Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.4.100.0

First Published: 2017-05-19

Last Modified: 2019-05-16

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*.

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Revision History

Table 1: Revision History

Modification Date	Modification Details
August 23, 2018	Open Caveat—Added CSCvk44249
July 24, 2018	Added the CIMC Utility Upgrade for 5520 and 8540 Controllers section.
January 29, 2018	Key Features Not Supported in Cisco Virtual WLCs section—Modified information about FlexConnect central switching.
October 16, 2017	Key Features Not Supported in 1560, 1810 OEAP, 1810W, 18915, 1830, 1850, 2800, and 3800 Series APs section—Added SIP snooping with FlexConnect in local switching mode
October 10, 2017	Key Features Not Supported in Cisco Virtual WLCs section—Added Wired Guest and FlexConnect central switching
June 02, 2017	What's New in This Release section—Added - Important Upgrade Information for 2500 Series Controllers

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 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 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 in Cisco 2504 WLCs.

- 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 1810 Series OfficeExtend Access Points
- Cisco Aironet 1810W Series Access Points

- Cisco Aironet 1815i and 1815w 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
- Cisco ASA 5506W-AP702
- Cisco Aironet 1530 Series Access Points
- Cisco Aironet 1550 Series Access Points with 128-MB memory

Note Cisco 1550 APs with 64-MB memory are not supported starting with Release 8.4.100.0.

- 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 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 8.4.100.0, you must upgrade the software in the Cisco 800 Series ISRs to Cisco IOS 15.1(4)M or later releases.

In Release 8.4, the following APs are not supported:

- Cisco Aironet 600 Series OfficeExtend Access Points

- Cisco Aironet 1550 Series Access Points with 64-MB memory
- Cisco Aironet 1040 Series Access Points
- Cisco Aironet 1140 Series Access Points
- Cisco Aironet 1260 Series Access Points

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 This Release

Cisco Umbrella WLAN

The integration of Cisco Umbrella WLAN and controller provides web classification and security for clients connecting to controller. Key differentiators involve granular web classification and reporting by WLAN, user role, and location. This feature is supported on these controllers: 2504, 5508, 5520, 8510, 8540, and WiSM2.

For more information, see the Cisco Umbrella WLAN section in the configuration guide.

Domain-Based Access Control Lists

Domain-based ACLs allow administrators to define domain access control list (ACL) to allow or disallow traffic. This additional level of security is added to the Cisco Wireless solution to allow you to put a specific set of domains in a blocked list or an allowed list.

Domain-based ACL extends the ACL from Layer 3 IP to domain-based ACL. This feature is supported on Cisco 5520 WLCs and Cisco 8540 WLCs, can have up to 64 ACLs, with each ACL supporting 100 rules.

For more information, see the Domain-based Filtering section in the configuration guide.

Simplifying Cisco ISE Configuration on Controllers

This is an option that is provided to apply the default Cisco ISE configuration for controller so that you do not have to explicitly configure some of the settings required to use Cisco ISE.

You can apply the default Cisco ISE configuration in the following scenarios:

- When you configure a RADIUS authentication server, and in the process enable the default Cisco ISE settings, the following configurations are applied:
  - CoA is enabled by default.
  - The authentication server details (IP and shared-secret) are also applied to the accounting server.
- When you configure the AAA server to override the use of default servers on a WLAN, and in the process enable the default Cisco ISE settings, the following configurations are applied:
  - When you add the authentication server for a WLAN, the authentication server details are also applied to the accounting server for the WLAN.

Note Change on Authentication server back to *None* is not applied on the accounting server.

- AAA override is enabled by default.
- The NAC state is set to ISE NAC by default.
- DHCP profiling and HTTP profiling are enabled by default, for RADIUS client profiling.
- Captive bypass mode is enabled by default.

- When you configure the Employee Network as part of the initial setup using the Cisco WLAN Express Setup method, and in the process enable the default Cisco ISE settings, the following configurations are applied:
  - CoA is enabled by default.
  - The authentication server details (IP and shared-secret) are also applied to the accounting server.
  - When you add the authentication server for a WLAN, the authentication server details are also applied to the accounting server for the WLAN.
  - AAA override is enabled by default.
  - The NAC state is set to ISE NAC by default.
  - DHCP profiling and HTTP profiling are enabled by default, for RADIUS client profiling.
  - Captive bypass mode is enabled by default.

Cisco TrustSec Enhancements

Cisco TrustSec enables organizations to secure their networks and services through identity-based access control to anyone, anywhere, anytime. The solution also offers data integrity and confidentiality services, policy-based governance, and centralized monitoring, troubleshooting, and reporting services. You can combine Cisco TrustSec with personalized, professional service offerings to simplify the solution deployment and management, and is a foundational security component to Cisco Borderless Networks.

- SXP—From Release 8.4, SXPv4 is supported in FlexConnect mode APs.
- PAC Provisioning and Device Enrollment—Any device that participates in a Cisco TrustSec network must be authenticated as a trusted device. To facilitate the authentication process, new devices connected to a Cisco TrustSec network undergo an enrollment process, wherein a device receives the credentials that are specifically needed for the device's authentication along with general Cisco TrustSec environment information.

  Controller device enrollment is initiated by controller as part of Protected Access Credential (PAC) provisioning with the Cisco ISE server. Controller initiates EAP-FAST and gets a PAC. This is accomplished by using the infrastructure of LOCAL-EAP EAP-FAST PAC provisioning. The PAC that is obtained uniquely maps to the device ID. If the device ID changes, the PAC data associated with the previous device ID is removed from the PAC store. PAC provisioning is triggered when a RADIUS server instance is enabled to provision the PAC.

- Environment Data—Cisco TrustSec environment data is a set of information or attributes that helps controller to perform Cisco TrustSec-related functions.
- Inline Tagging—Inline tagging is a transport mechanism using which a controller or a Cisco AP understands the source SGT.
- SGACL—You can control the operations that users can perform based on the security group assignments of users and destination resources, using the Security Group Access Control Lists (SGACLs). Policy enforcement in a Cisco TrustSec domain is represented by a permission matrix, with the source security group on one axis and destination security group numbers on the other axis. Each cell in the matrix body contains an ordered list of SGACLs, which specifies the permissions that must be applied to packets originating from the source security group and destined for the destination security group. When a wireless client is authenticated, it downloads all the SGACLs in the matrix cells.

For more information, see the Cisco TrustSec section in the configuration guide.

Cisco Virtual Wireless Controller N+1 High Availability

Support is added for High Availability (HA) with N+1 in Cisco Virtual Wireless Controller (vWLC).

HyperV Support for Cisco Virtual Wireless Controller

Support is added for Cisco vWLC in Hyper-V hypervisor. Cisco vWLC is now supported in any x86 server with VMware Hypervisor ESXi4.x, 5.x, and 6.x as well as KVM and Hyper-V.

