amount of memory in a Cisco Aironet 1550 AP by entering this command in Cisco WLC CLI:

show mesh ap summary

Key Features Not Supported on Cisco Aironet 1560, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800, and 3800 Series APs

Table 11: Key Features Not Supported on Cisco Aironet 1560, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800 and 3800 Series APs

Operational Modes	• Spectrum Expert Connect • Autonomous Bridge and Workgroup Bridge (WGB) mode • Mesh mode • Flex plus Mesh • 802.1x supplicant for AP authentication on the wired port • Link aggregation (LAG) behind NAT/PAT environment
Protocols	• 802.11u • Full Cisco Compatible Extensions (CCX) support • Rogue Location Discovery Protocol (RLDP) • Native IPv6 • Internet Group Management Protocol (IGMP) v3
Security	• TrustSec SXP • 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	• Per Client AAA (QoS Override) • Bidirectional rate-limiting • Split Tunneling • EoGRE • PPPoE • 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 • Link aggregation (LAG) • MAC Authentication Flex Local Authentication • SIP snooping with FlexConnect in local switching mode

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

Table 12: Key Features Not Supported on Cisco Aironet 1810 OEAP and 1810W Series APs

Operational Modes	• Monitor Mode • Mobility Express

Key Features Not Supported on Cisco Aironet 1830 and 1850 Series and 1815i APs

Table 13: Key Features Not Supported on Cisco Aironet 1830 and 1850 Series and 1815i APs

Operational Modes	• Monitor Mode

Key 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

Caveats

Open Caveats

Table 14: Open Caveats for Release 8.3.111.0 and 8.3.112.0

Caveat ID Number	Description
CSCuj27382	AP local authentication, PEAP authentication fails, with EAP-TLS enabled and with no or expired certificate
CSCuw45964	Mobility Express: while editing a WLAN in HTTP session, user is getting logged out
CSCux28505	Cisco 8510 WLC running 8.2.1.124 image reloads unexpectedly with "fp_main_task" during boot
CSCuz03702	New mobility:wired client behind WGB fails to pass traffic after roaming
CSCuz45986	CWA not working on Cisco 8500 WLC as guest anchor with accounting enabled
CSCuz69729	Cisco 3700 AP running 8.4.140.0 release - 802.11ac WGB not associates with root channel width 40-MHz above or below
CSCuz70648	Cisco 1800 APs : Radio core dump @ 0x009A395F QCA 2468119
CSCuz70879	MAP reloads on hitting 40 mins timer even when it is downloading image
CSCva31890	MIB table bsnMobileStationPerRadioPerVapTable has no data
CSCva33956	Cisco WLC freezes when sftp is used for transfer and shows spurious messages due to wrong credentials
CSCva38941	Clients are redirected to internal LWA URL instead of CMX cloud URL
CSCva39537	802.11h configuration not saved after restoring configuration backup
CSCva40580	Cisco 8.3 release: bulksync between active and standby WLC never completes and is stuck in 'in-progress' mode
CSCva58323	Cisco 3800 AP sends out multicast packets with no clients associated
CSCva66176	AP drop of from network due to large set of mobility groups in down/down state
CSCva66489	802.11r sess timeout after reassociation causing deauthentication 17 mismatch FTIE
CSCva68921	Cisco WiSM2 unexpectedly reloads when 'reaperWatcher' gets stuck on DP0 while retriving crash info
CSCva72044	BZ1388: Cisco 1572 mesh AP with no distance command implementation

