Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.5.103.0 and 8.5.105.0

First Published: 2017-07-25

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

Modification Date	Modification Details
August 23, 2018	Open Caveat—Added CSCvk44249
July 9, 2018	What's New in Release 8.5.103.0 section—Updated information about VLAN-based central switching support.
April 11, 2018	Software Release Types and Recommendations section—Added upgrade path information.
March 13, 2018	Supported Cisco Access Point Platforms section—Added information about support for Integrated Access Point on Cisco 1100 Integrated Services Router.
January 29, 2018	Key Features Not Supported in Cisco Virtual WLC section—Modified information about FlexConnect central switching.
November 24, 2017	Upgrading Cisco WLC Software Release section—Added note about change of filename format for Cisco Aironet 1700, 2700, 3700, and IW3702 AP software images and upgrade guidelines related to this change.

Modification Date	Modification Details
October 22, 2017	• Added Release 8.5.105.0 information. • Resolved Caveats section—Added CSCvf47808, CSCvg10793, CSCvg18366, CSCvg29019, and CSCvg42682.
October 16, 2017	Key Features Not Supported in Cisco Aironet 1800i, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800, and 3800 Series APs section—Added SIP snooping with FlexConnect local switching.
October 14, 2017	Upgrading Cisco WLC Software Release section—Added note about reintroduction of support for Dynamic WEP in Cisco Wave1 APs.
October 10, 2017	Key Features Not Supported in Cisco Virtual WLC section—Added Wired Guest.

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 8.5.105.0

Release 8.5.105.0 is a repost of Release 8.5.103.0 to address the caveats listed in the table below. There are no other updates in this release, all resolved and open caveats in addition to the five resolved bugs apply to this release.

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

Table 2: Resolved Caveats in Release 8.5.105.0

Caveat ID Number	Description
CSCvf47808	Cisco Wave 1 APs: Key Reinstallation attacks against WPA protocol
CSCvg10793	Cisco Wave 2 APs: Key Reinstallation attacks against WPA protocol

Caveat ID Number	Description
CSCvg18366	hostapd deleting client entry when client goes to FWD state in WCPD
CSCvg29019	AP18xx : Bypassed scan in returning to DFS channel after blocked-list timeout
CSCvg42682	Cisco Wave 1 APs: Additional fix for Key Reinstallation attacks against WPA protocol

What's New in Release 8.5.103.0

New Cisco WLC Support

The Cisco 3500 Series Wireless Controller is supported in this release. For more information, see:

http://www.cisco.com/c/en/us/support/wireless/3500-series-wireless-controllers/tsd-products-support-series-home.html.

New Access Point Support

The following new APs are supported:

- Cisco Aironet 1540 Series APs

  For more information about these APs, see:

  http://www.cisco.com/c/en/us/products/wireless/aironet-1540-series/index.html.

- Cisco Aironet 1815m and 1815t APs

  For more information about these APs, see:

  http://www.cisco.com/c/en/us/products/wireless/aironet-1815-series-access-points/index.html.

- Integrated Access Point on Cisco 1100 Integrated Services Router

  For more information about this AP, see:

  https://www.cisco.com/c/en/us/products/collateral/routers/1000-series-integrated-services-routers-isr/datasheet-c78-739512.html.

Access Point Extensions on Cisco Aironet 3800 Series APs

Access Point eXtensions (APeX) is a development framework to enable an ecosystem of expansion modules for Cisco Aironet 3800 Series APs.

The APeX Extender Module hardware development kit (HDK) enables developers to quickly prototype applications based on standard off-the-shelf development platforms. APeX HDK connectivity is currently supported in Cisco Aironet 3800 Series APs.

For more information, see: https://developer.cisco.com/site/apex/index.gsp.

Configuring the APeX Module (GUI)

1. Choose **Wireless** > **Access Points** > **All APs**.
2. Click the name of the Cisco Aironet 3800 Series AP.
3. Under the **Advanced** tab, check the **Override** and **External Module Status** check boxes to enable the APeX module.

Monitor Mode Support in Cisco Aironet 1540, 1560, and 18xx APs

Cisco APs collect RF channel information for various feature functions such as rogue detection, wIPS, and Cisco CleanAir. The APs in monitor mode do not transmit BSS serving Wi-Fi traffic. These APs are also excluded from the neighbor access list and RRM planning. In this release, support for monitor mode is added to the following Cisco Wave 2 APs:

- Cisco Aironet 1540 Series Access Points
- Cisco Aironet 1560 Series Access Points
- Cisco Aironet 1810 OfficeExtend Access Point
- Cisco Aironet 1810W Access Points
- Cisco Aironet 1815 Series Access Points
- Cisco Aironet 1850 Series Access Points
- Cisco Aironet 1830 Series Access Points

Note For information about other Cisco Aironet Wave 2 APs that support monitor mode, see http://cs.co/Wave2-AP-Feature-Matrix.

Mobile Concierge Support in Cisco Aironet Wave 2 APs

Mobile Concierge is supported in all Cisco Aironet Wave 2 APs.

Mobile Concierge is a solution that enables 802.1X capable clients to interwork with external networks. The Mobile Concierge feature provides service availability information to clients and can help them to connect available networks.

The services offered by the network can classified into two protocols:

- 802.11u MSAP
- 802.11u Hotspot 2.0

Cisco Spectrum Expert—Remote Sensor on Cisco Aironet Wave 2 APs

In Release 8.5, the Cisco Spectrum Expert remote sensor mode is supported in Cisco Aironet Wave 2 APs, using the Cisco CleanAir chipset.

Cisco Spectrum Expert monitors the RF spectrum used by a variety of wireless network and communications technologies, such as Wi-Fi (802.11) WLANs. Cisco Spectrum Expert consists of a hardware-based Spectrum

Sensor card and GUI-based Cisco Spectrum Expert Software, both of which provide complete visibility of the RF environment in which wireless network technologies operate. For more information about Cisco Spectrum Expert, see: http://www.cisco.com/c/en/us/support/wireless/spectrum-expert/tsd-products-support-series-home.html.

