Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.8.100.0

First Published: 2018-08-17

Last Modified: 2020-02-04

About the Release Notes

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

Content Hub

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

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

Do provide feedback about your experience with the Content Hub.

Revison History

Table 1: Revision History

Modification Date	Modification Details
January 30, 2019	Added a note about issues related to Cisco Wave 1 AP flash and the solution to address them in the Upgrading Cisco Wireless Release section.
October 30, 2017	Resolved Caveats—Added CSCvh65876, CSCvf66696, CSCve64652, CSCvf66723, CSCvi97023, CSCvj95336, CSCvi49059, CSCvh21953

Supported Cisco Wireless Controller Platforms

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

- Cisco 3504 Wireless Controller
- Cisco 5520 Wireless Controller
- Cisco 8540 Wireless Controller

- 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 (Support introduced in Release 8.4)
  - Kernel-based virtual machine (KVM) (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 3504 WLC, Cisco 5520 WLC, and Cisco 8540 WLC.
- Cisco Mobility Express Solution

Supported Cisco Access Point Platforms

The following Cisco AP platforms are supported in this release:

- Cisco Aironet 700 Series Access Points
- Cisco Aironet 700W Series Access Points
- Cisco AP803 Integrated Access Point
- Integrated Access Point on Cisco 1100, 1101, and 1109 Integrated Services Routers
- 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 2700 Series Access Points
- Cisco Aironet 2800 Series Access Points
- Cisco Aironet 3700 Series Access Points
- Cisco Aironet 3800 Series Access Points
- Cisco Aironet 4800 Series Access Points
- Cisco ASA 5506W-AP702
- Cisco Aironet 1530 Series Access Points
- Cisco Aironet 1540 Series Access Points
- Cisco Aironet 1560 Series Access Points

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

Note

- Cisco AP803 is an integrated access point module on the Cisco 800 Series Integrated Services Routers (ISRs). For more information about the stock-keeping units (SKUs) for the AP803 Cisco ISRs, see:

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

- For more information about Integrated Access Point on Cisco 1100 ISR, see the product data sheet:

  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 8.8.100.0

This section provides a brief introduction to the new features and enhancements that are introduced in this release.

Note For complete listing of all the documentation published for Cisco Wireless Release 8.8, see the Documentation Roadmap:

https://www.cisco.com/c/en/us/td/docs/wireless/doc-roadmap/doc-roadmap-release-88.html

Software-Defined Access Features

The following software-defined access (SDA) features are supported in this release:

- **IPv6 Client Support in SDA**: The following IPv6 features are supported in this release:
  - **IPv6 client support**: IPv6 and dual-stack wireless clients can be brought up and serviced by controllers in an SDA framework. The clients can be of Static, Stateful DHCPv6, or SLACC types.
  - **IPv6 client mobility**: IPv6 clients can move across APs within an SDA network and preserve their IPv6 connectivity when roaming. 802.11r Fast Roaming is supported if the client supports it.
  - **IPv6 DNS-based ACLs**: In Release 8.7, this feature was introduced with support for only IPv4. In Release 8.8, this feature is enhanced such that FlexConnect IPv6 ACLs accept internet domain names in addition to IPv6 addresses in their rules. With DNS-based ACLs, clients that are in the preauthentication phase are allowed to connect to the configured URLs.
  - **IPv6 client HA**: In an HA environment, client states are preserved even if there are any controller failures. Also, the access node and intermediate node redundancy mechanisms that are configured in an SDA network strive to provide an additional layer of HA protection to clients.

- **Multicast-to-Unicast of IPv4 VideoStream in SDA**: Multicast-to-unicast video traffic on APs operating in Local mode is supported in SDA.

  For more information about deploying VideoStream, see

  https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/112889-cuwns-vidstrm-guide-00.html.

- **Outdoor AP in SDA**: SDA is supported in Cisco Aironet 1540 and 1560 APs operating in Local mode.

- **Cisco Wave 1 APs as Workgroup Bridges in SDA**: Cisco Wave 1 APs operating as Workgroup Bridges (WGBs) is supported in SDA.

  Note Cisco Wave 2 APs as WGBs in SDA is in Early Field Trial state and not yet officially supported.

For more information about Software-Defined Access, see the following documentation:

- "Software-Defined Access" chapter in the configuration guide: https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-8/config-guide/b_cg88/sda_wireless.html

- *SD-Access Wireless Design and Deployment Guide*: https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-5/b_SD_Access_Wireless_Deployment_Guide.html

One-to-One Mapping of WLAN with EoGRE VLAN

The EoGRE implementation for open WLANs is limited to 10 WLANs per VLAN per controller. This limitation can be overcome by having a one-to-one mapping between open WLANs and EoGRE VLANs.

A one-to-one mapping of WLAN with EoGRE VLAN can be achieved by overriding the EoGRE VLAN configuration within the WLAN. All the existing rules are still applicable; however, if you enable EoGRE VLAN override, the VLAN ID that you specify is overridden with EoGRE VLAN ID, which is configured in the tunnel profile that is mapped to the WLAN.

The order of precedence is as follows:

1. If the AAA override option is enabled on the WLAN, then AAA values are applied.

2. If the EoGRE VLAN configuration override option is enabled, then EoGRE VLAN configuration values are applied on the VLAN ID specified.

3. Network Access Identifier (NAI) matched in the EoGRE profile rule.

You can track this enhancement in the CSCuy30302 caveat.

For more information, see

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-8/config-guide/b_cg88/client_data_tunneling.html#eogre.

Identity PSK with Peer-to-Peer Blocking

The Identity PSK (IPSK) feature is enhanced to configure peer-to-peer (P2P) blocking or bridging. This enhancement is applicable in scenarios where clients or IoT devices with different or same PSKs on the same

WLAN have to be prevented from communicating with each other. With this enhancement, it is possible to differentiate private PSK client traffic. This enhancement is supported only in Local mode.

For more information, see

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-8/config-guide/b_cg88/wlan_security.html#peer-to-peer-blocking-using-psk-tag.

Lawful Interception of Traffic

This feature is implemented to meet the need for lawful interception of traffic for monitoring purposes.

APs create syslog-based records for the traffic and send these records to the controller. Traffic from both IPv4 and IPv6 protocols is captured. At defined intervals, the controller sends these syslog records to the syslog server.

For more information, see

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-8/config-guide/b_cg88/lawful_interception_of_traffic.html.

Captive Portal Enhancement

It is possible to configure external redirect URL at the AP group level apart from the existing configuration options at the global and WLAN levels. This enhancement is to enable you to configure multiple splash pages for the same SSID.

If both WLAN and AP group configurations do not override the global configuration, then the global configuration is used.

If either WLAN or AP group configuration overrides the global configuration, then the specific redirect URL that is configured is used.

If both WLAN and AP group configurations override the global configuration, the AP group configuration is used because the AP group configuration takes precedence over the WLAN configuration.

For more information, see

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-8/config-guide/b_cg88/configuring_ap_groups.html#captive_portal_for_ap_group.

Policy Enforcement and Monitoring Usage

This feature helps in providing continued data bandwidth to clients after the allocated high-speed data bandwidth has exhausted albeit at lower data rates. This dynamic policy override works on L2 and L3 client authentication.

AP sends the client bandwidth usage report to the controller at a set duration. The controller sends these reports to the accounting server at a set duration. When the client exhausts the data limit, the AAA server sends a change of authorization (CoA) request. The controller changes the policy parameters after receiving confirmation from the AAA server.

The policy change and data rate change occur without disconnecting the client.

This feature is supported in the following modes:

- Central Switching; Local and Bridge mode
- Local Switching; FlexConnect and Flex+Bridge mode

For more information, see

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-8/config-guide/b_cg88/wlan_security.html#policy-enforcement-quota-mgmt.

Application Visibility and Control Enhancements

NBAR2 Protocol Pack Upgrade

Before Release 8.8, controllers supported NBAR engine version 23, and the default protocol pack version was 19.1. To support more applications on the controllers, especially Wi-Fi Calling, Zoom, and so on, Release 8.8 includes NBAR engine version 31 and protocol pack version 37 for controllers; for Cisco Wave 1 APs, the NBAR engine is version 23 and the protocol pack version is 14; for Cisco Wave 2 APs, the NBAR engine is version 35 and the protocol pack version is 33.

Note Enabling AVC in FlexConnect mode in an environment wherein both Wave 1 and Wave 2 APs are present will break AVC policies.

Default DSCP Value for AVC Profile

Before Release 8.8 with AVC enabled, you could override DSCP values for only those application flows that were configured on an AVC profile. For the application flows that were not configured, no action was performed and DSCP was left intact. The maximum number of application rules that the AVC profile can contain is 32. For managed service, to control and rewrite DSCP values (example with DSCP 0) for all flows that are not presented on the AVC profile is not possible.

In Release 8.8, the new enhancement includes a new *default-class* rule that you can use to override the DSCP values for all application flows in which AVC rule is not configured. The goal of this enhancement is to protect the network for all flows with unwanted or controlled DSCP values.

This enhancement comes with the following restrictions:

- Only the start of an application flow is captured.
- Supported only for marking. Rate limit and drop are not supported.
- Default DSCP works only if AVC is in enabled state.
- An AVC profile can support up to 32 rule, including the *default-class* rule. If the *default-rule* is configured, you can configure up to 31 rules.
- Multicast and broadcast flows are not supported.
- IPv6 is not supported in AVC.
- Cascading of rules is not supported, which means that for the same flow, it is not possible to have rate limiting and marking. Therefore, if rate limiting is performed for a flow, *default* marking is not performed on the flow.

Note

- The *default-class* setting overwrites all DSCP values for all the application flows that are not configured when the profile is applied to a WLAN.
- If you have an AVC profile with *default-class* setting and you downgrade from Release 8.8 to an earlier release, the *default-class* setting is still present in the controller, although the earlier releases do not support this setting.

Cisco Wave 2 AP Features

Support is added for the following features in Wave 2 APs in this release:

- Flex+Mesh
- CAPWAP IPv6
- Auto-LAG in FlexConnect mode

  Note This feature is supported only in Cisco Aironet 2800, 3800, and 4800 Series APs.

- USB port as a power source

  Cisco Aironet 2800 and 3800 Series APs have a USB port that can act as a source of power for some USB devices. The power can be up to 2.5W; if a USB device draws more than 2.5W of power, the USB port shuts down automatically. For more information, see

  https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-8/config-guide/b_cg88/ap_power_and_lan_connections.html#info_ap_usb_port_as_power_source.

- DHCP on root access points

  Internal DHCPv4 server is supported in root access points (RAPs) operating in Flex+Mesh mode. This feature is supported only in Cisco Aironet 1540 and 1560 APs.

  Network Address Translation (NAT) and Port Address Translation (PAT) in RAPs operating in Flex+Mesh mode is coupled with the internal DHCP server support. NAT/PAT on RAPs start when you start the DHCP server and stops when you stop the DHCP server.

