Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.5.151.0

First Published: 2019-06-20

Last Modified: 2021-02-12

Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.5.160.0

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.
- 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 8.5.151.0

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.

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

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 8.5.151.0

Current Software Release	Upgrade Path to 8.5.151.0 Software
8.0.x.x	You can upgrade directly to Release 8.5.151.0 **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 8.5.151.0 **Note** Release 8.2.16x.0 is affected by CSCvf12068. This issue is addressed by upgrading to 8.5.151.0.
8.3.x.0	You can upgrade directly to Release 8.5.151.0
8.4.100.0	You can upgrade directly to Release 8.5.151.0

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 8.5.151.0.

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 WLCs: Cisco Flex 7510, 8510, 5520, and 8540. Therefore, if you downgrade from Release 8.5 to an earlier release that does not include this enhancement, you might lose most of the AAA database configuration, including management user information. To retain at least 2048 entries, including management user information, we recommend that you follow these downgrade instructions and back up the configuration file before proceeding with the downgrade:
  1. From Release 8.5, downgrade to one of the following releases, which support 2048 database size and include the enhancement.
     - Release 8.4.100.0 or a later 8.4 release.
     - Release 8.3.102.0 or a later 8.3 release.
     - Release 8.2.130.0 or a later 8.2 release.
     - Release 8.0.140.0 or a later 8.0 release.
  2. Downgrade to a release of your choice.
- In Release 8.5, the search functionality in the Cisco WLC Online Help for all WLCs is disabled due to memory issues encountered in these WLCs: Cisco 2504, 5508, and WiSM2.
- Release 8.4 and later releases support additional configuration options for 802.11r FT enable and disable. The additional configuration option is not valid for releases earlier than Release 8.4. If you downgrade from Release 8.5 to Release 8.2 or an earlier release, the additional configuration option is invalidated and defaulted to FT disable. When you reboot Cisco WLC with the downgraded image, invalid configurations are printed on the console. We recommend that you ignore this because there is no functional impact, and the configuration defaults to FT disable.
- If you downgrade from Release 8.5 to a 7.x release, the trap configuration is lost and must be reconfigured.
- If you downgrade from Release 8.5 to Release 8.1, the Cisco Aironet 1850 Series AP whose mode was Sensor 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 WLC software image on all the Cisco WLCs along with the supplementary AP bundle images on Cisco 2504 WLC, Cisco 5508 WLC, and Cisco WiSM2, or perform a predownload of AP images on the corresponding Cisco WLCs.
  - Reboot Cisco WLC immediately or at a preset time.
  - Ensure that all Cisco APs are associated with Cisco WLC.
  - Disable IPv4 and DHCPv4 on the network.
- After downloading the new software to the Cisco APs, it is possible that a Cisco AP may get stuck in an upgrading image state. In such a scenario, it might be necessary to forcefully reboot Cisco WLC to

download a new image or to reboot Cisco WLC after the download of the new image. You can forcefully reboot Cisco WLC by entering the **reset system forced** command.

- It is not possible to download some of the older configurations from Cisco WLC because of the Multicast and IP address validations. See the "Restrictions on Configuring Multicast Mode" section in the *Cisco Wireless Controller Configuration Guide* for detailed information about platform support for global multicast and multicast mode.
- If you upgrade from Release 8.0.110.0 to a later release, the **config redundancy mobilitymac** *mac-addr* command's setting is removed. Manually reconfigure the mobility MAC address after the upgrade.
- If you downgrade to Release 8.0.140.0 or 8.0.15x.0, and later upgrade to a later release and and also have the multiple country code feature configured, then the configuration file could get corrupted. When you try to upgrade to a later release, special characters are added in the country list causing issues when loading the configuation. For more information, see CSCve41740.