Caveat ID Number	Description
CSCva83802	HA: SSH on redundancy management interface rejected
CSCva86077	In a dynamic interface "ap-manager"should not be allowed as valid name as it is a reserved name
CSCva92917	Observed traceback logs in show msglog and logging
CSCva95121	Stale IP route left on Flex AP configuration if booting up in standalone mode
CSCva99545	Invalid information displayed when CLI 'show certificate webauth/webadmin' is run
CSCvb09609	Cisco 802 AP not supported as subordinate on Mobility express
CSCvb11778	Cisco WLC running 8.1.131.18 release reloads unexpectedly on sisfSwitcherTask
CSCvb12026	Client load balance export to anchors fails with new mobility enabled
CSCvb13666	WiSM2 reloads unexpectedly with Task Name 'IPv6_Msg_Task'
CSCvb16441	Cisco 702w AP continuous failures on wbuf_alloc: pak Rx buffer allocation failure
CSCvb20553	CoA for session timeout not working using free RADIUS server
CSCvb21254	Cisco 8.0.140.0 release: AAA override VLAN lost on intercontroller roaming
CSCvb29996	Cisco 1810W AP hardware reloads unexpectedly when watchdog resets and the crash file shows PC=0xc03b3ffc, LR=0xc008af24, QCA 02698633
CSCvb32363	Management interface responds to CAPWAP messages after disabling AP-manager
CSCvb33076	WLC: GUI does not allow to change sniffer channel
CSCvb41794	Cisco WLC, Secondary RADIUS ISE statastics not getting incremented for IOS AP
CSCvb44979	WLC Local EAP with Cisco Unified Wireless IP Phone 7925 handshake failure
CSCvb45130	Part of ATF configuration is not pushed to uploaded configuration
CSCvb48354	RRM not updating as per configured on WLC
CSCvb51570	Cisco WiSM2 reloads unexpectedly on upgrading to Cisco 8.3.102.0 release with Task Name: spamApTask6
CSCvb61023	DHCP Option 82 (remote-id) not present is some AP
CSCvb61245	Cisco 1700, 3700 APs: reloads unexpectedly on CPUvector 400, PC = 10000200
CSCvb64560	CISCO-LWAPP-AAA-MIB: DEFVAL format incorrect for some objects
CSCvb72367	Transfer upload datatype run-config is missing several configuration sections
CSCvb81940	VLAN tagging for external module removed from AP after upgrade to 8.3.102.0 release
CSCvb86157	Clients cannot connect anymore to vWLC- Instrumented code added

Caveat ID Number	Description
CSCvb86604	High CCA threshold environment: clients show connected, and has a valid IP address, however will not pass any data traffic
CSCvb91832	Cisco1810W AP radio reloads unexpectedly due to firmware failure @0x009C30A0/0x0000, memory corruption, QCA 2689026
CSCvb96009	Cisco WLC running 8.3.102 release reloads unexpectedly on emweb task
CSCvb97383	Cisco WLC deauthenticating roaming client with idle timeout
CSCvb97656	Unexpected reload: Task Name: mmListen on 8.3.102.0
CSCvb98859	AP in local switching or local authentication disconnect EAP-SIM client idle for more than 0.5 second
CSCvb99468	AirOS WLC reloads unexpectedly in emWeb when serving an EmWebForm exclusion-list
CSCvc01761	Cisco WLC continuously probes Active RADIUS Server
CSCvc09805	Cisco WLC on 8.2 release: rejects client association even when only one AP is broadcasting SSID and multiple client attempts
CSCvc10730	IPv6 management station address not displayed properly in syslog
CSCvc12594	Controller fails to send SNMP when using untagged interfaces on different ports
CSCvc13497	Evaluation of orion for OpenSSL November 2016
CSCvc14378	Max number of NMSP connect set to 2, this is change from default of 10
CSCvc17678	Cisco 2800 APs: wrong "enable global mDNS snooping" message when clicking apply on AP edit page
CSCvc18129	Cisco WLC reloads unexpectedly on RF profile or client exclusion sync on HA scenario
CSCvc18670	Client stops passing traffic on DHCP reqd. WLAN after sending a reassociation request but does not send DHCP packet
CSCvc24485	#APF-3-UNKNOWN_RADIO_TYPE: [SS] apf_utils.c:571 unknown radio type 0 from standby flooding syslog
CSCvc24687	Cisco 2800 APs running 8.2.131.47 release: kernel panic due to memory corruption
CSCvc31268	CISCO-LWAPP-SYS-MIB: clsApTransferEntry is not provided values for AP primary and backup images
CSCvc37641	Cisco 700 AP in FlexConect mode and in wIPS submode does not provide SSH access
CSCvc38374	AP ignores U-APSD QoS null trigger frames with Draeger M300
CSCvc51666	IOS AP transmits on disabled 24Mb data rate
CSCvc52619	Local EAP do not support any of ciphers used by Cisco Wireless IP Phone 8821