Dual Radio Parallel Redundancy Protocol Enhancement on WGB

The Dual Radio Parallel Redundancy Protocol (PRP) enhancement is the second phase of the PRP feature, which enables dual radio (2.4 GHz and 5 GHz) workgroup bridge mode on a WGB simultaneously. The WGB is wirelessly connected to the APs, with redundant packet transmissions over the dual 2.4-GHz and 5-GHz subsystem.

Support is also added for configuration of PRP functions on Cisco WLC via GUI.

For more information about this feature, see the Dual Radio Parallel Redundancy Protocol Enhancement on WGB section in the *Cisco Wireless Controller Configuration Guide*.

Dynamic Link Exchange Protocol Client Support on WGB

The Dynamic Link Exchange Protocol (DLEP) client support feature allows the WGB to report radio link metrics to a router. The WGB acts as the DLEP client, and the router acts as the DLEP server. Routing path selection is based on radio link quality metrics.

For more information about this feature, see the DLEP Client Support on WGB section in the *Cisco Wireless Controller Configuration Guide*.

Cisco IW3702 AP-Related Enhancements

- Support is added for Air Time Fairness on Cisco IW3702 AP in local and FlexConnect modes.
- Support is added for Cisco IW3702 AP as subordinate AP in Mobility Express solution.
- Support is added for configuration of Rx-SOP in Cisco IW3702 AP on Cisco WLC via CLI.

Cisco AP Serviceability Commands

In Cisco Aironet 18xx, 2800, 3800, 1540, and 1560 Series Wave 2 APs, the following new commands are introduced:

- **show controllers dot11Radio 1 antenna**—Displays last seen power (per antenna RSSI) with the radio port as input.
- **show controllers dot11Radio 1 client** *mac-address*—Displays information on what the client is doing in terms of rate selection and streams. Also, displays non-zero RX, TX, or TX-Retries (cumulative) packet count for each rate, stream, or width combination.

Support for Client-Aware Flexible Radio Assignment in Cisco Aironet 2800 and 3800 Series APs

Support is added for client-aware Flexible Radio Assignment (FRA) in Cisco Aironet 2800 and 3800 Series APs.

The Cisco Aironet 2800 and 3800 Series APs have the following radios:

- Flexible radio (2.4-GHz and 5-GHz band)
- Dedicated radio (5-GHz band)

Client-aware FRA serves these purposes:

- Client select—Sets the utilization threshold for redundant dual-band radios to switch from monitor mode to 5-GHz client-serving role.
- Client reset—Sets the utilization threshold for redundant dual-band radios to switch back from 5-GHz client-serving role to monitor mode.

The default percentage value for client select and reset is 50% and 5% respectively.

You can view the client-aware FRA details for an RF profile. To view the flexible radio assignment settings, use the **show advanced fra** command.

IPv6 Support in AP Plug-n-Play

Support is added for IPv6 in the AP Plug-n-Play (AP PnP) feature in the following APs:

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

For more information, see the *Wireless Plug and Play Deployment Guide* at: http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-technical-reference-list.html.

VLAN-Based Central Switching Support for Cisco Wave 2 APs in FlexConnect Mode

VLAN-based central switching is supported in Cisco Wave 2 APs operating in FlexConnect mode. When the Wave 2 APs are operating in FlexConnect mode, VLAN-based central switching allows VLANs to switch between local and central termination based on authentication, authorization, and accounting (AAA) attributes.

For more information about this feature, see the FlexConnect section of the *Cisco Wireless Controller Configuration Guide*.

Sofware-Defined Access Wireless

The Enterprise Fabric provides end-to-end enterprise-wide segmentation, flexible subnet addressing, and controller-based networking with uniform enterprise-wide policy and mobility. It moves the enterprise network from current VLAN-centric architecture to a user group-based enterprise architecture, with flexible Layer 2 extensions within and across sites.

For more information about this feature, see the Software-Defined Access Wireless chapter in the *Cisco Wireless Controller Configuration Guide*.

EoGRE Enhancements

Prior to Release 8.5, EoGRE tunnel gateway (TGW) failover was not classified as primary or secondary. From Release 8.5, it is possible for you to classify TGW-1 and TGW-2 as Primary or Secondary for failover purposes.

In a domain, the primary gateway is active by default. When the primary gateway is not operational, the secondary gateway becomes the active gateway. Clients will have to associate again with the secondary gateway. During and after failover, Cisco WLC continues to ping the primary gateway. When the primary gateway is operational again, the primary gateway becomes the active gateway. Clients then fall back on to the primary gateway. The same option is available for TGWs from FlexConnect in local switched mode. EoGRE tunnels can be DTLS-encrypted CAPWAP IPv4 or IPv6. This feature is supported on all Wave 1 and Wave 2 APs that are supported from Release 8.5.

Options are available to view detailed TGW statistics:

- Tunnel from Cisco WLC:
  - On the Cisco WLC GUI, choose **Controller** > **Tunneling** and under TGW list, click **Get Statistics**.
  - On the Cisco WLC CLI, use the **show tunnel eogre gateway statistics** command.
- Tunnel from FlexConnect APs:
  - On the Cisco WLC GUI, choose **Wireless** > **All APs** > **AP name** > **FlexConnect** > **Tunnel Gateway List** and click **Get Statistics**.
  - On the Cisco WLC CLI, use the **show ap eogre gateway statistics** *ap-name* command.

For more information about the EoGRE feature, see the Ethernet over GRE Tunnels section in the *Cisco Wireless Controller Configuration Guide*.