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

- If you are upgrading from a 7.4.x or an earlier release to a release later than 7.4, the Called Station ID type information is mapped to the RADIUS Accounting Called Station ID type, which, by default, is set to apradio-mac-ssid. You can configure the RADIUS Authentication Called Station ID type information by using the **config radius auth callStationIdType** command.
- When a client sends an HTTP request, the Cisco WLC intercepts it for redirection to the login page. If the HTTP GET request that is intercepted by the Cisco WLC is longer than 2000 bytes, the Cisco WLC drops the packet. Track CSCuy81133 for a possible enhancement to address this restriction.
- We recommend that you install Cisco Wireless Controller Field Upgrade Software (FUS), which is a special AES package that contains several system-related component upgrades. These include the bootloader, field recovery image, and FPGA or MCU firmware. Installing the FUS image requires special attention because it installs some critical firmware. The FUS image is independent of the runtime image. For more information about FUS and the applicable Cisco WLC platforms, see the Field Upgrade Software release notes listing.

Note For Cisco 2504 WLC, we recommend that you upgrade to FUS 1.9.0 release or a later release.

- If FIPS is enabled in Cisco Flex 7510 WLC, the reduced boot options are displayed only after a bootloader upgrade.

Note Bootloader upgrade is not required if FIPS is disabled.

- When downgrading from one release to another, you might lose the configuration from your current release. The workaround is to reload the previous Cisco WLC configuration files that are saved in the backup server, or to reconfigure Cisco WLC.
- It is not possible to directly upgrade to this release from a release that is earlier than Release 7.0.98.0.

- When you upgrade Cisco WLC to an intermediate release, wait until all the APs that are associated with Cisco WLC are upgraded to the intermediate release before you install the latest Cisco WLC software. In large networks, it can take some time to download the software on each AP.
- You can upgrade to a new release of the Cisco WLC software or downgrade to an earlier release even if FIPS is enabled.
- When you upgrade to the latest software release, the software on the APs associated with the Cisco WLC is also automatically upgraded. When an AP is loading software, each of its LEDs blinks in succession.
- We recommend that you access the Cisco WLC GUI using Microsoft Internet Explorer 11 or a later version, or Mozilla Firefox 32 or a later version.
- Cisco WLCs support standard SNMP MIB files. MIBs can be downloaded from the software download page on Cisco.com.
- The Cisco WLC software is factory installed on your Cisco WLC and is automatically downloaded to the APs after a release upgrade and whenever an AP joins a Cisco WLC. We recommend that you install the latest software version available for maximum operational benefit.
- Ensure that you have a TFTP, HTTP, FTP, or SFTP server available for the software upgrade. Follow these guidelines when setting up a server:
  - Ensure that your TFTP server supports files that are larger than the size of Cisco WLC software image. Some TFTP servers that support files of this size are tftpd32 and the TFTP server within Cisco Prime Infrastructure. If you attempt to download the Cisco WLC software image and your TFTP server does not support files of this size, the following error message appears:

    ```
    TFTP failure while storing in flash
    ```

  - If you are upgrading through the distribution system network port, the TFTP or FTP server can be on the same subnet or a different subnet because the distribution system port is routable.
- When you plug a Cisco WLC into an AC power source, the bootup script and power-on self test is run to initialize the system. During this time, press **Esc** to display the bootloader **Boot Options** menu. The menu options for the Cisco 5508 WLC differs from the menu options for the other Cisco WLC platforms.

  The following is the Bootloader menu for Cisco 5508 WLC:

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

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

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

```
Enter 1 to run the current software, enter 2 to run the previous software, enter 4 (on
 Cisco 5508 WLC),
or enter 5 (on Cisco WLC platforms other than 5508 WLC) to run the current software and
 set
the Cisco WLC configuration to factory defaults. Do not choose the other options unless
 directed to do so.
```

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

- The Cisco WLC Bootloader stores a copy of the active primary image and the backup image. If the primary image becomes corrupted, you can use the Bootloader to boot with the backup image.

  With the backup image stored before rebooting, choose **Option 2: Run Backup Image** from the **Boot Options** menu to boot from the backup image. Then, upgrade with a known working image and reboot Cisco WLC.