Miscellaneous Enhancements

- **Disabling AP fallback to DHCP when configured for static IP addresses**: Cisco APs can fall back from static IP mode to DHCP mode when they are not able to associate with a controller. While it is useful to get the APs to fall back to DHCP mode so that they continue to serve clients by getting a new IP address, the APs retain their new IP address until they are rebooted. In a network where the APs are assigned static IP addresses, the DHCP IP addresses prevent the APs from being monitored. To address this issue, you can choose to retain the static IP addresses for APs by disabling the fallback to the DHCP option.

  This enhancement is tracked in CSCua58662.

  For more information, see

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-8/config-guide/b_cg88/managing_aps.html#retaining_static_ip_on_ap_cli.

- **ARP debugs**: In Release 8.8, when ARP debugs are enabled along with debugging of clients, it is possible to filter and view ARP debugs for a specific client instead of listing all the ARP transactions.

  This enhancement is tracked in CSCun60412.

- **Logging of configuration history**: You can view the logging buffer that is saved on the last reset or power cycle of the controller by entering this command:

  show logging config-history

  You can also retrieve the details of all the **config** commands that are executed in the current and up to two previous resets through a support bundle.

  This enhancement is tracked in CSCur14475.

  For more information, see

  https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-8/config-guide/b_cg88/debugging_on_cisco_wireless_controllers.html#ID200

- **FlexConnect client exclusion list**: You can view the FlexConnect clients in the exclusion list of an AP locally by entering this command on the Wave 2 AP console:

  show flexconnect client exclusion-list

  This enhancement is tracked in CSCux41096.

  For more information, see

  https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-8/config-guide/b_cg88/wlan_security.html#config-client-exclusion-policies.

- **SFP type information**: You can view the SFP type information on Cisco 5520 and 8540 controllers by entering this command:

  show port sfp-info

  This enhancement is tracked in CSCva88371.

- **Platform information in a debug session**: In the controller CLI, at the start of a debug session, a message is displayed indicating the platform details for which the debug session is being started. This message contains the following information: timestamp, controller model, software release information, serial number of the controller model, and the hostname.

  This enhancement is tracked in CSCvf03977.

  For more information, see

  https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-8/config-guide/b_cg88/debugging_on_cisco_wireless_controllers.html#ID200

- **Extension of | include filtering**: Before this release, some **show** commands on the Wave 2 AP console allowed filtering using the **| include** option. In Release 8.8, this option is extended to all the **show** commands.

  This enhancement is tracked in CSCvg42570.

- **IPv6 in Flex+Mesh mode**: IPv6 is supported in Flex+Mesh mode.

- **DHCP with NAT**: DHCP is supported in APs with NAT (only IPv4).
- **Federal certification requirements**: To meet federal certification requirements wherein, in a High Availability scenario, data between active and standby controllers must be encrypted. This requirement is achieved by doing IPsec encryption with certificates on the HA controllers.

Early Field Trial Features

The following features are in Early Field Trial state:

Note These features are not yet officially supported and there will be no assistance from Cisco's Technical Assistance Center.

- Controller Telemetry:
    - Wireless Service Assurance.

      For more information about configuring Wireless Service Assurance, see the applicable *Cisco DNA Center User Guide* at:

      https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-user-guide-list.html.
    - Intelligent Capture
- Cisco Wave 2 APs as Workgroup Bridges

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 releases 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 releases 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 Wireless Release 8.8.x

Current Software Release	Upgrade Path to Release 8.8.x
8.2.x	You must upgrade to an 8.5.x release and then upgrade to Release 8.8.x.
8.3.x	You must upgrade to an 8.5.x release and then upgrade to Release 8.8.x.
8.4.x	You must upgrade to an 8.5.x release and then upgrade to Release 8.8.x.
8.5.x	You can upgrade directly to Release 8.8.x.
8.6.x	You can upgrade directly to Release 8.8.x.
8.7.x	You can upgrade directly to Release 8.8.x.

Upgrading Cisco Wireless Release

This section describes the guidelines and limitations that you must be aware of when you are upgrading the Cisco Wireless release and the procedure to upgrade.

⚠

Caution Before you upgrade to this release, we recommend that you go through the following documents to understand various issues related to Cisco Wave 1 AP flash and the solution to address them:

- Field Notice: https://www.cisco.com/c/en/us/support/docs/field-notices/703/fn70330.html
- Understanding Various AP-IOS Flash Corruption Issues: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/213317-understanding-various-ap-ios-flash-corru.html

Guidelines and Limitations

- Legacy clients that require RC4 or 3DES encryption types are not supported in Local EAP authentication.
- If you downgrade from Release 8.8.x to Release 8.7, FlexConnect IPv6 ACLs are shown to be in their FlexConnect group.
- If you have an AVC profile with *default-class* setting and you downgrade from Release 8.8.x to an earlier release, the *default-class* setting is still present in the controller, although the earlier releases do not support this setting.

- If you want to downgrade from Release 8.8.x to Release 8.6.101.0 and if you have Wave 2 APs in Flex+Bridge mode, ensure that these APs are changed to Bridge mode before you perform the downgrade; else, the APs will have incorrect configuration after the downgrade process.
- If you are upgrading from Release 8.0.140.0 or 8.0.15x.0 to a later release and also have the multiple country code feature configured, the feature configuration is corrupted after the upgrade. For more information, see CSCve41740.
- 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 the controller to download a new controller software image or to reboot the controller after the download of the new controller software image. You can forcefully reboot the controller by entering the **reset system forced** command.
- It is not possible to download some of the older configurations from the controller 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.
- When a client sends an HTTP request, the controller intercepts it for redirection to the login page. If the HTTP GET request that is intercepted by the controller is longer than 2000 bytes, the controller drops the packet. Track the Caveat ID CSCuy81133 for a possible enhancement to address this restriction.
- When downgrading from one release to an earlier release, you might lose the configuration from your current release. The workaround is to reload the previous controller configuration files that are saved in the backup server, or to reconfigure the controller.
- When you upgrade controller to an intermediate release, wait until all the APs that are associated with the controller are upgraded to the intermediate release before you install the latest controller 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 controller 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 controller is also automatically upgraded. When an AP is loading software, each of its LEDs blinks in succession.
- Controllers support standard SNMP MIB files. MIBs can be downloaded from the software download page on Cisco.com.
- The controller software that is factory-installed on your controller and is automatically downloaded to the APs after a release upgrade and whenever an AP joins a controller. 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 controller 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 controller 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.

- The controller 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, from the **Boot Options** menu, choose **Option 2: Run Backup Image** to boot from the backup image. Then, upgrade with a known working image and reboot controller.

- 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 controller.

  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 controller or any AP during the upgrade process. If you do this, the software image might get corrupted. Upgrading controller 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 controller must not be reset during this time.

- After you perform the following functions on controller, 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.

Upgrading Cisco Wireless Software (GUI)

Procedure

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

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

Step 2 Follow these steps to obtain controller software:

a) Browse to the Software Download portal at: https://software.cisco.com/download/home.
b) Search for the controller model.
c) Click **Wireless LAN Controller Software**.
d) The software releases are labeled as described here to help you determine which release to download. Click a controller 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.

e) Click the filename <*filename.aes*>.
f) Click **Download**.
g) Read the Cisco End User Software License Agreement and click **Agree**.
h) Save the file to your hard drive.
i) Repeat steps *a* through *h* to download the remaining file.

Step 3 Copy the controller software file <*filename.aes*> to the default directory on your TFTP, FTP, or SFTP server.

Step 4 (Optional) Disable the controller 802.11 networks.

Note For busy networks, controllers on high utilization, and small controller 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 controller.

A message indicating the status of the download is displayed.

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 controller.

Step 17 If you have disabled the 802.11 networks, reenable them.

Step 18 (Optional) To verify that the controller software is installed on your controller, on the controller 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 4: 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 5: 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 6: 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 controller software with other client devices.

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

Table 7: Test Bed Configuration for Interoperability

Hardware or Software Parameter	Hardware or Software Configuration Type
Release	8.8.x.
Cisco Wireless Controller	Cisco 5520 Wireless Controller
Access Points	AIR-CAP3802E-B-K9, AIR-AP1852E-B-K9

Hardware or Software Parameter	Hardware or Software Configuration Type
Radio	802.11ac, 802.11a, 802.11g, 802.11n (2.4 GHz or 5 GHz)
Security	Open, PSK (WPA-TKIP-WPA2-AES), 802.1X (WPA-TKIP-WPA2-AES) (EAP-FAST, EAP-TLS)
RADIUS	Cisco ACS 5.3, Cisco ISE 2.2, Cisco ISE 2.3
Types of tests	Connectivity, traffic (ICMP), and roaming between two APs

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

Table 8: Client Types

Client Type and Name	Driver / Software Version
Laptops	
Acer Aspire 15 Windows 8 Home	Qc Atheros Qca9377 11.0.0.492
Acer Aspire E15 Windows 8	Qc Atheros Qca9377 15.1.1.1
Acer Aspire E 15 Windows 8.1	QC Atheros Qca9377 11.0.0.492
Acer Aspire E15 Windows 8.1 Pro	Qc Atheros Qca9377 11.0.0.492
Dell Inspiron 15 7569 Windows 10 Home	Ntel Ac 3165 18.32.0.5
Dell Latitude 6430 Windows 8.1 Pro	Intel 6205w8 15.16.0.2
Dell Latitude E5430 Windows 7	Intel Centrino N 6205 15.17.0.1
Dell Latitude E5450 Windows 7 Professional	Intel 7260 18.33.6.2
Dell Latitude E5540 Windows 7	Intel Dualband Ac7260 1.566.0.0
Dell Latitude E6430 Windows 7 Professional	Intel Centrino Ultn6300 15.9.2.1
Dell Latitude E6430 Windows 7 Professional	Intel 6250 15.11.0.7
Dell Latitude E6430 Windows 7 Professional	Intel 3160 6.30.223.215
Dell Latitude E7450 Windows 7 Professional	Broadcom 1560 15.1.1.1
Dell Latitude Windows 8.1 Pro	Intel Ac7260 18.33.3.2
Fujitsu Lifebook E556 Windows 10 Pro	Intel 8260 11.0.0.492
Lenovo Yoga 460 Windows 10 Pro	Intel Ac8260 19.1.0.4
Macbook Air Mac OS Sierra 10.12.3	Broadcom Bcm43xx 1.0 6.30.225.29.1
Macbook Air Macos Sierra 10.12.6	Broadcom Bcm43xx 1.0 7.21.171.68.1a4
Macbook Air OS X Yosemite (10.10.5)	Broadcom Bcm43xx 1.0 7.15.166.24.3
Macbook Mac OS Sierra 10.12 Beta	Broadcom Bcm43xx 1.0 7.21.149.34.1a7

