Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.5.171.0

First Published: 2021-02-15

Last Modified: 2021-02-15

Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.5.171.0

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 *Cisco WLCs*, and Cisco lightweight access points are referred to as *access points* or *Cisco APs*.

Supported Cisco Wireless Controller Platforms

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

- Cisco 2500 Series Wireless Controllers (Cisco 2504 Wireless Controller)
- Cisco 3500 Series Wireless Controllers (Cisco 3504 Wireless Controller)
- Cisco 5500 Series Wireless Controllers (Cisco 5508 and 5520 Wireless Controllers)
- Cisco Flex 7500 Series Wireless Controllers (Cisco Flex 7510 Wireless Controller)
- Cisco 8500 Series Wireless Controllers (Cisco 8510 and 8540 Wireless Controllers)
- Cisco Virtual Wireless Controller (vWLC) on the following platforms:
  - VMware vSphere Hypervisor (ESXi) Version 5.x and 6.x
  - Hyper-V on Microsoft Servers 2012 and later versions

Note Support introduced in Release 8.4.

- Kernel-based virtual machine (KVM)

Note Support introduced in Release 8.1. After KVM is deployed, we recommend that you do not downgrade to a Cisco Wireless release that is earlier than Release 8.1.

- Cisco Wireless Controllers for High Availability for Cisco 2504 WLC, Cisco 3504 WLC, Cisco 5508 WLC, Cisco 5520 WLC, Cisco Wireless Services Module 2 (Cisco WiSM2), Cisco Flex 7510 WLC, Cisco 8510 WLC, and Cisco 8540 WLC.

Note AP Stateful Switchover (SSO) is not supported in Cisco 2504 WLCs.

- Cisco WiSM2 for Cisco Catalyst 6500 Series Switches
- Cisco Mobility Express Solution

Supported Cisco Access Point Platforms

The following Cisco AP platforms are supported in this release:

- Cisco Aironet 1600 Series Access Points
- Cisco Aironet 1700 Series Access Points
- Cisco Aironet 1800 Series Access Points
- Cisco Aironet 1810 Series OfficeExtend Access Points
- Cisco Aironet 1810W Series Access Points
- Cisco Aironet 1815 Series Access Points
- Cisco Aironet 1830 Series Access Points
- Cisco Aironet 1850 Series Access Points
- Cisco Aironet 2600 Series Access Points
- Cisco Aironet 2700 Series Access Points
- Cisco Aironet 2800 Series Access Points
- Cisco Aironet 3500 Series Access Points
- Cisco Aironet 3600 Series Access Points
- Cisco Aironet 3700 Series Access Points
- Cisco Aironet 3800 Series Access Points
- Cisco Aironet 700 Series Access Points
- Cisco Aironet 700W Series Access Points
- Cisco AP802 Integrated Access Point
- Cisco AP803 Integrated Access Point
- Integrated Access Point on Cisco 1100 Integrated Services Router
- Cisco ASA 5506W-AP702

- Cisco Aironet 1530 Series Access Points
- Cisco Aironet 1540 Series Access Points
- Cisco Aironet 1550 Series Access Points with 128-MB memory

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

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

Note

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

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

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

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

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

What's New in Release 8.5.171.0

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 that is published for Cisco Wireless Release 8.5, see the Documentation Roadmap:

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

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

Software Release Types and Recommendations

Table 1: Release Types

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

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

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

Table 2: Upgrade Path to Cisco WLC Software Release 8.5.171.0

Current Software Release	Upgrade Path to 8.5.171.0 Software
8.0.x.x	You can upgrade directly to Release 8.5.171.0 **Note** This is applicable only to Cisco 5508 Wireless Controller and Cisco WiSM2.
8.2.16x.0 and later	You can upgrade directly to Release 8.5.171.0 **Note** Release 8.2.16x.0 is affected by CSCvf12068. This issue is addressed by upgrading to 8.5.164.x.
8.3.x.0	You can upgrade directly to Release 8.5.171.0
8.4.100.0	You can upgrade directly to Release 8.5.171.0
8.5.x	You can upgrade directly to Release 8.5.171.0

Note If you are using Release 8.2.15x or earlier, we recommend that you upgrade to Release 8.2.16x or 8.3.x and then upgrade to Release 8.5.171.0.

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

- We recommend you to perform the following procedure if you have the Cisco Smart License enabled and the Controller is registered on Cisco Smart Account.

  Perform this procedure before upgrading the Cisco Controller's boot image.

  1. Deregister the Cisco Controller running the old build from the Cisco Smart Software Manager (CSSM).
  2. Upgrade the Cisco Controller with new boot image.
  3. Reregister the upgraded Cisco Controller with new build on CiscoSmartSoftware Manager (CSSM).