Caveat ID Number	Description
CSCvc54575	Intel 7265 client fails to complete 802.11w Opportunistic Key Caching (OKC) roam
CSCvc55328	AP reloads unexpectedly due to kernel panic at WlLoadRateGrp
CSCvc65641	WLC reports tracebacks reported very frequently but no crashes
CSCvc67465	Cisco AP in FlexConnect mode loses VLAN mapping if VLAN tagging is enabled
CSCvc74515	Cisco 8.2.121.11 and 8.2.124.15 release: WLC Data Plane reloads unexpectedly due to fragmentation
CSCvc78510	Cisco 2702 AP aux port goes to disabled after the AP is rebooted
CSCvc81168	Cisco 2702 AP unable to upgrade and failing with error "Unable to create temp dir flash:/update"
CSCvc82053	The NMSP info and probe notification queue is saturating
CSCvc83490	Redundancy Mobility MAC does not stay, primary WLC's MAC is always set instead
CSCvc83583	Cisco 5520 controller reloads unexpectedly with taskname apfProbeThread
CSCvc84637	Cisco 1810W AP sending invalid AC_NAME when WLC hostname is 31 bytes long
CSCvc85063	Internal DHCP: unable to ping client IP from APs
CSCvc85164	802.11v: candidate neighbor list is empty in BSS transition management request
CSCvc85171	802.11v Optimized Roam Disassociation Timer is always zero in BSS transition management query
CSCvc85328	Cisco 1832, 1852 APs: power type indicates power injector, normal mode incorrectly inspite of power is supplied by AIR-PWR-C
CSCvc87409	Cisco 2800 AP Tx-reset causing radio reset
CSCvc87433	Web authentication with proxy does not work on 8.2 release or higher
CSCvc88997	FRA probe suppression configuration not saved after WLC reboot
CSCvc91195	ACL is not applied to the traffic from the client connected to internal AP towards WLC
CSCvc95222	Cisco 1810w AP LAN port dropping IPTV packets
CSCvc95444	Hostapd error and client failing to associate with PMF+PSK WLANs

Resolved Caveats

Table 15: Resolved Caveats for Release 8.3.111.0 and 8.3.112.0

Caveat ID Number	Description
CSCur63031	AP error: %ENTROPY-0-ENTROPY_ERROR: Unable to collect sufficient entropy

Caveat ID Number	Description
CSCur68316	Cisco 802AP-891 in FlexConnect mode are losing VLAN mapping after power cycle
CSCus83638	Cisco AP 5-GHz radio is stuck - beaconing continues but does not accept client associations.
CSCuw41092	AP not send traffic indication in beacon for power-save client after FT
CSCuw97688	ME: ping failed from control to guest client with web consent, no VLAN
CSCux48308	Broadcast delivery stops with with key rotation 1552 in RAP a d Cisco 819W running release 153.3JBB5 is in WGB mode
CSCux51833	Client fails on RAP with AAA Override ACL when AP is in Flex+Bridge Mode
CSCux78389	RADIUS failover should failover both authentication account server on WLAN
CSCux85357	WLC sends GARP for FlexConnect local switching clients after HA switch-over
CSCux88967	On MAC Filter failure client session timeout cannot associate again
CSCux95319	Clients roaming between central to local authentication may apply for local to FlexConect mode APs (not supported) causing 802.1x table failures
CSCux96500	Cisco WiSM2 WLC reloads unexpectedly on bcastReceiveTask
CSCuy30583	Cisco 5520 WLC reloads unexpectedly on show imm chassis shows no results
CSCuy53072	SNMP cLMobilityGroupMembersTable returns wrong value from WLC in PI
CSCuy53596	Cisco CleanAir fatal error and radio reset on Flex+Bridge AP
CSCuy64520	Access Points (AP) sending CDP packets to the wireless clients
CSCuy71409	Client detailed params not synced to standby in fast SSID scenario
CSCuy75241	Cisco 5508 WLC system unexpectedly reloads with task mmMobility
CSCuy82849	Memory leak found @mm_heartbeat module on guest anchor WLC
CSCuy92423	CWA broken in beta image 8.0.122.50
CSCuz11717	3-sec delay before sending "dot1x auth initiate" to SPAM with WSSI
CSCuz16883	Address registration issues for mobility scenarios
CSCuz22198	Cisco 5508 WLC silently reloads on with %OSAPI-0-TIMER_CREATE_FAILED: timerlib.c
CSCuz35221	Mobility handoff fails in new mobility 802.1x CWA client reconnect
CSCuz40066	Guest Anchor: foreign to foreign roam fails on GA scenario
CSCuz40970	Cisco 8510 WLC: WLC unexpectedly reloads on task osapiBsnTimer