Client Type and Name	Driver / Software Version
Macbook Pro Mac OS Sierra 10.12.4	Broadcom Bcm43xx 1.0 7.21.171.68.1a4
Macbook Pro OS X 10.8.5	Broadcom Bcm43xx 1.0 5.106.98.100.17
Macbook Pro Retina Mac OS Sierra 10.12.3	Broadcom Bcm43xx 1.0 7.15.166.24.3
Tablets	
Apple iPad	iOS 9.3.1
Apple iPad mini	iOS 12.0
Apple iPad mini 2	iOS 10.3.1
Apple iPad Air	iOS 10.1.1
Apple iPad Air 2	iOS 10.2.1
Mobile Phones	
Apple iPhone 4S	iOS 8.0
Apple iPhone 5	iOS 10.3.1
Apple iPhone 5C	iOS 9.3.2
Apple iPhone 6 Plus	iOS 12.0
Apple iPhone SE	iOS 10.3.1
AT100	Toshiba Android 4.0.4
Cisco 7925G-EX	CP7925G-1.4.8.4.LOADS
Cisco 7926G	CP7925G-1.4.8.4.LOADS
Cisco 8821	sip8821.11-0-4-14
ET1	Android VERSION 2.3.4
ET5	Android 5.1.1
LG-D855	LG Android 5.0
Mediapad X1 7.0	Huawei Android 4.4.2
Moto X 2nd Gen	Motorola Android 5.0
One Plus One	One Plus Android 4.3
One Plus Three	One Plus Android 6.0.1
Samsung Galaxy S4	Samsung Android 4.2.2
Samsung Galaxy S4	Samsung Android 5.0.1
Samsung Galaxy S6	Samsung Android 7.0
Samsung Galaxy S6	Samsung Android 6.0.1
Samsung Galaxy S8	Samsung Android 7.0
Samsung Tab Pro	Samsung Android 4.4.2

Client Type and Name	Driver / Software Version
SM-P600	Samsung Android 4.4.2
SM-T520	Samsung Android 4.4.2
TC510K	Zebra Android 6.0.1
TC8000	Zebra Android 4.4.3
8742	Spectralink Android 5.1.1
8744	Spectralink Android 5.1.1 2.5.0

Key Features Not Supported in Cisco WLC Platforms

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

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

Key Features Not Supported 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 5520 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

Key Features Not Supported in Cisco Virtual WLC

- Cisco Umbrella
- Software-defined access
- Domain-based ACLs
- Internal DHCP server
- Cisco TrustSec
- Access points in local mode

- Mobility or Guest Anchor role
- 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 Cisco WLC 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 only in local switching mode)
- Workgroup bridges
- Client downstream rate limiting for central switching
- SHA2 certificates
- Cisco WLC integration with Lync SDN API
- Cisco OfficeExtend Access Points

Key Features Not Supported in Access Point Platforms

This section lists the features that are not supported on various Cisco Aironet AP platforms:

Key Features Not Supported in Cisco Aironet 1800i, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800, 3800, and 4800 Series APs

For detailed information about feature support on Cisco Aironet Wave 2 APs, see:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-7/b_feature_matrix_for_802_11ac_wave2_access_points.html.

Table 9: Key Features Not Supported in Cisco Aironet 1800i, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800, 3800, and 4800 Series APs

Operational Modes	• Autonomous Bridge and Workgroup Bridge (WGB) mode • Mesh mode • 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)
FlexConnect Features	• Split Tunneling • PPPoE • Multicast to Unicast (MC2UC) **Note** VideoStream is supported • Traffic Specification (TSpec) • Cisco Compatible eXtensions (CCX) • Call Admission Control (CAC) • VSA/Realm Match Authentication • 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 10: Key Features Not Supported in Cisco Aironet 1800i, 1810 OEAP and 1810W Series APs

Operational Modes	Mobility Express
FlexConnect Features	Local AP authentication
Location Services	Data RSSI (Fast Locate)

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

Table 11: 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
Location Services	Data RSSI (Fast Locate)

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

Key Features Not Supported on Cisco Aironet 1560 APs

- MAC Authentication FlexConnect Local Authentication
- Noise-tolerant fast convergence
- Static WEP

Caveats

Open Caveats

Table 12: Open Caveats

Caveat ID Number	Description
CSCvg76166	Channel Utilization changes to 0% on Wave 1 Marvell APs
CSCvg91770	1810W AP stops to send data frame intermittently
CSCvg93221	802.11AC wave2 outdoor APs do not support all MESH modes for multicast
CSCvh81618	When adding a member to RF Group with Static Leader 8510, group size exceeded error
CSCvi06408	Wave 1 AP failed to send DHCP packet to wired side under VLAN Override
CSCvi38539	AP stops forwarding IPv6 Router Advertisements to random clients
CSCvi48503	Standby WLC constinuously reboots with "Reason: XMLs were not trasferred from Active to Standby"
CSCvi55945	8.8:NBN AP Neighbor Info show backhaul CH missing vs. CLI for 40MHz backhaul and Rate mismatched
CSCvi69688	8.8 - No of RUN state clients in standby is more than Active Controller.
CSCvi77694	WLC leaks dyn interface traffic from untrusted VLAN to trusted VLAN while in cntrl webauth req state
CSCvi80205	ETSI domain Compliance and Throughput testing
CSCvi82147	Failed to set Country Codes when WLC has redundant country codes CA2, KR, PH2, US2, USL, USX
CSCvi82746	Cisco WLC running 8.5.120.0 release reloads unexpectedly with Task Name SISF BT Process
CSCvi92170	Cisco 1800 series APs falsely shows 100% channel utilization on 5GHz
CSCvi96793	R0KHId and R1KHID going zero in assoc response for IPhone on 8.6 ME, causing connectivity issue.
CSCvi98368	AP 1815I stops working due to kernel panic in radio driver, PC is at ieee80211_node_unauthorize+0x48
CSCvi98415	AP 1815I stopped working due to kernel panic during radio reset in 8.3.140.0
CSCvj06563	AIROS WLC crashed at mmListenFsm with config mesh subset-channel-sync enable in IRCM with ewlc

Caveat ID Number	Description
CSCvj06837	MAP Wave 1 AP mesh security failures after roaming between 2 parents
CSCvj08387	WLC stopped working on spamApTask6
CSCvj11716	WLC failed to apply flex-acl returned from RADIUS server - policing not working, client passing traf
CSCvj23235	WLC: Need to change active fall-back of AAA probing w/probes of 'dead' RADIUS server
CSCvj23415	8.8: Wave 2 or Wave 1 AP cannot swap image after pre-download image completed successfully
CSCvj29870	8.8:Space detected on UI but CLI cannot for "flexconnect acl url-domain url"/"ext-webauth-url"
CSCvj30568	1832 AP stopped working due to beacon stuck, QCA case 03406780
CSCvj31604	8.8:"<IP addr> should be non zero and must have contiguous ones" but 0.0.0.0 can/ no sense for ones
CSCvj32199	SSH/Management Access of Primary WLC not possible when HA failover occurs in 8.5.120.0
CSCvj34879	AP reporting MD5 mismatch on poller script after running all flash bug fixes
CSCvj42758	RADIUS auth server insertion not proper with RADIUS DNS returning multiple entries
CSCvj43325	AP1850 running 3.7.5 is deauth client when received 2 assoc_req with same snonce
CSCvj50741	8.8: Clients get disconnected while AP joining back the WLC
CSCvj52635	ME Subordinate AP may send Disassociation after primary AP failover
CSCvj53235	Local policy using HTTP device profiling does not get applied to client.
CSCvj56689	8.5 MR3: AP1850 stopped working due to OOM
CSCvj58436	OID not increasing error when doing an IPv6 host query
CSCvj58606	8.8 ME: EoGRE Gateway entry gets removed from the AP when the tgw is down
CSCvj60609	vWLC Webauth not working
CSCvj65449	AIR-AP1562D-E-K9 with regulatory domain Kazakhstan does not join the WLC
CSCvj65592	Client static DNS ip support for openDNS
CSCvj69083	Guest user is removed from Standby controller after WLC reset
CSCvj69417	Wave 1 AP sends ACK at supported data rates
CSCvj70836	"show system slabtop" command not showing the system details

Caveat ID Number	Description
CSCvj72076	AP1800 drops a lot of packets
CSCvj72136	Barbados AP (2800/3800) loses its default gateway reachability
CSCvj73077	1810W APs may have power denied from older POE 802.3af switches
CSCvj73809	WLC: Invalid parameter specified error in CLI when trying config change
CSCvj74163	Monitor mode should not be allowed for AP1542
CSCvj74263	IPsec profile showing junk characters in show logging
CSCvj76009	Alpha 3800/2800 multiple WSA Agent process running, that might be the cause of OOM trigger
CSCvj76143	EoGRE tunnel profile VLAN is allowing to add alphanumeric values instead of numeric values
CSCvj79479	Cisco 8500 Wireless LAN Controller Web Interface Unvalidated Redirect Vulnerability
CSCvj79841	3802 AP unexpected reboot on 8.2.167.1
CSCvj79842	WLC does not reply keepalive and causes APs to drop line
CSCvj80129	Wave 1 AP uses invalid CAPWAP-Data keep-alive source port
CSCvj80359	Stale client entries exist in temporary data in Active WLC
CSCvj80688	Web: Remove APs or add APs in AP group pointing to main page if you try to add or remove APs
CSCvj80969	AP1530:8.3.141.153 5ghz 40 and 20Mhz Upstream Minimal TP drop is seen for Smaller packet size
CSCvj81510	When saving config on 1815I, UI throws error which does not tell the user about why it is failing
CSCvj82636	Client getting redirected to internal webauth instead of External webauth URL configured on AP Group
CSCvj83144	Able to configure the WLC interface without assigning any port from virtual wlc (vWLC) GUI
CSCvj83372	AP 1852 showing irregular data usage
CSCvj83659	8.8:Queueing WMI command back to TxQueue and buff leak messages on flex ap console
CSCvj85461	Disabling Data Rates of 6 or below disables 11 Mbps as well on Mobility Express UI
CSCvj86238	WLC stops working as emWeb spikes to 100% CPU usage after executing "show run-config"

Caveat ID Number	Description
CSCvj86324	1700 AP stopped working multiple times - SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header
CSCvj88091	custom-web ext-webauth-url getting corrupted with customer configuration
CSCvj88099	UsmDb:HA_send_usmDbSxpPeerConnectionSet, ErrType:Apply Config failed, Reason:19
CSCvj88984	FlexConnect efficient upgrade disables when invalid configuration is provided
CSCvj91539	3800 AP stops working at sxpd process during SGT-IP binding exchange with peer switch
CSCvj91645	Clients not getting exported to anchor on New Mobility
CSCvj91805	WLC not providing error message while creating wrong IPv6 address
CSCvj93292	IOS AP is changing to sensor mode without WSA enabled from AP console
CSCvj94236	AP: Radio Init failed causing multiple wcpd crashes
CSCvj94659	Unable to update TACACS+ DNS parameters on configuring IPv6 DNS server under global settings
CSCvj94880	1810W - Clients not getting DHCP
CSCvj94919	702w AP running vlan ID is NA after AP reboot
CSCvj95739	Standby failing to add exclusion client - exclusion client mismatch between Active and Standby WLC
CSCvj96809	8.8_ Edit all page in mobility is not working properly, when encryption is enabled
CSCvj96920	8.8 NBN: Unable to add Flex WLAN-ACL mapping on AP until WLAN is enabled at least once
CSCvj97430	Mobility Express AP - Loop detected causes AP reboot
CSCvj98913	8.8 - "%ACL-3-RULE_DONOT_EXIST: [SA]ace_api.c:983 Unable to get IP address parameter" msg in msglog
CSCvj98950	Primary/Secondary Backup-controller config with v6 address fails for Click AP
CSCvj98989	On every execution of "show capwap client ha" appends "set_snap"
CSCvk00884	The WLC is replying with the wrong value for the following OID: bsnAPIfProfileParamAssignment
CSCvk00889	3802/2802 APs with -S domain rejected to join the switch due to Invalid regulatory domain.
CSCvk02153	Wave 1 AP WLAN Client Stats cldcClientDataRetries counter is zero
CSCvk03686	EoGRE client count is not getting cleared in Standby on switching SSID