Cisco WLC Best Practices Updates

The following categories of Cisco WLC best practices have been added in the Main Dashboard of the Cisco WLC GUI:

- Apple Devices
- ISE RADIUS

Multicast-to-Unicast Support for Passive Client ARPs

Using this feature, you can enable Cisco 5520 WLCs to work with non-Cisco WGBs in multicast-to-unicast mode to route ARP traffic from the wired clients behind the non-Cisco WGBs to all the APs.

For more information about this feature, see the Information About Multicast-to-Unicast Support for Passive Client ARPs section in the *Cisco Wireless Controller Configuration Guide*.

AVC-Based Selective Reanchoring

Using this feature, you can reanchor client devices when they roam from one Cisco WLC to another. Reanchoring of client devices prevents depletion of IP addresses available for new clients in Cisco WLC.

Note Some client devices fail to reassociate with a Cisco WLC (with a new IP address), that they have roamed to from another Cisco WLC. These client devices do not release the old IP address and therefore do not reassociate with the Cisco WLC that they have roamed to.

For more information about this feature, see the Information About AVC-Based Reanchoring section in the *Cisco Wireless Controller Configuration Guide*.

Identity PSK

The Identity PSK (IPSK) feature supports the growing number of devices that are getting connected to the Internet and do not support the 802.1x security protocol. These devices can connect to the network using the WPA-PSK protocol.

Using the IPSK feature, you can easily and securely connect individual device or group of devices on the network with unique pre-shared keys.

IPv6 Support for CNAME

This feature enables the use of IPv6 addresses in the network for authentication of client traffic using Cisco WLC and external AAA server. You can add the FQDN of the IPv6 server in the pre-authentication access control list (ACL) in Cisco WLC so that the AAA server can allow or deny the requested traffic to a client.

For more information about this feature, see the CNAME IPv6 Filtering section in the *Cisco Wireless Controller Configuration Guide*.

Simplifying Cisco ISE Configuration on Cisco WLC - Phase 2

In phase 2 of simplifying Cisco ISE configuration on Cisco WLC, you have the option to apply the default Cisco ISE configuration for Cisco WLC so that you do not have to explicitly configure some of the settings required to use Cisco ISE. In Release 8.5, the default Cisco ISE configuration is applied in this additional scenario:

While mapping Cisco ISE-marked authentication server to a WLAN, the following security settings are applied:

- The Layer 2 security of the WLAN is set to WPA+WPA2
- 802.1X is the default AKM
- MAC filtering is enabled if the Layer 2 security is set to None

Note The Layer 2 security settings are either WPA+WPA2 with 802.1X or None with MAC filtering. It is possible to change these default settings if required.

For more information about phase 1 of simplifying Cisco ISE configuration, see *Release Notes for Cisco Wireless Controllers and Lightweight Access Points for Cisco Wireless Release 8.4.100.0* at http://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/crn84.html.

Software Release Types and Recommendations

Table 3: 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 4: Upgrade Path to Cisco WLC Software Release 8.5.10x.0

Current Software Release	Upgrade Path to 8.5.10x.0 Software
8.3.x.0	You can upgrade directly to Release 8.5.10x.0
8.4.100.0	You can upgrade directly to Release 8.5.10x.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

- The filenames of Cisco Aironet 1700, 2700, 3700, and IW3702 AP software images have been changed from ap3g2-x to c3700-x format. 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

- 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 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 5: 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-K9-8-5-105-0.aes	AIR-CT2500-AP_BUNDLE-K9-8-5-105-0.aes
Cisco 5508 WLC	AIR-CT5500-K9-8-5-105-0.aes AIR-CT5500-LDPE-K9-8-5-105-0.aes	AIR-CT5500-AP_BUNDLE-K9-8-5-105-0.aes AIR-CT5500-LDPE-AP_BUNDLE-K9-8-5-105-0.aes
Cisco WiSM2	AIR-WISM2-K9-8-5-105-0.aes	AIR-WISM2-AP_BUNDLE-K9-8-5-105-0.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 6: Test Bed Configuration for Interoperability

Release	8.5.103.0
Cisco WLC	Cisco 5508 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-WPA2-AES), 802.1X (WPA-TKIP-WPA2-AES) (LEAP, EAP-FAST)
RADIUS	ACS 5.3, ISE 2.2
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 7: 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
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 10.11.5
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 10
Apple iPad Pro	iOS 10
Samsung Galaxy Tab Pro SM-T320	Android 4.4.2

Client Type and Name	Version
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
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
Apple iPhone 6	iOS 10.2.1
Apple iPhone 6 Plus	iOS 10.2.1
Apple iPhone 6s	iOS 10.2.1
Apple iPhone 7	iOS 10.2.1
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

Client Type and Name	Version
Google Nexus 5X	Android 6.0.1
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 6.0.1
Samsung Galaxy S7	Android 6.0.1
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 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 8: 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 9: 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 10: 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 11: Open Caveats

Caveat ID Number	Description
CSCux97132	AP starts CAC timer after rolling back to lower bandwidth
CSCuy61155	802.11b inconsistent probe response - band select enabled - 2.4GHz
CSCuz59858	AP 3500(SC1), client association failure - R2H Buffer full
CSCuz72195	AP bridge does not forward BPDUs or VTP frames
CSCva58429	1532i low throughput (FlexConnect Local switching + EoGRE)
CSCvb57793	AP does not fragment EAP cert correctly
CSCvc78347	AP 1832 stops working in WLAN when voice traffic transmitted through
CSCvd06303	IPv6 ACL fails to block ICMP traffic
CSCvd12313	Wireless client fails to receive Multicast traffic when 802.1X is enabled
CSCvd42321	Cisco 1832 AP drops the CAC SIP 486 packet
CSCvd75447	PoE status on WLC GUI shows Power injector when it is powered via PoE.