- When the Cisco controller is downgraded from 8.5.140.0 to 8.3.x release, it is possible that the OSU SSID profile name information may be lost and only the OSU SSID name is retained. Reconfigure the controller with the desired profile name to have the HotSpot 2.0 in action after downgrading the controller to 8.3.x release is complete.
- In Release 8.5.135.0, the creation of Authorization server is deprecated. To create an Authorization server, you must create an Authentication server and duplicate it as an Authorization server. Due to this change in functionality, an alarm is generated in Cisco Prime Infrastructure 3.2 as follows:

  ```
  1.Successfully created Authentication server. 2.Failed to create
  authorization server:SNMP operation to Device failed: Set Operation
  not allowed for TACACS authorization server.1.Successfully created
  Accounting server.
  ```

  The workaround on Cisco PI is to uncheck the Authorization server on the Prime template.

  For more information about this change in functionality, see CSCvm01415.

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

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

- The image format of Cisco Aironet 1700, 2700, 3700, and IW3702 APs have been changed from ap3g2 to c3700. Therefore, if you are upgrading to Release 8.5 or a later release from Release 8.3 or an earlier release, these APs will download the image twice and reboot twice.
- Support for Dynamic WEP is reintroduced in Cisco Wave1 APs in this release.
- The AAA database size is increased from 2048 entries to 12000 entries for these Cisco controllers: Cisco 8510, 5520, and 8540. Therefore, if you downgrade from Release 8.5 to an earlier release that does not include this enhancement, you might lose most of the AAA database configuration, including management user information. To retain at least 2048 entries, including management user information, we recommend that you follow these downgrade instructions and back up the configuration file before proceeding with the downgrade:
  1. From Release 8.5, downgrade to one of the following releases, which support 2048 database size and include the enhancement.
     - Release 8.4.100.0 or a later 8.4 release.
     - Release 8.3.102.0 or a later 8.3 release.
     - Release 8.2.130.0 or a later 8.2 release.
     - Release 8.0.140.0 or a later 8.0 release.
  2. Downgrade to a release of your choice.
- In Release 8.5, the search functionality in the Cisco controller Online Help for all controllers is disabled due to memory issues encountered in Cisco 5508 controllers.
- Release 8.4 and later releases support additional configuration options for 802.11r FT enable and disable. The additional configuration option is not valid for releases earlier than Release 8.4. If you downgrade from Release 8.5 to Release 8.2 or an earlier release, the additional configuration option is invalidated and defaulted to FT disable. When you reboot Cisco controller with the downgraded image, invalid configurations are printed on the console. We recommend that you ignore this because there is no functional impact, and the configuration defaults to FT disable.
- If you downgrade from Release 8.5 to a 7.x release, the trap configuration is lost and must be reconfigured.
- If you downgrade from Release 8.5 to Release 8.1, the Cisco Aironet 1850 Series AP whose mode was Sensor before the downgrade is shown to be in unknown mode after the downgrade. This is because the Sensor mode is not supported in Release 8.1.
- If you have an IPv6-only network and are upgrading to Release 8.4 or a later release, ensure that you perform the following activities:
  - Enable IPv4 and DHCPv4 on the network—Load a new Cisco controller software image on all the Cisco controllers along with the supplementary AP bundle images on Cisco 5508 controller, or perform a predownload of AP images on the corresponding Cisco controllers.

- Reboot Cisco controller immediately or at a preset time.
- Ensure that all Cisco APs are associated with Cisco controller.
- Disable IPv4 and DHCPv4 on the network.

- After downloading the new software to the Cisco APs, it is possible that a Cisco AP may get stuck in an upgrading image state. In such a scenario, it might be necessary to forcefully reboot Cisco controller to download a new image or to reboot Cisco controller after the download of the new image. You can forcefully reboot Cisco controller by entering the **reset system forced** command.
- It is not possible to download some of the older configurations from Cisco 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.
- If you upgrade from Release 8.0.110.0 to a later release, the **config redundancy mobilitymac** *mac-addr* command's setting is removed. Manually reconfigure the mobility MAC address after the upgrade.
- If you downgrade to Release 8.0.140.0 or 8.0.15x.0, and later upgrade to a later release and and also have the multiple country code feature configured, then the configuration file could get corrupted. When you try to upgrade to a later release, special characters are added in the country list causing issues when loading the configuation. For more information, see CSCve41740.