Caveat ID Number	Description
CSCvk03882	Sensor mode AP coming as FlexConnect after ME forced failover
CSCvk09513	AP is not downloading the WLC 85Mr3 image rather it says image is already in the backup
CSCvk09627	In 8.9.1.60 in WLC "show ap config 802.11a <ap_name>" unable to print the correct Bandwitdth
CSCvk09764	WLC8.8 Smart License: AP In Use Count does not go UP when new APs are joining
CSCvk09888	AP1815 stopped working while changing mode from FlexConnect to local
CSCvk10190	8.8: HA sync failure: UsmDb:HA_send_usmDbSpamSetApMode, ErrType:Apply Config failed on Standby
CSCvk10891	8540: High latency under load with AVC, TCP fragmentation
CSCvk12146	Spurious messages getting printed on Barbados AP while Enable/Disable wlan
CSCvk12422	ME Controller rebooting twice after LSC AP Auth State to 802.1x port authentication /both
CSCvk13835	Sensor mode APs is not downloading the image after primary failover
CSCvk14062	ping delay happens with other traffic load
CSCvk14080	8.8: Standby WLC reboot with IPC failures: RP back to back connected
CSCvk14267	Observed XML and Invalid config during upload/download WLC config.
CSCvk14419	In WLC GUI with read only mgmt user able to ping LDAP server IP
CSCvk15043	Wave 1 APs - AP radio FW image install failure in the bootup loop
CSCvk15527	EoGRE tunnel configuration is not pushed to APs when AP moved from one WLC to another
CSCvk16522	show logging config-history and show logging last-reset issues
CSCvk17291	Operating system info missing on client 360 page for macos only
CSCvk17426	ME: ACLs are getting deleted after upgrade
CSCvk18752	Incorrect VCI string of DHCP option 60 on AP 1815
CSCvk19951	AP exec timeout value is not reflected properly
CSCvk20402	Last reset details not showing after reset/upgrade/downgrade
CSCvk20899	AP4800 "vendor_send_mgmt_frame VAP 14 is not up" message flooding console
CSCvk21153	AP3800: TxPower changes after moving channel and back to orginal channel
CSCvk22312	hotspot2 OSU SSID is picking profile name

Caveat ID Number	Description
CSCvk23248	ME controller rebooting twice after changing the LSC AP Auth configuration in UI
CSCvk23423	WLC GUI displaying error message while disabling dhcp proxy-mode
CSCvk23577	Client is unable to connect due to "Failed to create a timer"
CSCvk23664	8.8: FlexConnect split tunnel does not work when the ACL is configured in FlexConnect group
CSCvk23822	In 8.8.1.161 TP drop is observed in Downstream with 5ghz 80/40/20 Mhz in all packets size
CSCvk24360	WLC power supply status is incorrect when there is no power supply
CSCvk24427	Traps related to protocol pack load not sent on installing AVC protocol pack
CSCvk26002	Mesh links are not shown on Outdoor Area View if APs are in FlexBridge mode
CSCvk26519	1562 MAP stops sending Block ACK once the 1572 RAP moves to another WLC
CSCvk26539	AP1815 intermittently dropping packets
CSCvk26545	In 8.8.1.182 AP2700 TP drop in Upstream for 5Ghz 80/40/20 Mhz across all packet size
CSCvk26563	AP1810W 5G radio FW assert @0x009A4F9F 8.2.170.4
CSCvk26607	Global Multicast is disabling after ME reset
CSCvk27093	NAS-ID in WLAN cannot be changed in the startup-command after you saved once
CSCvk27250	System not operational with task apfRogueTask_3
CSCvk28143	WLC crashed with SNMPTask in 8.5.137.10
CSCvk28371	hotspot2 OSU SSID is picking profile name
CSCvk29178	1550 BVI interface uses a different MAC-Address than the Gigabit interface
CSCvk30585	8.8_"Missing 802.1X or client control block" Errors in WLC Message Logs
CSCvk30807	Wave 1 AP mesh AP reloading due to Reload requested by Net Background
CSCvk31484	Upstream traffic rate is slow via specific Wave 2 AP
CSCvk32494	Encrypted mobility:UI throws wrong error message while adding mobility peer
CSCvk33107	8.8: Clients not able to connect due to M2 MIC failure
CSCvk35047	WLC stops working when LAG mode is enabled on the AP
CSCvk35275	5508 WLC stopped working at Task Name - EAP_Framework_0
CSCvk36257	8.8 - Local-Split WLAN-ACL mapping is retained at AP after it is removed from WLC

Caveat ID Number	Description
CSCvk36463	Support Bundle output only genertaes WSA core bundle when WSA is enabled
CSCvk36887	Some clients cannot associate because their entry is not getting deleted at the WLC.
CSCvk37153	8.8 - 6K entries of "config ap syslog host global <IP>" in uploaded config
CSCvk37576	SessionID should be added and decoded from Handoff packet.
CSCvk37877	TACACS user:Getting faild msg"SNMPv3 user lockout attempts configuration failed"
CSCvk39841	Change SSID name with SNMP fails with commitFailed
CSCvk39948	WLC is not returning the expected prompt when logging in via SSH
CSCvk40074	Switchdrvr unresponsiveness triggered by DB services crash
CSCvk40132	8.8: UI accepts Prefix length 0 with error static IPv6 configured, but incorrect IPv6s or missing/
CSCvk40571	Partial Collection Failure state for WLC 3504
CSCvk41068	Advance IPMI is not set and causing fan noise
CSCvk41447	AP auth local user authentication fails once deleting and adding the local user back
CSCvk41500	Hotspot is enabling with Open/Guest security after change from WPA Enterprise
CSCvk41512	APX800 sniffer mode not sending frames with AMSDU 1500 Bytes to destination
CSCvk41583	Local Split traffic is goes through after removing ACL mapping
CSCvk41963	Observed "print_backtrace+48" message on all ME
CSCvk42191	AP3800 advertises RSN IE for an OPEN SSID.
CSCvk42314	8.8:"show client summary" pegged an extra count 1 without client data once a while periodically
CSCvk42592	Disabling "Out of box" in RF Profiles throws SNMP error
CSCvk42619	Client RF stats are not cleared when client role moving from Local to Export-Anchor
CSCvk43025	Local Split and Central path traffic stops after some time with 2800 APs
CSCvk43114	[SDA] WLC with a sensor AP is generating a "URL not reachable" error every hour
CSCvk43433	Passphrase as hex value is not supported in ME GUI for PSK WLAN
CSCvk44045	8.8:Config static IPv4 but still using DHCP IPv6 due to no reboot after IPv4 accepted
CSCvk44089	8.8:Note 8/Galaxy S7 Device Type improper, Local Profiling miss "Apple" for Manufacture Stats
CSCvk44492	WiSM2 continuously reloads without crash file

Caveat ID Number	Description
CSCvk44831	LSC cert:Click-AP not taking configured LSC cert keysize.
CSCvk45259	In Build 8.5.134.106 AP 2700 TP drop with 2% is seen in 5Ghz Downstream
CSCvk45492	AP TrustSec: AP does not retain CTS SXP peer connection and disabling CTS SXP state after reload
CSCvk46817	AIR-AP2802I not sending beacons with both radios in 5GHz
CSCvk46867	8.8: Unable to transfer code between HA controllers
CSCvk47740	Pre-auth ACLs are not configuring for RLAN in ME UI
CSCvk47879	Silent crash on WLC 5508 due to growing memory utilisation
CSCvk47937	Local-Split - Local traffic is failing when VLAN Tag is enabled.
CSCvk47949	Local-Split- Traffic to Local network fails after roaming from one ap to another in flexgroup
CSCvk51102	iOS captive portal taking 45 seconds to trigger in Local Web-Auth
CSCvk51464	8.8 ME: ME GUI doesn't display the IP the internal AP is using but rather the main IP
CSCvk51634	Wave 2 Flex Efficient Upgrade fails as primary AP sends empty image_str to WLC
CSCvk52144	8.5: SSH connection to WLC is not going through after longevity and stress conditions
CSCvk52187	Unable to configure TGW list with TACACS controller user in WLC UI
CSCvk52210	Cannot configure Management IP when WLC is in maintenance mode.
CSCvk52381	DNS-ACL - Webauth Redirect page is not working properly in CWA case
CSCvk52704	"config network multicast l2mcast disable <interface>" config is not blocking L2 mcast traffic
CSCvk52808	8.8 - SSH session closed with message "Incoming packet was garbled on decryption"
CSCvk52883	8.8:Local Profiling UI shows Manufacture Stats issues
CSCvk53015	IOS AP mapping incorrect FlexConnect VLAN
CSCvk53499	APs doesnt reconnect back, error log: System reached max concurrent DTLS Handshakes
CSCvk53511	8.5MR: 3504 Anchor WLC has multiple stale client entries after longevity/traffic test
CSCvk53743	8.5_New mobility:UI throws wrong error message while adding used public IP
CSCvk53873	8.5MR: Bulk sync completion traps flood from the Active WLC
CSCvk53963	DNS-ACL - 1815 ME switchdriver crashed in 8.8.2.18