EoGRE Enhancements

- Wave 1 APs (AP1600, AP1700, AP2600, AP2700, AP3600, and AP3700)—Added EoGREv6 tunnel support from FlexConnect+Local switching AP to gateway.
- Wave 2 APs (AP1560, AP1810, AP1815, AP1830, AP1850, AP2800, and AP3800)—Added EoGREv4 and EoGREv6 tunnel support from FlexConnect+Local switching AP to gateway.
- Path MTU discovery is supported in FlexConnect APs.

For more information, see the Ethernet over GRE Tunnels section in the configuration guide.

Cisco Aironet 1815i and 1815w Access Point Support

Cisco Aironet 1815i and 1815w Access Points are supported. For more information, see

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

IPv6 Support on Wave 2 Access Points

Support is added for infrastructure and native IPv6 functionality in Cisco 802.11ac Wave 2 Access Points.

FlexConnect Support on Wave 2 APs

Support is added for FlexConnect functionality in Wave 2 APs for these features:

- Proxy ARP—AP acts as an ARP proxy to respond to ARP requests on behalf of wireless clients.
- NAT/PAT—AP supports NAT and PAT for central DHCP.

- AAA QoS Override per Client—Clients can assign QoS profile based on AAA.

Mesh Enhancements

- Mesh mode and Mesh Ethernet Bridging is now supported in Cisco Aironet 1560 Series Access Points. For more information, see

  http://www.cisco.com/c/en/us/support/wireless/aironet-1560-series/tsd-products-support-series-home.html.

- Air Time Fairness (ATF) in 802.11ac Wave 1 APs in mesh mode allows you to regulate radio resources for mesh networks.

Support for Remote LAN on Wired ports of Cisco Aironet 702W APs

Support is introduced for remote LAN in wired ports of Cisco Aironet 702W APs.

For more information, see the RLAN Support for Wired Ports on Cisco Aironet 702w APs section in the configuration guide.

Support for VLAN on AUX ports of Cisco Aironet 2700 APs

Support is introduced for non-native VLAN in CAPWAP tunneled and non-tunneled mode in Cisco Aironet 2700 APs.

Support for Cisco Hyperlocation in High Availability Environment

Cisco Hyperlocation is supported in a High-Availability environment. The global and per AP group hyperlocation configuration is mirrored from the active controller to the standby controller. The standby controller updates only the internal state and does not forward any configuration information to the Cisco APs.

For Cisco MSE message encryption, the controller generates an encryption key and sends it to the Cisco APs and to the Cisco MSE, which uses it for encryption and decryption as end clients. The standby controller does not generate an encryption key and the Cisco APs and the Cisco MSE use the actual key shared by the active controller.

Guest User Management (Client Whitelisting)

This feature prevents unauthorized access of the network. Using this feature, users with read and write or lobby administrator privileges can control which clients can access the network. The administrators can filter the clients based on the client MAC address and group them to provide access to the network.

For more information, see the Client Whitelisting section in the configuration guide.

WeChat Authentication

Added support for the WeChat application for easy Wi-Fi connectivity, using QR-code scanning for redirection or captive portal redirection.

For more information, see the FlexConnect AP Easy Admin and WeChat Authentication-Based Internet Access sections in the configuration guide.

LAG in Transition

A controller that supports link aggregation (LAG) can go into a LAG-in-Transition (LAT) mode during transition between LAG to non-LAG mode or vice versa. The transition is complete only when controller is rebooted. In LAT mode, you can make configuration or interface changes and also revert to the previous LAG mode. After controller is rebooted, your configuration might get lost or you might encounter a system failure. However, from Release 8.4, it is possible to prevent such incidents by restricting interface-related configuration changes when controller is in LAT state.

Parallel Redundancy Protocol Enhancement on AP and WGB

Cisco Wireless Release 8.4 provides the Parallel Redundancy Protocol (PRP) enhancement to improve wireless network availability for wired clients behind Workgroup Bridge (WGB), and improve the roaming performance by allowing wired clients to have dual wireless connections.

For more information, see the Parallel Redundancy Protocol Enhancement on AP and WGB section in the configuration guide.

Support for NBAR2 Protocol Pack

NBAR2 Protocol Pack 19.1.0 is the default protocol pack for Release 8.4. Optionally, you can upgrade to NBAR2 Protocol Pack 24.0.0, which is also supported in Release 8.4.

For more information about NBAR2 Protocol Packs for controllers, see

http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-technical-reference-list.html

Important Upgrade Information for Cisco 2500 Series WLCs

If you are using a Cisco 2500 Series WLC and want to upgrade to Release 8.3.121.0, you must install Cisco Wireless LAN Controller Field Upgrade Software, Release 1.9.0.0 or a later release. For more information, see http://www.cisco.com/c/en/us/support/wireless/2500-series-wireless-controllers/products-release-notes-list.html#anchor512.

Download the Cisco Wireless LAN Controller Field Upgrade Software for Cisco 2500 Series WLC from the Download Software page.

For other controller platforms, see the respective Cisco Wireless LAN Controller Field Upgrade Software release notes for recommended FUS images.

Discontinuation of Support for Some Access Points

The following access points are not supported from this release:

- Cisco Aironet 600 Series OfficeExtend Access Points
- Cisco Aironet 1550 Series Access Points with 64-MB memory
- Cisco Aironet 1040 Series Access Points
- Cisco Aironet 1140 Series Access Points
- Cisco Aironet 1260 Series Access Points

GLC-TE Support in Cisco 5508 WLCs

The GLC-TE 1000BASE-T SFP module is supported in Cisco 5508 WLCs. The Cisco 5508 WLCs that have the GLC-TE SFP module must run Release 8.3 or a later release. The GLC-TE SFP module is a replacement of GLC-T, which has reached its end-of-sale date as of June 1, 2017. For more information about end-of-sale and end-of-life announcement for select Cisco 1000BASE-T SFP modules, see http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/eos-eol-notice-c51-737325.html.

Software Release Types and Recommendations

Table 2: Release Types

Release Type	Description	Benefit
Maintenance Deployment (MD)	Software releases that provide bug-fix support and ongoing software maintenance. These releases are categorized as Maintenance Deployment (MD). These are long-living releases with ongoing software maintenance.	Provides you with a software release that offers stability and long support duration with periodic maintenance releases (MRs).
Early Deployment (ED)	Software releases that provide new features and new hardware platform support in addition to bug fixes. These releases are categorized as Early Deployment (ED). These are short-lived releases.	Allows you to deploy the latest features and new hardware platforms or modules.

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

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

Table 3: Upgrade Path to Cisco WLC Software Release 8.4.100.0

Current Software Release	Upgrade Path to 8.5.105.0 Software
8.2.x.0	You can upgrade directly to Release 8.4.100.0
8.3.x.0	You can upgrade directly to Release 8.4.100.0

Upgrading the Cisco WLC Software Release

Guidelines and Limitations

- The AAA database size is increased from 2048 entries to 12000 entries for some Cisco WLC platforms (Cisco Flex 7510, 8510, 5520, and 8540 WLCs). Therefore, if you downgrade from Release 8.4 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 downgrade:

  1. From Release 8.4, downgrade to one of the following releases, which support 2048 database size and include the enhancement.
     - 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.