- You can control the addresses that are sent in the Control and Provisioning of Wireless Access Points (CAPWAP) discovery responses when NAT is enabled on the Management Interface, using the following command:

  config network ap-discovery nat-ip-only {**enable** | **disable**}

  The following are the details of the command:

  enable—Enables use of NAT IP only in a discovery response. This is the default. Use this command if all the APs are outside the NAT gateway.

  disable—Enables use of both NAT IP and non-NAT IP in a discovery response. Use this command if APs are on the inside and outside the NAT gateway, for example, Local Mode and OfficeExtend APs are on the same Cisco WLC.

  

  Note To avoid stranding of APs, you must disable AP link latency (if enabled) before you use the disable option in the **config network ap-discovery nat-ip-only** command. To disable AP link latency, use the **config ap link-latency disable all** command.

- Do not power down Cisco WLC or any AP during the upgrade process. If you do this, the software image might get corrupted. Upgrading Cisco WLC with 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 WLC must not be reset during this time.

- To downgrade from this release to Release 6.0 or an earlier release, perform either of these tasks:
  - Delete all the WLANs that are mapped to interface groups, and create new ones.
  - Ensure that all the WLANs are mapped to interfaces rather than interface groups.

- After you perform the following functions on Cisco WLC, reboot it for the changes to take effect:
  - Enable or disable LAG.

- Enable a feature that is dependent on certificates (such as HTTPS and web authentication).
- Add a new license or modify an existing license.

Note Reboot is not required if you are using Right-to-Use licenses.

- Increase the priority of a license.
- Enable HA.
- Install the SSL certificate.
- Configure the database size.
- Install the vendor-device certificate.
- Download the CA certificate.
- Upload the configuration file.
- Install the Web Authentication certificate.
- Make changes to the management interface or the virtual interface.

Changes in Images and Installation Procedure for Cisco 2504 WLC, Cisco 5508 WLC, and Cisco WiSM2

Due to an increase in the size of the Cisco WLC software image, the Cisco 2504 WLC, Cisco 5508 WLC, and Cisco WiSM2 software images are split into the following two images:

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

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

Image Details

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

Table 3: Image Details of Cisco 2504 WLC, 5508 WLC, and WiSM2

Cisco WLC	Base Install Image	Supplementary AP Bundle Image [1]
Cisco 2504 WLC	AIR-CT2500-K9-8-5-151-0.aes	AIR-CT2500-AP_BUNDLE-K9-8-5-151-0.aes
Cisco 5508 WLC	AIR-CT5500-K9-8-5-151-0.aes AIR-CT5500-LDPE-K9-8-5-151-0.aes	AIR-CT5500-AP_BUNDLE-K9-8-5-151-0.aes AIR-CT5500-LDPE-AP_BUNDLE-K9-8-5-151-0.aes
Cisco WiSM2	AIR-WISM2-K9-8-5-151-0.aes	AIR-WISM2-AP_BUNDLE-K9-8-5-151-0.aes

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

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

Upgrading Cisco WLC Software (GUI)

Procedure

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

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

Step 2 Follow these steps to obtain Cisco Wireless software:

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

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

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

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

- Early Deployment (ED)—These software releases provide new features and new hardware platform support as well as bug fixes.
- Maintenance Deployment (MD)—These software releases provide bug fixes and ongoing software maintenance.
- Deferred (DF)—These software releases have been deferred. We recommend that you migrate to an upgraded release.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

A message indicating the status of the download is displayed.