Caveat ID Number	Description
CSCvd80240	FlexConnect AP sends associate response with wrong HT capabilities
CSCvd83486	IW3702UX will not join vWLC after 3+days
CSCvd86206	SNMP trapflag adjchannel-rogueap config not retaining during upload/download
CSCvd87515	CVE-2017-3732 OpenSSL Jan 2017 vulnerability patch for WLC
CSCvd90160	AP2800 sending announce as 0 in Reassociation response in FlexConnect Mode in FT and adaptive FT
CSCvd92528	Local policy ACL does not apply when intf group mapped to WLAN and DHCP addr assign is disabled
CSCve02456	EAP-TLS on Flexconnect-group local authentication is not working
CSCve06890	Randomly, Wave 1 APs can't send NDP Tx on all channels and can't be found as neighbors on nearby APs
CSCve13779	AP2802 Rogue Detection config changed back to "Enabled" after AP reboot
CSCve13886	WPS signature is getting disabled upon upload or download
CSCve18213	Foreign WLC leaks IPv6 and IPv4 multicast client traffic out of EoIP tunnel
CSCve18359	Observed traceback on AP 1570 when changing AP mode to FlexConnect from Flex+Bridge
CSCve24232	AVC profile showing incorrect characters for an entry after upgrade
CSCve27910	AP2700 local mode dropping CAPWAP SIP info request packets from CUCM when call-snooping enabled
CSCve28491	APs in Flex mode with interface configured to be trunk with multiple VLANs missing links to switch
CSCve31474	WGB HSR 802.11v neighbor report error message when Infrastructure MFP is enabled
CSCve33506	Client EAP-TLS handshake does not succeed with the Cisco 1830 AP
CSCve36498	Ascom phones stop transmitting voice durning call
CSCve45905	WLC does not perform DAD for IPv6 unicast address every time it is brought up on a network
CSCve45938	Cisco WLC does not transmit ICMPv6 parameter problem messages
CSCve45997	Cisco WLC does not transmit destination unreachable messages
CSCve47928	Cisco 8.5 release: AP is not joining the Cisco WLC after image upgrade
CSCve56404	Cisco 8.5 release: Cisco XOR radio configured to Sensor mode using GUI has operational state down

Caveat ID Number	Description
CSCve59671	Cisco WLC and ME: RADIUS fail-over does not work when retransmit timeout is not set to default value
CSCve62402	'config mesh link test' works only the first time attempt
CSCve63755	Cisco WLC running 8.4.100.0: Cisco APs fail to join the WLC if it has LSC enabled on it
CSCve65242	Cisco 702w AP radio resets with reason code 71
CSCve68039	Some APs cannot join the WLC because the WLC misrecognizes the number of APs
CSCve68787	Cisco AP is not transmitting out the de-auth frame over the air that was received from the WLC
CSCve72187	Micro-Macro transition configuration should be limited to within the defined range
CSCve75022	Cisco WLC does not apply QoS tag upstream from foreign to anchor
CSCve75515	Configuration backup shows the time instead of the NAT IP
CSCve77082	WLC sends accounting to all the accounting servers when AP is moved from standalone to connected
CSCve77722	WLAN in FlexConnect local switching drops NAC+802.1X and WPA2-PSK-WebAuth traffic on MAC filter fail
CSCve78416	Cisco 3700 AP: two instances radio d1 reset: FW: vec=33, macenb, cmd=0x16 seq=6, ev=40,
CSCve78449	Cisco 3700 AP: radio d1 reset: Tx jammed
CSCve81269	Clients failed to get connected to the Cisco AP in Flex mode with message as AID already in use
CSCve81314	Clients fails to connect to AID with message as All AID are in use when the AP is in Local mode
CSCve84906	Traceback observed in Cisco WLC while something is fetched for Flex ACL with AVC
CSCve87947	'Show run-config no-ap' is missing AP Group and RF profile configuration
CSCve89376	Cisco Wave1 APs sends RA periodically when EoGRE tunnel profile is added to the AP
CSCve89758	vWLC code download fails with HTTP mode
CSCve91597	Station Count field of QBSS LOAD IE has value per WLAN instead of per radio
CSCve92127	WLC Data plane reloads unexpectedly on DP core 0 due to WDT
CSCve95309	'WL_IOCTL_SET_MGMT_SEND failed for apr1v0 error Bad address' messages on AP followed by Radio reset

Caveat ID Number	Description
CSCve96310	Cisco WLC installs certificate without a password. However, WebAuthentication fails.
CSCve96480	IOS AP stopped working when it is changed from sensor mode.
CSCve97039	Cisco 3800 AP drops P2P information element after adding 802.11u or HotSpot support on a WLAN.
CSCve98689	Repeated CDP-4-DUPLEX_MISMATCH is observed when 1852 and 3802 APs are connected to 3850 switch.
CSCve98892	DNS lookup for RADIUS/TACACS fails because it is queried before the physical port is up
CSCve99416	CAP3500 radio 0 is getting reset due to FST 24 and RST 71
CSCve99696	CPU ACLs are missing after the WLC reload.
CSCve99763	MAP2s experience roaming issues with DFS Channels
CSCvf01368	Evaluation of click-ap for Expat June 2017
CSCvf01433	The 1852 AP fails to send multicast packets to wireless.
CSCvf01576	Cisco 3504 WLC is not generating a crash file.
CSCvf02493	AIR-CAP3602I with AIR-RM3000AC-A-K9 External module containing itself
CSCvf02678	WPS signature is getting disabled upon upload or download
CSCvf02705	The IP-SGT binding is removed from SXP peer after a WLC redundancy switchover.
CSCvf02709	Cisco vWLC is not pushing Flexconnect ACL after the AP rejoin.
CSCvf03024	The power constraint value is advertised as 3, though it is configured as 0.
CSCvf05427	Cisco 2800/3800 AP cannot use the RX-SOP
CSCvf07775	Cisco 2800/3800 AP - Kernel panic FIQ or NMI - Panic in click
CSCvf07776	Cisco 2800/3800 AP - FIQ stopped working due to firmware core dump loop
CSCvf09168	Kernel panic is visible on Cisco 1542 MAP APs
CSCvf10157	Wism stopped working with emWeb in 8.5.1.183 build
CSCvf12728	Cisco 7510 WLC stopped working in SNMP task with no traceback
CSCvf15434	Traceback Message queue APF LBS task is nearing full *osapiBsnTimer when CPU ACLs are added
CSCvf15789	WLC stopped working due to reaper reset at SNMPTask while PI syncs configurations from Cisco 5508 HA