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

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

- Release 8.4 supports 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 this release 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 8.4 to a 7.x release, the trap configuration is lost and must be reconfigured.
- If you downgrade from Release 8.4 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 8.4.100.0 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 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 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 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 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 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 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 this release, 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 this release.

Note In case of FlexConnect VLAN mapping deployment, we recommend that the deployment be carried out 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 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.

- 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.

- 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 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 any intermediate release, you must 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 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 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 Center 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, 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 the 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 for 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
  - 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 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 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 this release for the applicable Cisco WLC platforms:

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

Cisco WLC	Base Install Image	Supplementary AP Bundle Image [1]
Cisco 2504 WLC	AIR-CT2500-K9-8-4-100-0.aes	AIR-CT2500-AP_BUNDLE-K9-8-4-100-0.aes
Cisco 5508 WLC	AIR-CT5500-K9-8-4-100-0.aes AIR-CT5500-LDPE-K9-8-4-100-0.aes	AIR-CT5500-AP_BUNDLE-K9-8-4-100-0.aes AIR-CT5500-LDPE-AP_BUNDLE-K9-8-4-100-0.aes
Cisco WiSM2	AIR-WISM2-K9-8-4-100-0.aes	AIR-WISM2-AP_BUNDLE-K9-8-4-100-0.aes

[1] AP_BUNDLE or FUS installation files from Release 8.4 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 the 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 the 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 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.

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, Cisco Aironet 1530 Series AP, Cisco Aironet 1550 Series AP (with 128-MB memory), Cisco Aironet 1570 Series APs, or all.

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 desired. To do so, enter the maximum number of times that 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 appears indicating the status of the download.

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, Cisco Aironet 1530 Series AP, Cisco Aironet 1550 Series AP (with 128-MB memory), and/or Cisco Aironet 1570 Series 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**.

CIMC Utility Upgrade for 5520 and 8540 Controllers

The AIR-CT5520-K9 and AIR-CT8540-K9 controller models are based on Cisco UCS server C series, C220 and C240 M4 respectively. These controller models have CIMC utility that can edit or monitor low-level physical parts such as power, memory, disks, fan, temperature, and provide remote console access to the controllers.

We recommend that you upgrade the CIMC utility to Version 3.0(4d) that has been certified to be used with these controllers. Controllers that have older versions of CIMC installed are susceptible to rebooting without being able to access FlexFlash, with the result that the manufacturing certificates are unavailable, and thus SSH and HTTPS connections will fail, and access points will be unable to join. See: CSCvo33873.

The CIMC 3.0(4d) images are available at the following locations

Table 5: CIMC Utility Software Image Information

Controller	Link to Download the CIMC Utility Software Image
Cisco 5520 Wireless Controller	https://software.cisco.com/download/home/286281345/type/283850974/release/3.0%25284d%2529
Cisco 8540 Wireless Controller	https://software.cisco.com/download/home/286281356/type/283850974/release/3.0%25284d%2529

For information about upgrading the CIMC utility, see the "Updating the Firmware on Cisco UCS C-Series Servers" chapter in the *Cisco Host Upgrade Utility 3.0 User Guide*:

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/lomug/2-0-x/3_0/b_huu_3_0_1/b_huu_2_0_13_chapter_011.html

Updating Firmware Using the Update All Option

This section mentions specific details when using CIMC utility with Cisco 5520 or 8540 controllers. For general information about the software and UCS chassis, see *Release Notes for Cisco UCS C-Series Software, Release 3.0(4)* at:

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/release/notes/b_UCS_C-Series_Release_Notes_3_0_4.html

Table 6: Open Caveats for Release 3.0(4d)

Caveat ID	Description
CSCvj80941	After upgrading CIMC to 3.04d, only after power reset, UCS-based controller is coming up.
CSCvj80915	Not able to logon to the CIMC GUI with the username and password that are configured from the controller.

Table 7: Resolved Caveats for Release 3.0(4d)

Caveat ID	Description
CSCvd86049	**Symptom**: The system will stop working or reboot during OS operation with PROCHOT, MEMHOT, and DMI Timeout-related events reported in the System Event Log (SEL). **Conditions**: C220-M4 or C240-M4 **Workaround**: No workaround is available. This bug fix changes the default BIOS option for ASPM (Active State Power Management) from 'L1 only' to 'Disabled', and the ASPM setting can no longer be modified. This change was made to help increase system stability and eliminate some system crash scenarios.
CSCvf78458	**Symptom**: The system will stop working or reboot during OS operation with PROCHOT, MEMHOT, and DMI Timeout-related events reported in the System Event Log (SEL). **Conditions**: C220-M4 or C240-M4 **Workaround**: No workaround is available. This bug fix changes the BIOS option "Package C-State limit" default value from C6 Retention to C0/C1 to help increase system stability and eliminate some crash scenarios. Once upgraded, reset the BIOS settings to default or manually change Package C-State limit to C0/C1.

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 8: Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	8.4.100.0
Cisco WLC	Cisco 5508 Wireless Controller
Access points	AIR-CAP3802E-B-K9, AIR-AP1852E-B-K9

Hardware/Software Parameter	Hardware/Software Configuration Type
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 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 9: 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

Client Type and Name	Version
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
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

Client Type and Name	Version
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
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 WLCs

- Domain-based ACLs
- Autoinstall

- Controller integration with Lync SDN API
- Application Visibility and Control (AVC) for FlexConnect local switched APs
- Application Visibility and Control (AVC) for FlexConnect centrally switched APs

Note However, 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 the local mode.

Key Features Not Supported in Cisco WiSM2 and Cisco 5508 WLCs

- Domain-based ACLs
- 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 5508 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

- Domain-based ACL
- Cisco Umbrella—Not supported in FlexConnect local switched WLANs; however, it is supported in central 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 join 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 the local mode should be converted to the 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)
- Spanning Tree Protocol (STP)
- Cisco Flex 7510 WLC cannot be configured as a guest anchor controller. However, it can be configured as a foreign controller to tunnel guest traffic to a guest anchor controller in a DMZ.
- Multicast

Note FlexConnect local-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
- Spanning Tree Protocol (STP)
- Port Mirroring
- VPN Termination (such as IPsec and L2TP)
- VPN Passthrough Option
- Configuration of 802.3 bridging, AppleTalk, and Point-to-Point Protocol over Ethernet (PPPoE)
- Fragmented pings on any interface

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

Key Features Not Supported in Cisco Virtual WLCs

- Cisco Umbrella
- Domain-based ACLs
- Internal DHCP server
- Cisco TrustSec
- 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 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 1560, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800, and 3800 Series APs

Table 10: Key Features Not Supported in Cisco Aironet 1560, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800 and 3800 Series APs

Operational Modes	• Autonomous Bridge and Workgroup Bridge (WGB) mode • Spectrum Expert Connect • Mesh mode **Note** Supported on 1560 APs. • Flex + Mesh • 802.1x supplicant for AP authentication on the wired port • LAG behind NAT or PAT environment