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

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

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

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

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

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

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

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

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

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 Cisco WLC 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	8.5.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
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	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

Client Type and Name	Version
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
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

Client Type and Name	Version
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
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

Client Type and Name	Version
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 9: 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 10: 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 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

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 12: Open Caveats

Caveat ID Number	Description
CSCvb26809	Cisco controller should use port MAC for non LAG and box MAC for LAG
CSCve42897	Controller unexpectedly reloads with "NMI received for unknown reason 2d on CPU 0" during traffic
CSCve82488	Cisco Wave 2 APs in FlexConnect mode stop redirecting CWA clients after WLAN change
CSCvf46247	Protocol field mismatch in CLI and GUI for 802.11n adaptor in Client Summary
CSCvf57867	Only single IMM / CIMC IP addr configured for both controller active and standby
CSCvf65133	Dynamic interface template fails to apply on Cisco WLC with DHCP Option 82 setting
CSCvf71177	8.7:3800/2800 ap aaa vlan name shows none for centralauth+localswitching
CSCvf84806	Cisco 2800, 3800 Series AP unexpected reboot due to FIQ/NMI crash
CSCvf92382	"debug client" reports wrong BSSID in (Re) association message

Caveat ID Number	Description
CSCvg61933	GUI is not accepting the valid IPv4 netmask (255.255.255.255) while updating SNMP community
CSCvg83836	Clients cannot pass traffic with Cisco 1810w MAB FlexConnect local switching RLAN
CSCvh11212	Cisco controller with Internal DHCP not sending NAK
CSCvh81525	Wireless Client unable to Access Mobility Express (ME) GUI or SSH when connected to the primary AP
CSCvi02980	Cisco Controller becomes inaccessible with client rate limiting
CSCvi06408	Wave 1 AP failed to send DHCP packet to wired side under VLAN Override
CSCvi25967	Cisco 5508 controller reloads unexpectedly on Taskname : fp_main_task
CSCvi29775	Cisco 8510 controller experiences DP0 CORE 9 Dataplane crash and reloads unexpectedly
CSCvi48503	Standby WLC continuously reboots with "Reason: XMLs were not transferred from Active to Standby"
CSCvi61244	Traplog shows IP address in reverse
CSCvi77219	Cisco 1800 series kernel panic mkp_lg: Take care of the HOST ASSERT first
CSCvj25194	Clean up debug lisp map-server output for AP onboarding
CSCvj32199	SSH/Management Access of Primary controller is not possible when HA failover occurs in 8.5.120.0
CSCvj32563	Transfer download on Cisco controller fails with error message when no APs are upgrading
CSCvj71373	Ping command does not use management interface as source interface
CSCvj83372	Cisco 1852 AP showing irregular data usage
CSCvk05150	OpenDNS profile keeps being mapped for client when the username changes
CSCvk27250	System not operational with task apfRogueTask_3
CSCvk36463	Support Bundle output only genertaes WSA core bundle when WSA is enabled
CSCvk39841	Change SSID name with SNMP fails with commitFailed
CSCvk64674	Cisco Wave 1 APs advertise Adaptive FT MDIE on probe response for open SSID
CSCvm10544	Cannot disable some SNMP traps
CSCvm37510	Cisco controller reloads unexpectedly due to SNMP memory corruption
CSCvm41771	Cisco allows RF-profile with all rates disabled

Caveat ID Number	Description
CSCvm46237	Cisco 1562 radio1 operational status down for all channels in the blocked list not going back up
CSCvm49047	AP 3702 reloads unexpectedly on 8.3.143.0
CSCvm63736	Erratic multicast throughput
CSCvm64232	COS APs DMS feature to be disabled if not supported by default
CSCvm68624	Cisco Wave 1 AP console display logs 'DTX DUMP'
CSCvm72007	Incorrect VLAN mapping when using MAC filtering and PSK
CSCvm95330	Cisco controller ignores DBS Max Best Channel Width Allowed
CSCvn00847	Cisco 702W AP loses connection to Cisco controller
CSCvn04046	Cisco 2800,3800 AP does not map the DSCP to the correct WMM UP Value for FlexConnect Local Switching
CSCvn04907	'length 0' line is automatically set to line VTY
CSCvn13314	Cisco 2802, 3802 APs: Default SSID "IP Cheetah" broadcasted during AP boot up
CSCvn14292	Cisco 3800 AP running 8.2.170.2 code reloads unexpectedly
CSCvn27144	Unable to restore 802.11ac MCS parameter
CSCvn31768	WLC cLWebAuthWlanConfigTable OID is broken when MS-OPEN feature is enabled on one of the SSIDs
CSCvn42067	MAPs Client radio (slot 0) chanAutoCfg changes from CONFIG_AUTO to CONFIG_STATIC at random
CSCvn88031	WLC uses lowest LDAP server index when configuring mutliple servers that have same IP/different OUs
CSCvn99809	Handling PAK scheduler during AID plumbing
CSCvo05093	Cisco controller reloads unexpectedly with task name radiusTransportThread
CSCvo09245	WLC sends incomplete Accouting packets using client's MAC as username after Flexconnect AP failover
CSCvo10708	Cisco 2800, 3800 APs does not defer off-channel scanning when multicast transmission is active
CSCvo18211	Static IP client is passing traffic in DHCP_REQ state on Cisco Wave 2 APs
CSCvo18656	Several AP configurations are changed after switchover
CSCvo24010	2.4 GHz Rogue clients stay in containment pending