Caveat ID Number	Description
CSCvf15991	Client data traffic drops when AAA override and link-local-bridging are enabled due to timing issue
CSCvf16153	Active WLC crashed with Task Name: SNMPTask
CSCvf16302	Flash corruption issue is observed on flex mode
CSCvf16629	The OUI string updates properly in Cisco 5508 WLC but disappears after a reboot
CSCvf16842	Tunnel Gateway (TGW) in Cisco 3802 AP comes up only after the Heartbeat interval expires
CSCvf17085	The radio of Cisco 3800 series AP stopped working after an image reload.
CSCvf17488	After an upgrade to 8.4.100.0, the Cisco 5520 WLC reloads unexpectedly atleast once a day
CSCvf18230	WLC Data Plane (DP) stopped working due to DP buffer shortage (CP detected)
CSCvf18363	Kernel panic stopped working in Cisco 1542 AP
CSCvf18505	When WLC adaptive/fastlane is disabled, the CCX IE is missing in probe response Wave 2 APs
CSCvf19891	Cisco 3800 and 2800 series APs stopped working when an SKB from Linux host was freed twice.
CSCvf20089	AP adder license is taking effect only after a reboot on the Cisco 3504 WLC.
CSCvf21673	Cisco 2800/3800 APs send ACK packets using disabled data rates
CSCvf22104	Identity PSK does not work when order of PSK mode and PSK key are interchanged
CSCvf22185	In Cisco 2800/3800 and Cisco 1562 APs, the Watchdog reset is observed (capwapd stopped working)
CSCvf22867	The Wireless LAN Controller stopped working while fetching the WLAN LDAP entry
CSCvf23929	Neighbors are visible on the AP but the WLC cannot view the AP neighbors
CSCvf23943	FRA is impacted when AP 3800 modules (like AIR-RMVBLE2) are in use
CSCvf24890	Cisco 2702 APs stopped working with process terminated on watchdog timeout
CSCvf25055	Cisco 2700 series APs are not accepting FlexConnect ACL when added to a flex-group
CSCvk44249	WLC 5508 - foreign mapping is missing on a WLAN when restoring a backup

Resolved Caveats

Table 12: Resolved Caveats

Caveat ID Number	Description
CSCuc78713	dWEP client cannot receive broadcast after broadcast key rotation
CSCuq12202	Enable global TCP-MSS of 1250 bytes as default config
CSCux92335	Cisco 3602 APs running on Cisco 8.0.120.0 release is losing MAC address
CSCuy75333	Cisco 2504 config restoration failure due to multicast mode command
CSCuz19004	Radio Resets on 702w
CSCuz33090	Cisco 3802 AP - antennas supported is always 4 in VHT Capabilities IE
CSCva37010	Invalid staid XXX received
CSCva87833	AIR-CT8510-K9 stopped working; SSO disabled
CSCvb27851	Need option to collect support bundle in Wave 2 APs
CSCvb68240	Need command to view port speed/duplex on 2800/3800 CLI
CSCvb68260	Translate output of show lacp internal/neighbor command on AP3800 to make sense
CSCvb71347	WLC multicast config not coherent for code upload/download
CSCvb86237	8510 WLC stopped working Task Name: TempStatus
CSCvb96299	AP3700 FlexConnect Mode gets error on console for OSEN WLAN
CSCvc06547	AP retransmits packet even though client sends ACK
CSCvc07274	3800 and 1562 association SS error between Beacon and Association Response
CSCvc18786	WLC stops working during multiple login sessions either with local user or with TACACS+
CSCvc24104	Rx-SOP threshold failed to set with AP model 1852/1700/1815/1830
CSCvc24917	Defect of msglog corresponding to 'AP Message Timeout: Max retransmissions reached on AP …'
CSCvc28035	clDLApBootTable shows blank when WLC has 2800I AP
CSCvc30828	AP does not allow world mode to be set via GUI on 15.3(3)JD
CSCvc30941	AP stats are not reflected correctly on WLC
CSCvc31551	IR829/AP803: uWGB cannot pass traffic downstream
CSCvc34930	Receiving DELETE_MOBILE, deleting client entry, but not sending any deauth to client

Caveat ID Number	Description
CSCvc35151	AP radio reset happens multiple times without trigger
CSCvc36788	AP (1810/1815) stopped working: [watchdog reset(capwapd)] due to LSC not found.
CSCvc37210	Remove the debug pm ikemsg command
CSCvc39213	Unable to delete IPsec profile from SNMP
CSCvc40668	WLC stops working while disabling Office-Extended mode on APs
CSCvc42008	'AP Time Sync Failure' remained on CLI and GUI though it is removed
CSCvc46002	TrustSec: WLC SXP version fails to sync to standby WLC
CSCvc47777	'AP Time Sync Failure' remained on CLI and GUI though it is removed
CSCvc47854	Expiry of User Idle timeout kicks in two dissoc with different reason code
CSCvc50390	AP1850 seems to work with 3x3 MIMO for 2.4GHz radio
CSCvc51666	IOS AP transmits on disabled rate 24Mb
CSCvc55430	WLC HA redundancy management interface not reachable for a short time after failover
CSCvc56757	WGB HSR 11v neighbor report validation fails when Infrastructure MFP is enabled
CSCvc56873	With 3800/2800 APs, AVC works only for existing WLAN and not for new WLAN when AVC enabled
CSCvc61795	IP call setup fail after L3 handover happens during call among 1832
CSCvc66547	CPU ACL configured to block access to Virtual IP does not work as expected
CSCvc67316	3800 - Kernel Panic - PC is at memzero+0x24/0x80
CSCvc69177	"Failed to add IPSec rules for trap receiver, Message Queue full" msg on disabling trapreceiver
CSCvc70819	GUI: Could not configure Global multicast mode for 7500 WLC image
CSCvc71537	WLC profiles 7925 incorrectly
CSCvc72724	8510 AP SSO stopped working on portalProcessLogout
CSCvc78857	AVC profile is not applied on client behind WGB.
CSCvc83861	Traceback seen after standby WLC reboot.
CSCvc84474	ISE Endpoint Purge not working on Foreign-Anchor setup
CSCvc84637	1810W sending invalid AC_NAME when WLC hostname is 31 bytes long
CSCvc85158	AP Group configs not retaining during upload and dowlnoad config.