Protocols	• 802.11u • 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)
	• DHCP Option 60
	• 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 1810 OEAP and 1810W Series APs

Table 11: Key Features Not Supported in Cisco Aironet 1810 OEAP and 1810W Series APs

Operational Modes	• Monitor Mode • Mobility Express
FlexConnect Features	Local AP Authentication

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

Table 12: Key Features Not Supported in Cisco Aironet 1830 and 1850 Series and 1815 Series APs

Operational Modes	Monitor Mode
FlexConnect Features	Local AP Authentication

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 on Cisco Aironet Mesh 1560 APs

- Noise Tolerant Fast Convergence

Caveats

Open Caveats

Table 13: Open Caveats

Caveat ID Number	Description
CSCux92335	3602 AP losing MAC address
CSCux97132	AP starts CAC timer after rolling back to lower bandwidth
CSCuy75333	Cisco 2504 WLC configuration restoration failure due to multicast mode command
CSCuz19004	Radio resets on 702w AP

Caveat ID Number	Description
CSCva58429	1532i AP low throughput (FlexConnect Local switching + EoGRE)
CSCva87833	AIR-CT8510-K9 stopped working; SSO disabled
CSCvb13666	WiSM2 stopped working with Task Name 'IPv6_Msg_Task'
CSCvb46044	Standby WLC reboots continuously with reason that XML were not transferred from Active to Standby WLC
CSCvb67724	Cisco 5508 WLC runs out of memory
CSCvb71347	Cisco WLC multicast configuration not coherent for code upload or download
CSCvb86237	Cisco 8510 WLC stopped working due to TempStatus task
CSCvb97383	Cisco WLC deauthenticating roaming client with idle timeout
CSCvc06547	AP retransmits packet even though client sends ACK
CSCvc18786	Cisco WLC stops working during multiple login sessions either with local user or with TACACS+
CSCvc24917	Defect of msglog corresponding to 'AP Message Timeout: Max retransmissions reached on AP ...'
CSCvc30828	AP does not allow world mode to be set via GUI on 15.3(3)JD
CSCvc31551	IR829/AP803: uWGB cannot pass traffic downstream
CSCvc33793	Cisco WLC tears down connected AP due to unequal load balance between SPAM queues high load
CSCvc35151	AP radio reset happens multiple times without trigger
CSCvc49713	AP generates flood of received and decoded a DMS client request payload successfully
CSCvc50436	WGB wired client randomly stuck in the DHCP_REQD state after layer 2 roaming between the controllers
CSCvc51666	Wave 1 AP transmits on disabled rate (24Mb)
CSCvc55430	Cisco WLC HA redundancy management interface not reachable for a short time after failover
CSCvc56757	WGB HSR 802.11v neighbor report validation fails when Infrastructure MFP is enabled
CSCvc61795	IP call setup fails after L3 handover occurs during call among 1832 AP
CSCvc65641	Cisco WLC reports tracebacks reported very frequently but no unresponsiveness
CSCvc66547	CPU ACL configured to block access to Virtual IP does not work as expected
CSCvc71537	Cisco WLC profiles 7925 incorrectly
CSCvc72724	Cisco 8510 WLC's AP-SSO stopped working on portalProcessLogout

Caveat ID Number	Description
CSCvc74515	Cisco WLC data plane stopped working due to fragmentation
CSCvc76969	Silent reboot on Cisco 5508 WLC or Cisco WiSM2
CSCvc78546	WLC sets Zero 11e QoS for downstream voice traffic when CAC is disabled
CSCvc78857	AVC profile is not applied on client behind WGB
CSCvc82845	Cisco WLC returns nothing for SNMP get WEB ACL - cldcClientAaaOverrideAclName
CSCvc83175	vWLC does not learn client IP address; client stuck in DHCP_REQD
CSCvc83465	3800 AP sometimes stops sniffing on DFS channel
CSCvc83490	Redundancy Mobility MAC address does not stay, Primary WLC's MAC address is always set instead
CSCvc84474	ISE endpoint purge not working on Foreign-Anchor setup
CSCvc84637	1810W AP sending invalid AC_NAME when WLC hostname is 31 bytes long
CSCvc85328	1832 or 1852 AP: Power injector/Normal mode in spite of power supply by AIR-PWR-C
CSCvc89532	1702I AP stopped working with DOT11-2-RADIO_RX_BUF: Corrupt buf: errors
CSCvc92070	Wave 2 APs: Allows direct routing to AP IP address from client WLANs with FlexConnect local switching
CSCvc93377	Tracebacks and MFP queue logs filling up the msglog on WLC
CSCvc94648	Evaluation of WLC for OpenSSL Jan 2017
CSCvc95821	GUI-ping output not throwing proper privilege error with read-only user
CSCvc96024	702W AP: Unable to view or configure dot11U manager in GUI
CSCvc96076	WiSM2 HA: Standby WLC stopped working with task name spamApTask2 in ideal state
CSCvc98310	1830 AP: 2.4-GHz radio stopped working at 0x009915D7
CSCvd00067	Wired WGB client is removed from parent AP's association table
CSCvd00289	2800 AP or 3800 AP: capwapd init unsuccessful creating 2 capwapd causing WCPD watchdog reset
CSCvd02303	Flex+Bridge AP stopped working while joining the WLC
CSCvd06848	Cisco WLC stopped working on SNMPTask
CSCvd07423	AP firmware corrupt after power cycle bad mzip file, unknown zip method reboot loop
CSCvd09507	Rogue Rule substring-ssid turns invalid on Cisco WLC when user-configured SSID is included in PI template

Caveat ID Number	Description
CSCvd12615	AP memory leak on QoS/AVC FlexConnect module
CSCvd15404	Rule creation with CLRuleConfigEntry stops the Cisco WLC from working
CSCvd15760	Cisco WLC stopped working on SNMP set performed on clrRrmDot11BandGrpMemberEntry
CSCvd16346	Cisco WLC memory corruption when TACACS+ responds with unknown attributes
CSCvd16380	3800 AP detecting DFS false triggers
CSCvd16800	Client associated to MAP does not get AAA override in Flex+Bridge mode. Bug ID CSCut91086 not fixed
CSCvd18025	Anchor1 WLC does not free client sessions after client roaming to Anchor2 WLC; client entries stale
CSCvd18535	ROKHid inconsistent for 802.11r roaming in FlexConnect and NAT setup
CSCvd21155	Cisco WLC stopped working when multicasting traffic and accessing WLC GUI
CSCvd21969	AAA AVC Override: AVC profile retained after roaming
CSCvd22402	WLAN-VLAN mapping is not removed after deleting WLAN
CSCvd23185	WGB wired clients not seen by Cisco WLC
CSCvd23301	Cisco WLC GUI trapflags for client association with statistics does not display correct configuration
CSCvd23902	1532 AP: Root bridge drops packets from non-root bridge in non-native VLAN
CSCvd24540	SNMP system stopped working when attempted to create tunnel with clGatewayTunnelEntry MiB
CSCvd26885	Unit of probe suppression hysteresis should be dB
CSCvd27065	EAP-FAST EAP-Chaining on wired 1810W AP port does not work
CSCvd27365	Incorrect number of clients reported on AP by WLC
CSCvd28374	AP802 incorrect base radio MAC assigned not ending with zero causing to only support one BSSID
CSCvd28645	AP sends RTS at 6 data rate when data rate 6 is disabled
CSCvd29653	Apple iPhone 7 dissociates after session timeout
CSCvd32632	Standby WLC stopped working @rmgrReboot
CSCvd34785	Mobility multicast IP address reverse in TACACS+ packets
CSCvd35701	3800 AP or 2800 AP: Not enforcing WLAN WFD policy