Caveat ID Number	Description
CSCvo31548	Cisco IW3702 AP and 3702 AP WGB reloads unexpectedly on 15.3(3)JF9 with PEAP authentication
CSCvo35484	RTS threshold is zero in show CAPWAP client config; excessive RTS sent; client connectivity problems
CSCvo57350	Cisco 1852 AP LED blinks amber even while it's successfully serving clients
CSCvo78698	Microsoft Workstation client is being profiled as Android Galaxy
CSCvo80444	Nearby AP name not showing for 5-GHz network
CSCvo99565	Static IP clients in DHCP_REQD state pass traffic if WLAN IDs are configured randomly
CSCvp05117	P-Q domain Wave 2 APs cannot join the controller and the AP reloads unexpectedly
CSCvp36496	The beamforming configuration gets back to the default after AP reload and rejoined to controller
CSCvp40627	Cisco controller fails to initiate 1x message
CSCvp43164	Cisco 2800, 3800 APs: 11k failure in flex LS mode as no RM IE in reassociation response
CSCvp48157	Cisco 1570 RAP intermittently drops broadcast packets

Resolved Caveats

Table 13: Resolved Caveats

Caveat ID Number	Description
CSCut85555	APF_HA-3-SYNC_RETRANSMIT_FAIL Messages in show msglog
CSCvh24354	Cisco ME/Flex local - MN_REASSOC_TIMEOUT / EAP negotiation failures
CSCvh69616	Cisco controller fails to load FP sometimes; reloads unexpectedly due to "dtl Driver Init Failure"
CSCvh72867	Radio reset with transmitter seems to have stopped
CSCvh81618	When adding a member to RF Group with static leader 8510 or 8540, group size exceeded error
CSCvh85849	8.7:After XOR connector disconnected and plugged back in, state Down while WLC showing connected
CSCvh97977	WLC Local Policy - Client Local Profiling assigns wrong Interface to Client
CSCvi10888	Cisco AP intermittently stops transmitting Beacon for 12 and 85 seconds