Caveat ID Number	Description
CSCuz45296	WLC sends account update multiple times in the same millisecond
CSCuz46892	ME: external AP rebooted because it detected another ME controller
CSCuz48289	FT-PSK PMF-Optional, EAPoL M2 MIC error on change to local auth-flex
CSCuz50774	WLC losing pings to itself, Reaper cleaning up exited task osapi_ping_rx
CSCuz52435	Evaluation of Cisco WLC for OpenSSL May 2016
CSCuz54125	Cisco 5500 WLC: SSHpmCert memory corruption (overrun) on Pmalloc/Pfree buffers
CSCuz65175	ME 1852 AP: HTTP profiling causes CPU spikes and degraded performance
CSCuz78555	Bulk sync status "In-progress" after standby boots up
CSCuz79869	Cisco 8510 WLC reloads unexpectedly
CSCuz81180	Cisco 2800, 3800 APs: RIE cascading check failing
CSCuz85820	Mobility Express Cisco 1850 AP: unable to disable web-authentication secure web
CSCuz90785	Cisco 8.2 release: traffic black hole WEP errors on Cisco IW3702 WGB during roaming mesh
CSCva01249	Auto Restart check box should persist the state made by the user
CSCva01762	Cisco 1815, 1850 APs: Over-ride global credentials cleared on GUI after reboot
CSCva03376	UX-AP3702i after primed carrier set 5-GHz only allowing four UNII3 channels
CSCva11919	Loaded EoGRE pulls CAPWAP traffic under slow path, brings performance down
CSCva12055	Link is down after Cisco 5520 and 8540 WLCs reboot
CSCva15190	WLC CCX client location calib shows low cLD11ClientCalibSamplesCollected
CSCva17231	Active WLC RF group stuck on 'HA Standby' and RRM stopped on HA failure
CSCva18981	Cisco 8510 WLC reloads unexpectedly while running on 8.2.100 release
CSCva22440	Cisco 3800 AP: QBSS STA Count keeps incrementing with STA associating again
CSCva25760	GUI: setting static DNSv6 entries do not work
CSCva28211	AireOS UX AP : 'JP' should be used as world mode in beacon/Probe Res
CSCva28524	Cisco WLC with 8.3 release- creating SNMP community fails
CSCva31178	Cisco AP with 8.3 release - radio reset due to offchannel stuck
CSCva32411	Clients losing connectivity when reauthenticates with 802.1x over Cisco 702w AP
CSCva33663	Cisco 8510 WLC reloads unexpectedly with task:emweb on changing radio

Caveat ID Number	Description
CSCva34774	Cisco WLC reloads unexpectedly at apfReceiveTaskwith reason "System Crash"
CSCva35509	Data rates reported incorrectly in Cisco 1572 AP MA/RAP deployment
CSCva46486	Cisco 5520 WLC reloads unexpectedly with no core or crash file written
CSCva47891	Cisco WLC reloads unexpectedly at task 'EAP_Framework_0'
CSCva49651	Flex Data DTLS enabled, WLC to flush old data DTLS sessions on WAN flap
CSCva50196	Memory corruption EAP for Mesh
CSCva50370	On AP Performance, the "% Interference Impact" greyout by black or red
CSCva52825	Cisco 2800, 3800 APs does not do PMTU discovery during join/image download
CSCva55011	Cisco WLC reloads unexpectedly on Task Name redXmlTransferMain with HA SSO
CSCva59741	ME: incorrect pop-up error while setting channel width for radio2(5-GHz)
CSCva63310	Cisco WLC running 8.2 release: unable to enable mode Trunk on Mesh mode AP
CSCva63541	Cisco 2800, 3800 APs CAPWAP restarts continuously during FTP transfer of large file
CSCva65408	Cisco WLC reloads unexpectedly when client is not associated with EAP profile using PEAP method
CSCva65643	WLC reports Load Profile failed but clients connected under threshold
CSCva65826	Wireless LAN Controller reboots unexpectedly
CSCva66339	Flex AP's in standalone mode deauthenticate client during EAPoL exchange
CSCva66496	Cisco 3802 AP reloads unexpectedly on Watchdog reset on CAPWAPd
CSCva70440	Cisco 801 AP is rebooting continously
CSCva72724	Cisco 2602 AP reloads unexpectedly on "disc_tx_requeue_client" "dot11_get_rate_shift"
CSCva74487	Cisco 8540 WLC reloads unexpectedly on running show commands task: emWeb
CSCva76731	ME GUI does not show localization language with Internet Explorer
CSCva76982	Need a command to disable DFS Blacklist Time Doubling
CSCva78358	Cisco 1810w APs: RLAN VLAN local switch LAN mappings not applied on N+1 failover
CSCva81217	Edit of RF profile settings via GUI resets RxSOP threshold value to Auto
CSCva81409	Clients stuck in WEBAUTH_REQD state, emweb form cannot be submitted