Caveat ID Number	Description
CSCvc87347	Guest LAN MIB CISCO-LWAPP-DOT11-CLIENT-MIB::cldcClientLoginTime does not match system uptime
CSCvc87461	cldcSleepingClientRemainingTime shows incorrect remaining time for the sleeping client
CSCvc87661	constituent OID cldcClientAuthMode not present in the trap ciscoLwappDot11ClientKeyDecryptError
CSCvc89400	Trap ciscoLwappDot11ClientStaticIpFailTrap shows incorrect client IP address
CSCvc89599	cLGuestUserBytesReceived/ cLGuestUserBytesTransmitted are always zero byres
CSCvc91784	bsnDot11StationAssociateFail trap reason code 102 is not in MIB defined enum values
CSCvc92070	Allows direct routing to AP IP address from client WLANs with FlexConnect local switching.
CSCvc93373	Trap bsnAuthenticationFailure shows usertype as wlanuser for mgmt user login fail
CSCvc93377	Tracebacks and MFP queue logs filling up the msglog on WLC.
CSCvc96076	Cisco WiSM2 HA - standby stopped working with task name spamApTask2 in ideal state
CSCvc97727	HA traps dumps junk data for cLHaBulkSyncCompleteEventStr, and cLHaPeerHotStandbyEventStr OIDs
CSCvc99151	Traceback seen in message log when invalid-config command is executed
CSCvc99237	Cisco Wave2 AP retransmits Heartbeat 3 times more than configured value
CSCvd00629	Dashboard UI rogue AP after navigating to 2.4-GHz AP pages, the 5-GHz APs are not seen
CSCvd02236	cLApDataEncryptionStatus shows wrong enum value '0' for link encryption disabled
CSCvd02303	Flex-Bridge AP stopped working while joining the Cisco WLC
CSCvd02506	bsnDot11StationAssociate trap is sent twice on association with 802.1x WLAN
CSCvd04251	ciscoLwappApMonitorModeChangeNotify trap shows value not present in the defined MIB
CSCvd06084	Assisted roam prediction list displays the RAD ID of the AP in the client detail output
CSCvd06644	**show advanced 802.11a/b channel** DCA restart countdown is not consistent
CSCvd08816	Message dump in standby WLC while enabling the AP multicast mode to Unicast mode
CSCvd09507	Rogue rule substring-ssid turns invalid on WLC when user configured SSID is included in PI template

Caveat ID Number	Description
CSCvd09699	Cisco 2800, 3800 AP: capwap ap erase all should default to apmac#
CSCvd13371	Some configuration change on a WLAN causes the radio to reset
CSCvd13520	**show dot11 clients** shows local mode when AP is in FlexConnect mode
CSCvd16170	Cisco AP sending incorrect AKM in FT authentication response in Flex Mode with adaptive FT
CSCvd16189	802.11ac UI : Changing 802.11a antenna type shuts the 802.11ac radio
CSCvd16346	WLC memory corruption occurs when TACACS+ responds with unknown attributes
CSCvd16386	TrustSec: GUI does not clear the number of RBACL when policy download is in failed state
CSCvd16800	Client associated to MAP does not get AAA override in Flex+Bridge mode
CSCvd18744	PMK keys are not plumbed to all APs in the flexgroup when one of the AP reloads
CSCvd20158	Cisco 1562D AP: incorrect antenna type displayed on WLC GUI and CLI
CSCvd22342	Cisco WLC caps the traffic as per QoS WLAN policy instead of applying exception
CSCvd22402	WLAN-VLAN mapping is not removed after deleting WLAN
CSCvd22506	TrustSec: AP SXP connections does not give the correct value on WLC
CSCvd23185	WGB wired clients not seen by WLC
CSCvd23301	WLC GUI trapflags for client association with statistics does not display correct configuration
CSCvd23533	ciscoLwappDot11ClientMovedToRunStateNewTrap shows IP address reversed for cldcClientAnchorAddress
CSCvd23864	cldcClientTrapEventTime has wrong type set in the trap ciscoLwappDot11ClientAssocTrap
CSCvd23902	Cisco 1532AP: root bridge drops packets from non-root bridge in non-native VLAN
CSCvd26885	Unit of probe suppression hysteresis should be 'dB'
CSCvd27365	Cisco WLC reports incorrect number of clients associated on the AP
CSCvd27398	WLC management access stops working while WLAN services are still up
CSCvd28374	Cisco 802AP incorrect base radio MAC assigned not ending with zero results in only one BSSID support
CSCvd30950	Cisco 8.4: Flex.LSCA Clients(5/100) held in dot1x when linktropy with 1Mbps or 100Mbps BW is enabled