Caveat ID Number	Description
CSCvi33671	Wrong OID mapping for detecting ap name in bsnRogueAPRemoved trap varbinds
CSCvi77141	HA_send_usmDbSpamSetRadSlotBand, ErrType:Apply Config failed on Standby
CSCvi82746	Cisco controller reloads unexpectedly with Task Name SISF BT Process
CSCvj61869	20-30 Mbps downlink speed on 702w AP with WPA2+802.1x SSID
CSCvj69298	Data Plane reloads unexpectedly due to RPE/Double bit errors
CSCvj74144	9800:AP keep flap with Failed to receive data keepalive with CAPWAP v6 tunnel having link-encryption
CSCvj79841	Cisco 3802 AP reboots unexpectedly
CSCvj80129	Cisco Wave 2 AP uses invalid CAPWAP-Data keep-alive source port
CSCvj97602	Controller Client RSSI and SNR values to be updated as part of Assoc & reassoc request processing
CSCvk09135	Unexpected reload in emWeb while monitoring rogue APs
CSCvk29178	Cisco 1550 AP: BVI interface uses a different MAC-Address than the Gigabit interface
CSCvk53499	Cisco APs do not reconnect, error log: System reached max concurrent DTLS Handshakes
CSCvk64928	AP stops working when we configure LSC keysize as 4096
CSCvk68688	Client traffic seen on the 5508 Standby Hot WLC causing MAC flapping on switch
CSCvk70379	8.5_ Stale clients exist in Cisco controller
CSCvk76386	Reaper Reset due to too much CPU while SW Watchdog is disabled - various processes
CSCvk79597	Frequent DFS detection
CSCvm11861	Cisco Wave 2 APs FIQ/NMI reloads unexpectedly on the radio driver
CSCvm15167	MSCB are not cleared, when client joins a WLAN, reassociates, and joins 2 different WLANs
CSCvm48446	Unexpected reload in "Dot1x_NW_MsgTask_*"
CSCvm53457	Cisco AP reloads unexpectedly with Memory ALLOC Failed - LWAPP DHCP REAP process is bloated
CSCvm54487	WLC sends Accounting Start without Framed-IP-address while WLAN has DHCP required
CSCvm58235	Cisco 2802E AP with DART connector - custom RF profile not always applied properly to XOR
CSCvm63975	Cisco controller loses config if specific countries are enabled together

Caveat ID Number	Description
CSCvm64787	[IOS-Autonomous AP]: NVRAM loses configuration in IW-3702 Or NVRAM might be corrupted
CSCvm65411	Cisco 2700 AP radio resets with FC71 code
CSCvm65858	Cisco 2800 APs using Flexible Radio Assignment has admin status and clean air status down
CSCvm66217	MC2UC traffic downgraded to BE with UP 0 for COS access points; when ACM enabled
CSCvm68341	Cisco controller is sending duplicate interim accounting packets to ISE
CSCvm69246	Cisco controller applying wrong interface policy to re-associated client after SSO
CSCvm71393	Serviceability Enhancement: dtl driver init failure
CSCvm73244	Cisco 3800AP in sniffer mode not capturing ACK,RTS in 8.7 and 8.8 CSCvf74377
CSCvm80592	Cisco 2800 AP reloads unexpectedly with ERROR TAMD device 'ap-tam' heartbeat failure
CSCvm81901	Cisco 3800 AP does not acknowledge the client frames
CSCvm82471	FT 802.1x/PSK Clients are not able to authenticate to Flexconnect Wave 2 AP after HA Failover
CSCvm91854	Cisco 8540 controller becomes inaccessible with systemDb corruption
CSCvm92486	WLC unable to clear stale client entries on anchor controller 8.5.135
CSCvm93785	Cisco 2800, 3800 AP reloads unexpectedly on Click: Client update cache from write handler
CSCvn01004	AirPrint not working with printers that do not explicitly advertise sub-type
CSCvn03915	After controller upgrades it reloads unexpectedly due to kernel panic
CSCvn05881	Cisco Phone 8821 has roaming issues with Cisco 2802, 3802 access points because of MIC mismatch
CSCvn07126	Cisco FlexConnect - Cisco 2802 AP's lowers the priority UP on QoS on the downlink transmit
CSCvn15777	Cisco 5508 controller reloads unexpectedly with high CPU util on emWeb process
CSCvn17267	702AP: WGB disconnects from root AP 'parent lost: Too many retries' RTS when root AP is offchanl
CSCvn18965	EAP-MD5 Authentication Fails on RLAN
CSCvn20446	Wireless client moves from local switching SSID to central switching SSID DHCP traffic gets dropped