Caveat ID Number	Description
CSCvd36190	Cisco 5520 WLC stopped working due to haSSOServiceTask6 task
CSCvd36736	AP in local switching or local authentication disconnects EAP-SIM client idle for more than 0.5 second
CSCvd37522	show run-config commands: Incorrect index numbers for RADIUS Accounting Servers
CSCvd38006	1600 AP ping loss on Ethernet interface
CSCvd40978	Wave 1 AP on Release 8.2 falsely show 100% channel utilization
CSCvd42321	1832 AP drops CAC SIP 486 Packet
CSCvd42348	Standby WLC stopped working on performing SNMP Set on bsnDot11QosProfileEntry
CSCvd42669	Cisco 2500 WLC stopped working
CSCvd44573	ACL counter was not incremented after applying ACL rule
CSCvd44909	Client traffic dropped in anchor foreign AirOS setup with new mobility if foreign WLC is behind NAT
CSCvd45744	AP reboots after 4 hours while doing Site Survey
CSCvd48333	Cisco WLC stopped working due to emWeb task
CSCvd48852	Audit-Session-ID information is missing after reauthentication
CSCvd50044	System stopped working multiple times on ping rx task
CSCvd52587	1140 AP: 2.4GHz radio resets with reason code 71 on event.r0
CSCvd53765	After restarting WLC NMSP goes down on CMX
CSCvd54154	All 1850 APs connected to primary AP stop working in a loop due to watchdog reset
CSCvd56064	FlexConnect local switching, local auth not supported when PMF is enabled
CSCvd56422	Error cause 403 generated for 'RFC-3576 Disconnect-Request'
CSCvd56588	2800 AP or 3800 AP: Incorrect RSSI values displayed when client associates with XOR radio
CSCvd63187	WLC is allowing selective reanchor to be enabled on wrong WLAN
CSCvd63539	Getting 'max containments reached...:3' message on 1852 AP in monitor mode
CSCvd64928	System stopped working on PMIPV6_Thread_0 during creation of LMA entry
CSCvd67178	Anchor not deleting webauth req client beyond webauth timeout
CSCvd67485	FlexConnect AP reconnect, radio reset during DTLS setup
CSCvd68141	Cisco WLC stopped working at task nmspRxServerTask
CSCvd68648	cLApWlanStatsOnlineUserNum is not current number of online user

Caveat ID Number	Description
CSCvd72131	Cisco Flex 7510 WLC stopped working due to Taskmaster Reaper reset
CSCvd72432	Local EAP LDAP request with incorrect password lockout users
CSCvd76773	Antenna Gain on 2.4-Ghz radio resets to default after 3800 E AP reboot
CSCvd79464	AP with WSM module enabled sending RRM data every 5 seconds for each radio
CSCvd84015	Blackberry passport is not redirected to the webauth portal
CSCvd86566	Client with incorrect NAI realm gets Access-Accept message from RADIUS Server
CSCvd87065	Cisco WLC stopped working due to nmspTxServerTask
CSCvd90377	Cisco WLC applies incorrect ACL to clients when performing CWA
CSCvd91894	AP 3800 and/or AP 2800: Kernel panic, stopped working at insectivorous+0xc/0xa4 [ap8x]
CSCve00464	1852 AP detects high noise level on 5-GHz radio
CSCve01552	Unknown user name when switching from open to dot1x SSID
CSCve02210	Incorrect SNMP OID issue for FT - 1.3.6.1.4.1.9.9.521.1.1.1.1.10
CSCve02612	HA: configuration sync failed on standby WLC when FlexConnect AP configuration is modified
CSCve02689	Silent reboot after memory usage goes to 85%
CSCve13779	2802 AP rogue detection configuration changed back to Enabled state after AP reboot
CSCve15860	WLC data plane is not responding to capwap-data keep-alive
CSCve18213	Foreign WLC leaks IPv6 and IPv4 multicast client traffic out of EoIP tunnel
CSCve20123	When client roams between AP, DP may not plumb tclas while having active call
CSCve23581	2800 AP or 3800 AP sends multicast with AES when client is TKIP
CSCve24871	FlexConnect ARP responds to wired clients
CSCve26935	2800 AP or 3800 AP IPv4 TCP low throughput with Windows 10 Creator
CSCve27052	AP shows public IP address on Cisco WLC GUI, but private IP address in CLI
CSCve27955	Configuration upload fails due to WLANs having special or invalid characters
CSCve30922	Cisco 8540 WLC modifies IP Header 'Router Alert' to 'End of Option List' when IGMP snooping enabled
CSCve38070	2800 AP or 3800 AP: False 100% channel utilization seen
CSCvk44249	WLC 5508 - foreign mapping is missing on a WLAN when restoring a backup

Resolved Caveats

Table 14: Resolved Caveats

Caveat ID Number	Description
CSCva17063	IPv6 traffic-filter command not working on subinterface
CSCuz90361	AP with Hyperlocation module: AP dot1x credentials are lost after second reload
CSCux14242	HTTP profiling support for 1850 AP
CSCuz48863	Cisco 602 AP private key extraction vulnerability
CSCvb61800	3800 AP sending unencrypted ARP requests over the air
CSCuz18799	3802 AP sends VHT SGI frames to STA that does not support SGI
CSCuz68479	3800 AP does not reassemble wireless fragmented frames
CSCva54809	3800 FlexConnect AP: Does not honor Operating Mode Notification IE from STA
CSCva84903	3800 AP incorrectly shows 0x01 (extension channel above) for ch 161
CSCuz68498	3800 AP indicates support for MCS32 Duplicate mode
CSCuz65017	3800 AP not updating HT Op Mode bits in presence of legacy AP
CSCva58323	3800 AP sends out multicast packets with no clients associated
CSCvb25120	WLC GUI: client Current TxRateSet shows wrong value for 802.11ac rates
CSCva29463	3800 AP: WLAN client fails on >= 1500 bytes with ICMP traffic in standalone mode
CSCva29554	Wave 2 APs: FlexConnect AAA overridden ACL is not plumbed in the WLC
CSCvb66994	Cisco AP IOS software TCP Denial of Service Vulnerability
CSCva15083	No bridge-group X spanning-disabled command is lost after reboot
CSCuz62592	Web passthrough URL redirection fails with HTTPS web addresses
CSCuz94264	AP might fail to get an IP address if hostname is short
CSCva16449	AIR-CAP1552 not showing temperature on Cisco WLC
CSCuz90954	MAP not joining Cisco WLC when invalid static IP configured
CSCva88494	Mode changed from wireless mesh to FlexConnect when auto-convert enabled
CSCvb05881	No data connectivity on wired client when RAP from SPF fiber to wireless
CSCvb53332	Improper message: Received unsupported MSG event 0 for Hotspot task
CSCvb78325	1810 AP stops forwarding multicast traffic to RLAN port randomly
CSCvb90173	602 OEAP Txpower set to static minimum after upgrade from 8.0 to 8.2.x release