Caveat ID Number	Description
CSCvd31705	AP: Offchannel cleanup in IRQ context can trigger an indefinite loop if sensorD owns the radio
CSCvd34785	Mobility multicast IP address reverse in TACACS+ packets
CSCvd35701	Cisco 3800, 2800 APs: not enforcing WLAN WFD policy
CSCvd36190	Cisco 5520 WLC stopped working with taskname haSSOServiceTask6
CSCvd37031	Consolidated GUI issue for 802.11r + 802.11w
CSCvd37522	**show run-config** commands: incorrect index numbers for RADIUS Accounting Servers
CSCvd40203	Cisco 3700AP FlexConnect reloads unexpectedly with FT or adaptive FT roaming with Iphone6s plus+WGB
CSCvd40978	Cisco Wave2 APs (Cisco AP2800, 3800, 1850 APs) falsely show 100% channel utilization
CSCvd42172	Mobility: PMK cache is not getting updated after roaming the client from Anchor to Local
CSCvd42669	Cisco 2500 WLC stopped working
CSCvd43327	'%APF-3-UNKNOWN_RADIO_TYPE: [PS]apf_utils.c:549 Unknown Radio Type 0' message in standby WLC
CSCvd44909	Client traffic dropped in Anchor foreign AirOS setup with new-mobility if foreign client behind NAT
CSCvd45504	CHDM: no traplog noticed for client who has detected coverage hole
CSCvd45744	Customer reports that AP reboots after 4 hours while doing site survey
CSCvd46374	Client with lower signal strength than the Rx-SOP threshold was able to connect radio
CSCvd47347	cLMobilityGroupMemberGroupName accepts more than 31 characters
CSCvd48852	Audit-Session-ID information is missing after re-authentication
CSCvd52760	WLC stopped working with task spamApTask3
CSCvd55938	Client fails to pass traffic after 802.11r roaming with 802.11w set to optional
CSCvd56588	In 2800 and 3800 series APs, incorrect RSSI values are displayed when client associates to XOR radio
CSCvd58651	AKM is not syncing up from flex local auth AP to WLC after client connectivity for PMF WLAN
CSCvd59293	Unable to enable gateway proxy on AAA using CLI
CSCvd60923	Mobility keep-alive statistics are not getting displayed in the show command output

Caveat ID Number	Description
CSCvd61468	Custom mDNS profile is not saved on the WLAN config after the reboot
CSCvd62568	XML validation is failing for the AVC profile
CSCvd63067	Client Auth state is showing wrong info in the **show client summary security** command output
CSCvd65441	Revision timestamp is incorrect for MIBs: CISCO-LWAPP-TUNNEL-MIB.my and CISCO-LWAPP-PMIP-MIB.my
CSCvd67374	Consolidated Accounting and Authentication statistics issue is observed
CSCvd67730	Client fails PSK SSID authentication after primary AP reboot (EAPOL M3 not sent on 4-way handshake)
CSCvd68141	WLC stopped working at task nmspRxServerTask
CSCvd68412	Wireless client Rx statistics are not getting updated
CSCvd68441	The "config network multicast l2mcast disable <interface>" config is not blocking L2 mcast traffic
CSCvd68510	Memory utilization in Mobility Express primary AP (with CMX unreachability) is increasing
CSCvd68648	cLApWlanStatsOnlineUserNum is not updated with the number of online users
CSCvd72064	GUI does not show the active accounting servers
CSCvd72131	Cisco 7500 WLC in flex-mode stopped working after the SNMPTask Reaper reset
CSCvd75965	AP sends deauth to iPhone leading to 11r roaming failure while doing continuous roaming using JFW
CSCvd76189	Client is stuck in DHCP_REQD on flex AP with a WLAN mapped to VLAN 1
CSCvd76773	Antenna Gain on 2.4Ghz Radio resets to default after 3800 E AP reboot
CSCvd76783	Daisy Chain RAP takes a long time to switch from MAP to RAP mode
CSCvd78452	APs joining the WLC in flex-mode fails to use the flex ACLs in the group policies
CSCvd78655	RAP to MAP linktest for 1562 APs are showing -ve percentage
CSCvd79416	In and Out counters for LAN port and clients connected via switch are reset after a few seconds
CSCvd79464	APs with WiSM module are sending RRM data every 5 seconds for each radio
CSCvd79745	Clients are failing authentication when using Layer 2 and Web-Auth on MAC failure on the same WLAN
CSCvd80508	LAN ports of the 1810W AP are stuck on Admin-Down after modifying RLAN settings

Caveat ID Number	Description
CSCvd84229	WLC is wrongly reporting 4SS HT rates for 1852 AP in 2.4-GHz band
CSCvd84773	WLC stopped working due to nmspRxServerTask
CSCvd85691	SNMP get on device for indices of bsnMeshNeighsTable returns no data
CSCvd86566	Client with incorrect NAI realm gets Access-Accept from Radius Server
CSCvd90110	2800 series APs are sending incorrect AKM in reassociation response in Flex Mode with adaptive FT
CSCvd90377	WLC is applying wrong ACL to clients when doing CWA
CSCvd96678	Vocera B3000N badge is failing to associate with 3800 and 2800 series APs when 11r is enabled
CSCve02210	SNMP OID that is used to monitor WLAN status for FT is returning wrong results
CSCve02585	Webauth login page is not showing up after enabling TLS1.2 on WLC
CSCve02612	HA-Config sync fails on standby when flex AP configs are modified
CSCve02679	VMs with Bridged Mode NIC on wireless client fails to get IP address
CSCve02689	Silent reboot is observed after the memory usage goes up to 85%
CSCve05507	Retransmit configuration is not reflected when new 1800, 2800, and 3800 series APs join the WLC
CSCve07597	eping gives an EOIP ping response even when motility peer IP is not provided
CSCve07912	WLC stopped working at peap_inner_method_callback
CSCve11523	Client count reported by AP is incorrect
CSCve13879	In FlexConnect, IP NAT translation is not happening with local split tunneling
CSCve15860	WLC data plane is not responding to capwap-data keep-alive
CSCve17406	The **show client detail** *mac-address* CLI output shows gateway/netmask of Flexconnect AP client as unknown
CSCve19429	1852 Mobility Express stopped working due to "radio failure (firmware crash)"
CSCve20123	Corrupt voice packets are observed when a client with an active call does an inter-AP roam
CSCve23581	2800 and 3800 series APs sends multicast data with AES when client is TKIP
CSCve24587	Client reconnect issue on MAC filter failure
CSCve24687	Channelization issue occurs when Cisco 3802 AP reverts to channel 36 for 75% of APs at a site