Caveat ID Number	Description
CSCvn20609	AP1552C 128MB not forming EoGRE tunnel.
CSCvn21425	Cisco 2800 3800 APs not responding to dot11 association frames
CSCvn23565	Cisco 702w AP enables POE in LAN 4 before joining Cisco controller after reboot
CSCvn24369	New mobility members not config and stale after WLC reloads
CSCvn25524	Cisco 5520, 8540 controllers: Throughput is low with Port 2 with 1 Gig SFP
CSCvn27111	Controller on 8.8.114.54 reloads unexpectedly due "pmalloc detected memory corruption spamAP Task4"
CSCvn32314	Cisco 2800 AP on 8.8.114.54 reloads unexpectedly due to WCPD
CSCvn37957	Cisco controller FTIE not saved sending Association Response FT 802.11r
CSCvn49888	Cisco 702, 1532 AP has tracebacks and beacons stuck with load 8.5.140.0
CSCvn53514	AP Syslog Facility does not work on IOS AP
CSCvn55904	WLC modified FlexACLs rules are not populated on the Flex AP
CSCvn56211	Cisco 702W AP radio resets, tracebacks and other radio buffer errors
CSCvn56617	%BROFFU-0-DP_BUFFER_POOL_EARLY_WARNING messages appear on WLC even after change of logging levels
CSCvn59061	Cisco 8510 controller on on 8.3.141.10 DP unexpectedly reloads at broffu_fp_dapi_cmd.c:4588
CSCvn61436	Cisco 5520 controller reloads unexpectedly on taskname : NFV9_Task
CSCvn62176	Cisco 3802 series APs unable to associate clients when using UNII-1 Channels
CSCvn66715	Cisco 3800 AP stops passing traffic under client with Intel NIC 8260/8265 load in MU-MIMO deployment
CSCvn68423	Passive client config is lost upon WLC Reload or HA failover
CSCvn68501	WLC LSC : Device certificate can not be installed and showing as "Not Present"
CSCvn69015	Cisco Wave 2 APs in local mode forwards layer 2 multicast control traffic from their wired interface
CSCvn74948	Cisco APs reloads unexpectedly with watchdog process sxpd
CSCvn79255	Cisco controller reloads unexpectedly with task emweb after Opening VLAN Mappings on GUI
CSCvn80147	BPDU frames are forwarded by the Cisco Wave 2 APs causing the switch to AP err-disabling port

Caveat ID Number	Description
CSCvn87656	Cisco Wave 2 APs reloads unexpectedly in the context of QCA driver @ click_packet_type_event_hook
CSCvn95727	XOR Radio in 5GHz is sending some traffic at disabled data rates
CSCvn98214	Cisco 1830 AP: core-radio1FW found during WGB association, WGB did not join
CSCvn98598	FT 802.1X clients cannot authenticate after ME primary AP / N+1 controller failover
CSCvo07377	2.4GHz mesh backhaul on 8.5.140.0 build: Cisco 1552 MAP failed to join Cisco 1552 RAP
CSCvo11241	After Cisco 3800E AP reboots, the antenna gain on Slot0 (5GHz band) resets to default
CSCvo17872	Cisco 3800 AP running 8.5.140.0: FIQ/NMI reloads unexpectedly
CSCvo20540	Wave 2 AP rejecting association request on 5-GHz if it does not include 36Mbps
CSCvo26556	WLC reloads unexpectedly on the command "config network ssh host-key use-device-certificate-key"
CSCvo40092	Cisco controller reloads unexpectedly on HA setup with task name apfMsConnTask_0
CSCvo41016	Cisco controller reloads unexpectedly when adding 4096 bit key size device cert for LSC
CSCvo41622	AP Port 80(http access) open
CSCvo41763	Cisco 1600 AP reloads unexpectedly with error: Bad refcount in | datagram_done
CSCvo48363	Cisco controller reloads unexpectedly when viewing multicast MGID in GUI
CSCvo50532	Cisco 1572 AP reporting "nokey" errors
CSCvo58611	Cisco 1562 AP Incorrect Single-Band 5.0GHz Antenna Mapping.
CSCvo60307	Cisco controller reloads unexpectedly at Client Profiler Task
CSCvo64035	PIM hello will not be forwarded downstream when "unified-vlan-client" is configured
CSCvo64075	Deauth during AID change : Continuation of CSCvn99809
CSCvo70730	Cisco 2802 AP reloads unexpectedly in Click path [CapwapMgidTable11write_param]
CSCvo71753	AP side: Multicast Traffic stops working when enabling Inline Tagging on CTS
CSCvo76633	Failed to add/delete new mobility foreign mappings in guest anchor
CSCvo82869	Cisco controller running 8.5.135.0 reloads unexpectedly on "Task Name: radiusTransportThread"
CSCvo85485	5 GHz radio Rx high due to incorrect 802.11ac MCS9 with 1SS/2SS in 20 MHz