Caveat ID Number	Description
CSCvk54001	IRCM: v6 peers not synched to standby - UsmDb:HA_send_usmDbMmMwarAddIPv6, ErrType:Apply Config fail
CSCvk54272	8.5MR: 3504 WLC stops working on task: reaperWatcher during webauth testing
CSCvk55651	AP1852 failure of association due to set CAPWAP tunnel failed
CSCvk56120	ME: Unable to create IPv6 ACL after creating and deleting multiple ACLs
CSCvk56509	Mobility:Edit all page hangs when some mobility group member doesn't have req args
CSCvk57014	AP: Sometimes creates empty radio core files without any information
CSCvk57269	Sanity: ME-4800 multicast traffic did not pass, tested with internal AP
CSCvk57361	FQ NMI reset on 2802 AP mrvlfwd dies
CSCvk58160	Stress test: AP1552H RAP stops working when AP CPU hits nearly 100 percent usage
CSCvk58429	WLC shows wrong pop-up when downloading web-auth certificate
CSCvk58501	AP radio unresponsiveness happened because of beacon stuck
CSCvk58625	Wireless management interface change should not be allowed when IPsec is enabled
CSCvk58924	8.5MR4 - IPv4 ACL is wrongly externalized in case of Flexconnect Local Switching.
CSCvk59040	8.5MR: 3504 mGig port should be allowed to be disabled when not mapped to MGMT/RMI interface
CSCvk59252	8.5MR: Service port configuration is lost after switchover
CSCvk59259	8.5MR4 - 3504 standby controller rebooted (Standby IPC failure) instead of maintenance state
CSCvk59498	AP3702 High CPU Utilization under NCI Rx. Unable to join WLC
CSCvk60394	2700 AP not ACK on QoS data packet from client occasionally
CSCvk60596	8.5MR4 - Clients/Security/eap-type is externalized as 3 when EAP-FAST is selected
CSCvk60986	AP CAPWAP MTU discovery fails for CAPWAP data
CSCvk61078	VLAN priority tag inside the EoGRE packet set to non-zero when 802.1p set to none in LOCAL mode
CSCvk61124	Samsung TV drops connection on its mgmt server due to incorrectly assemabled Packets received 1810w
CSCvk61577	AP: OOM stops working seen in 8.8.3.25 when intelligent capture enabled
CSCvk61599	RADIUS does not fall back to primary RADIUS server.
CSCvk61968	Incorrect QoS marking for upstream traffic when connecting Platinum WLAN

Caveat ID Number	Description
CSCvk62008	Sometimes AP does not send EAPOL frame after client reassociation
CSCvk62025	DNS-ACL- Wild card entry for v4 ACL is not getting applied in Client when v4 and v6 acls are used
CSCvk62034	DP stops working on WLC running 8.2.154.53
CSCvk62093	8.5MR4 - Non-Flexconnect IPv6 ACL is applied for Local switching Client
CSCvk62240	WLC Smart license 8.8: The license summary(information) is not syncing in after switchover
CSCvk62355	AP2800 running ME image 8.6.101.0, 8.7.106.0 crash in ewsContexSendRedirect200->ewaDate
CSCvk62680	WiSM2 not releasing licenses after reboot
CSCvk62909	Device profile does not work for certain Android phones. Profiled as Linux-workstation
CSCvk62915	'Nearby AP' stats shown multiple times with different dBm values for the same slot
CSCvk63215	Cisco 1852 series APs Kernel Panic due to NSS memory corruption
CSCvk63291	WGB not responding M3 message on 4-way handshake
CSCvk63452	8.5MR4:2800/3800 XOR CleanAir state is Down when Band in 160MHz while Up for 20, 40, 80MHz
CSCvk63459	3802, 4800 AP drops packets larger than 1426 (inner IP) with VxLAN
CSCvk63784	8.5MR4 - Error String is not getting updated in Last Error field in "show network assurance summary"
CSCvk64669	8.8.3.22 AP2700 TP drop is seen in Downstream and Upstream in 5 ghz 80/40/20 Mhz all packet size
CSCvk64674	Wave1 APs advertise Adaptive FT MDIE on probe response for open SSID
CSCvk64809	8.8 3504 WLC Mgig Stanby struck with ERROR: cvmx_cmd_queue_shutdown: Queue still has data in it.
CSCvk64829	Observing CMX Certificate error and WSA cert releated XML message on Mob Exp
CSCvk64928	AP stops working when we configure LSC keysize as 4096
CSCvk65128	8.5MR4:tar:can't open '/tmp/part.tar': No such file/"tar -xf /tmp/part.tar -C /bootpart/part2" fail
CSCvk65150	8.5MR4:UI pop-ups incorrectly when swap image fine, inconsistent error vs, CLI when image going
CSCvk65680	Profile: AP3602 has a radio core after transmitter seems to have stopped
CSCvk65886	Profile: AP3602 stops working in process Init after tracebacks with 8.5.137.24

Caveat ID Number	Description
CSCvk66354	8.5MR4 - GUI issues with Assurance Stats
CSCvk66635	8.5MR4: 3702NOS module AP stops working with Dot11 Driver
CSCvk66700	3500 series access point 5GHz radio stops working.
CSCvk66762	8.5MR4:Error sending/receiving register device request/rsp&ACT2 could not be registered in tam
CSCvk66896	FlexConnect AVC profiles not marking DSCP traffic
CSCvk66975	AP as a sensor reports all configured tests status as onboarding failure
CSCvk67140	Client unable to join SSID reason 54 from AP and WLC

Resolved Caveats

Table 13: Resolved Caveats

Caveat ID Number	Description
CSCvb26809	WLC should use port MAC for non LAG and box MAC for LAG
CSCvc62540	Smart Licensing next communication attempt pre-dates the controller time after reboot
CSCvc66728	WLC: Traceback pattern #2 on 8.2MR5 in apfProcessAssocReq
CSCvc80047	Unexpected AP reloads - dpaa_get_pool_id_from_ios_pool_ptr
CSCvd67485	Cisco 3700 AP Tx stop Radio reset due to false radio TX inprog count
CSCve64652	Cisco Access Point 802.11r Fast Transition Denial of Service Vulnerability
CSCve70752	SNMP issue: TX power level returns null causing Cisco PI, WLC sync to not update AP information
CSCve82488	Cisco Wave 2 APs in FlexConnect mode stop redirecting CWA clients after WLAN change
CSCvf10811	Sniffer mode APs should log more layer 1 information
CSCvf28459	Write of the Private File nvram:/lwapp_ap.cfg Failed on compare RCA needed (try = 1)
CSCvf31881	Cisco 2800 AP detects Intel Dual Band Wireless-AC 8260 as rogue client/AP
CSCvf63455	Linux Kernel 3.14.43 - inotify_handle_event() and vfs_rename() Privilege Escal ...
CSCvf66696	Cisco WLC Control &amp; Provisioning of Wireless Access Points Protocol Denial of Service Vulnerability
CSCvf66723	Cisco Wireless LAN Controller Directory Traversal Vulnerability

Caveat ID Number	Description
CSCvf80409	AP1815 not sending all traffic after period under load
CSCvf83391	Cisco 8.3 Release: AP reloads unexpectedly at TAMD ap-tam process
CSCvf86161	Bad magnitude calibration values in Triggerfish EEPROM
CSCvf89335	Cisco 3700 AP stopped working with memory allocation failure CAPWAP
CSCvf90411	[IOT 8.6 HSR]:IW3702 WGB radio 0 core after 30M up EAP-FAST security and script common cleanup
CSCvf99887	MAP Gigabit port being learned in Mesh management VLAN instead of client VLAN
CSCvg00507	Cisco 3700 AP reloads unexpectedly- PID 104: Process LWAPP Rogue Monitoring process
CSCvg07617	AP1810W:Kernel Panic reloads unexpectedly PC is at _ZN17ContentHashFilter11clear_staleEv+0x1ac/0x1d0
CSCvg18543	Cisco 3700AP TX jammed and radio reloads unexpectedly
CSCvg23810	PMTU change to 1500 from a lesser value is not reflected in AP
CSCvg28378	AP: cmd timeout AP radio reloads unexpectedly in 8.6 due to Rx hang
CSCvg35115	Cisco 3802 running 8.3.130 shows radio core without the crash file
CSCvg35220	Cisco 3702 AP- Fails to correctly map data traffic to SGACL
CSCvg35547	Cisco 3700 AP beacon stuck seen on 8.5.107.x image
CSCvg40339	Cisco 2800 AP in sniffer mode is missing huge amount of data packets
CSCvg40792	Client global IPv6 not correctly mapped to MAC address under certain conditions
CSCvg44450	Cisco 2800,3800,1560 AP cannot forward packets downstream; 'Failed to get ARP entry for WLC'
CSCvg53640	Cisco 1830 AP triggered FW assert for radio failure (beacons stuck)
CSCvg60758	Cisco Wave 2 APs drops TCP retransmit from server
CSCvg61878	Cisco Wave 2 APs: does not send k9w8 in LLDP Packets leading to false classification
CSCvg62039	False radar detection on AP 1832 with 40MHz CW
CSCvg62508	3702 AP sometimes maps SGT 0 to client even though ISE returns correct SGT
CSCvg67509	Cisco 1810W AP reloads unexpectedly over a kernel panic
CSCvg70352	Cisco 1832,1852 APs reloads unexpectedly due to kernel panic at 'kmalloc_poolid+0xb8/0x16c'
CSCvg70384	Cisco 1832/1852 AP radio reloads unexpectedly at 0x009A497D

Caveat ID Number	Description
CSCvg70787	8.6: 3802 Kernel panic PC is at skb_release_data+0xe0/0x230
CSCvg71816	Cisco 8510 controller: reaper reset due to unexpected reload with task tempstatus
CSCvg72918	Cisco 4800 AP on 8.7.1.x code configures channel of slot_0 band 5Ghz
CSCvg73522	Cisco 5508 WLC reloads unexpectedly due to memory leak in snmpApPowerTrap()
CSCvg73797	Cisco 2800, 3800 AP: Command timeout at 0x8000 in FW
CSCvg75182	MC:8.3MR4: Continuous stack trace print due to error on Wave 2 AP with 8.3.134.30
CSCvg75189	Cisco 1800 AP: Radio failure and firmware freeze
CSCvg75933	CPU ACL does not block webauth related ports
CSCvg76168	Cisco 1532AP 5GHz radio interface remains down due to DFS even when not all channels are in blocked list.
CSCvg77711	System reloads at random on running mesh commands
CSCvg78210	AP syslog config does not change level from AP syslog to informational it remains in emergencies
CSCvg78624	Cisco 2800, 3800 APs: channelization issue, all the APs are stuck on channel 36
CSCvg79381	AP: AP failed to send ApSecurityContext; resulting all hyperlocation dropped by CMX
CSCvg82066	Cisco 1815I AP reloads due to kernel panic
CSCvg82156	Cisco 2802E AP: Radio1 reloads unexpectedly
CSCvg82215	Silent reloads, data plane crashes, high latency when WLC receives jumbo frames
CSCvg82450	[vEWLC]:After SSO, wired-wireless and wireless-wireless traffic drops for 4-12 seconds.
CSCvg82672	NAT-PAT- AP losing NAT translation entry for ongoing continuous client traffic
CSCvg82784	Cisco Wave 2 APs start the Channel Availability Check (CAC) timer after rolling to a lower bandwidth
CSCvg83836	Clients cannot pass traffic with 1810W MAB FlexConnect local switching RLAN
CSCvg84824	AP Sensor: Does not forward DHCP offer data packet to sensor client over the air
CSCvg84897	AP-4800: XOR radio Rx-SOP threshold remains same after changing band from 2.4 GHz to 5GHz
CSCvg85175	Cisco WLC reloads unexpectedly with task name spamApTask0
CSCvg86324	WLC reloads unexpectedly with SNMP operation with Flex ACL
CSCvg86741	vEWLC:SGT tag not getting deleted when client is in webauth_pending