Caveat ID Number	Description
CSCvb41204	1572 AP Inventory incorrect on WLC CLI and GUI for NAME&DESCR
CSCuz61598	A-MSDU cannot be enabled on VO
CSCva37159	2800 AP: Client upstream data packets drop due to CCMP PN mismatch
CSCuz67257	1810 AP: show ip int brief and show interfaces commands to be updated correctly
CSCva86515	1810 OEAP associated with Cisco 8540 WLC: Network diagnostics reports an error on the AP
CSCvb30918	1810 AP: Interface status in CLI output not matching with OEAP GUI
CSCvb39726	LED state on 1852 ME reenables even after manually disabling
CSCva47491	AP load information not clear/reset after AP radios are disabled
CSCvb26116	1570 MAP Best-Effort tx queue stuck on 5-GHz interface
CSCuy86449	AP803 error in setting antenna type when channel changed
CSCuy93000	SC2 Radio randomly sending corrupted timestamp BCN on hidden SSID
CSCuy60650	Wi-Fi Interface Input Counter Not Reflecting Total Packets
CSCva29195	Changes from CSCux82091 need backed out and fixed
CSCva55942	SSID name is NULL when using Hotspot 2.0
CSCva56926	AP returns incorrect value for 1.3.6.1.4.1.9.9.272.1.1.2.14.1.10
CSCvb58083	SGT-IP bindings through SXP are not propagated by WLC after WAN connectivity restored
CSCva32370	702W AP LAN port clients do not get IP addresses on Cisco 8510 WLC
CSCva24182	Configurations allowed on 802.11ac radio Sniffer mode AP
CSCva49960	Dot2 radio up even after 11ac-support disabled in WLC
CSCva42917	Same AP image shows up on primary and backup side
CSCva62061	Able to delete RADIUS server without index number or value in 8540 WLC
CSCva87608	Controller Interface override issues when user changes-INTERFACE group
CSCva71978	In WLC GUI, user is unable to apply ACL in local policy
CSCvb71235	IP address of PC for failed authentication displayed in reverse format in WLC msglog
CSCvb05067	Local EAP fails after wrong username login
CSCvb95343	RADIUS interim accounting updates GUI/CLI config option should be removed for Guest WLAN

Caveat ID Number	Description
CSCvb71600	Cisco WLC stopped working after applying CPU ACL
CSCvb27848	AP SSH/telnet global configuration missing on the standby WLCs
CSCuz81823	config ap tftp-downgrade command does not recognize valid IPv6 TFTP address
CSCvb57350	SNMP trap for "AP Interface Up/down Traps" not getting generated.
CSCva46376	#DHCP-4-INVALID_VLANID_ARP:
CSCva52609	WLC EoGRE profile name above 31 characters does not work
CSCva86093	'ap-manager' should not be accepted as dynamic interface name
CSCvb87219	8510 WLC DP packet-capture size swapped due to endianness
CSCvb30793	Data plane stopped working on Cisco 5508 WLC
CSCux28505	Cisco 8510 WLC stopped working with "fp_main_task" during boot
CSCva07048	WLC DP stopped working; wqe stuck
CSCva30714	WLC incorrectly sends disassociation frame using base radio MAC address
CSCuy82313	AP core dump config not synced to standby when config is done via GUI
CSCvb64042	WLC HA transfer download failure with legitimate network latency
CSCva08773	ciscoLwappReapMIB table not returning all APs for FlexConnect and Flex+Bridge
CSCuz97671	default-flex-group shows wrong count in FlexConnect and Flex+Bridge combination
CSCva05000	FlexConnect AVC config not pushed if WLAN is added to the AP group later
CSCva46506	FlexConnect group RADIUS configurations are not pushed to AP
CSCvb17671	WLAN and L2ACL mapping config is not applied on the FlexConnect AP
CSCva39994	Cisco 2500 WLC client display error: UnavailableUnavailable
CSCva85361	Cisco WLC losing IPv6 connectivity
CSCux26440	Observing Traceback after joining AP to WLC (ARP entry Related traceback)
CSCva58634	vWLC: Silent reboots with Kernel error
CSCuy77912	Cisco WLC failed to handle ARP request from wired server within the same VLAN
CSCva44397	Cisco WLC gateway not reachable after disabling LAG
CSCuz92913	Bad Payload Len 4 - dropping packet error on WLC
CSCvb27893	Check wireless LAN controller AP radios are installed properly
CSCva69083	Cisco WLC drops NMSP packet from MSE

Caveat ID Number	Description
CSCvb77390	Cisco WLC stopped working accessing MAC Address Database
CSCva67364	Able to configure mesh backhaul slot ID with character
CSCva79950	Mesh: SNMP not returning value for VHT Data Rates
CSCvb93124	Cisco WLC stopped working on spamApTask5
CSCuz60117	'config mobility group anchor' config is removed after WLC upgrading
CSCvb16806	Cisco 5500 WLC as MC showing stale connections from MA clients
CSCva66176	AP drop of from network due to large set of mobility groups in down/down
CSCva26652	Client unable to get anchored at GA controller
CSCuz47010	Old Mobility Ping traffic drops in wired m/c when roaming from F to F
CSCva96095	Tracebacks on sh run in Release 8.3, due to partially removed feature
CSCva57205	Media stream is not showing the client details
CSCvb78912	WLC Netflow: Flow durations showing higher than 90 seconds
CSCva03230	Maximum length for NTP key configuration fails on Cisco Flex 7510 WLC with HEX
CSCva40609	Cisco 8510 WLC in HA stopped working; Task Name: nmspRxServerTask
CSCvb12565	Cisco WLC stops working when running 'show run-config' command with no APs
CSCva55165	IPv6 MLD from PMIPv6 client show client MAC on Layer3/2 switch
CSCuz45986	CWA not working on Cisco 8500 WLC as Guest anchor with Accounting enabled
CSCva58498	Token Bucket leak messages with QoS Roles and with WebAuth on 8.0.134.13
CSCva63025	WLC cap the traffic as per QoS WLAN policy instead of applying exception
CSCvb27974	5-GHz radio using higher power than max TPC channel UNI III
CSCva92447	5-Ghz radio down with Macedonia as the country code
CSCva59067	802.11a RF Grouping CLI returns redundant info and incorrect characters
CSCva54530	802.11a/b l2roam rf-param configs output not present in show running-config
CSCva27419	Channel changed trap with Unknown Radio Type on dual band radio
CSCuz68241	clrRrmDot11BandGrpMemberTable row creation is success; still throwing error
CSCvb68876	clrRrmDot11BandGrpMemberTable row creation is success; still throwing error
CSCuz65391	config 802.11a or abgn command hit several issues for 3802 AP
CSCva00912	Cisco WLC stopped working while editing RF profiles