Caveat ID Number	Description
CSCvo98569	Cisco Wave 1 AP: EoGRE upstream/downstream packet drops observed for flex local EoGRE
CSCvp01439	Cisco 1815 AP leaking RLAN VLAN traffic when port looped
CSCvp03798	Wave1 APs: FlexConnect local EoGRE reloads unexpectedly due to Memory fragmentation "Net Background"
CSCvp05891	In AP SSO, FT 802.1x/PSK auth break in Flex COS AP when mobility MAC different from burned in MAC
CSCvp07442	Cisco controller reloads unexpectedly on task 'tplusTransportThread'
CSCvp11765	Wireless client fail to associate to Cisco 1830 APs until reboot
CSCvp18422	Cisco controller running 8.5.135.0 reloads unexpectedly with taskname spamApTask6
CSCvp21915	RSN IE length mismatch between assoc and EAPOL-M2 frame
CSCvp26465	AireOS HA: The mobility hash keys are not getting synced UP in AireOS
CSCvp34148	Memory leak causing WLC to reboot
CSCvp52994	WLC fails to learn AAA VLAN, fails to send Central Switched VLAN on second Add mobile
CSCvp71305	Traceback : APF-3-NO_FRAMED_IP_ADDRESS: on Acct Start and Interim while running scale test
CSCvp73499	Cisco 3800 AP transmits ACK at lower RSSI

Related Documentation

Wireless Products Comparison

- Use this tool to compare the specifications of Cisco wireless access points and controllers:

  https://www.cisco.com/c/en/us/products/wireless/wireless-lan-controller/product-comparison.html

- Product Approval Status:

  https://prdapp.cloudapps.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL_SEARCH

- Wireless LAN Compliance Lookup:

  https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html

Cisco Wireless Controller

For more information about the Cisco WLCs, lightweight APs, and mesh APs, see these documents:

- The quick start guide or installation guide for your particular Cisco WLC or access point
- Cisco Wireless Solutions Software Compatibility Matrix
- *Cisco Wireless Controller Configuration Guide*
- *Cisco Wireless Controller Command Reference*
- *Cisco Wireless Controller System Message Guide*

For all Cisco WLC software related documentation, see:

http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/tsd-products-support-series-home.html

Cisco Mobility Express

- *Cisco Mobility Express Release Notes*
- *Cisco Mobility Express User Guide*
- *Cisco Aironet Universal AP Priming and Cisco AirProvision User Guide*

Cisco Aironet Access Points for Cisco IOS Releases

- *Release Notes for Cisco Aironet Access Points for Cisco IOS Releases*
- *Cisco IOS Configuration Guides for Autonomous Aironet Access Points*
- *Cisco IOS Command References for Autonomous Aironet Access Points*

Open Source Used in Controller and Access Point Software

Click this link to access the documents that describe the open source used in controller and access point software:

https://www.cisco.com/c/en/us/about/legal/open-source-documentation-responsive.html

Cisco Prime Infrastructure

Cisco Prime Infrastructure Documentation

Cisco Mobility Services Engine

Cisco Mobility Services Engine Documentation

Cisco Connected Mobile Experiences

Cisco Connected Mobile Experiences Documentation

Cisco Digital Network Architecture

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

Communications, Services, and Additional Information

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

Cisco Bug Search Tool

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

Documentation Feedback

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