Caveat ID Number	Description
CSCva82369	Cisco 8.3.102.0 release: WLC reloads unexpectedly on applying custom rogue rule using GUI
CSCva83234	Cisco 2800, 3800 APs: Kernel reloads unexpectedly during image download
CSCva83884	Cisco WLC system reloads unexpectedly on aaaQueueReader
CSCva85056	Cisco 2800, 3800 APs: is not detecting RFID Tags
CSCva87295	Flex AP radio reset during FT with Central DHCP and Nat-pat enabled
CSCva89698	WLC is leaking packets from virtual IP onto LAN
CSCva90343	Unable to do VLAN to RLAN mapping at FlexConnect Group
CSCva90980	EoGRE high ping latency/SNMP polling fails
CSCva91457	Cisco WLC: unexpectedly reloads repeatedly with reason: spamApTask4
CSCva92615	Access Point antenna gain changes to 0dBi randomly
CSCva93401	WLC system reloads unexpectedly on (spamApTask) immediately after upgrade to 8.2.121.0 release
CSCva95251	DSCP traffic is not limited to maximum QoS Profile value
CSCva95424	GUI: For All Clients AVC top application usage is 16KB
CSCva96899	Cisco 8510 WLC reloads unexpectedly on task "tplusTransportThread" when 8.2MR2 release upgrade
CSCva98592	Unexpected reload: fatal condition at broffu_fp_dapi_cmd.c
CSCva98597	Emweb task stuck at 100% CPU usage
CSCva98904	Cisco 2800, 3800 APs reload on rcu_sched self-detected stall
CSCva99864	EAP-TLS fails with Windows and ME using "Smart card or certificate" authentication
CSCvb00327	Cisco WISM2 and 5508 WLCs reloads unexpectedly in Process Bonjour_Process_Task
CSCvb02180	ARP table full. Unable to delete ARP mappingIP
CSCvb02472	Cisco WLC reloads unexpectedly on radiusTransportThread, memory corruption
CSCvb03710	Cisco 1852, 3802 AP unexpectedly reloads on "capwapd" process while data-dtls enabled
CSCvb09381	Unable to add or modify SNMP strings on a Cisco 5520 WLC HA Pair running 8.1.122.0 release
CSCvb13455	sub._apple-mobdev2._tcp.local is not snooped by controller
CSCvb18339	DTLS connection failed because max control DTLS connections reached

Caveat ID Number	Description
CSCvb18640	Mobility Express: Manual Channel-widths overwritten by DCA
CSCvb19115	WLC mDNS Service group MAC address count does not decrement
CSCvb19729	Cisco WLC reloads unexpectedly on Task name EAP_Framework_0
CSCvb28231	Cisco 5508 WLCs reloads unexpectedly due to memory corruption
CSCvb29483	SNMP traps are not sent to the receiver
CSCvb31857	Cisco WLC rejects client association with 802.11k assisted roaming on Cisco 2800 AP dual 5G
CSCvb32659	Syslog message for DP_BUFFER_POOL_EARLY_WARNING
CSCvb34951	Cisco 5520 and 8540 WLCs not sending AP up or down traps on APs association or disassociation from them
CSCvb35018	Cisco WiSM2 reloads unexpectedly with task mdnsHATask
CSCvb35173	Cisco 2800, 3800 APs: Radio crash, beacon stuck - due to lost Txq reference
CSCvb35815	High CPU in Cisco 2504 WLC with directly connected AP on upgrade to 8.2 and 8.3 release
CSCvb36432	SSIDs vanishes from standalone AP after reboot
CSCvb38441	ME_2800 APs: kernel reloads unexpectedly on PC at 0x939c8400
CSCvb38912	Flex ACL does not get applied when client roams in 'CENTRAL_WEB_AUTH'
CSCvb40473	NAC failed to send data when controller is in HA
CSCvb41738	Cisco 1832i AP: kernel panic reloads unexpectedly on PC at unmap_single_vma+0x324/0x5e4
CSCvb43105	Cisco 2800, 3800 APs outer DSCP not same as inner with DSCP Trust upstream NSS
CSCvb44169	emWeb reaper reset after "clear mdns service-database all"
CSCvb44699	NMSP queue full due to rouge AP task
CSCvb48603	Evaluation of Cisco WLC for OpenSSL September 2016
CSCvb52310	Silent Boot on Cisco 2800, 3800 APs
CSCvb54166	Malformed 802.11v element on HSR WGB with WLC 8.2 or later release
CSCvb59734	AP sending incorrect information about ciphers configured in WLAN
CSCvb60485	Cisco 2800 APs: watchdog reset (WCPD no heartbeat)
CSCvb60500	ME_2800 AP: memory corruption, SKB_Consume kernel panic crash