Caveat ID Number	Description
CSCve24871	Flex ARP responds for wired clients
CSCve25007	Target assert radio stopped working in Cisco 1830 AP
CSCve26935	Cisco 2800/3800 AP displays low throughput for IPv4 TCP with Windows 10 Creator
CSCve26948	When Cisco 2800/3800 AP boots up, the CAPWAPd stops working resulting in a watchdog reset (wcpd)
CSCve26976	Cisco 2800/3800 AP stops working with FIQ/NMI as block_all function interrupts all the Click tasks
CSCve27052	APs display public IP address on the Cisco 5500 WLC GUI and private IP address on the AP CLI
CSCve31989	WLC stops working due to apfRogueTask
CSCve32279	Cisco 2800/3800 AP displays incorrect security fields when scanned
CSCve35431	Downstream QoS 802.11 UP marking does not work for Flex AVC profile
CSCve36706	AP cannot clear the client Exclusion list after an Exclusion timeout
CSCve37579	Cisco 3800 AP stops working due to WIPS kernel panic
CSCve37770	Cisco 5508 WLC stops working with 8.3.102.0 when AP's radio CLI command is executed
CSCve37819	Cisco WLC running 8.3.121.0 release fails to classify the Samsung Galaxy S7 running Android 7.0
CSCve38070	Cisco 2800/3800 AP reports false 100% channel utilization
CSCve38191	Duplicated SSID after WLC fallback causes disconnection issues and traffic drop in Cisco 3800/2800AP
CSCve40462	Inspite of ACM being globally enabled, the ACM is disabled in the probe response from Cisco 1832 AP
CSCve42311	Cisco 3800 AP experiences kernel panic due to double free in wireless driver during radio coredump
CSCve43860	Cisco 3802 AP stops working due to kernel panic with exception stack values
CSCve45744	Cisco 1850 AP stops working due to memory leak in slab SUnreclaim
CSCve47790	Cisco 1800 APs on 8.2 falsely shows 100% channel utilization
CSCve49741	Cisco WLC fails to send SFTP and FTP when using untagged interfaces on different ports
CSCve50284	XOR radio flaps and goes down after an RF profile is applied
CSCve54948	WCP detects incorrect beacons stuck in Cisco 3800 AP running 8.3 release

Caveat ID Number	Description
CSCve55044	Cisco WLC Dataplane stopped working due to CAPWAP fragment buckets being full
CSCve55604	Cisco 3702 APs fail to download their image after joining Cisco 8510 WLC
CSCve56580	Cisco 3800 AP stopped working
CSCve59097	Cisco WLC stopped working while configuring the SNMP MIB OID
CSCve61049	Radio resets in Cisco 2700 AP
CSCve61390	Multiple kernel panics occur in Cisco 1852 AP
CSCve62065	XOR radio marked redundant stays in 2.4 GHz band
CSCve62472	PMIPv6 client does not get the IP and binding update packet request goes via redundancy management
CSCve63497	Cisco WLC stops working with Task Name emWeb when timer changes
CSCve63800	Prime Infrastructure does not show all WLANs when querying MIB bsnAPGroupsVlanMappingSsid
CSCve64152	Cisco WLC stopped working while deleting the rogue client entry
CSCve65330	Observed F/W dump on Cisco 3802 AP
CSCve65397	Kernel panic occurs in Cisco 3800 AP due to double free in wireless driver
CSCve66007	Cisco 8540 WLC stops working with Task Name emWeb
CSCve66630	Clients cannot connect to Cisco 3800 AP when configuring TKIP only WLAN and PSK with central auth
CSCve66819	Cisco 2800/3800 AP stopped working due to FIQ or NMI reset
CSCve68194	AP's 2.4-GHz or 5-GHz interfaces are down and do not come up although the hyperlocation interface is up
CSCve72299	Cisco 3802 APs detecting and containing own BSSID as Rogues are classified as Malicious
CSCve76202	WLC IPv4 CPU ACL is applied as IPv6 CPU ACL during backup recovery or SSO failover
CSCve78942	Cisco 2802 AP stopped working due to kernel panic
CSCve84130	Cisco 3802 AP stops working with kernel crash in WIPS code
CSCve85947	Cisco 1815 AP POE LAN allows the CDP power requirement to pass and resets the switch port for reboot
CSCve86609	Dynamic interface default gateway must not be configured to "0.0.0.0" in CLI
CSCve90085	Active WLC in HA pair crashes with task apfRogueTask_0

Caveat ID Number	Description
CSCve96101	RLAN client drops from the WLC when radio b change channel or power level
CSCvf03782	WLC stopped working on emWeb with "ewaFormSubmit_file_upload" in stack
CSCvf09458	Cisco 2800/3800 series XOR radios are not moving to 5GHz or Monitor mode
CSCvf09581	Samsung S8 not able to stay associated with 11v Enabled on Click AP
CSCvf47808	Cisco Wave 1 APs: Key Reinstallation attacks against WPA protocol
CSCvg10793	Cisco Wave 2 APs: Key Reinstallation attacks against WPA protocol
CSCvg18366	hostapd deleting client entry when client goes to FWD state in WCPD
CSCvg29019	AP18xx : Bypassed scan in returning to DFS channel after blocked list timeout
CSCvg42682	Cisco Wave 1 APs: Additional fix for Key Reinstallation attacks against WPA protocol

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.