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

- If you are upgrading from a 7.4.x or an earlier release to a release later than 7.4, the Called Station ID type information is mapped to the RADIUS Accounting Called Station ID type, which, by default, is set to apradio-mac-ssid. You can configure the RADIUS Authentication Called Station ID type information by using the **config radius auth callStationIdType** command.
- When a client sends an HTTP request, the Cisco controller intercepts it for redirection to the login page. If the HTTP GET request that is intercepted by the Cisco controller is longer than 2000 bytes, the Cisco controller drops the packet. Track CSCuy81133 for a possible enhancement to address this restriction.
- We recommend that you install Cisco Wireless Controller Field Upgrade Software (FUS), which is a special AES package that contains several system-related component upgrades. These include the bootloader, field recovery image, and FPGA or MCU firmware. Installing the FUS image requires special attention because it installs some critical firmware. The FUS image is independent of the runtime image. For more information about FUS and the applicable Cisco controller platforms, see the Field Upgrade Software release notes listing.
- When downgrading from one release to another, you might lose the configuration from your current release. The workaround is to reload the previous Cisco controller configuration files that are saved in the backup server, or to reconfigure Cisco controller.
- It is not possible to directly upgrade to this release from a release that is earlier than Release 7.0.98.0.
- When you upgrade Cisco controller to an intermediate release, wait until all the APs that are associated with Cisco controller are upgraded to the intermediate release before you install the latest Cisco 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 Cisco 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 Cisco controller is also automatically upgraded. When an AP is loading software, each of its LEDs blinks in succession.
- We recommend that you access the Cisco controller GUI using Microsoft Internet Explorer 11 or a later version, or Mozilla Firefox 32 or a later version.
- Cisco controllers support standard SNMP MIB files. MIBs can be downloaded from the software download page on Cisco.com.
- The Cisco controller software is factory installed on your Cisco controller and is automatically downloaded to the APs after a release upgrade and whenever an AP joins a Cisco 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 Cisco 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 Cisco 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.
- When you plug a Cisco controller into an AC power source, the bootup script and power-on self test is run to initialize the system. During this time, press **Esc** to display the bootloader **Boot Options** menu. The menu options for the Cisco 5508 controller differs from the menu options for the other Cisco controller platforms.

  The following is the Bootloader menu for Cisco 5508 controller:

  ```
  Boot Options
  Please choose an option from below:
  1. Run primary image
  2. Run backup image
  3. Change active boot image
  4. Clear Configuration
  5. Format FLASH Drive
  6. Manually update images
  Please enter your choice:
  ```

  The following is the Bootloader menu for other Cisco controller platforms:

  ```
  Boot Options
  Please choose an option from below:
  1. Run primary image
  2. Run backup image
  3. Manually update images
  4. Change active boot image
  5. Clear Configuration
  Please enter your choice:

  Enter 1 to run the current software, enter 2 to run the previous software, enter 4 (on
   Cisco 5508 WLC),
  ```

```
or enter 5 (on Cisco WLC platforms other than 5508 WLC) to run the current software and
 set
the Cisco WLC configuration to factory defaults. Do not choose the other options unless
 directed to do so.
```

Note See the Installation Guide or the Quick Start Guide of the respective Cisco controller platform for more details on running the bootup script and the power-on self test.

- The Cisco 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, choose **Option 2: Run Backup Image** from the **Boot Options** menu to boot from the backup image. Then, upgrade with a known working image and reboot Cisco 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 Cisco 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 Cisco controller or any AP during the upgrade process. If you do this, the software image might get corrupted. Upgrading Cisco controller with many APs can take as long as 30 minutes, depending on the size of your network. However, with the increased number of concurrent AP upgrades supported, the upgrade time should be significantly reduced. The APs must remain powered, and Cisco controller must not be reset during this time.
- To downgrade from this release to Release 6.0 or an earlier release, perform either of these tasks:
  - Delete all the WLANs that are mapped to interface groups, and create new ones.
  - Ensure that all the WLANs are mapped to interfaces rather than interface groups.
- After you perform the following functions on Cisco 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.

Changes in Images and Installation Procedure for Cisco 5508 Controllers

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

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

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

Image Details

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

Table 3: Image Details of Cisco 5508 Controller

Cisco Controller	Base Install Image	Supplementary AP Bundle Image [1]
Cisco 5508 controller	AIR-CT5500-K9-8-5-171-x.aes AIR-CT5500-LDPE-K9-8-5-171-x.aes [2]	AIR-CT5500-AP_BUNDLE-K9-8-5-171-x.aes AIR-CT5500-LDPE-AP_BUNDLE-K9-8-5-171-x.aes [3]

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

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

[2] x is the release number
[3] x is the release number

Upgrading Cisco WLC Software (GUI)

Procedure

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

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

Step 2 Follow these steps to obtain Cisco Wireless software:

a) Browse to Cisco Software Central at: https://software.cisco.com/download/navigator.html.
b) Click **Software Download**.
c) On the **Download Software** page, choose **Wireless** > **Wireless LAN Controller**.

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

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

d) Select the Cisco WLC model number or name.
e) Click **Wireless LAN Controller Software**.
f) The software releases are labeled as described here to help you determine which release to download. Click a Cisco WLC software release number:

- Early Deployment (ED)—These software releases provide new features and new hardware platform support as well as bug fixes.
- Maintenance Deployment (MD)—These software releases provide bug fixes and ongoing software maintenance.

- Deferred (DF)—These software releases have been deferred. We recommend that you migrate to an upgraded release.