Caveat ID Number	Description
CSCva53980	Issue in CleanAir when client serving band is 5 GHz
CSCuz83689	MA is connected but Mobility Agents RF membership information shown 0
CSCva58535	Optimized roaming trap log shows reason as: Unknown Reason Code 34
CSCuz49147	RF Profiles only has MCS indices 0-23 vs global 0-31
CSCva54108	Rx-SOP threshold values are pushed to unsupported model AP
CSCva60796	SNMP: Channel Number returned for NOS module inserted to an AP
CSCuz92568	New active (Secondary) WLC sending trap using redundancy Management IP
CSCvb59710	SGT-IP bindings CTS tag is missing from WLC after reauth WAN connection recovery
CSCvb56265	Cisco WLC not propagating SGT-IP bindings via SXP after role change
CSCvb05495	IN WLC CLI, url-acl not accepting special characters as profile name
CSCva30806	WLC FlexConnect MediaStream client count is wrong
CSCva66284	3802 XOR operational state inconsistent issues
CSCuw03373	5 indices with same 1601 after changing EAP to PSK on GUI without applying the changes
CSCuy86768	Downloaded AVP page keeps reloading automatically-readonly user
CSCvb87486	During editing of Guest User, it is accepting out of range value
CSCuz96109	Either local or RADIUS profiling must be supported; not both at the same time
CSCva85805	Error in creating ACL name in UTF-8 character in WLC GUI.
CSCuw03353	GUI error configuration failed when deleting a key while PSK is disabled
CSCuz99816	GUI of WLC must display channel as NA for 2800 AP in monitor mode
CSCuz73626	In GUI observing error message while creating WLAN with 802.1X security
CSCva77085	Mismatch in WLC CLI and GUI page for NTP polling time interval range
CSCva66260	Monitor annoying warning and operational state of radio provisioning
CSCva75716	Refresh button not working in interface groups page in WLC GUI
CSCva32959	TACACS+ Accounting Message is not sent when CPU ACL changed
CSCva84032	Unable to configure anything on "FlexConnect" tab of FlexConnect mode AP
CSCvb01645	Unable to create IPSec profile name with UTF-8 Char
CSCva60422	Unable to set the radio in Rapid Update mode when right-clicked on CleanAir

Caveat ID Number	Description
CSCva04984	WebUI displays wrong WLAN ID under AP for FlexConnect AVC mappings at FlexConnect group
CSCva97976	WLAN name not shown properly on monitor and client page in WLC GUI
CSCva71002	WLC GUI client filter fails with spaces used in the Client Name
CSCvb33076	WLC: GUI does not allow to change sniffer channel
CSCva27922	Cisco TrustSec: DHCP Proxy IP empty unable to determine which DHCP server not work
CSCvb40591	Display showing unreasonable 110% or 120% in % interference Impact
CSCva18225	WLC 8510/2504 flooding Tracebacks on syslog level debugs enable
CSCvb00781	8510 WLC stopped working on apfProcessClientAssocRespForRldp
CSCva91376	Issues regarding CLI command of 'config rogue ap'
CSCva05412	Old AP keeps doing containment even after enabling auto contain monitor
CSCuz89259	Cisco Catalyst 3850 switch elected as RF group leader instead of Cisco 5508 WLC running Release 8.2
CSCuz96996	CHD-WLC CLI command to set voice packet count does not work properly
CSCva50180	AIR-CAP1602I-E-K9 stopped working
CSCvb66073	RLAN clients being sent as RADIUS:NAS-Port-Type = Wireless - IEEE 802.11 for RLAN
CSCva42271	2800 AP entry removed from WLC with Exception stack message
CSCva03113	FlexConnect: WLAN Ordering-AP specific VLAN gets changed to Native VLAN
CSCva03427	FlexConnect: WLAN mappings change to WLAN specific during fault tolerance
CSCvb59172	Controller log messages do not report RTU licensing status or issues
CSCuz17445	Rx-SOP: WLC setting global threshold values after upgrading/reloading WLC
CSCva89704	Inconsistent LED behavior on AIR-AP1810W
CSCvb25382	1810 OEAP: Channel selection when set to Auto shows blank on the UI
CSCvb80938	OEAP 1810 Local UI can be accessed with IP address even when it is disabled globally
CSCvb97603	TrustSec: Wave1 FlexConnect AP to update client SGT info when switching from standalone to connected
CSCva04054	EoGRE client gateway IP is different as per the WLAN interface IP
CSCva59149	SNMP set fails when attempted to set a URL ACL rule with 32 characters
CSCva82117	SNMP get-response returns '0' value for the 'adminStatus' value =1
CSCvb17520	Fastlane: Fastlane enable on a WLAN overwrites existing profile

Caveat ID Number	Description
CSCvb62874	Radio interface input queue gets filled on Autonomous APs.
CSCuz47559	Error saving config file happens on multiple 2702 APs
CSCvc08052	DFS false detection on 2700 AP
CSCvc85932	3802E AP in sniffer mode does not see NullFrames
CSCvd66657	3802 AP: SensorD stuck in offchannel causing radio to stop working
CSCvd46374	Client with lower signal strength than Rx-SOP threshold can connect radio
CSCvb91832	1810W AP radio firmware stopped working (@0x009C30A0/0x0000), memory corruption
CSCvd58664	AP dropping EAP packets on radio which is seen on wired uplink
CSCvd15742	AP stopped working with %ENTROPY-0-ENTROPY_ERROR: Unable to collect sufficient entropy
CSCvc81168	2702 AP unable to upgrade and failing with error: Unable to create temp directory "flash:/update"
CSCvd36259	ME intermittently flaps with external AP
CSCvd81926	CCX proxy ARP flag not set in Wave 1 APs
CSCvd86274	1800/2800/3800 Series AP does not send the platform value via CDP when it is brand new
CSCvd70755	AIR-AP3802I stopped working due to kernel panic
CSCvd29564	Layer 2 packet drop of CDP packets for Wave 2 APs
CSCvd46216	AP1832/AP1852 sometimes does not send authentication response
CSCux11777	1532 AP non-root bridge high retransmission and latency rate
CSCvd06463	AMSDU packets transmission cause 5-second gap of packet transmission to 8821 from Wave 1 AP
CSCvc68156	Full support for "distance" on 1572 AP
CSCvd44446	Retried EAP response dropped as a duplicate while first EAP response was not even received on the AP
CSCvd30952	RM3010L-B-K9 Hyperlocation module stopped working
CSCuu59589	False positive AP sourced AP impersonation on corrupted beacon
CSCvc74507	Fix incorrect commit of CSCuu59589 in 8.0 maintenance release
CSCvc67005	2802 AP drops client ARP packets after web authentication