Caveat ID Number	Description
CSCvb61217	Workaround for CSCva81409 clients stuck in WEBAUTH_REQD state, emweb form cannot be submitted
CSCvb62537	Cisco 2800 APs detects another ME controller
CSCvb64869	Anomalous Interference/channel utilization observed in Cisco 8.3 release
CSCvb67415	ATF optimization config did not sync up when AP joined
CSCvb68541	Cisco 1850 AP reloads unexpectedly on radio failure at 0x00990C98, QCA 02653512
CSCvb69962	Client traps not showing session ID's
CSCvb71168	RSA256-AES256 DTLS encryption lowers PMTU but AP does not respect it
CSCvb72084	Cisco 8.2.121.11 and 8.2.124.15 release: Unexpected reload: fatal condition at broffu_fp_dapi_cmd.c
CSCvb72192	Cisco 1850 APs running Click OS: IPhone6S fails to connect to adaptive 802.11r WLAN
CSCvb72380	Cisco 2800, 3800 APs: performance profile show all values as 0 after clearing the configuration for XOR radio
CSCvb75481	Cisco WLC: unable to create local policies from security web UI
CSCvb76850	Cisco 8510 controller running 8.2 MR2 release- DP reloads unexpectedly while sending the application captures from pagent
CSCvb77168	Halo - AP HL cfg has all zeroes for WLC Gateway MAC
CSCvb78834	Cisco WLC reloads unexpectedly with task name emweb
CSCvb78906	Invalid logs about "Subnet mismatches while registering IP address"
CSCvb79274	WGB wired client expiring periodically
CSCvb80511	CWA is not working for flex-bridge APs pointing ACL Rx from RADIUS does not exist
CSCvb81003	Cisco WLC reloads unexpectedly as emWeb uses 100%
CSCvb81359	Cisco 8540 WLC HA. RMI ping and access to standby fail when using non-default ap-manager
CSCvb82813	WLC reloads unexpectedly with "debug nmsp all enable"
CSCvb85052	Cisco 3800 AP: PMF client gets stuck trying to associate to PMF WLAN
CSCvb85576	Evaluation of Cisco WLC for CVE-2016-5195 (DIRTY CoW)
CSCvb87315	Cisco 2800, 3800 APs- ERP IE is missing in beacons for 802.11g only SSID
CSCvb87319	RF utilization trap log wrongly output is as 655 multiples