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

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

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

h) Click **Download**.
i) Read the Cisco End User Software License Agreement and click **Agree**.
j) Save the file to your hard drive.
k) Repeat steps *a* through *j* to download the remaining file.

Step 3 Copy the Cisco WLC software file (*filename.aes*) to the default directory on your TFTP, FTP, or SFTP server.

Step 4 (Optional) Disable the Cisco WLC 802.11 networks.

Note For busy networks, Cisco WLCs on high utilization, and small Cisco WLC platforms, we recommend that you disable the 802.11 networks as a precautionary measure.

Step 5 Choose **Commands** > **Download File** to open the **Download File to Controller** page.

Step 6 From the **File Type** drop-down list, choose **Code**.

Step 7 From the **Transfer Mode** drop-down list, choose **TFTP**, **FTP**, or **SFTP**.

Step 8 In the **IP Address** field, enter the IP address of the TFTP, FTP, or SFTP server.

Step 9 If you are using a TFTP server, the default value of 10 retries for the **Maximum Retries** field, and 6 seconds for the **Timeout** field should work correctly without any adjustment. However, you can change these values, if required. To do so, enter the maximum number of times the TFTP server attempts to download the software in the **Maximum Retries** field and the amount of time (in seconds) for which the TFTP server attempts to download the software, in the **Timeout** field.

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

Step 11 In the **File Name** field, enter the name of the software file (*filename.aes*).

Step 12 If you are using an FTP server, perform these steps:

a) In the **Server Login Username** field, enter the username with which to log on to the FTP server.
b) In the **Server Login Password** field, enter the password with which to log on to the FTP server.
c) In the **Server Port Number** field, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 13 Click **Download** to download the software to the Cisco WLC.

A message indicating the status of the download is displayed.

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

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

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

Step 14 After the download is complete, click **Reboot**.

Step 15 If you are prompted to save your changes, click **Save and Reboot**.

Step 16 Click **OK** to confirm your decision to reboot the Cisco WLC.

Step 17 For Cisco WiSM2, check the port channel and re-enable the port channel, if necessary.

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

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

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 a version 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 recommended versions addresses the vulnerability tracked in CSCvo01180 caveat.

The certified CIMC images are available at the following locations:

Table 4: CIMC Utility Software Image Information

Controller	Current CIMC Version	Recommended CIMC Version	Link to Download the CIMC Utility Software Image
Cisco 5520 Wireless Controller Cisco 8540 Wireless Controller	2.x	3.0(4r)	https://software.cisco.com/download/home/286281345/type/283850974/release/3.0(4r) **Note** We recommend you to upgrade the firmware from 2.0(13i) to 3.0(4r) using TFTP, SCP protocols only.

Controller	Current CIMC Version	Recommended CIMC Version	Link to Download the CIMC Utility Software Image
Cisco 5520 Wireless Controller Cisco 8540 Wireless Controller	3.0(4d)	3.0(4r)	https://software.cisco.com/download/home/286281345/type/283850974/release/3.0(4r)
Cisco 5520 Wireless Controller Cisco 8540 Wireless Controller	4.0(1a)	4.0(2n)	https://software.cisco.com/download/home/286281345/type/283850974/release/4.0(2n)

Table 5: Firmware Upgrade Path to 4.x version

Current Firmware Version	Upgrade Path to 4.x version
2.x	You must upgrade to a 3.x version and then upgrade to the recommended 4.x version.
3.x	You can upgrade directly to the recommended 4.x version.

- For information about upgrading the CIMS utility version 2.x , see the *Introduction to Cisco IMC Secure Boot* section in the *Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 3.0*:

  https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/cli/config/guide/3_0/b_Cisco_UCS_C-Series_CLI_Configuration_Guide_301/b_Cisco_UCS_C-Series_CLI_Configuration_Guide_201_chapter_01101.html#d92865e458a1635

  For information about upgrading the CIMS utility version 2.x using webUI , see the *Updating the Firmware* section https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/gui/config/guide/3_0/b_Cisco_UCS_C-Series_GUI_Configuration_Guide_for_HTML5_Based_Servers_301/b_Cisco_UCS_C-Series_GUI_Configuration_Guide_207_chapter_01101.html#task_C137961E9E8A4927A1F08740184594CA.

Note When upgrading the firmware using the webUI method, you must select **Install Firmware through Remote Server** option when prompted in the webUI.