Caveat ID Number	Description
CSCvd88630	3800 AP stopped working due to 'WCPD'
CSCve13183	2800/3800/1800 AP WCPD stopped working due to double-free in RRM off-channel element
CSCvd62333	3800 AP: WCPD stopped working at off-channel
CSCvd56581	Client not getting IP address when moving between SSID
CSCvc51637	802.1x CCKM roams fail on WGB at GTK key rotation
CSCvc41438	WGB running 15.3(3)JD WGB takes ~500 ms longer to scan DFS channels vs JBB
CSCvd66117	WGB sticky to the current AP despite better candidate being available
CSCvd09240	Local authentication EAP-TLS not working on Microsoft Windows 10
CSCvb44979	WLC Local EAP with 7925 handshake failure
CSCvc65568	8821 fails 11r FT roam with "Invalid FTIE MIC"
CSCvd18773	Release 8.2: Clients unable to authenticate for extra 3 seconds post 1-second cleanup timeout
CSCvd91308	apAuth flag reset while changing SSID from local switching to central switching having Fast SSID enabled
CSCvb93365	WLC msglog showing a lot of traceback
CSCvd20251	DP stopped working on Cisco 5508 WLC running Release 8.0.140.0
CSCvd81303	2800/3800 AP: Limit 'best' DCA to 80 MHz also for RF profiles
CSCvd14806	APs randomly not showing any neighbors on both radios
CSCvd53205	DCA lists in RF profiles are broken after a backup or restore of Cisco WLC's configuration
CSCvc79811	When adding or removing country codes, 2.4-GHz channels change
CSCve01109	SXP connection on WLC stays off
CSCvd79597	Smart License on Cisco 5520/8540 WLC: Unable to reset HTTP-Proxy on call home configuration from GUI
CSCvc87433	Webauth with proxy does not work after Release 8.2
CSCve14081	Same channel has been assigned to both the 5-Ghz radios after CAPWAP restart
CSCvd69992	2800 or 3800 AP: Unable to send proper sequence number and burst rate upstream
CSCvd83741	1850 AP: Unable to send proper sequence number and burst rate upstream from AP to MSE

Caveat ID Number	Description
CSCvb70551	Wave 1 APs rebooted due to Kernel Panic-Not Syncing: Out of Memory
CSCvd20271	AP 3800 stopped working in Monitor mode with wIPS submode
CSCvd23175	2800/3800 AP WCPD memory leak observed
CSCvd61977	2800 AP or 3800 AP: Radio coredump generation may get stuck with ca_status leading to IPC call function failures
CSCvc74876	Wave 2 AP: CAPWAP disconnect stuck in discovery loop
CSCvd40646	2802 AP: Kernel panic, Dot11Classifier: Mgmt frame not supported 0
CSCvd49909	Kernel panic at ClientCapabilitiesTracker virtual address invalid band select
CSCvc86170	Wave 2 AP: FlexConnect Local Auth does not work on WLAN with CCKM security
CSCvd33219	An AP 3800's radio stopped working due to chatter: wl1: fwHangDetect(357): FTR!
CSCvc55328	AP stopped working due to kernel panic at WlLoadRateGrp
CSCvc00328	3800 AP: Surface Pro gives less throughput
CSCvb29996	1810W Hardware Watchdog reset unresponsiveness PC=0xc03b3ffc, LR=0xc008af24, QCA 02698633
CSCvc78510	2702 AP aux port goes to disabled after the AP is rebooted
CSCvb61023	DHCP Option 82 (remote-id) not present is some APs
CSCva95121	Stale IP route left on FlexConnect AP config if booting up in standalone mode
CSCuz72195	AP bridge does not forward BPDUs/VTP frames
CSCva82261	1532 AP uplink drops when sending heavy upstream traffic
CSCvc04089	2700 AP Series radio resets; reason code 71 RADIO_RC_NO_REPORT
CSCvb93189	AP drops retransmitted M3 from WLC
CSCva90265	iPad Pro with iOS10 is getting deauthenticated at times due to M3 timer
CSCva62084	Add Kuwait support for Universal AP
CSCvb15871	aIOS does not forward broadcast multicast frames with dynamic VLAN
CSCvb21254	AAA override VLAN lost on intercontroller roaming
CSCvc57427	Cisco WiSM2: Memory leak while handling Cisco AVP POLICY_ROLE_TYPE (cisco_avp_pair="role")
CSCvd97103	IPv4 CPU ACL - IP-Address with netmask other than 255.255.255.255 does not work

Caveat ID Number	Description
CSCvb76654	Clients not getting excluded on max EAPid timeouts; reassociation rejected with reason 12
CSCvb20553	CoA for session timeout not working using free RADIUS server
CSCvc45620	Cisco WLC stopped working in SNMPTask due to missed software watchdog
CSCvd61701	SSH to Standby RMI or Service port fails
CSCvc67465	FlexConnect AP loses VLAN mapping if VLAN tagging is enabled
CSCvc40267	Cisco WLC sends incorrect VLAN for AAA overridden client reassociating to AP belonging to FlexConnect Group
CSCvb11778	Cisco WLC stopped working on sisfSwitcherTask
CSCvc40852	Active controller in HA pair shows different socket errors
CSCvc83583	Cisco 5520 WLC stopped working with taskname apfProbeThread
CSCvc82053	The NMSP info/probe notification queue is saturating
CSCvb91652	Cisco WLC sluggishness due to flooding probe, need probe throttling configurations
CSCvb97656	Unexpected reload: Task Name: mmListen on 8.3.102.0
CSCva68921	Cisco WiSM2 reaperWatcher stuck on DP0 while retrieving crash and crashed
CSCvc28168	Cisco WLC set ZERO 802.11e QoS UP for part of the downstream voice packets and APs trust it
CSCvc62277	Cisco 5520 stops working on running RRM commands on task emWeb
CSCvb48354	RRM does not update as per configuration on Cisco WLC
CSCvb67378	Too many channel changes occur on dual radio if working as 5 GHz
CSCvc94704	Cisco WLC stopped working due to task dtlArpTask
CSCvc12594	Cisco WLC fails to send SNMP when using untagged interfaces on different ports
CSCvc65675	Cisco WLC: Constantly increasing memory consumption by SNMPTask
CSCvb99468	Cisco WLC stopped working due to emWeb when serving an EmWebForm exclusion-list
CSCvb96009	Cisco WLC stopped working due to emweb task
CSCvb72389	CWA: Redirect traffic from client goes through CAPWAP tunnel instead of VxLan
CSCvd39346	AP 2800 and/or AP 3800 WCPD slow memory leak
CSCvb94716	Cisco WLC stopped working at task:spamReceiveTask

Caveat ID Number	Description
CSCvd63350	702W AP wired client keeps disconnecting when it is connected to switch with dot1x configured

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