Caveat ID Number	Description
CSCvg87401	Cisco 1542 AP reloads unexpectedly when in Flex + Mesh mode
CSCvg87547	AP: Client disconnected due to idle timeout wrongly kicking in when client is going to power save
CSCvg88269	CTS-SXP default password not retain after upload and download the config.
CSCvg89145	[cmd timeout] wifi1: 0x801f=unknown intCode:0x001f last 0x8120=unknown
CSCvg89442	Cisco 5500 and 8500 Series Wireless LAN Controller Information Disclosure Vulnerability
CSCvg89705	Cisco 8540 standby WLC reloads unexpectedly on rsyncmgrIpcqTask while disabling HA
CSCvg89807	Silver QoS profile is assigned to RLAN when configuration is imported
CSCvg90113	8.7: AP removing the client wrongly though IPv6 pre-auth ACL present in the database with URL rules
CSCvg91108	WQE size constantly increasing, error messages
CSCvg91708	WLC emweb reloads unexpectedly at commandConfigSpamApAntennaMonitor
CSCvg91734	Cisco 1852/1832 AP: AP data traffic stall in HD environment
CSCvg91811	Cisco 4800 FW freeze on radio 1
CSCvg93191	Cisco 3800 AP beacon stuck when radio reloads unexpectedly with signature 'B0B0'
CSCvg94522	TxFSM stuck on Radio 0 with new signature
CSCvg94718	Standby WLC reloads unexpectedly on spamApTask
CSCvg94780	Cisco WLC reloads unexpectedly on 8.5.105.0 release
CSCvg94967	8.7.1.79 - Cisco 2800, 3800 APs ASKU - Unable to push config for APBeacon V-Ibeacon profile
CSCvg95476	Cisco 1810,1850 AP reloads unexpectedly with switch behind RLAN/Aux Port
CSCvg96160	Cisco WLC reloads unexpectedly after 1-day on 8.7 Alpha
CSCvg96183	Proxy ARP always enabled in Beacon IE for Flex mode AP irrespective of ARP cache config
CSCvg96852	Cisco 1815W SnifferMode AP beacons allows clients to join and blackhole traffic
CSCvg96864	Cisco 8.5MR1 to 8.5.107.110 Releases - Cisco 3702 AP radio core with reason 'Bad acq dtx'
CSCvg97013	Cisco 8540 WLC reloads unexpectedly on Task Name: emWeb on 8.5.110.0
CSCvg97208	Cisco 1852AP: Apple clients connection fails in 802.11r adaptive mode in WLAN

Caveat ID Number	Description
CSCvg97712	Cisco 1850 AP console flooded with 'Total NR report Length exceeds Max Buffer Size -1067447752'
CSCvg98048	Sensor: Getting error during test run: CRITICAL - Stuck at test index -1 Will restart WSA !
CSCvg98078	AP with Flex AVC visibility Tx frames with sequence jumps causing client to not process packets
CSCvg98786	IOS AP DTLS flap issue seen in pre commit sanity
CSCvg99101	MC:8.5:Radio FW crash seen on Cisco 1850 APs @0x009A646B
CSCvg99108	8.5 MR1 on Cisco 2702 AP reloads unexpectedly on dot11_rm_offchan_handle_fw_response_isr
CSCvg99310	8.7: AP IPv6 URL ACL rule miss-match leads to client packet drop
CSCvg99890	**config certificate generate** line of uploaded config is corrupted
CSCvh00153	Download of PKCS12 bundle failed for EAP-TLS WLAN
CSCvh00256	Cisco WLC has multiple open ports, cannot be properly secured
CSCvh00398	WSA: Flex RADIUS Stats data parsing fails
CSCvh01089	False beacon stuck issue due to no beacon updates in WCP message Host triggered a radio freeze
CSCvh01470	Cisco 5520, 8540 WLC: Little Endian issue while adding rules in iptables for snmptrap over IPsec
CSCvh02937	Sensor: wireless sensor is choosing SSIDs with very poor signals during Cisco Provisioning
CSCvh03995	WLC 3504: Returns error code 500 / unauthorized token error when trying to send data to Assurance
CSCvh04880	Sensor: Intermittent connectivity issues with EAP-FAST security
CSCvh05749	AP IP address showing as '0.0.0.0' on GUI while downloading new image
CSCvh07545	Cisco 2800, 3800APs Kernel Panic due to processing of Rx frames before driver is initialized
CSCvh08020	AP stuck in AP after upgrade: flashfs[0]: writing to flash handle Illegal Operation
CSCvh11158	Cisco Wave 2 APs do not apply TCP adjust MSS on Fabric or Flex local SSIDs
CSCvh11212	WLC with Internal DHCP not sending NAK
CSCvh12081	Time not synced with Version 4 and getting unwanted message and NTPQ status also not showing

Caveat ID Number	Description
CSCvh12398	8.7: IPv6 enforcement not working with 8.8.1.8
CSCvh12504	8.7: IP learning not happening for IPv4 URL ACL on configuring both IPv4 and IPv6 pre-auth ACLs
CSCvh12768	IOS 3700 AP could not join WLC over CAPWAPv6 tunnel using DHCPv6 address
CSCvh12943	Cisco 2800,3800APs on 87 code TLV-DEC-ERR-1 No proc for 1912,TLV-DEC-FAILED for TLV_VAP_PAYLOAD(276)
CSCvh14509	Queue full issue observed with NmspNormalTxQ, breached 1 time. having Capacity 65535
CSCvh14849	8.7:'Disable' selected for 'fabric' cannot filter qualified APs out
CSCvh14989	Client in RUN state on anchor with 0.0.0.0 IP address
CSCvh15015	Level-1 list for Radio 0 is blank
CSCvh15852	WLC GUI/SSH not accessible - emweb consuming 100% CPU
CSCvh16413	WLC system reloads unexpectedly with apfRogueTask_0
CSCvh16970	Cisco WLC does not apply ACL Template from PI correctly
CSCvh18096	CPU ACL does not block HTTPS traffic to management interface from wired client
CSCvh18868	In VWLC unable to config WLAN once created through GUI
CSCvh19127	Cisco 1815I AP no response from wired side
CSCvh20238	Cisco 2800, 3800 APs joining the WLC in flex-mode fail to update FlexACL in group policies
CSCvh20731	WLC-HA: Certificate transfer during HA pair up
CSCvh21486	WLC reloads unexpectedly due to Task apfMsConnectionTask when MBUF debug is enabled
CSCvh21605	ME - wired clients drop-off shortly after being started from **show client ap remote-lan**
CSCvh21632	ME: Console freezes while **transfer upload datatype signature**
CSCvh21812	Cisco 3802 AP - Apple Broken Antenna Detection feature - XML support
CSCvh21942	8.7: Cisco WLC reloads unexpectedly during FW upgrade on 2 Floor Beacons with task: dx_sync_task
CSCvh21953	Cisco Aironet 1560, 1800, 2800 and 3800 Series Access Point Denial of Service Vulnerability
CSCvh23344	Cisco Controller reloads unexpectedly on taskname emweb @ewaFormSubmit_route_list

Caveat ID Number	Description
CSCvh23473	Cisco 1572 AP shows incorrect regulatory power level for Qatar domain
CSCvh23785	AireOS WLC: Multiple wireless clients failing the broadcast Key refresh (M5).
CSCvh25039	SNMP causes unexpected reloads
CSCvh25368	Cisco Controller memory leak on CDP
CSCvh27557	Cisco 1562 AP limited to 54 Mbps in 2.4-GHz backhaul
CSCvh27570	cLSiIdrClusterAffectedChannels OID returning unexpected values
CSCvh28229	Incorrect count for cLApWlanStatsOnlineUserNum when SSID is changed
CSCvh28506	Cisco 3504 controller cannot use USB for file transfer
CSCvh30447	MAP changes its statically assigned non-backhaul channel after it rejoins RAP
CSCvh30872	Decrypt errors on Cisco 1532 AP
CSCvh31233	AP fails to resend data on getting 401 error from Cisco DNA
CSCvh32561	Cisco 3700 AP reloads unexpectedly due to 'Per-Second Jobs' on 8.3.134.57
CSCvh32590	Cisco 1852 AP: Observed a radio core on loading the image, 5G @0x0099B20C,
CSCvh32971	Management through Wireless Not Working
CSCvh33064	Config logging traceinfo setting not restored correctly
CSCvh47521	Cisco IOS AP shows decrypt failed messages on driver debug
CSCvh48916	Cisco 1815I should consume power draw mentioned in the datasheet
CSCvh49623	Cisco Controller reloads unexpectedly with XML parse error during boot up
CSCvh50132	AP Sensor: PSK password being display in plain text test config
CSCvh50166	Cisco 2802e model without DART connector being considered as RRF candidate and assigned 5 GHz role
CSCvh50446	8.7: Hyperlocation destination IP missing from AP fast path
CSCvh51835	WGB client not getting IP address from the VLAN returned as AAA override
CSCvh51873	WLC reloads unexpectedly on Task Name: emWeb due to DATACORRUPTION-DATAINCONSISTENCY
CSCvh51936	Cisco 3504 controller flooding with emc1403 0-007c: Read failure of status register error msg
CSCvh52101	L1 list is not generated when AP moved from Monitor mode to Client serving mode

Caveat ID Number	Description
CSCvh52237	8.7:Dropping ADD_MOBILE due to mismatch in client radio/vap id slot id: 0 client_assoc_id: 1 vapid:
CSCvh53814	Cisco Wave 2 AP in Flex LS: IPv6 RA dropped with high level of multicast on wired interface
CSCvh54235	Cisco 3800 AP FW stopped working on Radio 0
CSCvh54459	Cisco AP console display logs 'DTX DUMP'
CSCvh55157	Cisco Controller reuses Acct-Session-Id when Client changes WLANs
CSCvh57198	Wired Cisco 1800 AP after Cisco DNA image refresh requires resetting from console
CSCvh57945	Cisco 3500, 5520 Controller reloads unexpectedly with sim_task on 8.7.1.107
CSCvh58148	Cisco Wave 2 APs uses invalid CAPWAP-Data keep-alive source port
CSCvh58266	WLC reloads unexpectedly on Task Name: ccxL2RoamTask 0x162ad5d l2roamGetRrmNeighborList+77
CSCvh58401	Address security issues in older curl and libxml libraries
CSCvh58467	Kernel Panic with PC at skb_release_data+0xe0/0x230
CSCvh58486	WLC reloads unexpectedly on Task Name: emWeb osapiMsgQueueDetailClear+42/usmDbMsgQueueDetailClear+27
CSCvh58917	Cisco WLC MAC authentication web redirected URL is broken
CSCvh59834	ME : Cannot change the role of XOR radio from Auto to Manual on AP2802E without DART
CSCvh60627	Cisco 3504 WLC reloads unexpectedly with taskname 'osapiReaper'
CSCvh60970	WLC reloads unexpectedly on Task Name:emWeb osapiMutexDumpAllLocked+890 after timezone setting of AP
CSCvh61107	GUI : EAP-TLS not working on Cisco 1815, 1562 AP models
CSCvh61355	WLC need remove WGB behind wired client after WGB changes to worst uplink
CSCvh61939	Cisco 1562 MAP is not forwarding BPDUs sent by the RAP when using Ethernet bridging
CSCvh62112	1832, 1852 APs reload unexpectedly due to memory leak in 4k slab with Spectrum Intelligence enabled
CSCvh62827	Wireless client cannot communicate each other with dynamic VLAN
CSCvh63417	d0: *** sensord died (src/dspm_main.c:1662/0) - slot 0 ***
CSCvh63454	Cisco 1261 AP standalone unexpectedly reloads on 8.3MR3 escalation image