- 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

  Release Notes for Cisco UCS C-Series Software, Release 4.0(2) at:

  https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/release/notes/b_UCS_C-Series_RN_4_0_2.html

Table 6: Resolved Caveats for Release 4.0(2f)

Caveat ID	Description
CSCvn80088	NI-HUU fails to handle the special characters in the password of CIFS remote share

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

Caveat ID	Description
CSCvp41543	SSH weak KeyExchange algorithm [diffie-hellman-group14-sha1] has to be removed

Interoperability with Other Clients

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

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

Table 8: Test Bed Configuration for Interoperability

Hardware or Software Parameter	Hardware or Software Configuration Type
Release	8.5.x.x
Cisco WLC	Cisco 5520 Wireless Controller
Access Points	AIR-AP2802I-B-K9, AIR-AP1852E-B-K9, AIR-AP1810W-B-K9, AIR-AP3802I-B-K9
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

Hardware or Software Parameter	Hardware or Software Configuration Type
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 9: Client Types

Client Type and Name	Version
Laptop	
Intel 6300	15.16.0.2
Intel 6205	15.16.0.2
Intel 7260	18.33.3.2
Intel 7265	19.10.1.2
Intel 3160	18.40.0.9
Intel 8260	19.10.1.2
Broadcom 4360	6.30.163.2005
Dell 1520/Broadcom 43224HMS	5.60.48.18
Dell 1530 (Broadcom BCM4359)	5.100.235.12
Dell 1560	6.30.223.262
Dell 1540	6.30.223.215
Samsung Chromebook	55.0.2883.103
HP Chromebook	55.0.2883.103
MacBook Pro	OSX 10.12.6
MacBook Air	OSX 10.12.6
Macbook Pro with Retina Display	OSX 10.12.3
Macbook New 2015	OSX 10.12 beta
Tablets	
Amazon Kindle	Android 6.2.2
Apple IPad	iOS 9.3.1
Apple iPad3	iOS 10
Apple iPad mini	iOS 9.3.5
Apple iPad mini 2	iOS 10.3.1
Apple iPad mini 4	iOS 10
Apple iPad Air	iOS 10.1.1

Client Type and Name	Version
Apple iPad Air 2	iOS 10.2.1
Apple iPad Pro	iOS 11.0.3
Samsung Galaxy Tab Pro SM-T320	Android 4.4.2
Samsung Galaxy Tab 10.1- 2014 SM-P600	Android 4.4.2
Samsung Galaxy Note 3 - SM-N900	Android 5.0
Microsoft Surface Pro 3	Windows 8.1
	Driver: 15.68.3093.197
Microsoft Surface Pro 2	Windows 8.1
	Driver: 14.69.24039.134
Microsoft Surface Pro 4	Windows 10
	Driver: 15.68.9040.67
Google Nexus 9	Android 6.0.1
Google 10.2" Pixel C	Andriod 7.1.1
Toshiba Thrive AT105	Android 4.0.4
Zebra ET50PE	Android 5.1.1
Mobile Phones	
Apple iPhone 4S	iOS 10.2.1
Apple iPhone 5	iOS 10.3.1
Apple iPhone 5s	iOS 10.2.1
Apple iPhone 5c	iOS 10.3.1
Apple iPhone 6	iOS 11.3
Apple iPhone 6 Plus	iOS 10.3.1
Apple iPhone 6s	iOS 10.2.1
Apple iPhone 7	iOS 11.0.3
Apple iPhone X	iOS 11.1.2
HTC One	Android 5.0.2
Motorola MotoX 2nd Gen	Android 5.0
OnePlusOne	Android 4.3
OnePlus3	Android 6.0.1
Samsung Galaxy S4 T-I9500	Android 5.0.1
Sony Xperia Z Ultra	Android 4.4.2
Nokia Lumia 925	Windows 8.1 Mobile

Client Type and Name	Version
Nokia Lumia 1520	Windows 10 Mobile
Google Nexus 5	Android 6.0.1
Google Nexus 6	Android 5.1.1
Google Nexus 7	Android 6.0
Google Nexus 9	Android 6.0.1
Google Pixel	Android 7.1.1
Samsung Galaxy Note3	Android 5.0
Samsung Galaxy Note4 edge	Android 6.0.1
Samsung Galaxy S4	Android 5.0.1
Samsung Galaxy S6	Android 7.0
Samsung Galaxy S7	Android 7.0
Samsung Galaxy S8	Android 7.0
Samsung Galaxy Nexus GTI9200	Android 4.4.2
Samsung SM-P600	Android 4.4.2
LG G4	Android 5.1
LG D855	Android 5.0
Xiaomi Mi 4c	Android 5.1.1
Zebra ET1	Android 2.3.4
Zebra TC510K	Android 6.0.1
Zebra TC8000	Android 4.4.3

Key Features Not Supported in Controller Platforms

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

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

Key Features Not Supported in Cisco 2504 WLC

- Domain-based ACLs
- Autoinstall
- Controller integration with Lync SDN API

- Application Visibility and Control (AVC) for FlexConnect locally switched APs
- Application Visibility and Control (AVC) for FlexConnect centrally switched APs

Note AVC for local mode APs is supported.

- URL ACL
- Bandwidth Contract
- Service Port
- AppleTalk Bridging
- Right-to-Use Licensing
- PMIPv6
- EoGRE
- AP Stateful Switchover (SSO) and client SSO
- Multicast-to-Unicast
- Cisco Smart Software Licensing

Note
- The features that are not supported on Cisco WiSM2 and Cisco 5508 WLC are not supported on Cisco 2504 WLCs too.
- Directly connected APs are supported only in local mode.