Caveat ID Number	Description
CSCvb89781	Cisco 2700-B AP unable to join WLC: unable to create temp dir "flash:/update"
CSCvb90403	Cisco 1810W AP: hardware watchdog reset at PC= 0xc03b3ffc, LR= 0xc011e2dc
CSCvb90793	AP name unknown in SNMP bsnDot11StationDeauthenticate traps
CSCvb91603	Data rate in the 5-GHz cannot be locked to 6Mbps for Cisco 1810AP, QCA 02702647
CSCvb92562	Evaluation of all for OpenSSL 1.0.1 September 2016
CSCvb94003	WLAN configuration updates not working through webUI on 8.4.1.110 release
CSCvb94413	Cisco 2800, 3800 APs: low Tx power observed in certain RF conditions
CSCvb94610	Restore command to disable GARP
CSCvb94697	Cisco 2800, 3800 APs: 802.11n macbook client has dropping connectivity while connecting to Cisco 3800 APs
CSCvb94799	Cisco 3800 AP: mc2uc packet packet lost
CSCvb95147	Cisco 1572EAC APs unable to use 80 MHz
CSCvc00358	Cisco WLC reloads unexpectedly "apfRogueTask_0" missed software watchdog
CSCvc01365	Reaper Reset: Task "NFV9_Task" missed software watchdog
CSCvc01563	Cisco 2800, 3800 APs: command timeout observed in Cisco 8.2.140.0 release
CSCvc01923	Cisco 3800 APs RTS frames sent at hardcoded 6 Mbps instead of minimum mandatory configured rate
CSCvc09824	Cisco 2800 APs: band select statistics counter show zero
CSCvc13175	Cisco 5520 WLCs: GLC-T SFP stopped working (1G Port down)
CSCvc15149	Cisco 8.2.140.0 release - not beaconing a SSID when it is in an AP group and SSID enabled later
CSCvc16755	Cisco 3802 AP custom power level not initialized after reboot
CSCvc18699	Cisco 1800 APs: high pings drops, traffic connectivity drops seen 8.2.131.40 release, QCA 02706502
CSCvc20813	Cisco 2800, 3800 APs running 8.2.140.0 release - after trying configuration change on the WLAN, clients not able to join some APs
CSCvc22291	8.2 beta - WLC keeping some Cisco 2800, 3800 APs in 20 MHz when 40 MHz is selected in the RF profile
CSCvc22394	Cisco 1852 APs: disabled radios start up when changing from local mode to flex mode
CSCvc23658	Clients not removed from Cisco FlexConnect and CAPWAP in APs FlexConnect central-sw

Caveat ID Number	Description
CSCvc25669	'rfidTask' is causing a high CPU on the WLC
CSCvc26901	Cisco 1852 APs: optimized roam failed
CSCvc30561	COS AP's clients cannot subscribe to multicast stream after a while
CSCvc30827	Cisco 2800, 3800 APs - WLC when configured for WPA or TKIP advertises in probe response TKIP+AES
CSCvc31304	AP syslog flood for TLV-DEC-ERR: cannot process TLV for TLV_DMS_CLIENT_REQUEST_PAYLOAD(325/0)
CSCvc32706	Cisco 3800 APs: not seeing all COS neighbors
CSCvc32856	Cisco 2800, 3800 APs: sends a AQ event as soon as RRM changes channel causing bad channel selection and changes
CSCvc33258	Cisco WLC: unable to config Rx-SOP threshold for Cisco IW3702 AP
CSCvc33511	SNMPv3 access failing with either unknown user or no response
CSCvc38214	Cisco 2800, 3800: APs sending acknowledgements to client at 54 data rate although basic rate is 12 and 24
CSCvc39904	ME: efficient upgrade is disabled for default-flexgroup
CSCvc40470	AP radio hang chatter: wl0: rxRingStuckDetect(271): Rx-hang detected!!
CSCvc42566	Cisco 1702I AP - radio resets observed due to Cisco CleanAir error count exceeded
CSCvc42939	Cisco 3800: AP duplicating multicast packets
CSCvc44619	Passphrase on CLI with special characters apply but not on GUI
CSCvc45038	Cisco 2800, 3800 APs: beacon drift 25ms with offchannel/cleanair scanning @3sec mc9060 client drops
CSCvc48232	Cisco 2800, 3800 APs reloads unexpectedly due to kernel panic at mhsm_transition
CSCvc49492	Cisco 1852 AP detects high noise level on 5-GHz radio
CSCvc50228	Cisco 2800, 3800 APs sending data packets to the 802.11g clients sometimes with messed up data rates
CSCvc50377	Cisco Flex7510 WLC running 8.0.110.11 release: emWeb reloads unexpectedly while doing "show run-config"
CSCvc52004	iOS device connect to the 802.1x network slowly, QCA 02745009
CSCvc59252	Cisco 1852 APs show only power level 1 instead of power level 1 to 8 under 5-GHz radio
CSCvc61560	WLC RADIUS authentication request fails - aaaQueueReader "Unable to fit Radius packet in allocated memory"

Caveat ID Number	Description
CSCvc64343	Cisco 1530 AP in Japan domain in mesh mode: detects a lot of radars
CSCvc69564	Cisco 1852E APs: multiple beacons stuck
CSCvc76148	Cisco 2800, 3800 APs beacon drift causing Motorola mc9060 client drops
CSCvc87207	Cisco 2800 APs 802.11b/g radio dropping RTP packets
CSCvc90559	Rx hang seen on alpha running 8.2.145.36 release
CSCvd07657	Cisco 1810 APs fails to get ARP response intermittently leading to a full reboot
CSCvd16939	Cisco 1800 AP band-select does not work
CSCvd23510	Cisco 2800, 3800 APs, and 1800 ME: SSH affected by CVE-2016-7406 - 7409
CSCvd48226	Cisco 1800, 2800, and 3800 APs: unable to see SSID configuration after upgrade

Cisco Mobility Express Solution Release Notes

Overview

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 controller functionality bundled into the Cisco Aironet 1560, 1815, 1830, 1850, 2800, and 3800 Series access points.