Caveat ID Number	Description
CSCvh64065	Cisco 3800, 2800 AP: Beacons stuck because VAP is disabled
CSCvh65876	Cisco Wireless LAN Controller Software GUI Privilege Escalation Vulnerability
CSCvh66002	AP sniffer does not capture traffic when enabled for the first time on a channel
CSCvh66610	Cisco 3800,4800 APs unstable after upgrading to 8.7.1.115-vmalloc: allocation failure -FIQ/NMI reset
CSCvh66793	AP 1815W - continuously logs: missing case for op class XXX in ieee80211_mbo_operating_class_to_chan
CSCvh67548	Cisco 1600AP sending de-auth frame with reason code 7 to Random MAC Address XX:XX:00:00:00:00
CSCvh67549	Cisco 8540 WLC Data Plane reloads unexpectedly on __udp_input
CSCvh67590	WLC delay packets due to high DP packet buffers in use
CSCvh67738	Observed Traceback and FP0.05:(36)Pkt Ptr Unaligned, WQE-080000000037e6e00 on WLC HA while reset
CSCvh70051	Cisco 3800 AP DFS CAC failures on repeated channel changes/radar injection
CSCvh70067	WLC 8.7 not sending SPI keys, when added to CMX with HL enabled.
CSCvh72613	Cisco AP reloads unexpectedly when running **show controller d1 atf cfs client**
CSCvh72803	AP stops working during sh tech collection command that includes show CAPWAP client config
CSCvh72867	Radio reset with transmitter seems to have stopped
CSCvh73146	Cisco Controller reloads unexpectedly due to clientTroubleShootingTask 8.3.133.0
CSCvh73674	Cisco 1562 MAP not sending Air Quality reports to WLC
CSCvh73821	Cisco WLC reloads unexpectedly on sh run-config
CSCvh74663	IOS AP unexpectedly reloads during show CAPWAP client config using SSH
CSCvh77575	ATF monitor mode config for AP group is not reflecting on GUI
CSCvh77719	External MDNS resolution fails with WLC 'link local bridging' enabled
CSCvh78106	Cisco 2800,3800 AP on 8.7 code hangs for an hour with radio UP followed by silent reload
CSCvh78149	Cisco 1815 AP idle clients are not removed after 24 hrs
CSCvh78884	Cisco AP reloads unexpectedly on NBAR timer tick task
CSCvh79344	WLC is returning values for 'cLSiIdrDeviceSignature' OID with a length greater than 32 bytes

Caveat ID Number	Description
CSCvh79699	8.7:Task Name: spamApTask4 cSendConfigurationStatusResponse capwap_error_handler2
CSCvh79809	Sensor: poor on boarding connectivity with Cisco 1800S AP compared to Cisco 3800 AP
CSCvh81391	Cisco 2800, 3800 AP add CAPWAP ap-primed-join-timeout logic
CSCvh82606	LSC configurations are not persistent after certificate installation followed by system reboot
CSCvh82671	Clients are not able to load the Web-authentication login portal in Foreign-Anchor scenarios.
CSCvh83197	Cisco 1560 AP will create a loop when failing over to wireless and wired connection comes back
CSCvh83328	WLC reloads unexpectedly in loop while trying to download old config from TFTP
CSCvh83925	Webauth configuration is supported at testconfig level, rather than SSID level
CSCvh84101	ICMP reachability should not be performed by sensor tests other than host reachablity
CSCvh85082	Cisco 1562-I AP failed to decode discovery response and unexpectedly reloads
CSCvh85830	Cisco controller blocks client MAC authentication for wrong WLAN profile
CSCvh86834	802.11w client association data traffic drops after 802.11r roaming with PMF enabled or optional
CSCvh86845	Cisco Controller is unable to fetch CRL
CSCvh86970	ATF Mesh MIB Memory Leak observed during SNMPWALK from root
CSCvh89195	Unable to set 40MHz bandwidth for either channels 169 or 173 on Cisco 1542E AP
CSCvh89286	Cisco 2802,3802 APs: reloads with watchdog reset(wcpd) after mrvlfwd: Init of radio failed
CSCvh89438	Cisco 8510 WLC SNMP Traps for duplicate IP reported with IP address inversely
CSCvh91290	Cisco Wave 2 APs need to send XID broadcast on client association for FlexConnect local switching
CSCvh94458	Cisco Wave 1 APs last reload reason shows invalid image opcode
CSCvh94755	Client is able to ping management gateway before webauth login
CSCvh95762	Show traplog:Client Enhanced Traps Sent are not included in Number of Traps Since Last Reset
CSCvh96132	Cisco 8.5.110.0 release has many channel changes on XOR 5GHz
CSCvh96192	Cannot enable VLAN Support on AP 1562

Caveat ID Number	Description
CSCvh96895	Cisco 2800,3800,1560 APs: Perform duplicate check of assoc-req in clients with seq number as 0
CSCvh96956	Cisco 2800 AP cannot convert CAPWAP DSCP to 802.11e UP value correctly
CSCvh97469	Cisco Controller reloads unexpectedly with show run-config at commandConfig80211aSpectrumIntfDevList
CSCvh97739	Cisco 2800,3800 APs devshell to trace conversion
CSCvh97977	WLC Local Policy - Client Local Profiling assigns wrong Interface to Client
CSCvh98439	Cisco Controller stopped working while executing **config client deauthenticate** *mac-addr* command
CSCvh98496	Fan failure errors seen after upgrade to 8.3.133.10 release
CSCvh99287	Cisco OEAP drops wired client traffic after N+1 failover
CSCvi00786	IPsec stale entry observed with syslog
CSCvi01147	LSC cert keysize not retain after upload/download config
CSCvi01675	New Mobility with 3650MA and 5520 Anchor - Guest users cannot reach DG on 8.3.x
CSCvi01918	Cisco 3702 AP: RRM stall - RF neighbor list empty on both WLC and AP on 5GHz
CSCvi02072	Cisco Wave 2 APs: ETSI 5G adaptive Wi-Fi compliance fix
CSCvi02980	Cisco Controller becomes inaccessible with client rate limiting
CSCvi03114	Cisco 1852 Series APs reloads unexpectedly due to kernel panic
CSCvi04088	Ascom and Cisco 8821 phones on Cisco 3802 AP unable to make calls
CSCvi05095	Cisco 1040 AP in FlexConnect mode: radio reset with '%SOAP_BUF-2'
CSCvi06528	VLAN priority tag inside the EoGRE packet set to non-zero when 802.1p set to none
CSCvi06629	Not able to config the host name to 24 characters
CSCvi07460	WLC is incorrectly returning '5' for snmpwalk on bsnMobileStationApMode OID
CSCvi07565	Cisco 3800AP: Client EAP auth not working with wireless devices which sends certificate in fragments
CSCvi07609	Cisco 5520 WLC experiences fatal dataplane reloads unexpectedly at broffu_fp_dapi_cmd.c:4588
CSCvi08398	Cisco 5500 Controller reloads unexpectedly while adding LSC Dev cert multiple times [GUI or CLI]
CSCvi09025	Msglog flooded 'The Socket send operation has failed on the socket descriptor rmgrPhyMgrSock'

Caveat ID Number	Description
CSCvi09095	Radio Reset Tx Jammed seen on both 8.3 and 8.5
CSCvi09153	Cisco Wave 1 APs radio reset due FST14 FW: cmd=0x31 seq=6 due to mcast stuck in radio
CSCvi09424	Layer 3 Roam fails back to L2 Anchor with MAC Filtering MAB
CSCvi11287	Cisco 2800 AP consistently reboots around 1 second after joining to the WLC
CSCvi11609	DNS snooping not working for URL ACL after upgrade to 8.5 release
CSCvi11611	ME - 3802AP had FIQ/NMI reset during rate limiting test
CSCvi12046	FlexConnect AP WLAN-VLAN Mapped incorrectly on AP2800
CSCvi12726	UCAPL: login activity data is mismatched after telnet session
CSCvi13589	Locally generated webadmin certificate shows as 3rd party after upgrade on 8.3 code
CSCvi14638	Rogue BSSID containment count display incomplete
CSCvi14641	Cisco 2802, 3802 APs cannot connect with 100 Mbps LAN speed
CSCvi17079	Cisco Controller on 8.7 code reloads unexpectedly when accessing CMX AP groups over GUI
CSCvi17380	TxFSM stuck on Radio 0 with TCQVerify patch.
CSCvi17786	EoGRE client does not receive IP and stays in DHCP_REQ
CSCvi19706	Cisco 602 AP flapping when 2.4GHz and 5GHz radio are disabled
CSCvi20869	Cisco 1260,3500, 1550 Series APs: heavy packet loss in UDP downstream on 5GHz
CSCvi22594	Cisco DNAC: Adding new WLC successful or existing devices show that inventory poll fails with SNMP issue
CSCvi23698	Cisco 1560 AP on FlexConnect local-sw+802.1x+NAC:-ping traffic not going from client side
CSCvi25420	Cisco Wave 2 APs always send RTS at 6 data rate when data rate is supported
CSCvi25532	Standby 8540 WLC-reloads unexpectedly with rmgrMain due to IPC timeout
CSCvi25724	Cisco IOS APs unexpectedly reloads due to bad CPQ on 8.5 release code
CSCvi27226	Cisco 3802 AP: Radio core - receive path hang - RX-RING-STUCK
CSCvi29775	Cisco 8510 controller experiences DP0 CORE 9 Dataplane crash and reloads unexpectedly
CSCvi30627	Config missing after WLC failover
CSCvi30899	WLC 8.5 - AP fails to join the WLC when QA country code is used (-E AP)