Key Features Not Supported in Cisco 3504 WLC

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

Key Features Not Supported in Cisco WiSM2 and Cisco 5508 WLC

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

- Cisco Smart Software Licensing

Key Features Not Supported on Cisco Flex 7510 WLC

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

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

- IPv6 and dual-stack client visibility

Note IPv6 client bridging and Router Advertisement Guard are supported.

- Internal DHCP server
- APs in local mode

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

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

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

- PMIPv6
- Cisco Smart Software Licensing

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

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

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

Key Features Not Supported in Cisco Virtual WLC

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

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

- FlexConnect central switching in large-scale deployments

Note
- FlexConnect central switching is supported in only small-scale deployments, wherein the total traffic on controller ports is not more than 500 Mbps.
- FlexConnect local switching is supported.

- Central switching on Microsoft Hyper-V deployments
- AP and Client SSO in High Availability
- PMIPv6
- Datagram Transport Layer Security (DTLS)

- EoGRE (Supported in only local switching mode)
- Workgroup bridges
- Client downstream rate limiting for central switching
- SHA2 certificates
- Controller integration with Lync SDN API
- Cisco OfficeExtend Access Points

Key Features Not Supported in Access Point Platforms

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

Table 10: Key Features Not Supported in Cisco Aironet 1540, 1560, 1800i, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800 and 3800 Series APs

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

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

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

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

Table 11: Key Features Not Supported in Cisco Aironet 1800i, 1810 OEAP and 1810W Series APs

Operational Modes	Mobility Express
FlexConnect Features	Local AP authentication

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

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

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

Key Features Not Supported in Mesh Networks

- Load-based call admission control (CAC). Mesh networks support only bandwidth-based CAC or static CAC.
- High availability (Fast heartbeat and primary discovery join timer).
- AP acting as supplicant with EAP-FASTv1 and 802.1X authentication.
- AP join priority (Mesh APs have a fixed priority)

- Location-based services

Key Features Not Supported in Cisco Aironet 1540 Mesh APs

- Dynamic Mesh backhaul data rate.

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

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

Key Features Not Supported on Cisco Aironet 1560 Mesh APs

- Noise Tolerant Fast Convergence
- Flex+Mesh

Caveats

Open Caveats

Table 13: Open Caveats for Release 8.5.171.0

Caveat ID Number	Description
CSCvb26809	Cisco controller should use port MAC for non LAG and box MAC for LAG
CSCve62394	Controller unexpectedly reloads with "pmalloc detected memory corruption" in SpamApTask<n>
CSCvf37633	Error in mapping QoS role during the creation of local net users
CSCvh21912	Access point broadcasts a disabled or deleted SSID
CSCvi46532	ME AP reloads: "switchdrvr no heartbeat"; ME LWA logout.html is timed out
CSCvj76573	"Software Failed while accessing the data" reload in mmListen or mmListenFsm
CSCvk57014	AP: Sometimes creates empty radio core files without any information
CSCvm36002	AP 3802 not broadcasting SSID that is configured on the WLC
CSCvm63736	Erratic multicast throughput
CSCvn04046	Cisco 2800,3800 AP does not map the DSCP to the correct WMM UP Value for FlexConnect Local Switching

Caveat ID Number	Description
CSCvn47019	Ping test failure from WGB wired client; IPv6 connectivity lost after roam
CSCvo41224	Cisco 1832,1852 Observing False RADAR detection in 20 MHz
CSCvp00688	Cisco 2800, 3800 AP radio reloads unexpectedly
CSCvp97478	WLC new mobility 2 members in the mobility group deleted after reboot
CSCvq53705	ME UI not operational due to "error in setting port number"
CSCvq81315	Cisco 2700 AP PCI0 reloads unexpectedly when Cisco CleanAir is enabled
CSCvq88051	9130AP reloads unexpectedly in a loop in Longevity testbed with PC _Z18clickps_atomic_incP8atomi
CSCvr20539	Controller not assigning correct channel width to Cisco APs - diagnostic enhancement only
CSCvr23173	Access point operates on different channel than configured
CSCvr38675	Client connectivity failure seen after LAN link flap
CSCvr50556	Half Duplex Mismatch messages seen on mGig port of 9300, 9400 switches
CSCvr87573	Cisco 2800, 3800, 4800, 1560 series AP stops sending broadcast ARP to wireless
CSCvr93760	VLAN bridging problem on Cisco 1810W AP with RLANs
CSCvr95403	Client ARP entry remains even if the client is disconnected
CSCvr97142	RAP Thows Tracebacks, Causing MAPs to Drop & Stranding Switches
CSCvs08427	Error "config network multicast mode multicast <ip> Invalid ip address" when restoring cfg
CSCvs46665	8.10MR2 - mobility anchor configuration is not retained after upload and download config
CSCvs55071	RRM fails with "empty 802.11a/b RF group"
CSCvs65189	AP Ethernet PHY interop issue when using IEEE Fast Retrain when connected at mGig speeds
CSCvs72880	Stale client entries getting created in WLC
CSCvs78454	Unexpected reload in Task Name: NFV9_Task
CSCvs89702	Controller reset due to switch-driver unexpectedly reloads on 8.5.151.0
CSCvt04710	AP3700:FlexConnect:Change deauth status code from 28 to 53 if no 11r pmk is present
CSCvt09744	Cisco 9120 AP: AP sends Deauth when it moves from Standalone to Connected
CSCvt56329	Cisco 1552H AP: LED not green when in autonomous state