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

The primary AP operates as a wireless 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 the setup and configuration, see the *Cisco Mobility Express User Guide for Release 8.3*, at http://www.cisco.com/c/en/us/td/docs/wireless/access_point/mob_exp/83/user_guide/b_ME_User_Guide_83.html

Supported Cisco Aironet Access Points

APs Supported as Primary (Support Integrated Wireless Controller Capability)	APs Supported as Subordinate
Cisco Aironet 1560 Series Cisco Aironet 1830 Series Cisco Aironet 1850 Series Cisco Aironet 2800 Series Cisco Aironet 3800 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 1810W Series Cisco Aironet 2600 Series Cisco Aironet 2700 Series Cisco Aironet 3500 Series Cisco Aironet 3600 Series Cisco Aironet 3700 Series

Cisco Mobility Express Features

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

- Support for the following access points:
  - Cisco Aironet 1560 Series
  - Cisco Aironet 2800 Series
  - Cisco Aironet 3800 Series
- Simple Network Management Protocol (SNMP) Version 3 polling; configurable through the GUI.
- Support for the Flexible Radio Assignment (FRA) functionality for the radio in slot 0 on Cisco Aironet 3800 Series access points. FRA automatically detects when a high number of devices are connected to a network, and changes the dual radios in an access point from 2.4GHz/5GHz to 5GHz/5GHz to serve more clients.
- Improvements in software update and access point image management with direct download from Cisco.com.
- Integration with Cisco CMX Cloud for both guest services and presence analytics. This is enabled by the integrated cloud connector on the Cisco Mobility Express controller for seamless integration and easier provisioning.
- Localization to Japanese and Korean for the Cisco Mobility Express controller GUI.
- Setting up and managing an internal DHCP server through the GUI.
- Importing a customized guest login page.

- Forced failover to a specified AP as primary.

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 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).
- GUI and CLI-based initial configuration wizards.
- Up to three Network Time Protocol (NTP) servers, with support for FQDN names.
- Simple Network Management Protocol (SNMP) Version 3 polling, configurable through the CLI.
- 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 TFTP and HTTP.
- Priming at distribution site.
- Default Service Set Identifier (SSID), set from factory. Available for initial provisioning only.
- Management through the 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.
- 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—SNMPv1, by default, and SNMPv2c.
- Management—SSH, Telnet, Admin users.
- Reset to factory defaults.
- Serviceability—Core file and core options, Logging and syslog.
- Cisco Prime Infrastructure.
- 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 Changing
- 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.

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

The following table lists the Cisco Mobility Express software for Cisco Wireless 8.3.112.0.

Access Points Supported As Primary	Software to be Used only for Conversion from Unified Wireless Network Lightweight AP Software To Cisco Mobility Express Software	AP Software Image Bundle, to be Used for Software Update, or Supported Access Point Images, or Both
1560	AIR-AP1560-K9-8-3-112-0.tar	AIR-AP1560-K9-ME-8-3-112-0.zip
1830	AIR-AP1830-K9-8-3-112-0.tar	AIR-AP1830-K9-ME-8-3-112-0.zip
1850	AIR-AP1850-K9-8-3-112-0.tar	AIR-AP1850-K9-ME-8-3-112-0.zip
2800	AIR-AP2800-K9-8-3-112-0.tar	AIR-AP2800-K9-ME-8-3-112-0.zip
3800	AIR-AP3800-K9-8-3-112-0.tar	AIR-AP3800-K9-ME-8-3-112-0.zip

Installing Mobility Express Software

See the “Getting Started” section in the *Mobility Express User Guide* at http://www.cisco.com/c/en/us/td/docs/wireless/access_point/mob_exp/83/user_guide/b_ME_User_Guide_83.html

Caveats

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

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