Caveat ID Number	Description
CSCvi30993	Lost neighbor AP field on WLC GUI - NEIGHBOR AND ROGUE APS
CSCvi31343	Cisco WLC HA pair continues to reload unexpectedly due to system crash on broffu_SocketReceive
CSCvi32951	Cisco Wave 2 APs go offchannel if scan deferral value > 255 msec.
CSCvi33105	ODU sensor issue: WSA process disappeared after edit/delete/create of tests
CSCvi33984	HA pair does not sync VLAN support configuration for Cisco Mesh APs
CSCvi34440	Secondary Cisco 3504 WLC reloads unexpectedly in a loop
CSCvi36032	Missing AVC records on JSON data export from WLC 8.5 in FEW or Flex mode
CSCvi37522	Primary Cisco 5500 WLC on 8.5.124.22 reloads unexpectedly while joining AP due to 'Switchdrvr exited'
CSCvi38017	Standby WLC goes into a reboot loop after the software upgrade
CSCvi42526	Cisco Mesh 1562AP: AP will not go into bridge mode for I domain
CSCvi42919	Cisco 702w AP - Radio resets with ath_ACIF_radio_dead message
CSCvi42929	Sensor: webauth test failing in 1800 platform due to EOF occurred in violation of protocol
CSCvi43963	AP1562D to AP1562D bridge does not transmit fragmented traffic on 8.5.120.0
CSCvi45088	Cisco 2800, 3800 APs: adjust NDP pkt transmission power level
CSCvi45149	No RSSI/SNR info displayed with show client detail
CSCvi46306	Cisco 8510, 8540 controller on 8.5.124.27: Observed a traceback on booting up the image
CSCvi48427	'Enable DHCP Option 82 - VPN select' setting is lost after WLC reload
CSCvi49059	[FALL WLC BUNDLE] NO CVE Cisco Wireless LAN Controller Privilege Escalation Vulnerability
CSCvi49114	Cisco 3700 AP: memory allocation issue on IOS AP
CSCvi49126	RSN IE validation fails in M2 (802.11r session timeout) after reassociation causing deauth code 17
CSCvi49590	Bad phase calibration values in Triggerfish EEPROM
CSCvi50929	Cisco 3504 WLC reloads unexpectedly on 8.6.101 release
CSCvi51372	Client unable to reach RUN state on anchor WLC with 802.1x + ISE NAC
CSCvi51536	Access Point is not sending TCP fragments over the air

Caveat ID Number	Description
CSCvi51858	WLC not sending proper VSA list at acct-stop when client moves to another SSID
CSCvi53601	New Mobility Anchor Controller unexpectedly reboots with Task Name: mcListen
CSCvi54067	Cisco Wave 2 APs do not clear client statistics after device removed from client's database
CSCvi56046	Cisco 1560 RAP after reboot will lose the VLAN support configuration.
CSCvi56738	IW3702 on auto-bridge mode not preserving channel width more than 20MHz
CSCvi57043	WLC: WLC hang suddenly without crash file, osapiReaper accessing file that does not exist
CSCvi57169	SDA-Wireless AAA Override VNID ID is lost when roaming from one AP Group to another
CSCvi57213	Cisco 1832 AP unexpectedly reloads with 'PC is at __napi_complete+0x28/0x60'
CSCvi57232	CAP1815w-specific VLAN override RLAN fails, SSID FlexConnect VLAN takes precedence after AP reboot
CSCvi59432	Creation time of Local Net User set to Jan 1 00:00:00 1970
CSCvi61401	WLC remote access failing after upgrade
CSCvi65222	dot11 arp-cache does not work if BVI VLAN and client VLAN are different
CSCvi67365	Cisco 1850,3800AP: WPA_supplicant process reloads unexpectedly when used by WSA feature
CSCvi67565	TrustSec: AP picks wrong SXP Node ID
CSCvi69201	Line **config wlan wifidirect xconnect-not-allow** *wlan-id* manually entered in config backup is rejected
CSCvi70783	Wireless Service Assurance WSA: Cisco DNA Assurance certificate is not updated on WLC
CSCvi72800	Polaris COS-APs not correctly marking traffic when set/match policies and using multiple class-maps
CSCvi73013	Cisco Wave 1 AP deauthenticating client due to idle timeout
CSCvi73402	Cisco 1810W AP not giving IPs to cell phones using WPA/TKIP protocol
CSCvi74683	AIR-CT3504 mGig showing FCS errors incrementing
CSCvi78286	WLC Dashboard does not display the correct values for client throughput
CSCvi78819	HA : config service statistics not synced after failover
CSCvi79851	CPU ACL not configured after upgrading to Cisco 8.5.120.0 release

Caveat ID Number	Description
CSCvi81204	Cisco 2800, 3800 APs MTU issue with Fabric enable network
CSCvi84511	Cisco 3800 AP with Wired1 (aux) LAN enabled - CDP-4-DUPLEX_MISMATCH messages constantly logged
CSCvi84843	Client filter matches WLAN SSID, not WLAN Profile or WLAN ID
CSCvi84849	Cisco 1852 series APs unexpectedly reloads due to Kernel Panic
CSCvi85464	AP specific configuration lost post AP reload; WLAN-ACL mappings and policies lost
CSCvi85834	New Mobility CAPWAP control keepalive should not plumb keys when receiving unencrypted responses
CSCvi86276	Cisco WLC reloads unexpectedly on emWeb due to too many HTTP buffers received
CSCvi86834	Mesh Ethernet bridging - wired client associated to MAP fails to pass traffic over tagged VLAN
CSCvi90766	Cisco AP with regulatory domain Morocco cannot join the Cisco WLC
CSCvi91017	The FlexConnect groups are missing in backup configuration file
CSCvi91285	Install mapping on radio backhaul for Wave 2 APs Flex+Bridge setting is not retained after reboot
CSCvi93045	Cisco 2800 AP CleanAir goes down (sensord died)
CSCvi96690	Cisco 2800 AP detects Intel Dual Band Wireless-AC 8260 as rogue client/AP
CSCvi97023	Cisco Wireless LAN Controller Cross-Site Scripting Vulnerability
CSCvi97282	Assigning a NetFlow monitor to the WLAN will internally enable AVC on WLC
CSCvi98357	Cisco AP1815I : reloads unexpectedly due to 'watchdog reset(sync_log)'
CSCvi98514	MAP Ethernet port comes up as TRUNK and Allowed VLAN 4095
CSCvj03021	After upgrade the AP VLAN Trunking config changed to Disabled state
CSCvj03161	IOS AP not reporting known interference with disabled WSSI module
CSCvj04401	Client remains stuck in DHCP-REQD state on Anchor side unless ISE NAC is disabled on the anchor side
CSCvj07190	Cisco 2800 AP not joining WLC if 'Enable NAT Address' feature is enabled
CSCvj07930	Cisco 3802, 2802 AP with DART connectors has a Tx power value of 0
CSCvj11251	Cisco 2802 AP not sending re-association response to Cisco 8821 phone
CSCvj11270	Watchdog reset out of memory on Cisco 3800 AP running 8.3.133.0 code

Caveat ID Number	Description
CSCvj11397	Cisco 3504 Controller - OpenDNS registration failure - Return 77
CSCvj13920	WLC system reloads unexpectedly due to task name RRM-MGR-2_4-GRP
CSCvj13958	Cisco Wave 2 3800,2800 APs sending beacon on wrong channels intermittently on 5GHz
CSCvj17181	Creating a webauth CSR cert on the WLC GUI does not allow spaces
CSCvj18004	8.5MR3 Interim AP cannot join with NAT address on management interface of controller
CSCvj25194	Clean up debug lisp map-server output for AP onboarding
CSCvj25768	Bridge mode Cisco Wave 2 Mesh APs bridging issues
CSCvj25842	Cisco 1815I AP: Kernel panic: PC is at vfs_read+0x14/0x134
CSCvj28658	Cisco 1810wAP kernel panic leads to unexpected reload on PC at ieee80211_node_authorize+0x90/0xb8
CSCvj29270	Flex AP's WLAN-VLAN mapping mismatch in multiple WLC scenarios
CSCvj30550	Cisco WLC reloads unexpectedly when configuring PSK Provisioning key
CSCvj32624	702 AP as WGB keeps being disconnected from the WLAN due to parent lost: Missed beacons
CSCvj32964	WGB is only allowing 8 MAC addresses pass traffic using 3802 AP [as CAPWAP AP and 3702 AP as WGB]
CSCvj33894	Add 'show advanced hyperlocation summary' to 'show run-config' and 'show tech'
CSCvj35883	Allow Cisco 2800, 3800 APs to be able to convert to sensor mode
CSCvj36633	Cisco IOS AP: fail to boot after upgrade due to file corruption
CSCvj36853	AP name corruption after upgrade
CSCvj36923	Cisco AP name mismatch with controller on join
CSCvj37393	Cisco Wave 2 APs not sending probe response when SSID is not broadcast
CSCvj38456	WLC is losing its EoGRE configuration after reboot
CSCvj39005	[SDA] Wireless Clients losing L2VNID override when performing Switchover on Cisco 5520 WLC
CSCvj41040	Cisco 1800 APs in Cisco FlexConnect mode, fail FT roam
CSCvj41853	Incorrect Tx power on AP3802P-Q on some channels
CSCvj44533	SSH CBC ciphers are present from 8.6 and onwards releases

Caveat ID Number	Description
CSCvj45550	Cisco 1800 AP is appearing again in unclaim list after PnP provision
CSCvj47445	Cisco WLC sending CAPWAP discovery response when it has no available licenses
CSCvj48364	Cisco Controller is generating client traps without a session-id
CSCvj50170	Client coming back within 10 seconds of cleanup time is stopping the DHCP timer on the WLC
CSCvj53743	Cisco 1572IC AP: Channels and Maximum Power Settings settings spreadsheet incorrect values for V02
CSCvj54432	Cisco WLC unexpectedly reloads on task Dot1x_NW_MsgTask_2
CSCvj61140	Having Sensor-Driven tests configured cause 3802I AP to intermittent unexpected reload
CSCvj62672	WLC sending wrong NAS ID when AAA override is enabled
CSCvj69146	CME reloads unexpectedly in a loop due to PMALLOC_DOUBLE_FREE (capwap_ac_sm.c)
CSCvj70569	Cisco 2800, 3800,4800 APs: Incorrect Tx power on power on till we configure Tx power using Cisco WLC
CSCvj72890	Cisco 5520 WLC reloads unexpectedly when RADIUS server returns invalid value in Airespace-ACL-Name
CSCvj76378	Local policy is not applied when foreign WLC is running 8.3.141.0
CSCvj77078	WLC unexpectedly reboots on Dot1x_NW_MsgTask_1
CSCvj79108	WSA-8.5- NAC restarted with signal 6 after few minutes of WSA enabled in scale setup
CSCvj80388	Flex-ACL on Wave 2 AP's denying host instead of subnet
CSCvj83460	Cisco OEAP: client not associating for local SSID for default DHCP
CSCvj95336	Cisco Wireless LAN Controller Software Information Disclosure Vulnerability
CSCvk02024	Cisco 1850 APs experiencing frequent and unexpected reloads due to memory corruption
CSCvk05150	OpenDNS profile keeps being mapped for client when the username changes
CSCvk05965	Cisco WLC in HA SSO: standby controller is in a reboot loop
CSCvk06178	Uplink BPDUs are not bridged
CSCvk09135	Cisco 5520 Controller reloads unexpectedly for emweb in 8.6.101.0 release
CSCvk15068	IOS APs, recovery logic for MD5 checksum failure on primary Image

Caveat ID Number	Description
CSCvk15165	Cisco Controller reloads unexpectedly after modifying SNMP trap controls via GUI
CSCvk20484	IPC timeout and tracebacks reported on HA pair running 8.5.131.0 (8.5MR3)
CSCvk25644	WLC HA standby reboots reaching maintenance mode due to missing NaServCaCert_p12.pem on Active
CSCvk26732	New Flash recovery logic

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

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 Marketplace.
- 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 web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.