Caveat ID Number	Description
CSCvt89481	AC Wave 1 AP not sending Cisco NDP Packets on the 2.4GHz band
CSCvt92754	Cisco 1532 AP ethernet interface lost packet
CSCvt99064	WLC GUI HTTPs stops working after downloading a web authentication certificate
CSCvu25264	AIR-AP2802I-H-K9 WCPd reloads unexpectedly on 8.5.135.0 lick-install/include/click/vector.hh:291
CSCvu83242	Cisco 1852 AP reloads unexpectedly, creates a radio firmware assert file with reason Beacon stuck
CSCvv17931	Cisco Wave 1 APs: Inconsistent AP logging level config behavior
CSCvv52618	Cisco 2800, 3800 APs exhibit choppiness during the multicast voice call
CSCvv63863	Clients behind a WGB facing limited connectivity after a 2nd failover (HA SSO)
CSCvv72578	WLC is not accepting the Web-Auth (CSR) certificate password via GUI
CSCvv78719	AP2800/3800/4800/1560/6300 fails to transmit data frame to the client from the radio interface
CSCvv81240	Mixed WIFI Mesh: [IOS-RAP + COS-MAP]: 1552H - MAP Failover and convergence issues (PETRONAS)
CSCvv90831	Wired DHCP clients are unable to get IP address after OEAP reload
CSCvw05117	AireOS controller running 8.10.130.0 reloads unexpectedly on SNMPTask consuming 100% CPU
CSCvw99507	Cisco controller reloads unexpectedly with task name "Dot1x_NW_MsgTask_4"

Resolved Caveats

Table 14: Resolved Caveats for Release 8.5.171.0

Caveat ID Number	Description
CSCvg67509	Cisco 1810W AP reloads unexpectedly over a kernel panic
CSCvh02937	Sensor: wireless sensor is choosing SSIDs with very poor signals during Cisco Provisioning
CSCvh57198	Wired Cisco 1800 AP after DNA image refresh requires resetting from console
CSCvk68585	WMM : WLC marks a BK traffic passing through a BE WLAN as BE traffic even though BK is less than BE
CSCvm07536	Native client cannot get DHCP address in Flexconnect, AP VLAN tagging mode
CSCvm49047	AP 3702 reloads unexpectedly on 8.3.143.0

Caveat ID Number	Description
CSCvm84001	WLC is sending wrong nasid for Flexconnect Local switching Clients
CSCvn19132	Cisco 1852 Kernel Panic with PC is at ieee80211_mu_cap_client_join_leave+0x17c/0x3ac [umac]
CSCvn25452	Cisco 2800/3800/4800/1560 APs unexpectedly reloads - variety of symptoms
CSCvo18663	'Native VLAN Inheritance' is changed after controller switchover
CSCvo33808	Cisco 2802,3802,4800,1562 AP reloads unexpectedly with radio firmware crash
CSCvo83091	8.5 FlexConnect AP in Standalone mode get stranded and does not send CAPWAP Discovery
CSCvp06909	Traceback, DOT11-2-RADIO_FAILED, Not Beaconing for too long, get_vap_mcast_q_len: invalid interface
CSCvp54103	Cisco Wave 1 APs reload unexpectedly with 'Unexpected exception to CPU' in logs
CSCvp62281	Cisco 2800, 3800 APs: [cmd timeout] wifi1: 0x8120=unknown intCode:0x0120 last 0x9184=unknown
CSCvp69474	Access point reloads unexpectedly generating CAPWAPd core dumps
CSCvp81355	Cisco Controller reloads unexpectedly in mmMobility or Dot1x_NW_MsgTask
CSCvp88559	Cisco Aironet 1810W Access Point reloads unexpectedly due to kernel panic
CSCvq16085	Cisco 3504 controller boots with interfaces unreachable for some protocols
CSCvq41013	Cisco DNAC - Web auth client traffic stops working post intra WLC roam
CSCvq51420	AP reloads due to wifi1: RxRing memory corruption
CSCvq55777	Roaming client immediately gets "expiring mobile"
CSCvq59233	Cisco 2802AP: Kernel panic crash: PC is at _Z27clickps_atomic_dec_and_testP8atomic_t
CSCvq71200	WLC Sent RST after TACACS+ authentication request cause login failed
CSCvq76143	Cisco 2800 AP reloads unexpectedly on Sxpd process
CSCvq82562	Cisco Wave 1 Access points not passing BPDUs in flex+bridge mode when connected to eWLC
CSCvq83205	After N+1 failover, WLC fails to send EAPOL M1
CSCvq90572	Receive throughput degrades for Cisco 2800, 3800, 4800, 1560 APs - AP fails to send block ACKs
CSCvr10424	Cisco FlexConnect AP drop UDP packet(port 2598).
CSCvr34339	Cisco AP unexpectedly reloads with "watchdog reset(wcpd)"

Caveat ID Number	Description
CSCvr43311	Unable to set syslog login level to all the APs "Unable to set the Log Trap level"
CSCvr62140	WLC is duplicating the packets coming from Vocera Badges to the Vocera Server
CSCvs19137	Authentication failure EAP timeout on a Cisco 1852 AP with data DTLS encryption enabled
CSCvs36177	Cisco Wave 2 APs - AP sending the EAP identity req with incorrect BSSID
CSCvs38511	Cisco 5508 controller enters a silent reload unexpectedly
CSCvs41893	Cisco 3702 AP running 8.5.151.0 release software reloads unexpectedly
CSCvs58195	Multicast and Broadcast traffic generated on FlexConnect WLAN is observed in Central Switching WLAN.
CSCvs63478	Cisco 3504 controller: webauth unexpectedly reloaded on ewsContextSendRedirect
CSCvs72639	AP3802 AP sends action frame with base radio MAC; after client roams to another AP
CSCvs74755	PRP:WGB BVI IP is not reachable from default gateway with ARP entry timeout on core switch
CSCvs88238	FEW client ARP/DHCP failures after roaming among Cisco Wave 1 APs
CSCvs89410	Cisco 3602 AP Image corruption issue
CSCvs98970	Controller Reaper Reset in Process SNMPTask
CSCvt17006	Cisco 1850AP: /usr/sbin/capwapd: writing to fd 17 failed!: Input/output error
CSCvt22353	Cisco 2800, 3800, 4800, 1560 APs are not transmitting data frames over the air
CSCvt28616	Flexconnect reap count for current users not getting decremented causing new Wi-Fi client disconnect
CSCvt32886	EoGRE Deployemnt with IOS AP in flexconnect - AP removes DHCP option 82 Remote-ID
CSCvt53819	CPU increases to 90+% with high volume traffic.
CSCvt75359	85mr6 & later release: Cisco Wave 1 APs not sending deauth rc 7 after Rx frame from non assoc client
CSCvt84649	Cisco 2800, 3800 APs: dropping ARP_REPLY packet post fix for CSCvm07536
CSCvt96416	DCA sets channel width to 20MHz although 40MHz is set on RF Profile
CSCvu02448	Cisco 3702 AP unable to join controller. Shows high CPU utilization under NCI Rx
CSCvu10516	AireOS drops ARP request or reply when local client tries to reach L3 roamed client
CSCvu12372	Cisco AireOS Controller Web GUI Jquery vulnerability

Caveat ID Number	Description
CSCvu44664	Cisco 8821 phones experiencing call drops intermittently; packets stuck at AP
CSCvu46244	WLC not updating fastpath table after a GW GARP failover
CSCvu71263	EoGRE Flexconnect Local Switching Deployment - client gets IP from native VLAN after AP reboot
CSCvu83817	WLC reloads unexpectedly on DHCP socket task
CSCvu84025	Cisco 1815W after failover to N+1 WLC does not move the client to FWD state when switching SSIDs
CSCvu91002	AireOS controllers unexpectedly reloads randomly at tunnelProfileGwRadiusProxyGetSafe task
CSCvv13214	Anchor deliberately closing DTLS with New Mobility member after session is re-established
CSCvv14005	RF profile not applied properly on Cisco 3802P AP XOR radio with DART connector
CSCvv76781	QoS Priority incorrectly marked with WMM UP 5 when DSCP value is 46
CSCvv83754	Multiple Vulnerabilities in dnsmasq DNS Forwarder Affecting Cisco Products: January 2021
CSCvw10681	8.10.14x.x: Traffic fails between wireless clients(Foreign and Local) during L3 or IRCM roaming
CSCvw19746	Cisco AireOS controller shows stale AP list entries even after changing peer mobility group
CSCvx12030	Cisco AP3802I: wrong channels available on AP

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 controllers, lightweight APs, and mesh APs, see these documents:

- The quick start guide or the installation guide for your particular controller 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 controller 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 Connected Mobile Experiences

Cisco Connected Mobile Experiences Documentation

Cisco Digital Network Architecture

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

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

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

Documentation Feedback

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

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